

under law. Copyright © 1996-2025 MDaemon Technologies, Ltd. MDaemon® and related trademarks are the property of MDaemon Technologies, Ltd. and are registered and/or used in the U.S. and countries around the world. All

trademarks are property of their respective owners.



Manuel d'utilisation v25.0

MDaemon® Email Server Manuel d'utilisation

Copyright © 1996-2025 MDaemon Technologies. Alt-N®, MDaemon®, and RelayFax® are trademarks of MDaemon Technologies.

Apple is a trademark of Apple Inc. Microsoft and Outlook are trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

Table des matières

Section I MDaemon Email Server 25.0

1 Fonctionnalités de MDaemon	14
2 Configuration système requise	17
3 Nouveau dans MDaemon 25.0	17
4 Mise à jour vers MDaemon 25.0.0	60
5 Obtenir de l'aide	65

Section II Interface principale de MDaemon

69

13

3

1 Statistiques	70
Service d'autodécouverte	75
2 Suivi des événements et journalisation	80
Menu contextuel	82
3 Journal détaillé	83
4 Icône de la zone de notification	83
Menu contextuel de l'icône	84
Verrouiller/Déverrouiller l'interface principale de MDaemon	85
5 Fenêtre de session	85
6 Flux SMTP de MDaemon	86

Section III Menu Configuration

aramètres du serveur	90
Paramètres du serveur	
Serveurs	
Distribution	
Sessions	
Temporisateurs	
Courrier inconnu	
DNS & IPs	
DNS	
Ports	
IPv6	
Liaison	
Cache IP	
Partage de domaine	
Dossiers publics et partagés	
Dossiers publics et partagés	
Rappel de message	
Authentification de l'hôte	
Courrier prioritaire	
Conversion d'en-tête	
Exceptions de la conversion d'en-tête	
Archivage	
Nettoyage	131
Signatures	

	Signatures par défaut	132
	Signatures client par défaut	
	MultiPOP	144
	DomainPOP	150
	Hôte & Paramètres	
	Analyse	
	Traitement	
	Routage	
	Courrier étranger	
	Correspondance de noms	
	Archivage	
	Paramètres de connexion RAS	
	Connexion RAS	
	Identifiant	
	Traitement	
	Paramètres duxy	
	Journalisation	
	Node de iournalisation	
	Journal détaillé	170
	lournal de statistiques	172
	Journaux d'événements Window s	174
	Maintenance	175
	Paramètres	177
	Plus de naramètres	181
2	Gestionnaire de domaines	184
-		
	Hote de relais	
	Comptes	
	Calendrier	
	Webmail	
	Retrait de la file d'attente	
	Relais du courrier à la demande (ODMR)	
	Signatures	
	Signatures clients	
	Paramétres	
	ActiveSync	
	Paramètres client	
	Gestionnaire de politiques	
	Politique attribuée	
	Comptes	
	Clients	
3	Gestionnaire de passerelles	
	Paramètres globaux des passerelles	
	Création automatique de passerelles	
	Éditeur de passerelle	
	Domaine	
	Vérification	
	Configuration de plusieurs requêtes de vérification LDAP	273
	Transfert	
	Retrait de la file d'attente	
	Quotas	
	Paramètres	

Copyright $\textcircled{\sc c}$ 1996-2025. All rights reserved. MDaemon Technologies

4 Gestionnaire de listes de diffusion	281
Paramètres de liste de diffusion	
Éditeur de liste de diffusion	
Membres	
Paramètres	
Nettoyage de liste avancé	
En-têtes	
Inscription	
Inscription aux listes de diffusion	
Rappels	
Compilation	
Notifications	
Modération	
Routage	
Fichiers de support	
Dossier public	
Active Directory	
ODBC	
Configuration d'une source de données ODBC	
Création d'une source de données	
5 Gestionnaire de dossiers publics	
Liste de contrôle d'accès	
6 Services web & MI	
Webmail	333
Vue d'ensemble	333
Calendrier & système de planification	334
MDaemon Instant Messenger	
Messagerie instantanée.	
Intégration avec Dropbox	
Utilisation de MDaemon Webmail	
Serveur Web	
SSL & HTTPS	
MDIM	
Calendrier	
Service de disponibilité	
RelayFax	
Dropbox	
Google Drive	
OneDrive	
Catégories	
Paramètres	
Personnalisation du logo	
MDaemon Remote Admin	
Serveur w eb	
SSL & HTTPS	
Conditions d'utilisation	
Liens vers les pièces jointes	
CalDAV & CardDAV	
ХМРР	
7 Programmation d'événement	402
Programmation antivirus	402
Mises à jour antivirus	
Programmation	

	Programmation de courrier	
	Envoi & collecte de courrier	405
	Collecte MultiPOP	406
	Programmation de courrier	407
8	MDaemon Connector	409
	Paramètres du serveur MC	410
	Paramètres	410
	Comptes	412
	Paramètres du client MC	
	Général	415
	Avancé	419
	Dossiers	
	Envover/Recevoir	
	Divers	
	Base de données	
	Signature	
	Compléments	429
9	Service de cluster	431
-	Ontions (nors annalisation	124
	Citeminis d'acces partages	
40	Diagnostics	
10	AcuveSync	
	Système	441
	Réglages	
	Paramètres client	447
	Sé curité	454
	Diagnostics	
	Restrictions de protocoles	
	Domaines	
	Gestionnaire de politiques	
	Comptes	
	Clients	
	Groupes	
	lypes de clients	
11	Indexation des messages	511
	Options/Personnaliser	511
	Diagnostics	513
12	Service API XML	515
13	Préférences	521
	Preterences	
	Internace utilisateur	
	Libyue	
		529
	⊡retes	
	Iviises a juur	
	LIVEIS	
4.4	of vice willows	
14	em Gienl	538

Section IV Menu Sécurité

541

1	Health Check	545
2	Gestionnaire de sécurité	
	Paramètres de sécurité	
	Contrôle de relais	
	Vérification inverse	
	POP avant SMTP	
	Hôtes autorisés	
	IP autorisées	
	Authentification de l'expéditeur	
	Bouclier IP	
	Authentification SMTP	
	Vérification SPF	
	DomainKeys Identified Mail	
	Vérification DKIM	
	Signature DKIM	
	Paramètres DKIM	
	Paramètres ARC	
	DMARC	
	Vérification DMARC	
	Rapports DMARC	
	Paramètres DMARC	
	Certification de messages	
	Certification VBR	
	Domaines approuvés	
	Analyse	
	Liste de blocage d'expéditeurs	
	Liste de blocage de destinataires	
	Écran IP	
	Écran d'hôte	
	Écran SMTP	
	Détournement de compte	
	Robots spammeurs	
	Filtrage de pays	
	Analyse de l'en-tête From	
	SSL & TLS	613
	MDaemon	
	Webmail	
	MDaemon Remote Admin	
	Exceptions STARTTLS	
	Liste STARTTLS	
	SMTP Extensions	
	DNSSEC	
	Let's Encrypt	
	Autres	634
	Retours de courrier - Présentation	
	Retours de courrier	635
	Régulation de la bande passante - Présentation	
	Régulateur de bande passante	
	Répulsion	641
	Liste grise	643
	Domaines LAN	646
	IP LAN	647
	Politique du site	

3 Écran dynamique	650
Options/Personnaliser	
Suivi des échecs d'auth	654
Protocoles	657
Notifications	658
Diagnostics	
Liste d'autorisation dynamique	
Liste dynamique des blocs	667
Exceptions NAT	
Liste des Comptes Exceptions	671
Liste des comptes bloqués	674
4 MDPGP	677
5 Protection instantanée	688
6 Filtre de contenu et antivirus	693
Éditeur du Filtre de contenu	
Règles	
Création d'une règle de filtrage de contenu	
Modification d'une règle de filtrage de contenu	
Utilisation d'expressions régulières dans les règles de filtrage de	
contenu	
Pièces jointes	
Notifications	
Macros de messages	711
Destinataires	
Compression	
Antivirus	718
Analyse antivirus	
7 Filtre anti-spam	725
Filtre anti-spam	725
Filtre anti-spam	726
Classification bayésienne	730
Apprentissage bayésien	734
Daemon anti-spam (MDSpamD)	736
Liste d'autorisation (automatique)	739
Liste d'autorisation (pas de filtrage)	742
Liste d'autorisation (destinataires)	743
Liste d'autorisation (expéditeurs)	744
Liste de blocage (expéditeurs)	745
Mises à jour	
Rapports	747
Paramètres	
DNS-BL	751
Hôtes	752
Liste d'autorisation	753
Paramètres	754
Générer automatiquement un dossier de spam et un filtre pour chaque	
Pieges a spam	

Section V Menu Comptes

8

1 003		
	Editeur de compte	
	Informations générales	
	Dossier de courrier et groupes	
	Services de messagerie	
	Services w eb	
	Autorépondeurs	
	Transfert	
	Restrictions	
	Quotas	
	Pièces jointes	
	Filtres IMAP	
	MultiPOP	
	Alias	
	Dossiers partagés	
	Liste de contrôle d'accès	
	Mots de passe d'application	
	Signatures	
	Rôles d'administration	
	Liste d'autorisation	
	Settings	
	ActiveSync pour MDaemon	
	Paramètres du client	
	Politiques assignées	
	Clients	
2 Gro	oupes & Modèles	
	Gestionnaire de groupes	836
	Propriétés du groupe	
	Client Signature	841
	Gestionnaire de modèles	847
	Propriétés du modèle	
	Services de messagerie	853
	Services web	855
	Groupes	861
	Autorépondeur	
	Transfert	
	Restrictions	
	Quotas	
	Pièces jointes	
	Rôles d'administration	
	Liste d'autorisation	
	Paramètres	
3 Para	amètres de compte	
	Active Directory	
	Authentification	884
	Surveillance	
	LDAP	
	Alias	894
	Alias	894
	Paramàtras	
		X9h
	Autorépondeurs	
	Autorépondeurs	
	Autorépondeurs Comptes Pèces jointes	

	Exceptions	901
	Paramètres	
	Créer des scripts de réponse automatique	
	Exemples de scripts de réponse automatique	
	Autres	
	Base de données des comptes	
	Assistant de sélection ODBC	
	Créer une source de données	
	Mots de passe	
	Quotas	
	Minger	
4	4 Importation de comptes	925
	Importer des comptes depuis un fichier texte	
	Intégration de comptes Windows	927

Section VI Menu Files d'attente

931

957

1	Files d'attente	932
	File de relance	
	File temporaire	934
	Files personnalisées	937
	Restaures les files	939
	Paramètres DSN	
2	Pré/Post-traitement	942
3	3 Gestionnaire de files d'attente et de statistiques	943
	Files d'attente	
	Utilisateurs	
	Journaux	
	Rapport	
	Personnaliser le Gestionnaire de files d'attente et de statistiques	
	Fichier MDstats.ini	
	Paramètres de ligne de commande MDStats	

Section VII Autres fonctionnalités de MDaemon

1	MDaemon et fichiers texte	958
2	Contrôle du serveur à distance par e-mail	958
	Contrôle des listes de diffusion et catalogues	
	Commandes générales	961
3	Spécification des messages RAW	961
	Spécification des messages RAW	
	Contourner le Filtre de contenu	
	En-têtes RAW	
	Champs spéciaux compatibles avec RAW	
	Exemples de message RAW	
4	Fichiers sémaphores	964
5	Re-routage	971
Section VIII	Création et utilisation de certificats SSL	973
1	Création d'un certificat	

	Table des matières	11
2 Utilisation de certificats émis par une autorité de certification tierce.	۱ 	974
Index		977

Г



1 MDaemon Email Server 25.0

Introductio n

Le serveur MDaemon® Email Server de MDaemon Technologies est un serveur de messagerie SMTP/POP3/IMAP basé sur les standards. Email Server de MDaemon Technologies est un serveur de messagerie



SMTP/POP3/IMAP basé sur des normes, compatible avec Windows 7, Server 2008 R2 ou plus récent, et offrant une gamme complète de fonctionnalités de serveur de messagerie. MDaemon est conçu pour gérer les besoins en courrier électronique d'un nombre quelconque d'utilisateurs individuels et est fourni avec un ensemble puissant d'outils intégrés pour la gestion des Comptes de courrier et des formats de messages. MDaemon est un serveur de messagerie SMTP, POP3 et IMAP4 évolutif qui prend en charge LDAP et Active Directory, un client de messagerie intégré basé sur un navigateur, des filtres de contenu et de spam, des fonctions de sécurité étendues et bien d'autres choses encore.

Fonctionnalités de MDaemon

MDaemon est doté de nombreuses fonctionnalités en plus du traitement des messages SMTP, POP3 et IMAP4. Voici une liste de quelques-unes de ces fonctionnalités.

- Une prise en charge complète de l'analyse et de la protection antivirus est disponible en tant qu'extension de votre licence MDaemon ou MDaemon Private Cloud. Cela vous permet d'accéder à la <u>Protection</u> instantanée <u>contre les</u> <u>épidémies</u> et à <u>MDaemon AntiVirus</u> [718]. Les messages peuvent alors être analysés pour détecter les virus et être nettoyés ou supprimés automatiquement avant même d'atteindre les destinataires. De plus, vous pouvez configurer MDaemon pour qu'il envoie un message à l'administrateur, à l'expéditeur et au destinataire du message infecté pour les informer de la présence du virus.
- MDaemon dispose d'une suite complète de fonctions de gestion de listes de diffusion ou de groupes de courrier électronique permettant de former un nombre illimité de listes de distribution distinctes pouvant contenir des membres locaux et/ou distants. Les listes peuvent être paramétrées pour autoriser ou refuser les inscriptions par e-mail, être publiques ou privées, envoyer des réponses à la liste ou à l'auteur du message, être envoyées au format "digest" et être configurées à l'aide de nombreuses autres fonctions.

- Le <u>Webmail</u> best un composant intégré à MDaemon . Cette fonctionnalité permet à vos utilisateurs d'accéder à leur courrier électronique à l'aide de leur navigateur web préféré plutôt qu'à partir d'un client de messagerie dépendant d'un poste de travail. Cet outil est parfait pour le personnel mobile et les utilisateurs qui ne disposent pas d'une machine dédiée à partir de laquelle ils peuvent accéder à leur courrier électronique.
- MDaemon Webmail est équipé d'une suite complète de fonctionnalités de client • de messagerie. Vous pouvez : envoyer et recevoir du courrier électronique, vérifier l'orthographe des messages, gérer votre courrier électronique dans plusieurs dossiers personnels, afficher l'interface dans l'une des 18 langues disponibles, planifier des réunions et des rendez-vous et partager des calendriers et des tâches avec d'autres utilisateurs , gérer les paramètres de votre compte MDaemon (lorsqu'il est utilisé avec l'<u>Administration à distance</u> (376)), gérer les contacts, et bien d'autres choses encore. Le Webmail est également équipé de <u>MDaemon Instant Messenger (MDIM</u> [335]), un petit utilitaire qui peut être téléchargé et installé sur l'ordinateur local d'un utilisateur. Celui-ci permet d'accéder facilement à son courrier électronique et à ses dossiers et de vérifier l'existence de nouveaux messages sans devoir ouvrir son navigateur web. Il comprend également un système complet de messagerie instantanée qui peut être utilisé pour "chatter" rapidement avec d'autres utilisateurs de MDaemon qui utilisent également MDIM ou un autre client XMPP 3981.
- MDaemon est équipé de nombreuses fonctionnalités conçues pour vous aider à sécuriser votre système de messagerie. Les fonctions Filtre anti-spam et Liste blocage des DNS vous aideront à mettre fin à la plupart des messages de "spam" que les "spammeurs" tentent d'acheminer par l'intermédiaire de votre domaine ou vers celui-ci. L'Écran IP et hôte et les Listes bloquées d'adresses permettent de filtrer et d'empêcher certaines adresses et certains domaines de se connecter à votre système ou d'envoyer du courrier par son intermédiaire. Ils permettent également de se connecter à des adresses IP spécifiques tout en filtrant toutes les autres.
- Doté d'une prise en charge du protocole LDAP (Lightweight Directory Access Protocol), MDaemon peut maintenir votre serveur LDAP à jour sur tous ses comptes utilisateurs. Vous pouvez ainsi tenir à jour un carnet d'adresses LDAP afin que les utilisateurs disposant de clients de messagerie compatibles avec LDAP puissent y accéder. Vous pouvez également choisir d'utiliser Active Directory ou votre serveur LDAP comme base de données des comptes MDaemon au lieu d'une base de données compatible ODBC ou du systèmelocal USERLIST.DAT. Ainsi, vous pouvez configurer plusieurs MDaemon à différents endroits pour qu'ils partagent la même base de données de comptes.
- Les fonctionnalités étendues d'analyse de MDaemon permettent de fournir du courrier électronique à tout un réseau local avec une seule boîte aux lettres POP3 d'un fournisseur d'accès à distance. Il est ainsi possible de fournir du courrier électronique à tout un réseau pour une fraction du coût normalement associé.
- Les Alias d'adresses permettent de router les messages électroniques adressés à des boîtes aux lettres "fictives" vers un compte ou une liste de diffusion valide. Il est ainsi possible pour des comptes et des listes individuels d'avoir plusieurs adresses électroniques dans un ou plusieurs domaines.

- La fonction Paramètres des passerelles permet de configurer des domaines distincts pour divers services ou groupes qui peuvent être locaux sur votre réseau ou situés ailleurs sur l'Internet. Grâce à cette fonctionnalité, tous les courriers adressés à un domaine pour lequel MDaemon joue le rôle de passerelle seront placés dans la boîte aux lettres de ce domaine par MDaemon. Il peut ensuite être collecté par le serveur MDaemon ou le client de messagerie de ce domaine et distribué aux utilisateurs du domaine. Cette fonctionnalité peut également être utilisée pour permettre à MDaemon d'agir en tant que serveur de messagerie de secours pour d'autres domaines.
- Administration à distance intégrée basée sur le web. Le composant<u>Administration Remote Administration</u> Remote Administration est intégré à MDaemon et au Webmail et permet à vos utilisateurs de consulter et de modifier les paramètres de leur compte par le biais de leur navigateur Web. Vous pouvez définir les paramètres que vos utilisateurs peuvent modifier et attribuer des autorisations d'accès pour chaque compte. L'Administration Remote Admin peut également être utilisée par l'Administrateur (et toute autre personne que vous souhaitez autoriser) pour consulter ou modifier les paramètres de MDaemon et tout autre fichier que vous souhaitez mettre à la disposition du système d'Administration Remote Admin.
- Un système interne de transport des messages, appelé RAW mail, fournit une méthode simple pour placer les messages dans le flux de courrier et simplifie grandement le développement d'un logiciel de courrier personnalisé. Avec RAW, un système de messagerie complet peut être conçu à l'aide d'un simple éditeur de texte et de quelques fichiers batch.
- Un système de Filtrage du contenu très polyvalent vous permet de personnaliser le comportement du serveur en fonction du contenu des messages entrants et sortants. Vous pouvez insérer et supprimer des en-têtes, ajouter des pieds de page aux messages, supprimer des pièces jointes, envoyer des copies à d'autres utilisateurs, faire en sorte qu'un message instantané soit envoyé à quelqu'un, exécuter un programme suivant, et bien d'autres choses encore.

MDaemon Private Cloud

MDaemon Private Cloud (MDPC) est une édition spéciale du serveur de messagerie MDaemon Email Server qui a été développée spécifiquement pour les fournisseurs de services gérés (MSP) qui souhaitent utiliser le logiciel MDaemon pour fournir des services de messagerie électronique hébergés à leurs clients. Contrairement à MDaemon, qui est vendu pour une utilisation sur site, MDPC a été construit sur une nouvelle base de licence et de code spécialement conçue pour une utilisation dans un environnement hébergé. MDaemon Private Cloud comprend toutes les fonctionnalités de MDaemon ainsi que les fonctionnalités supplémentaires suivantes :

- Nouvelles licences et facturation (par utilisateur/par mois)
- Prise en charge d'Outlook
- Amélioration du contrôle multi-domaines
- Marquage par domaine (marque blanche)
- Rapports par domaine

- Comptes utilisateurs de test non facturables (le nombre de comptes ne sera pas inclus dans le total des comptes facturés)
- Protection instantanée, MDaemon AntiVirus et le moteur antivirus ClamAV (en option avec un coût supplémentaire)
- ActiveSync Options pour MDaemon (en option avec un coût supplémentaire)

Configuration requise

Pour obtenir les informations les plus récentes sur la configuration requise et les recommandations de MDaemon, consultez la page <u>Configuration requiseSystème</u> à l'adresse <u>mdaemon.com</u>.

Marques déposées

Copyright © 1996-2025 MDaemon Technologies. Alt-N $\mbox{\ensuremath{\mathbb{R}}}$, MDaemon $\mbox{\ensuremath{\mathbb{R}}}$, and RelayFax $\mbox{\ensuremath{\mathbb{R}}}$ are trademarks of MDaemon Technologies.

Apple is a trademark of Apple Inc. Microsoft and Outlook are trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

Voir :

Nouveautés de MDaemon 25.0Mise à jour vers MDaemon 25.0.0Affichage principal de MDaemon0Obtenir de l'aide

1.3 Nouveau dans MDaemon 25.0

Nouveautés dans MDaemon 25.0

Modifications et nouvelles fonctionnalités

Serveurs MDaemon

- <u>MDaemon Private Cloud</u> n'est plus un téléchargement séparé. Votre licence (clé d'enregistrement) détermine si MDaemon agit en tant que version Private Cloud.
- <u>Let's Encrypt</u> [632] Les fichiers PFX datant de plus de 30 jours seront supprimés du disque.
- Mises à jour du module PowerShell Acme-PS utilisé par le script PowerShell Let's Encrypt a la version 1.5.9.
- Le serveur SMTP consulte désormais la politique DMARC de l'expéditeur lorsque cela est nécessaire pour les <u>options de la Liste de diffusion liées à DMARC</u> [574], même si la connexion est exemptée du traitement DMARC.
- Ajout d'une nouvelle condition au <u>filtre de contenu</u> qui permet d'effectuer des actions sur les messages contenant un code QR.

• MDaemon Connector a été mis à jour vers la version 8.0.2.

Remote Administration (MDRA)

- Ajout de la possibilité de trier les comptes en fonction de la colonne Dernier accès dans "Main | Gestionnaire de comptes" et "Main | Domaines | Edit | Comptes".
- Ajout de la possibilité de trier les comptes en fonction de la colonne Dernier accès sur <u>Main | Gestionnaire de comptes</u>
 1961 et <u>Main | Gestionnaire de</u> <u>domaines | Edit | Comptes</u>
- Ajout des paramètres d'indexation des messages à : <u>Messages et files d'attente</u> <u>Indexation des messages | Paramètres</u> ₅₁₁ et <u>...Diagnostics</u> <u>513</u>. Les options Message Search sont désormais également disponibles sous Message Indexing.
- Ajout des paramètres de gestion de l'API XML à : <u>Configuration | Gestion de</u> <u>l'API XML | Système / Restrictions d'adresses / Diagnostics</u>

Webmail

Thème Pro

- Le thème Pro est désormais le thème par défaut du Webmail pour les nouvelles installations. Lors de la mise à jour, le programme d'installation vous demandera si vous souhaitez changer votre thème par défaut pour le thème Pro.
- Ajout de menus contextuels par appui long sur les dossiers et les éléments de liste pour les périphériques mobiles.
- Ajout d'une bordure plus épaisse sur le bord gauche des événements dans la vue Calendrier.
- Ajout d'une case à cocher Tout sélectionner pour le sélecteur de contact.

Autre

- Le thème Lite de MDaemon Webmail a été supprimé des nouvelles installations de MDaemon, et il ne sera plus mis à jour dans les installations existantes.
- Ajout de délais d'expiration pour les sessions IP locales. Il existe des délais d'expiration distincts pour les utilisateurs qui composent des messages ou qui n'en composent pas. Les options sont situées dans MDaemon Admin sous <u>Main</u> <u>Paramètres Webmail</u> <u>Serveur Web</u>
- Création d'une page GitHub qui explique comment intégrer le MDaemon Webmail à un site intranet : <u>https://github.com/mdaemon-technologies/intranet-</u> <u>integration</u>
- Ajout des photos de contact dans la liste des messages. Si un contact figure dans la liste des contacts de l'utilisateur et qu'il possède une photo, les messages de ce contact afficheront la photo du contact au lieu de la première lettre du Nom de l'utilisateur. Cette fonctionnalité n'utilise pas les indicateurs de marque pour l'identification des messages (BIMI).
- Le processus de connexion au Webmail a été mis à jour pour fournir un message d'erreur significatif lorsque les informations d'identification sont correctes mais

que l'accès est refusé parce que le compte est figé, désactivé, non autorisé à utiliser l'accès à distance, ou lorsque la fonction "Ne pas déranger" est activée.

Notes de mise à jour du serveur MDaemon

Dans une liste exhaustive de ces ajouts et de tous les autres changements et corrections inclus dans MDaemon 25.0.0, consultez les notes de mise à jour.

Nouveautés dans MDaemon Private Cloud 12.5.0

• MDaemon Private Cloud 12.5.0 inclut MDaemon 24.5.2 avec MDaemon Connector 8.0.1.

Pour obtenir la liste de toutes les modifications apportées à MDaemon, consultez les notes de mise à jour de MDaemon 24.5.2.

Pour une liste de toutes les modifications apportées à MDaemon Connector, voir les notes de mise à jour de MDaemon Connector 8.0.1.

Nouveautés de MDaemon 24.5

Changements et nouvelles fonctionnalités

MDaemon Remote Admin (MDRA)

- (Nouveau dans 24.5.1) Les licences du <u>Client eM</u> peuvent désormais être gérées via l'Administration MDaemon Remote Admin en allant dans Configuration | Client eM. A partir de cette boîte de dialogue, les administrateurs globaux de MDaemon peuvent demander 3 activations eM Client GRATUITES pour chacun de vos domaines, acheter des licences supplémentaires et gérer les activations.
- Il y a maintenant un lien "Paramètres de Recherche" sur la barre d'outils titre en haut de la page. Cette fonction permet de localiser plus facilement l'un des nombreux paramètres ou l'une des nombreuses pages de MDaemon. Il vous suffit de taper les mots contenus dans le paramètre ou la page que vous recherchez, et les liens vers les pages contenant ces mots seront listés en dessous.
 (Nouveau dans la version 24.5.1) Lorsque vous suivez un lien vers un paramètre, le nom de ce paramètre clignote plusieurs fois en alternant les couleurs pour vous aider à le localiser sur la page.
- Plusieurs nouvelles options de blocage des images dans les <u>Paramètres</u> <u>Webmail</u> et les <u>Paramètres Webmail Nouveau domaines</u> with permettent de bloquer les images HTML distantes dans tous les messages ou certains d'entre eux. Vous avez la possibilité de permettre au destinataire de visualiser les images s'il le souhaite, ou de bloquer "toujours" ces images sans possibilité de les visualiser. Enfin, vous pouvez également appliquer les options de blocage d'images aux images en ligne/incorporées.

- MDaemon Webmail prend désormais en charge l'intégration de OneDrive 300 pour • vos utilisateurs. À l'instar des fonctionnalités d'intégration de Google Drive 35 et Dropbox 352, MDaemon Webmail peut présenter aux utilisateurs des options leur permettant d'enregistrer les pièces jointes des messages directement sur leur compte Microsoft OneDrive Work ou School, et de modifier et travailler avec les documents qui y sont stockés. Pour activer cela, un ID client et un Code client secret sont nécessaires, qui sont obtenus directement auprès de Microsoft en créant une App à l'aide de l'Azure Active Directory de Microsoft. Un composant d'authentification OAuth 2.0 fait partie de cette appli, qui permet aux utilisateurs de votre Webmail de se connecter à OneDrive, puis d'autoriser l'accès à leur compte OneDrive Work ou School par le biais de MDaemon. Une fois autorisés, les utilisateurs peuvent consulter leurs dossiers et fichiers qui se trouvent dans OneDrive. En outre, ils peuvent charger, télécharger, déplacer, copier, renommer et supprimer des fichiers, ainsi que copier/déplacer des fichiers depuis et vers les dossiers de documents locaux. Le processus d'installation de OneDrive est similaire à la fonctionnalité d'intégration OAuth pour MultiPOP 141 de MDaemon.
- Des outils de gestion WebAuthn ont été ajoutés à la page <u>Détails du compte</u> dans l'Éditeur de compte et sous Mon compte, affichant toutes les connexions sans mot de passe ou les identifiants 2FA qui ont été configurés dans MDRA ou Webmail, .
- La page <u>Informations générales</u> [765], dans l'éditeur de compte et sous Mon compte, inclut désormais l'option E-mail Récupération de Passe.
- Ajout d'un bouton bascule **Tout sélectionner** pour l'<u>éditeur d'appartenance à</u> <u>un groupe</u>
- Ajout d'une boîte de dialogue de confirmation pour les boutons Supprimer et Supprimer Tout à Messages et files d'attente | File différée

Webmail

Thème Pro

- (Nouveau dans 24.5.1) Les <u>fonctionnalités des messages AI</u> (374) ont été mises à jour pour utiliser le modèle gpt-40-mini
- Ajout d'options pour souligner l'en-tête From et mettre en italique l'en-tête To dans la liste des messages sous Afficher les options FROM : Disposition de la liste des messages.
- Dans la liste des messages, une icône "Rappel" a été ajoutée pour les messages du dossier Éléments envoyés. Le survol de l'icône d'un message différé affiche la date à laquelle il a été différé. Cliquez sur l'icône pour rappeler le message.
- Ajout de la possibilité de trier les modèles d'e-mail par glisser-déposer Paramètres | Modèles d'e-mail
- Dans MDaemon/WorldClient/HTML/All/StyleSheets, un squelette "modified.css" a été ajouté pour permettre à n'importe quel administrateur de modifier les css dans le thème Pro. Ce fichier n'est pas écrasé lors de l'installation.

Copyright © 1996-2025. All rights reserved. MDaemon Technologies

- Ajout d'une pièce jointe pour "Afficher les pièces jointes dans la liste des messages" dans Paramètres | Personnaliser. Certaines pièces jointes, telles que les signatures de clés publiques, sont exclues. Les pièces jointes ne sont affichées que dans la vue multiligne.
- Dans la liste des messages, une option permettant de "Toujours afficher les messages au format multiligne" a été ajoutée dans Voir les messages dans la rubrique Options d'affichage | Disposition de la liste des messages.
- Ajout d'une fonction de recherche de paramètres. Les utilisateurs peuvent cliquer sur l'option "Paramètres de Recherche" dans la vue des paramètres et taper une phrase pour rechercher un paramètre. Les utilisateurs peuvent alors cliquer sur un résultat pour être dirigés vers la page de paramètres appropriée.
- Ajout de la prise en charge de l'intégration de Microsoft OneDrive. Pour vous connecter, allez dans Paramètres | Cloud Apps et cliquez sur "Configurer OneDrive". Microsoft n'autorise pas la connexion des comptes personnels ; seuls les comptes d'entreprise et d'étudiant sont autorisés. Les utilisateurs peuvent consulter leurs lecteurs, dossiers et fichiers. Ils peuvent également charger, télécharger, copier, déplacer, supprimer et même visualiser des fichiers (en utilisant le lien de visualisation de Microsoft).
- Lors de l'utilisation des fonctions "Nouvel événement", "Nouvelle tâche" ou "Nouvelle note", les pièces jointes du message sont désormais ajoutées au nouvel élément.
- Ajout d'un bouton permettant d'utiliser l'IA pour traduire le corps d'un message à côté du bouton "Résumer".

Autre

- Ajout d'une option permettant d'alterner le format horaire AM/PM pour les calendriers publiés. Utilise les paramètres par défaut de l'utilisateur (UseAMPM).
- Thèmes WorldClient et LookOut Chercher la date début de la recherche avancée par défaut à une année.
- Non (par utilisateur Paramètres par défaut).
- Ajout de l'option HideDeleteAttachmentButton. Doit être définie dans le fichier MDaemon\WorldClient\Domains.ini [Domaine par défaut – Domaine – Domaine] ou par utilisateur dans le fichier User.ini [User].

Serveur MDaemon

- Sur la page <u>Paramètres de</u> 2001 l'éditeur de liste de diffusion, l'option "*Supprimer les adresses e-mail non valides de la liste*" vous permet désormais de configurer le nombre d'échecs de livraison permanents consécutifs qui doivent se produire avant que le membre ne soit supprimé. Non (par défaut), la valeur par défaut est de 3, afin d'éviter que les membres ne soient supprimés après un seul échec.
- MDaemon utilise toujours une canonisation d'en-tête "détendue" lors de la génération de <u>signatures ARC</u> [572].
- L'enregistrement des adresses IP des tentatives d'échouées SMTP, IMAP, POP, afin de signaler les nouvelles adresses IP et celles qui ont échoué

précédemment, est désormais facultatif. Elle est activée par défaut et les adresses IP peuvent désormais être supprimées après un certain nombre de jours (365 par défaut). Voir les paramètres "Historique des IP" sur la page " <u>Filtrer SMTP</u> [103] ".

- Le Texte d'en-tête et le Nom du fichier HTML utilisés dans les Liens pièces jointes peuvent maintenant être spécifiés sur la page <u>Liens pièces jointes</u>
- La boîte de dialogue À propos affiche les clés d'enregistrement d'AntiVirus, de MDaemon Connector et d'ActiveSync s'ils utilisent des clés d'enregistrement différentes de celles de MDaemon.
- L'écran <u>Webmail RelayFax</u> and n'est pas filtré par l'interface graphique à moins que RelayFax ne soit installé ou que le Webmail n'utilise RelayFax.
- Les courriels d'<u>avertissement de manque d'espace disque</u> [527] indiquent désormais le lecteur concerné par l'avertissement.
- Le <u>rapport sur les mots de passe peu</u> [915] sécurisés mentionne désormais le nombre de comptes qui n'ont pas pu être vérifiés parce qu'ils utilisent l'authentification AD ou le cryptage non réversible des mots de passe.
- Après l'installation d'une nouvelle version, l'intégralité des notes de version de MDaemon sera envoyée par e-mail aux administrateurs et non plus uniquement les considérations spéciales.
- Ajout des noms de domaine aux avertissements journalisés au démarrage lorsqu'un postmaster ou un alias d'abus est manquant.
- L'Écran and dynamique and dispose d'une nouvelle option permettant d'ajouter l'IP d'une connexion SMTP à la Liste de blocage dynamique and si elle tente de s'authentifier alors que l'authentification est désactivée. Cette option est activée par défaut.

ActiveSync

 ActiveSync supporte depuis longtemps les Dossiers sélectionnés, pour empêcher un client individuel de synchroniser un dossier sélectionné. À partir de cette version, il prend désormais en charge les exclusions de dossiers au niveau global, du domaine, du type de client et du compte. L'API XML a été mise à jour pour permettre la gestion de ces exclusions dans le cadre de l'opération ActiveSync.

Autre

- Écran dynamique a) Au lieu de figer un compte lorsqu'il a échoué trop souvent à l'authentification, il est ajouté à la nouvelle <u>Liste des Comptes Bloqués</u> a). Les comptes bloqués peuvent toujours se connecter à partir d'IP autorisées et d'IP figurant sur la Liste d'autorisation dynamique. Les comptes figurant dans la nouvelle <u>Liste des comptes exemptés</u> of ne seront pas ajoutés à la Liste des comptes bloqués.
- XMPP L'option <u>Activer la synchronisation de la liste amis</u> [346] permet d'alimenter automatiquement la liste amis d'un utilisateur pour le domaine. Ce paramètre est également disponible <u>par domaine</u> [193], et il est désactivé par défaut.

- XMLAPI Possibilité de télécharger des fichiers journaux via l'opération FileTransfer.
- XMLAPI Gestion des comptes et rapport de l'URL des horaires publiés pour un compte. Il est désormais possible de récupérer les Informations du calendrier publié pour un compte en utilisant GetUserInfo. Elle se trouvera dans l'élément de publication sous l'élément WorldClient pour un compte. Pour publier ou rétracter un dossier de calendrier via l'API, voir les actions FolderOperation 'publish' et 'retract'.
- Le client de migration ActiveSync prend désormais en charge OAUTH pour les migrations depuis Office 365.
- Amélioration des Exclusions de l'analyse antivirus.
- LetsEncrypt modifie le FQDN et les AlternateHostNames pour utiliser des caractères minuscules.

Notes de version du serveur MDaemon

Dans une liste exhaustive de ces nouveautés et de tous les autres ajouts, changements et correctifs inclus dans MDaemon 24.5.2, consultez les notes de mise à jour.

Nouveautés dans MDaemon Private Cloud 12.0.0

• MDaemon Private Cloud 12.0.0 inclut MDaemon 24.0.1 avec MDaemon Connector 8.0.1.

Pour obtenir la liste de toutes les modifications apportées à MDaemon, consultez les notes de mise à jour de MDaemon 24.0.1.

Pour une liste de toutes les modifications apportées à MDaemon Connector, voir les notes de mise à jour de MDaemon Connector 8.0.1.

Nouveautés de MDaemon 24.0

Changements et nouvelles fonctionnalités

Serveur MDaemon

- MDaemon peut collecter et envoyer des données d'utilisation anonymes à MDaemon Technologies. Nous utiliserons ces informations pour améliorer le produit et ses fonctionnalités afin de mieux répondre aux besoins de nos clients. Vous pouvez désactiver cette fonction en décochant la case "Envoyer des données d'utilisation anonymes" dans Configuration | Préférences - <u>Divers.</u>
 Voir notre <u>politique de confidentialité</u> pour plus d'informations.
- L'option DKIM permettant de <u>signer les messages des listes de diffusion</u> ne nécessite plus de traitement par le Filtre de contenu pour chaque message individuel de la liste.

- L'e-mail <u>Bad Queue Summary</u> [334] comporte désormais un lien permettant de supprimer tous les messages. Dans ce cas, comme pour les autres liens figurant dans les e-mails de résumé de la file d'attente, l'option "<u>Inclure un lien d'action</u> <u>dans l'e-mail de résumé</u> [334]" doit être activée et le paramètre <u>MDaemon Remote</u> <u>Admin URL</u> [377] doit être défini.
- Protocole ARC (Authenticated Received Chain 572)) ARC est un protocole • d'authentification du courrier électronique qui permet aux serveurs de messagerie intermédiaires de signer numériquement les résultats d'authentification d'un message. Il fournit une "chaîne de conservation" authentifiée pour un message, permettant à chaque serveur qui traite le message de voir quels serveurs précédents l'ont traité et s'il a été authentifié ou non à chaque étape. Lorsqu'un serveur de messagerie en aval effectue une vérification DMARC et constate que SPF ou DKIM ont échoué (en raison d'un transfert ou de modifications apportées à une liste de diffusion, par exemple), il peut rechercher les résultats de l'ARC auprès d'un serveur de confiance et les utiliser pour décider d'accepter ou non le message. La vérification et la signature ARC peuvent être activées dans la nouvelle boîte de dialogue Paramètres ARC 572, sous Authentification de l'expéditeur. Pour plus d'informations sur le protocole ARC, voir : RFC 8617 : The Authenticated Received Chain (ARC)Authenticated.
- Par nom, nous avons ajouté le support pour les <u>fichiers SEM</u> ans "blacklist" et "whitelist" dans leurs fichiers : BLOCKLIST.SEM, SENDERBLOCKLIST.SEM, RCPTBLOCKLIST.SEM, CREDSMATCHEXEMPTLIST.SEM, DMARCEXEMPTLIST.SEM.
- Modification de l'e-mail de notification du Compte figé de <u>Détection</u> <u>détournement</u> bour indiquer la raison exacte pour laquelle le compte a été figé.
- MDaemon désactive la <u>mise à jour automatique du client</u> (424) MDaemon Connector dans les versions antérieures à la version 7.0.6, afin de résoudre un problème de mise à jour automatique dans ces versions.

MDaemon Remote Admin (MDRA)

- Liens de Documents Cette fonctionnalité permet aux utilisateurs du Webmail de créer des liens temporaires vers des documents personnels. Ces liens peuvent être partagés avec n'importe qui et seront actifs pendant 30 jours avant d'être automatiquement supprimés. Le Non (parètres défaut) global de cette option se trouve sur la page Paramètres de MDaemon Webmail (365). Il peut également être défini par domaine dans le Gestionnaire des domaines (197) ou par utilisateur dans le Gestionnaire des comptes (815). Les Administrateurs globaux peuvent utiliser la page Liens de Documents pour voir quels liens sont partagés, quand ils ont été créés, combien de fois le fichier lié a été téléchargé et le dernier téléchargement. Ils peuvent également utiliser cette page pour révoquer les Liens.
- La page Status affiche désormais l'état de la licence et le nombre de comptes utilisés pour MDaemon, MDaemon Connector, AntiVirus et ActiveSync. Ces informations sont également affichées sur la page d'enregistrement (cliquez sur A propos, puis sur Enregistrement dans la barre d'outils).
- Il existe maintenant un <u>Paramètres Webmail</u> bour "Désactivez les hyperliens dans les spams et les messages qui échouent à l'authentification DMARC,

DNSBL, ou SPF", qui est activé par défaut. Vous pouvez éventuellement exempter les messages de ce paramètre lorsque l'en-tête From correspond à un contact figurant dans la liste des Expéditeurs autorisés du domaine ou de l'utilisateur. Une option d'exception pour les Expéditeurs autorisés a également été ajoutée à l'option "Bloquer les images HTML" sur la même page.

- Dans l'option <u>Personnalisation du Webmail</u> [375], il est possible de télécharger une image d'arrière-plan personnalisée pour la page de connexion au Webmail.
- Vous pouvez désormais configurer MDaemon pour qu'il permetteà WebAuthn de contourner la connexion à deux facteurs sur la page Paramètres du Webmail and et sur la page correspondante du Gestionnaire de domaines and la page forme d'authentification à plusieurs facteurs, l'utilisation d'une autre forme d'authentification à deux facteurs (2FA) après que quelqu'un a déjà utilisé WebAuthn pour se connecter pouvait être considérée comme redondante ou excessive par certains utilisateurs ou administrateurs.
- La liste des informations d'identification enregistrées sur la page des paramètres de l'utilisateur a été modifiée pour afficher uniquement les informations d'identification Connexion sans mot passe et le même type de liste a été ajouté à la partie Authentification à deux facteurs de la page pour les informations d'identification enregistrées correspondantes. Vous pouvez accéder à votre page de paramètres utilisateurs en cliquant sur votre nom de compte dans le coin supérieur droit du menu de navigation.
- Les paramètres du proxy ont été déplacés de l'outil de mise à jour d'AV Config à Mettre à jour | Paramètres du serveur | Paramètres <u>du proxy</u>
- Un bouton **Suppression** a été ajouté à la page Recherche de message sous le menu Messages et files d'attente. Les administrateurs peuvent l'utiliser pour supprimer les messages de la boîte aux lettres d'un utilisateur. Les administrateurs globaux peuvent également choisir de rechercher **Toutes les Boîtes aux Lettres** pour un domaine donné.

Webmail

Thème Pro

Le thème Pro dispose désormais d'une option permettant aux utilisateurs de créer des liens temporaires vers des dossiers individuels dans leur dossier Documents, qui peuvent ensuite être partagés avec n'importe qui. Dans la liste des documents, l'utilisateur crée le lien en cliquant sur l'icône Lien à droite de chaque fichier listé. À l'aide de cette même icône, l'utilisateur peut supprimer un lien précédemment créé ou le remplacer par un nouveau, les liens étant automatiquement supprimés au bout de 30 jours. Si un lien existe pour un fichier, une icône apparaîtra devant le nom du fichier dans la liste des documents. Dans MDRA, l'option "*Permettre aux utilisateurs de créer des liens temporaires vers des documents personnels*" régissant cette fonctionnalité se trouve sur la page <u>Paramètres du Webmail</u> (les options correspondantes se trouvent également dans les Gestionnaires de <u>domaines</u> 197] et de <u>comptes</u> 1915), et il y a une page Liens de Document pour voir et gérer les liens que vos utilisateurs ont créés.

- Lorsque vous affichez un message auquel vous avez déjà répondu ou que vous avez transféré, une note apparaît sous les en-têtes, indiquant la date et l'heure auxquelles vous avez répondu ou transféré le message.
- Dans le coin supérieur droit de la barre de navigation, une icône de cloche de notification permet désormais de consulter et de marquer comme vus les rappels d'événements et de tâches passés. Si vous souhaitez supprimer l'icône de cloche de la barre de navigation, vous pouvez désactiver cette fonction en désactivant l'option "Afficher les rappels d'événements et de tâches dans la barre de navigation" sur la page Paramètres | Notifications dans le Webmail.
- Il existe désormais une option "Afficher les détails de l'en-tête" dans Paramètres | Personnaliser pour toujours afficher les détails de l'en-tête dans les messages.
- Ajout d'instructions sur l'utilisation de l'interface utilisateur de disponibilité dans la boîte de dialogue Publier un calendrier.
- Mise à jour de l'éditeur HTML, TinyMCE, de la version 6.0 à la version 6.8.
- Mise à jour des traductions pour la messagerie instantanée dans le navigateur.
- Ajout d'une option de police à la page Paramètres de mise en page en page.
- Ajout de la possibilité de glisser-déposer des pièces jointes et des liens de téléchargement de documents sur le bureau. Ne fonctionne qu'avec les navigateurs basés sur Chrome.
- Dans la vue de composition, une flèche de basculement a été ajoutée pour les champs CC et BCC.
- Par taille de la liste et le rembourrage du menu pour les tailles de navigateur de bureau.
- Après avoir copié ou déplacé un message dans un autre dossier, la prochaine fois que vous ouvrirez le menu Copier/déplacer, il contiendra un nouveau lien vers Copier ou Déplacer dans le même dossier que celui utilisé précédemment. Exemple : si vous copiez un message vers la boîte de réception, la prochaine fois que vous ouvrirez le menu contextuel, il y aura une nouvelle option "* Copier vers la boîte de réception" sous l'option normale " Copier ".
- Ce texte a été mis à jour sur la page "Publier le planning" afin d'utiliser "Dupliquer" au lieu de "Copier" pour ajouter des disponibilités existantes à d'autres jours.
- Mise à jour de la page Actions sur les dossiers.

Autres améliorations

- Amélioration des performances en réduisant la quantité d'E/S sur le disque.
- Les hrefs vides dans les ancres HTML des courriels seront désormais supprimés pour éviter un comportement invalide.
- Création d'un Dossier Expéditeurs*bloqués* public qui est vérifié pour les options Webmail "*Ne pas bloquer les images pour les Expéditeurs bloqués*" et "*Ne pas désactiver les hyperliens pour les Expéditeurs bloqués*". Ce dossier n'est actuellement utilisé que par le Webmail, et non par le serveur MDaemon ou le Filtre anti-spam.

- Ajout des options utilisateur "Demander une confirmation de distribution" et "Demander une confirmation de lecture" dans Paramètres de distribution. Dans ces options, les cases à cocher correspondantes sont activées dans la vue de composition.
- Ajout d'une option "*Ne pas désactiver les hyperliens pour les Expéditeurs autorisés*" dans Paramètres | Personnaliser. Lorsque les hyperliens sont désactivés dans un message, la mention "*Les hyperliens sont désactivés. Cliquez ici pour les activer*" s'affiche en haut de la fenêtre du message.
- Dans le thème Pro, la possibilité de définir la couleur d'un calendrier a été ajoutée. Le paramètre est disponible en cliquant avec le bouton droit de la souris sur un calendrier dans la vue Calendriers, en allant dans Paramètres | Dossiers et en cliquant sur un calendrier dans la liste des dossiers, et lors de la création d'un nouveau calendrier dans la boîte de dialogue Nouveau dossier. Le paramètre de couleur est respecté dans les thèmes LookOut et WorldClient.
- Modification de la liste des informations d'identification enregistrées sur la page Paramètres | Sécurité pour afficher uniquement les informations d'identification Connexion sans mot passe et ajout du même type de liste à la partie Authentification à deux facteurs de la page pour les informations d'identification enregistrées correspondantes.
- L'icône "Importer des messages" a été remplacée par une flèche vers le bas au lieu d'une flèche vers le haut.
- Ajout d'un contraste plus marqué entre l'état lu et non lu des messages dans la liste des messages.
- Mise à jour de CKEditor vers la version 4.22.1.

ActiveSync

 Amélioration de l'opération SmartForward/SmartReply lorsque <ReplaceMime/> n'est pas spécifié.

Les versions précédentes contenaient du code conforme à la spécification EAS 2.5 pour SmartForward. Dans les versions précédentes, le code était conforme à la spécification EAS 2.5 pour SmartForward. En outre, SmartReply ne prenait pas en charge les images en ligne dans le message de réponse. Ce nouveau code prend en charge cette fonctionnalité. Le fragment de style css qui contrôle la div dans laquelle le message répondu/transféré est placé, continue d'être personnalisable. Voir les exemples d'opérations ActiveSync ActiveSync_DomainSettings_*.xml et ActiveSync_GlobalSettings.xml. Sauf indication explicite, les paramètres de domaine utiliseront les paramètres de formatage globaux.

- Les modifications apportées à la gestion d'ActiveSync sont consignées dans le fichier journal AirSync-Mgmt.
- Le serveur ActiveSync honore l'option Webmail d'utiliser l'en-tête X-Forwarded-For.

Autre

• XMLAPI - Ajout de la gestion des Mots passe d'application.

- Filtre du contenu Ajout de la prise en charge des caractères étrangers pour l'édition des règles et les recherches. Les fichiers de configuration du filtre de contenu (CFilter.ini et CF*.dat) ont été convertis en UTF-8. Si vous devez revenir à une version précédente et que ces fichiers contiennent des caractères non ASCII, convertissez-les en ANSI ou restaurez-les à partir d'une sauvegarde.
- Mise à jour des fichiers DQS SpamAssassin pour le contenu HBL et les corrections.
- Écran dynamique Si vous rencontrez des erreurs du type "Le chemin d'accès au réseau n'a pas été trouvé", modifiez le registre dans HKLM\SOFTWARE\Alt-N Technologies\MDaemon\DynamicScreening\Configuration et définissez Serveur sur "." et UseCustomServer (DWORD) sur 1.
- Utilitaire de mise à jour ClamAV à la version 1.0.6 LTS.
- Mise à jour de MDaemon Connector vers la version 8.0.1.
- Les modifications apportées à la gestion d'ActiveSync sont consignées dans le fichier journal AirSync-Mgmt.
- Le serveur ActiveSync honore l'option Webmail d'utiliser l'en-tête X-Forwarded-For.

Notes de version du serveur MDaemon

Pour obtenir une liste complète de ces éléments et de tous les autres ajouts, modifications et corrections inclus dans MDaemon 24.0.0, consultez les notes de mise à jour.

Nouveautés dans MDaemon Private Cloud 11.5.0

- MDaemon Private Cloud 11.5.0 inclut MDaemon 23.5.2 avec MDaemon Connector 7.0.7.
- Correction de MDRA Des fonctionnalités de Gérer les serveurs Cloud telles que Serveurs gérés manquent dans le menu.

Pour une liste de tous les changements apportés à MDaemon, voir les notes de mise à jour de MDaemon 23.5.2.

Pour une liste de toutes les modifications apportées à MDaemon Connector, voir le document MDaemon Connector 7.0.7.

Nouveautés de la version 23.5 de MDaemon

Changements et nouvelles fonctionnalités

Webmail

Prise en charge de WebAuthn 365

MDaemon prend en charge l'API d'authentification Web (également connue sous le nom de WebAuthn), que les utilisateurs de Webmail peuvent utiliser pour bénéficier d'une expérience de connexion sans mot passe sécurisée, en leur permettant d'utiliser la biométrie, les clés de sécurité USB, Bluetooth, etc. pour l'authentification. WebAuthn peut également être utilisé pour l'authentification à <u>deux facteurs</u> (2FA), mais si vous utilisez à la fois l'authentification sans mot de passe et l'authentification à deux facteurs, vous ne pouvez pas utiliser la même méthode d'authentification pour les deux. Vous trouverez les paramètres de mise en Webmail sur la page <u>Paramètres de</u> (MDRA (176)).

Visitez : <u>webauthn.guide</u>, pour plus d'informations sur WebAuthn et son fonctionnement.

Fonctionnalités des messages AI 374

Dans MDaemon 23.5.0, le thème Pro du client Webmail de MDaemon inclut diverses fonctionnalités d'Intelligence Artificielle (IA) pour aider vos utilisateurs à gérer leur courrier électronique et à augmenter leur productivité. Dans MDaemon Webmail, vous pouvez utiliser l'IA (en particulier ChatGPT d'OpenAI) pour obtenir un résumé du contenu d'un message électronique, suggérer une réponse à un message en fonction de critères que vous choisissez, et vous aider à composer un nouveau message à partir de votre propre texte et d'autres critères.

Les fonctions de messages AI du Webmail sont désactivées par défaut pour tous les domaines. Elles peuvent être activées en utilisant l'option "*Activer les messages IA*" sur la page <u>Paramètres du</u> ³⁶⁵ Webmail ou sur la page Webmail du Gestionnaire de domaines. Les fonctions de messages AI du Webmail sont également désactivées par défaut pour chaque utilisateur. Vous pouvez les activer par utilisateur sur la page <u>Services web</u> ⁷⁷¹ de l'Éditeur de comptes, ou dans le cadre d'un <u>groupe</u> ³⁶⁶ contrôlé par un <u>Paramètres comptes</u> ³⁶⁴⁷. Lorsque le paramètre du domaine est désactivé, il a la priorité sur le paramètre de l'utilisateur. Par conséquent, aucun des utilisateurs de ce domaine ne pourra utiliser les fonctionnalités des messages AI, quel que soit leur paramètre utilisateur.

Voir : <u>Fonctionnalités des messages AI du webmail</u> (374), pour plus d'informations et de précautions concernant l'utilisation de ces fonctionnalités. En outre, vous trouverez la politique d'utilisation de l'IA de MDaemon Technologies sur notre <u>page d'information sur l'intelligence artificielle (IA) - MDaemon</u>. Sur cette même page, vous trouverez également un lien vers les Conditions d'utilisation d'OpenAI.

Améliorations du thème

23.5.2

- Pro : Les utilisateurs peuvent désormais cliquer sur le dossier en cours et la liste sera rechargée. Tous les contacts et tous les documents seront désactivés.
- Pro : Ajouté le paramètre de composition avancée à : Paramètres | Composer. Dans ce cas, les champs CC et BCC seront toujours visibles dans la vue de composition.

23.5.1

- Pro : Programmation d'une publication Ajout de champs facultatifs de localisation et de commentaire qui seront inclus dans tout événement créé par le biais de la page de programmation.
- Pro : Amélioration de l'organisation de la page Actions de dossier.

23.5.0

- Pro et WorldClient : Il y a maintenant une option pour supprimer toutes les pièces jointes d'un message donné.
- Pro et WorldClient : Ajout d'une colonne Description dans la vue Documents.
- Pro : Le sélecteur de contact de la vue Composition dispose désormais d'une boîte de dialogue permettant d'ajouter un contact dans trois champs (Nom, Email, Téléphone portable).
- Pro : Il y a de nouvelles options de style dans : Paramètres | Personnaliser.
- Pro : Les rappels d'événements multiples sont désormais pris en charge.

Autres améliorations du Webmail

- Ajout d'une option de planification publique, afin que les utilisateurs puissent permettre à d'autres personnes de planifier une réunion.
- Séparation du processus de configuration de la vérification par e-mail de l'Authentification à deux facteurs du processus de configuration de la vérification de l'app Authentification.
- La fonction de Récupération de Passe envoie maintenant un e-mail sans révéler à l'utilisateur où l'e-mail a été envoyé. L'Auth à deux facteurs se produit après avoir cliqué sur le lien de secours dans l'e-mail.
- Modifier la façon dont le Serveur SMTP Webmail s'authentifie auprès du Serveur SMTP de MDaemon afin que le mot de passe de l'utilisateur ne soit pas nécessaire.
- Ajout d'une option pour "Marquer les messages delete comme lus" dans : Paramètres | Personnaliser.
- Il y a maintenant un bouton "Tous les documents" dans la vue "Documents".

MDaemon Remote Admin (MDRA)

Health Check 545

Il y a maintenant une page Health Check dans MDRA à : Sécurité | Health Check : Sécurité | Health Check. Cette page fournit une liste pratique des paramètres de sécurité importants consolidés sur une seule page, et affiche la valeur

actuelle de chaque paramètre ainsi que sa valeur par défaut. Lorsque ces valeurs diffèrent, le paramètre est mis en évidence afin que les Administrateurs globaux puissent rapidement examiner ces paramètres particuliers et les restaurer à leurs valeurs par défaut si nécessaire. Chaque groupe de paramètres est également accompagné d'une icône de raccourci permettant d'accéder à la page où se trouvent ces paramètres. Dans cette session du navigateur, vous pouvez également consulter la liste de tous les changements apportés au Health Check et les annuler si nécessaire.

Autres améliorations du MDRA

- Ajout d'interfaces graphiques d'édition pour tous les fichiers d'édition directe.
- Il y a maintenant une icône "X" sur laquelle vous pouvez cliquer pour cacher n'importe quel graphique dans les pages Graphiques - boîtes résumant le trafic résumé pages de rapport. Pour restaurer un rapport masqué, cliquez sur votre nom de compte dans le coin supérieur droit de la page, puis sur la case située à côté du rapport que vous souhaitez restaurer.
- Ajout d'un bouton **Tout supprimer** à la page <u>Membres listes de diffusion</u> 287.
- Comme pour le Webmail, la prise en charge de WebAuthn a été ajoutée à MDRA, ce qui donne aux utilisateurs une méthode d'authentification sécurisée, sans mot de passe, et il peut également être utilisé comme une méthode d'Authentification à deux facteurs. Les options WebAuthn dans MDRA se trouvent sur la page <u>Paramètres de MDaemon Remote Admin</u> [377]. Voir : <u>Support WebAuthn</u> and la section Webmail ci-dessus.
- L'<u>Éditeur Dossiers publics</u> bet l'<u>Éditeur Dossiers partagés</u> bisposent désormais d'une option **Imbriquer sous** qui permet de choisir le dossier parent sous lequel le dossier public ou partagé sélectionné sera imbriqué.
- Ajout d'un texte à la page Listes de diffusion de l'éditeur de comptes pour expliquer qu'un utilisateur peut apparaître comme membre d'une liste de diffusion en raison de son appartenance à un groupe 336.
- Dans la page Recherche du message et files d'attente, a ajouté la possibilité de voir le message électronique, en plus de la possibilité de voir sa source. Les messages RAW sont toujours uniquement en text/plain.
- Ajout de liens vers les files d'attente sur la page d'état.
- Ajout de la possibilité d'inclure plusieurs adresses (séparées par des virgules) lors de l'ajout de nouveaux Droits d'accès à la page Contrôle d'accès d'un Dossier public. Vous ne pouvez pas ajouter d'adresses lorsque vous modifiez des droits existants.

Sécurité

- Utilitaire mis à 3 AM vers 1.0.3.
- LetsEncrypt Ajout de la prise en charge de TLS 1.3
- Mise à jour de SpamAssassin vers 4.0.0.

XMLAPI

MDaemon 23.5.0 apporte de nombreux ajouts et améliorations à l'interface XMLAPI. Voir les notes de version pour une liste complète de ces améliorations.

Autre

- Ajout d'une option <u>Mots passe d'application au permet de supprimer les mots</u> passe d'application d'un compte lorsque le mot de passe du compte est modifié. Cette nouvelle option est activée par défaut.
- Ajout d'une page <u>Restrictions</u> aux Modèles de comptes. Lorsqu'un compte est supprimé d'un groupe avec un modèle de compte qui contrôle les restrictions, les restrictions du compte reviennent à leurs valeurs précédentes, ou éventuellement au modèle de compte d'un autre groupe si le compte est membre de plusieurs groupes.
- L'option de filtrage par localisation il "Les connexions SMTP sont acceptées mais l'authentification est bloquée" est maintenant par pays et non plus globale. Bloquer les connexions SMTP empêche votre serveur de recevoir du courrier en provenance d'un pays. Autoriser les connexions SMTP avec l'authentification désactivée permet à votre serveur de recevoir du courrier d'un pays tout en bloquant les attaques par force brute ou par dictionnaire provenant de ce pays. Les protocoles autres que SMTP ne sont pas concernés.
- Suppression de l'option Webmail obsolète "Rédiger dans nouvelle fenêtre navigateur" de l'interface utilisateur.
- LetsEncrypt Ajout de la prise en charge de TLS 1.3.

Notes de version du serveur MDaemon

Pour obtenir une liste complète de ces nouveautés et de tous les autres ajouts, changements et corrections inclus dans MDaemon 23.5.2, consultez les Notes de mise à jour.

Nouveautés dans MDaemon Private Cloud 11.0.0

- MDaemon Private Cloud 11.0.0 inclut MDaemon 23.0.2 avec MDaemon Connector 7.0.7.
- MDaemon désactive la mise à jour automatique du client MDaemon Connector dans les versions antérieures à 7.0.6, afin de résoudre un problème de mise à jour automatique dans ces versions.

Pour obtenir la liste de toutes les modifications apportées à MDaemon, consultez les notes de mise à jour de MDaemon 23.0 = tout).

Pour une liste de toutes les modifications apportées à MDaemon Connector, voir le document MDaemon Connector 7.0.7.

Nouveautés de MDaemon 23.0

Modifications et nouvelles fonctionnalités

Serveur MDaemon

- (23.0.2) Ajout d'une option <u>MultiPOP</u> [144] permettant d'envoyer un e-mail de notification après plusieurs échecs lors de la vérification d'un compte MultiPOP. Les échecs temporaires n'étant pas rares, une option permet de définir le nombre d'échecs consécutifs nécessaires pour déclencher la notification. Il est également possible de définir le nombre de jours d'attente entre les notifications, afin d'éviter d'en envoyer un trop grand nombre. Le contenu et les destinataires des e-mails de notification peuvent être personnalisés en modifiant le fichier \MDaemon\App\MPOPFailureNotice.dat. Par défaut, les notifications sont envoyées après 5 échecs, au maximum une fois tous les 7 jours, au propriétaire du compte MultiPOP.
- Il y a une nouvelle page <u>MultiPOP</u> 144] sous Paramètres de serveur. À partir de cette page, vous pouvez activer/désactiver le serveur MultiPOP de MDaemon et utiliser l'option "*MultiPOP supprime toujours le courrier…*" (anciennement située sur la page <u>Collecte MultiPOP</u> 406]) pour remplacer l'option<u>Laisser une copie</u> du message sur le serveur POP 792] pour tous les utilisateurs. Cette nouvelle page contient également des options de prise en charge OAuth 2.0 pour Collecte MultiPOP courrier depuis Gmail et Office 365.

Prise en charge d'OAuth pour MultiPOP 2.0 pour la collecte de courrier depuis Gmail et Office 365 [145] - OAuth 2.0 est une authentification moderne, que ces services requièrent désormais car ils désactivent la prise en charge de l'authentification héritée/de base. Dans le but que la fonctionnalité MultiPOP de MDaemon utilise OAuth 2.0 pour collecter le courrier de Gmail ou d'Office365 au nom de vos utilisateurs, vous devez enregistrer votre serveur MDaemon auprès de Google ou de Microsoft, respectivement, en créant une application OAuth 2.0 à l'aide de la Google API Console ou de l'Azure Active Directory de Microsoft. Cette procédure est similaire à celle requise pour utiliser l'<u>Intégration avec</u> <u>Dropbox</u> [362] de MDaemon pour vos utilisateurs de Webmail. Consultez la rubrique d'aide de <u>MultiPOP</u> [145] pour plus d'informations sur la configuration de la prise en charge d'OAuth pour <u>MultiPOP</u> [145].

- Le serveur IMAP de MDaemon prend désormais en charge les drapeaux de motsclés. Cela permet aux clients de messagerie tels que Mozilla Thunderbird de stocker les Paramètres de messages sur le serveur, ce qui vous permet de voir les balises dans une instance d'un client qui ont été définies dans une autre instance du client.
- Amélioration des performances du serveur IMAP lors de l'ouverture de dossiers courrier volumineux.

Sécurité

 (23.0.2) Ajout de la prise en charge du Data Query Service (DQS) de Spamhaus au <u>Filtre anti-spam</u> [725]. Pour plus d'informations sur Spamhaus DQS, visitez : <u>https://info.spamhaus.com/getting-started-with-dqs</u>.

33

- Une nouvelle option Bloquer les violations de la politique de connexion a été ajoutée à l'Écran dynamique (50), que vous pouvez utiliser si vous souhaitez bloquer toute adresse IP qui tente de se connecter sans utiliser l'adresse e-mail complète. [Cette option est désactivée par défaut. Cette option est désactivée par défaut. Voir la page Systèmes (525) pour plus d'informations sur l'option correspondante, "Les serveurs demandent l'adresse e-mail complète pour l'authentification".
- Une option Uniquement pour les comptes valides a été ajoutée pour étendre l'option Ignorer les tentatives d'authentification utilisant des mots de passe identiques sur la page Suivi des échecs d'authentification and la compte option si vous souhaitez ignorer les tentatives d'authentification par mot de passe identique uniquement lorsqu'elles tentent de se connecter à un compte valide. Par nom, si, par exemple, un utilisateur met à jour son mot de passe, les tentatives de Connexion de cet ancien client seront toujours ignorées, puisqu'il aura le nom de connexion correct. Un robot essayant des noms de connexion aléatoires avec un mot de passe similaire ne bénéficiera pas du même avantage et sera bloqué dès qu'il dépassera le seuil d'échec d'authentification. Cela permettra de vaincre les robots beaucoup plus rapidement. L'opération DynamicScreen de l'API XML a également été mise à jour pour refléter ces nouvelles fonctionnalités.
- Une option<u>Filtrage du contenu | Pièces jointes</u> [708] a été ajoutée pour : "Ajouter un avertissement en haut du corps du message si la pièce jointe est supprimée". Lorsque MDaemon supprime une pièce jointe d'un message, par exemple parce qu'un virus a été détecté, il ajoute un message d'alerte en haut du corps du message. Il y a également un bouton**Messages avertissement** à utiliser si vous souhaitez revoir ou modifier le modèle de ce message. Cette option est activée par défaut.
- Ajout d'une option permettant d'<u>exclure les IP autorisées de l'analyse</u> <u>antivirus</u> [718].
- À propos de MDaemon envoie un e-mail d'avertissement aux administrateurs lorsque les <u>certificats SSL</u> [613] configurés pour être utilisés par <u>MDaemon</u> [614], <u>Webmail</u> [617] ou <u>MDaemon</u> [614] <u>Remote Admin</u> [621] sont sur le point d'expirer.
- MTA-STS dispose désormais d'une liste d'exemptions, de sorte que les domaines problématiques peuvent être exemptés au lieu que MTA-STS doive être désactivé lorsque des défaillances affectent la délivrabilité.
- Le composant ClamAV AntiVirus a été mis à jour à la version 0.105.2 (dans 1 AM 23.0.1).

Webmail

 Intégration de Google Drive ssi - Webmail peut désormais être lié aux comptes Google de vos utilisateurs pour leur permettre d'enregistrer les pièces jointes des messages directement dans leur Google Drive, ainsi que de modifier et de travailler avec les documents qui y sont stockés. Pour ce faire, une clé API, un ID client et un Code secret client sont nécessaires. Vous pouvez les obtenir directement auprès de Google en créant une application à l'aide de la console API de Google et en enregistrant votre MDaemon auprès de leur service. Un composant d'authentification OAuth 2.0 fait partie de cette application, qui

permet à vos utilisateurs de Webmail de se connecter à Webmail, puis d'autoriser l'accès à leur compte Google Drive via MDaemon. Une fois autorisés, les utilisateurs peuvent consulter leurs dossiers et fichiers qui se trouvent dans Google Drive. En outre, ils peuvent charger, télécharger, déplacer, copier, renommer et supprimer des fichiers, ainsi que copier/déplacer des fichiers vers et depuis les dossiers de documents locaux. Si l'utilisateur souhaite modifier un document, il lui suffit de cliquer sur l'option d'affichage du fichier dans Google Drive pour pouvoir y apporter des modifications conformément aux autorisations définies dans Google Drive. Le processus de configuration de Google Drive est similaire aux fonctionnalités Intégration avec Dropbox [362] et Intégration OAuth pour MultiPOP [144] de MDaemon. Voir Intégration de Google Drive [355] pour plus d'informations.

- Ajout d'une option dans tous les thèmes sauf Lite pour "Activer le glisserdéposer pour déplacer les dossiers". La nouvelle option est située dans le Webmail sur la page **Dossiers** sous le menu Options, et elle est activée par défaut.
- Le cookie de session est désormais sécurisé par HTTPS.
- La notification de changement de catégorie est désormais envoyée à MDaemon.
- WorldClient ne modifie plus le fichier robots.txt au démarrage.
- Le serveur Web intégré empêche le téléchargement de fichiers .dll depuis le répertoire HTML.
- Ajout d'un à la longueur maximale de l'entrée du nouveau mot de passe, de sorte que l'exigence "Maximum de 15 caractères" non satisfaite s'affiche.
- Ajout d'un rapport sur les tentatives de connexion sans adresse électronique complète, afin de prendre en charge la nouvelle option de Filtrage dynamique pour bloquer les violations de la politique de connexion [650].
- (23.0.2) L'option "unsnooze" a été rendue plus visible grâce à une surbrillance orange.

Thème Pro

- Ajout de la prise en charge des accusés de réception.
- Ajout d'une option pour désactiver le menu contextuel de l'éditeur HTML.
- Ajout de la possibilité de redimensionner la liste des dossiers.

MDaemon Remote Admin (MDRA)

23.0.2

- Ajout d'une option <u>AntiVirus</u> [718] pour *"Exclure les IP autorisées de l'analyse AntiVirus*".
- Ajout de l'option "*Ne pas autoriser l'authentification sur le port SMTP*" dans <u>Authentification SMTP</u> [558].
- Ajout d'une option <u>Gestionnaire des dossiers publics</u> pour spécifier un Nom d'affichage ActiveSync.

- Ajout de quatre options de filtrage supplémentaires au <u>Gestionnaire de</u> <u>comptes</u> [762]: Administrateurs uniquement, Non-administrateurs uniquement, Administrateurs globaux uniquement et Administrateurs de domaine uniquement.
- Ajout d'une page pour le Data Query Service (DQS) de Spamhaus au <u>Filtre anti-spam</u>
 <u>spam</u>
 Pour plus d'informations sur Spamhaus DQS, visitez : https://info.spamhaus.com/getting-started-with-dqs

23.0.0

- Dans le Gestionnaire de domaines, il y a maintenant un <u>Paramètres Webmail</u> pour "Autoriser les utilisateurs à recevoir les codes de vérification Authentification à deux étapes par e-mail", afin que les utilisateurs puissent recevoir leur code de vérification via une autre adresse e-mail plutôt que d'utiliser l'application Google Authenticator. Ce paramètre est activé par défaut.
- Modification des autorisations par défaut lors de l'ajout d'une nouvelle entrée ACL à Lookup et Read.
- Les boutons **Test** à : <u>Filtre anti-spam | Hôtes DNS-BL | Hosts</u> [752] and <u>Setup |</u> <u>Active Directory » Authentification</u> [884] sont désormais désactivés lorsque le processus est en cours.
- Le serveur Web intégré empêche l'exécution et le téléchargement de fichiers .dll dans le répertoire Templates.
- Les utilisateurs peuvent désormais personnaliser l'apparence de l'interface web de MDaemon Remote Admin en cliquant sur leur nom d'utilisateur (par exemple frank.thomas) dans le coin supérieur droit de la fenêtre. Des options permettent de passer l'interface en mode sombre, de définir la Taille de la police et de choisir la langue préférée.
- La confirmation de la suppression du compte a été modifiée pour utiliser la fonction de confirmation personnalisée.
- Ajout d'un rapport sur l'Écran dynamique pour les tentatives de connexion sans adresse électronique complète.

ActiveSync

- Ajout d'une option dans les Paramètres clients pour <u>bloquer l'expéditeur lors du</u> <u>déplacement d'un courrier dans le Dossier de courrier indésirable</u> [447]. Si cette option est activée, lorsqu'un client déplace un e-mail dans le dossier Courriers indésirables du compte, le service ajoute l'adresse expéditeur ou l'adresse de provenance de cet e-mail au dossier Courriers bloqués.
- Vous pouvez désormais désactiver le <u>bouton Effacer</u> [488] complètement pour les clients ActiveSync si vous le souhaitez, de sorte que vous ne pouvez pas effectuer un effacement complet à distance sur un périphérique ActiveSync sans désactiver au préalable la nouvelle option <u>Interdire les réinitialisations</u> <u>usine</u> [447].
- Les données de BodyPreferences sont désormais lisibles par l'homme afin de faciliter la résolution des problèmes de synchronisation.
- Amélioration des performances d'arrêt lorsque les clients synchronisent des boîtes aux lettres volumineuses.
- Ajout de la possibilité de définir un nom d'affichage personnalisé pour la boîte aux lettres et les Dossiers publics.
- Amélioration des performances d'arrêt.
- Les clients ActiveSync peuvent désormais envoyer des messages à des listes de distribution personnelles dans des dossiers de contacts.
- Modification de la disposition de la boîte de dialogue des paramètres clients dans l'interface graphique afin d'ajouter de la place pour les nouveaux paramètres.

Autre

- (23.0.2) Filtre du contenu <u>\$LIST_ATTACHMENTS_REMOVED</u>
 itilisé dans les actions des règles (par exemple "envoyer une note", "ajouter un avertissement...")
- Dans l'interface graphique de MDaemon, modification des permissions par défaut lors de l'ajout d'une nouvelle entrée ACL en Lookup et Read.
- Dans l'interface graphique de MDaemon, ajout d'un avertissement si vous tentez de configurer les ports du Serveur Webmail, MDaemon Remote Admin, ou XMPP BOSH pour qu'ils aient des valeurs contradictoires.
- XMLAPI Ajout de l'opération Editor qui peut être utilisée pour éditer les différents fichiers INI de MDaemon.
- Modification de plusieurs plug-ins pour permettre l'exécution de versions plus récentes afin que les clients puissent tester d'éventuelles versions hotfix/patch.
- LetsEncrypt Mise à jour du script pour vérifier les commandes qui sont prêtes ou valides.

Notes de mise à jour du serveur MDaemon

Dans une liste complète des ajouts, modifications et corrections inclus dans la version 23.0.2 de MDaemon, voir les Notes de version.

Nouveautés dans MDaemon Private Cloud 10.0.2

 MDaemon Private Cloud 10.0.2 inclut MDaemon 22.0.5 avec MDaemon Connector 7.0.7.

Considérations particulières

 La Protection instantanée a été restaurée. Veuillez vérifier vos paramètres de Protection instantanée, car ils peuvent avoir été réinitialisés à leurs valeurs par défaut.

Pour obtenir la liste de toutes les modifications apportées à MDaemon, consultez les notes de mise à jour de MDaemon 22.0 = tout).

Nouveautés dans MDaemon Private Cloud 10.0.1

 MDaemon Private Cloud 10.0.1 inclut MDaemon 22.0.4 avec MDaemon Connector 7.0.7.

Considérations particulières

- Cyren Anti-Virus a été remplacé par IKARUS Anti-Virus. Cyren a récemment annoncé son intention de <u>cesser ses activités</u> sans préavis. Il nous a donc fallu trouver un nouveau partenaire antivirus. Après une évaluation approfondie, IKARUS Anti-Virus s'est distingué par son excellent taux de détection et sa rapidité. Il offre une protection fiable contre les programmes malveillants et potentiellement hostiles, et combine les méthodes traditionnelles de défense antivirus avec les dernières technologies proactives. IKARUS Anti-Virus met automatiquement à jour ses définitions toutes les 10 minutes. L'analyse avec IKARUS est désactivée si votre licence AntiVirus a expiré.
- La Protection instantanée de Cyren a été supprimée. Cyren a récemment annoncé son intention de cesser ses activités sans préavis. Nous recherchons activement et considérons des technologies anti-spam viables comme des ajouts appropriés aux mécanismes anti-spam existants trouvés dans nos produits logiciels.

Pour obtenir la liste de toutes les modifications apportées à MDaemon, consultez les notes de mise à jour de MDaemon 22.0 = tout).

Nouveautés dans MDaemon Private Cloud 10.0.0

 MDaemon Private Cloud 9.5 inclut MDaemon 22.0.3 avec MDaemon Connector 7.0.7.

Pour une liste de tous les changements apportés à MDaemon, voir le document Notes de mise à jour de MDaemon 22.0.3.

Pour une liste de tous les changements apportés à MDaemon Connector, voir le document MDaemon Connector 7.0.7.

Nouveautés de MDaemon 22.0

Changements et nouvelles fonctionnalités

Webmail

Thème Pro

 Lorsque vous consultez un message, vous pouvez survoler le nom de l'expéditeur pour ouvrir une fenêtre contextuelle qui contient des options permettant d'ajouter l'expéditeur à vos contacts et aux dossiers Expéditeurs bloqués ou autorisés.

- Les affichages Composer, Message, Événement, Contact, Tâche et Note peuvent désormais s'ouvrir dans une nouvelle fenêtre.
- Vous pouvez désormais ouvrir le prochain message non lu à partir du volet d'aperçu des messages et de l'affichage des messages.
- Dans la liste des messages, des extraits de messages ont été ajoutés en mode multiligne.
- Vous pouvez désormais mettre à disposition des utilisateurs du thème Pro une option *Modifier les noms alias d'affichage*, située sous Paramètres » Composer. Cette option permet aux utilisateurs de modifier le nom d'affichage de leurs alias associés à leur compte. Utilisez les nouveaux <u>Paramètres du Webmail</u>
 "Autoriser les utilisateurs à modifier les noms d'affichage de leurs alias" si vous souhaitez autoriser cette option. Notes de l'administrateur : Cette option n'est disponible que dans l'interface web de l'Administration MDaemon Remote Admin (MDRA)
- Les options et les liens qui indiquaient "Liste noire d'expéditeurs" ou "Liste blanche d'expéditeurs" indiquent désormais "Autoriser" ou "Bloquer" l'expéditeur. En outre, les dossiers Liste d'autorisation d'expéditeurs (Liste blanche) et Liste d'interdiction d'expéditeurs (Liste noire) s'appellent désormais "Expéditeurs autorisés" et "Expéditeurs bloqués".
- La liste des messages peut être triée en fonction de la colonne Drapeau.
- Dans la liste des tâches, les tâches en retard apparaissent désormais en rouge.
- Mise à jour du client XMPP vers la version 4.4.0.

Autre

- Lorsque des mots de passe sécurisés sont requis, il y a maintenant une liste des mots de passe requis qui s'affiche en vert et qui est cochée au fur et à mesure que l'utilisateur répond aux exigences. Des messages d'erreur plus descriptifs ont également été ajoutés pour expliquer ce qui ne va pas avec un mot de passe non valide lors de la soumission.
- Les options de composition contiennent désormais des options permettant de sélectionner l'adresse "De :" par défaut qui sera utilisée lors de la composition, de la réponse ou du transfert d'un message.
- Un paramètre "1 minute" a été ajouté à l'option "Temps de rafraîchissement de la liste", située sur la page "Options" "Personnaliser".
- Dans la page de Connexion au MDaemon Webmail, la prise en charge des CSRFTokens a été ajoutée. Cette fonction est activée lorsque l'option"Utiliser les jetons Cross-Site-Request-Forgery" est activée sur la page <u>Paramètres de</u> <u>MDaemon Webmail » Serveur Web</u>[33]. Si vous utilisez des modèles personnalisés pour le Webmail, ajoutez une entrée cachée au formulaire de connexion comme suit : <input type="hidden" name="LOGINTOKEN" value=<\$LOGINTOKEN\$> />
- Calendrier public Modification de l'affichage de la liste pour commencer par le jour en cours et afficher les 30 prochains jours.
- Ajout de la conversion automatique des URL en hyperliens dans l'affichage des messages.

- Les noms des dossiers par défaut (Brouillons, Envoyés, etc.) sont traduits dans la langue de l'utilisateur du Webmail, quelle que soit la langue de MDaemon installée (auparavant, seul le MDaemon anglais le faisait).
- Il existe désormais une option permettant d'envoyer les codes de vérification de l'Authentification à deux facteurs à une adresse électronique secondaire.
- Thèmes LookOut et WorldClient Aucune modification à afficher dans les catégories de listes.
- Les dossiers Expéditeurs autorisés et Expéditeurs bloqués ont désormais des icônes différentes pour indiquer qu'il s'agit de dossiers spéciaux.

MDaemon Remote Admin (MDRA)

- Ajout d'une page Auth à deux facteurs IP exemptées dans MDRA, située sous le menu principal. Elle permet aux utilisateurs de se connecter à MDaemon Remote Admin ou au Webmail sans avoir besoin de 2FA, lorsqu'ils se connectent à partir d'une des adresses IP spécifiées.
- Il y a une nouvelleoption"Autoriser les utilisateurs à modifier leursaffichages alias" dans les Paramètres Webmail de MDRA. Activez cette option si vous souhaitez permettre aux utilisateurs de modifier l'affichage de leurs alias associés à leur compte. Ils peuvent le faire en utilisant l'option Modifier les noms d'affichage des alias, située dans le thème Pro de Webmail.
- Modifier autocomplete="off" en autocomplete="new-password" dans les champs mots de passe pour empêcher Firefox de compléter automatiquement les mots de passe en dehors de la page de connexion.
- Ajout de l'Éditeur de message de notification à la page Notifications du Filtre de contenu.
- Ajout de la prise en charge des CSRFTokens sur la page de Connexion. Cette fonction est activée lorsque l'option "Use Cross-Site-Request-Forgery tokens" est activée sur la page <u>Paramètres de MDaemon Remote Admin</u> (377) dans MDRA.
- Toutes les <u>Files d'attente personnalisées</u> [337] locales ou distantes que vous avez créées peuvent être gérées dans la section Messages et files d'attente de MDRA.

Sécurité

 AM supporte désormais TLS 1.3 sur les nouvelles versions de Windows. Windows Server 2022 et Windows 11 ont TLS 1.3 activé par défaut. Les versions 2004 (OS Build 19041) et plus récentes de Windows 10 ont une prise en charge expérimentale de TLS 1.3 qui peut être activée pour les connexions en entrée en paramétrant ce qui suit dans le registre :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
    ders\SCHANNEL\Protocols\TLS 1.3\Server
Désactivé par défaut (DWORD) = 0
```

```
Activé (DWORD) = 1
```

- MDaemon enregistre la suite de chiffrement (par exemple, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) utilisée par les connexions SSL/TLS.
- Ajout d'une option <u>Mots de passe</u> aux mots passe forts demandant un caractère spécial. Elle est activée par défaut pour les nouvelles installations et désactivée par défaut pour les installations existantes.
- Scanner de boîtes aux lettres AV Lorsqu'un message infecté est trouvé au cours d'un scan de boîtes aux lettres, le compteur d'infections de MDaemon est incrémenté.
- Utilitaire de mise à jour à jour ClamAV à la version 0.104.3.

ActiveSync

- Amélioration des performances de FolderSync.
- La boîte de dialogue de surveillance des connexions ActiveSync dispose d'une nouvelle commande de menu par clic droit pour mettre fin à une session et bloquer un client.
- Ajout d'une option à la boîte de dialogue <u>Paramètres des clients</u> [488] pour permettre à Outlook d'envoyer du courrier à l'aide d'un alias. Si Reply-To est défini sur un alias valide pour le compte d'envoi, le message sera envoyé via cet alias.
- Ajout de la prise en charge de la commande Find de 1 AM 16.1. Suppression de la <u>restriction de protocole</u> [459] empêchant iOS d'utiliser EAS 16.1.

Autre

- Filtre de contenu Ajout de la prise en charge des macros \$CONTACT...\$ dans l'action "Ajouter une signature". Ces macros peuvent être utilisées pour personnaliser la signature avec les informations du contact de l'expéditeur dans son dossier de contacts publics. Voir : <u>Macros de signature</u> pour une liste complète des macros prises en charge.
- Filtre de contenu Ajout d'une action pour <u>extraire les pièces jointes</u> et ajouter le <u>lien vers les pièces jointes</u> and le message.
- Suppression Les<u>E-mails de attente</u> la file d'attente, de la quarantaine et de la mauvaise file d'attente peuvent maintenant avoir des liens pour libérer, remettre en file d'attente ou supprimer chaque message. Cette nouvelle option "*Inclure un lien d'action*" est activée par défaut. Note : Le paramètre <u>URL de MDaemon Remote Admin ari</u> doit être défini pour que les liens soient générés.
- <u>LetsEncrypt</u> [632] Mise à jour du script pour qu'il fonctionne avec PS 7.
- Ajout d'une option de <u>Rappel de message</u> 120 Distribution différée pour remplacer l'en-tête 'Date:' par la date et l'heure actuelles lorsqu'un message est libéré de la file d'attente différée. Cette option est désactivée par défaut.
- <u>MDaemon Connector</u> a été mis à jour vers la version 7.0.7.
- XMLAPI Ajout de la prise en charge de la planification des transferts.

Notes de version du serveur MDaemon

Pour obtenir une liste complète des ajouts, modifications et corrections inclus dans la version 22.0 de MDaemon 22.0, consultez les notes de version.

Nouveautés dans MDaemon Private Cloud 9.5.0

 MDaemon Private Cloud 9.5 inclut MDaemon 21.5.2 avec MDaemon Connector 7.0.6.

Pour une liste de tous les changements apportés à MDaemon, voir le document Notes de mise à jour de MDaemon 21.5.2.

Pour une liste de toutes les modifications apportées à MDaemon Connector, voir le document MDaemon Connector 7.0.6.

Nouveautés de la version 21.5 de MDaemon

Principales nouveautés

Mots de passe d'application

Les Mots passe d'application sont des mots de passe très forts, générés aléatoirement, à utiliser dans les clients de messagerie et les applications, afin de rendre vos applications de messagerie plus sécurisées car elles ne peuvent pas être protégées par l'Application <u>d'authentification</u> à deux facteurs π_1 (2FA). L'authentification à deux facteurs est un moyen sûr pour un utilisateur de se connecter au Webmail ou à MDaemon Remote Admin (MDRA), mais une application de messagerie ne peut pas l'utiliser, car l'application doit pouvoir accéder à votre messagerie en arrière-plan sans que vous ayez à saisir un code à partir de votre application d'authentification. La fonctionnalité Mots de passe d'application vous permet de créer des mots de passe forts et sécurisés à utiliser dans vos apps, tout en conservant le mot de passe de votre compte sécurisé par 2FA. Les Mots passe d'application ne peuvent être utilisés que dans les applications de messagerie, ils ne peuvent pas être utilisés pour se connecter à Webmail ou MDRA. Cela signifie que même si un Mot passe d'application était compromis, l'utilisateur non autorisé ne pourrait pas accéder à votre compte pour modifier votre mot de passe ou d'autres paramètres, mais vous, vous seriez toujours en mesure de vous connecter à votre compte avec votre mot de passe de compte et 2FA, pour supprimer le Mot passe d'application compromis et créer un nouveau mot de passe si nécessaire.

Exigences relatives aux mots de passe d'application et recommandations

- Dans le but de créer des Mots passe d'application, 2FA doit être activé pour le compte (bien que vous puissiez <u>désactiver cette exigence</u> si vous le souhaitez).
- Les Mots passe d'application ne peuvent être utilisés que dans les applications de messagerie. Ils ne peuvent pas être utilisés pour se connecter à Webmail ou MDRA.

- Chaque Mot de passe d'application n'est affiché qu'une seule fois, lors de sa création. Il n'y a aucun moyen de le récupérer plus tard. Les utilisateurs doivent donc être prêts à le saisir dans leur application dès sa création.
- Les utilisateurs doivent utiliser un Mot de passe d'application différent pour chaque application de messagerie, et ils doivent révoquer (supprimer) leur mot de passe chaque fois qu'ils cessent d'utiliser une application ou en cas de perte ou de vol d'un appareil.
- Chaque Mot de passe d'application indique la date de sa création, la date de sa dernière utilisation et l'adresse IP à partir de laquelle il a accédé pour la dernière fois à la messagerie du compte. Si un utilisateur trouve quelque chose de suspect dans les données de Dernière utilisation ou de Dernière IP, il doit révoquer ce Mot de passe d'application et en créer un nouveau pour son application.
- Lorsqu'un mot de passe de compte est modifié, tous les Mots passe d'application sont automatiquement supprimés - l'utilisateur ne peut pas continuer à utiliser d'anciens Mots passe d'application.

Exigences relatives aux mots passe d'application pour SMTP, IMAP, ActiveSync, etc.

Il existe une option de compte sur la page <u>Paramètres des comptes de l'éditeur de</u> <u>compte</u> [815] que vous pouvez utiliser pour "*Exiger un mot de passe d'application pour se connecter à SMTP, IMAP, ActiveSync, etc.*".

Demander des Mots passe d'application peut aider à protéger le mot de passe d'un compte contre les attaques par dictionnaire et par force brute via SMTP, IMAP, etc. Cette solution est plus sûre car même si une attaque de ce type permettait de deviner le mot de passe réel d'un compte, elle ne fonctionnerait pas et l'attaquant ne le saurait pas, car MDaemon n'accepterait qu'un Mot passe Mon compte correct. De plus, si vos comptes dans MDaemon utilisent l'authentification <u>Active Directory</u> et que Active Directory est configuré pour verrouiller un compte après un certain nombre de tentatives échouées, cette option permet d'éviter que les comptes ne soient verrouillés, car MDaemon ne vérifiera que les Mots passe d'application, sans essayer de s'authentifier auprès d'Active Directory.

Autres nouveautés et améliorations

Thème Pro

- Le thème Mobile s'appelle désormais le thème **Pro**. Il a été étendu et amélioré pour être réactif et adaptable à une utilisation sur différents types d'appareils et de tailles d'écran, sans sacrifier les fonctionnalités.
- Ajout de jetons Cross-Site-Request-Forgery pour des transactions plus sûres. Cette fonctionnalité est désactivée par défaut. Pour l'activer via MDRA, allez dans <u>Main | Paramètres Webmail | Serveur Web</u> and et cochez "Use Cross-Site-Request-Forgery tokens".
- Ajout d'une option dans Paramètres | Personnalisation pour activer le mode sombre, afin d'afficher le thème Pro avec un fond sombre.
- Ajout d'un lien vers "Suivre mon colis" dans les messages ouverts.

- Les numéros de suivi des transporteurs surveillés par défaut sont les suivants : USPS, UPS, OnTrac, FedEx et DHL.
- Le fichier de configuration par défaut se trouve à l'adresse suivante : \MDaemon\MondeClient\package_tracking.json
- Les administrateurs peuvent ajouter d'autres transporteurs en créant le fichier : \MDaemon\WorldClient\package_tracking .custom.json, en utilisant le même format que le fichier package_tracking.json par défaut. Il faut au moins un nom de service, une URL de suivi et au moins une expression régulière valide. Dans les messages, incluez les noms de service susceptibles d'apparaître afin de réduire les risques de correspondance faussement positive.
- La boîte de dialogue Disposition de la liste des messages a été adaptée à la taille réduite du navigateur. Seul le paramètre Densité de la liste des messages est affiché.
- Ajout d'un indicateur de force du mot passe.
- Ajout d'une fonction de diaporama d'images dans l'Affichage message.
- Ajout d'une vue en carte pour la liste des contacts.
- Déplacer le bouton "Nouvel élément" de la barre d'outils vers l'espace au-dessus de la liste des dossiers pour les tailles de bureau.
- Dans l'affichage du calendrier, une icône plus a été ajoutée à côté de "Personnel" pour créer un nouveau calendrier.
- Ajout d'une infobulle sur les événements avec les options de modification et l'option Envoyer un e-mail à un participant.
- La barre de recherche est désormais toujours visible lorsque la largeur de la fenêtre du navigateur est égale ou supérieure à 1 200 pixels.
- Ajout d'une boîte de dialogue permettant aux utilisateurs de supprimer un contact de la liste noire lorsqu'ils l'ajoutent à la liste blanche et vice-versa.
- Ajout d'un message d'erreur en cas d'erreur lors de la création ou du changement de nom d'un dossier.
- Ajout de la prise en charge des notes HTML dans les événements, les contacts, les tâches et les notes.
- Remplacé l'éditeur HTML actuel (CKEditor) par Jodit.
- Modification des en-têtes de base pour afficher l'adresse électronique From.
- Ajout de l'enregistreur vocal.

Autres améliorations du Webmail

- Ajout d'un lien de désabonnement à côté de l'adresse From lorsque l'en-tête List-Unsubscribe existe dans un message. Ce lien peut être désactivé dans le Webmail sous Paramètres | Personnaliser.
- Ajout de la possibilité d'importer des e-mails dans la liste de messages actuelle.

- Mise à jour de l'intégration avec Dropbox pour utiliser le refresh_token fourni par Dropbox pour reconnecter les utilisateurs sans interaction avec la boîte de dialogue OAuth. Lorsque l'access_token expire, le Webmail tentera d'utiliser le refresh_token pour obtenir un nouvel access_token. Les paramètres qui ne sont plus nécessaires ont été supprimés de la page Cloud Apps. L'administrateur n'a PAS besoin d'apporter des modifications à l'application Dropbox sur Dropbox.com.
- Les requêtes Chercher tout / Sous-dossiers ne recherchent plus les dossiers non abonnés lorsque les dossiers non abonnés sont masqués.
- Par nom, une case à cocher "Ignorer la recherche" a été ajoutée pour exclure des dossiers spécifiques des requêtes "Tout rechercher" et "Sous-dossiers".
- Dans MDaemon Remote Admin, un paramètre permet de masquer la case à cocher "Se souvenir de moi" de l'Authentification deux facteurs.
- Ajout d'un effet de flou pour l'arrière-plan lorsque la session de l'utilisateur est expirée.
- Ajout d'une fonction CC et BCC automatique dans Paramètres | Composer.
- Ajout d'une option pour : DomainClient\Domains.ini [Défaut:Paramètres] PreventComposeWithAlias, pour empêcher la composition de messages avec un alias. Le paramètre est désactivé par défaut.
- Thème Lite Ajout de l'enregistrement automatique des brouillons de messages dans la vue "Composer".
- Dans la vue Options | Dossiers, une option a été ajoutée pour permettre aux utilisateurs d'ignorer les dossiers de contacts dans les recherches par autocomplétion. Dans le menu du clic droit, l'option a également été ajoutée.
- Ajout d'une entrée dans le journal du Webmail pour l'Agent utilisateur lorsqu'un utilisateur se connecte.
- Ajout d'une notification dans la vue Compose si un destinataire local a activé son autorépondeur.
- Thème WorldClient Ajout d'une icône de trombone aux tuiles d'événements comportant des pièces jointes.
- La taille maximale des pièces jointes est fixée à 25 Mo pour les nouvelles installations.
- L'action "Tout supprimer" a été remplacée par l'action "Vider le dossier".
- Thème WorldClient Ajout des boutons "Modifier le mot passe" et "Modifier l'email de Récupération" à la page Sécurité.

MDaemon Remote Admin (MDRA)

- Ajout de la possibilité de glisser-déposer des Règles du Filtre de contenu. Les boutons de copie, d'édition et de suppression se trouvent maintenant sur chaque règle respective.
- Ajout de jetons Cross-Site-Request-Forgery pour des transactions plus sûres. Cette fonctionnalité est activée par défaut. Pour la désactiver, allez sur : <u>Main</u>

<u>| Paramètres de MDaemon Remote Admin | Settings</u> 377 et décochez "Use Cross-Site-Request-Forgery tokens".

- Ajout d'un indicateur de force du mot de passe dans certains champs À :.
- Ajout de l'option "Activer l'Authentification à deux facteurs à facteurs" à <u>Options de domaine | Gestionnaire de domaines | Modifier | Paramètres</u> <u>Webmail</u> [197] et <u>Principal | Paramètres Webmail | Paramètres</u>
- Ajout de rapports IP bloquées et IP refusées pour l'Écran dynamique.
- Ajout des vues <u>Groupes</u> [497] et <u>Types de clients</u> [504] sous ActiveSync.
- Mise à jour des pages <u>Diagnostics</u> [457] ActiveSync et <u>Réglages</u> [443].
- Ajout d'un graphique et d'un tableau d'utilisation du navigateur par OS à Rapports graphiques trafic statistiques de connexion à Webmail.
- Ajout de boutons permettant d'ouvrir une fenêtre contextuelle Parcourir les utilisateurs et Parcourir les groupes, afin de les ajouter aux listes de diffusion, à l'adresse suivante : <u>Main | Mes listes de diffusion | Editer | Nouveau[287]</u>. Aucun <u>Administrateurs globaux [812]</u> uniquement n'a accès à ces boutons.
- Ajout d'options Effacer uniquement le compte dans Main | Mon compte | Clients ActiveSync et dans <u>ActiveSync | Gestion des client</u> 488 s.
- La Pas de journalisation des modifications a été ajoutée. Elle enregistrera chaque changement effectué via MDaemon Remote Admin.
- Mise à jour du <u>Rappel de message</u> 120 pour qu'il corresponde à l'interface graphique de MDaemon.
- Ajout de l'option "Extraire les pièces jointes de winmail.dat" dans <u>Sécurité</u> <u>Filtre de contenu | Compression</u> 715
- Ajout de la langue slovène dans l'Administration de MDaemon Remote Admin.

Autres améliorations de MDaemon

- Prise en charge de la fonction SMTP Command Pipelining (RFC 2920). MDaemon envoie les commandes MAIL, RCPT et DATA par lots plutôt qu'individuellement, ce qui améliore les performances sur les liaisons réseau à forte latence. La fonction SMTP pipelining est toujours activée pour les connexions en entrée. Il est activé par défaut pour les connexions sortantes, mais peut être désactivé dans <u>Paramètres de serveur | Serveurs et distribution | Serveurs</u>
- Ajout de la prise en charge de SMTP CHUNKING (RFC 3030). La fonction CHUNKING permet de transférer des messages qui ne sont pas orientés vers la ligne. Il est Activer par défaut pour les connexions en entrée, mais désactivé par défaut pour les connexions en sortie. Les sauts de ligne dans les messages reçus sont convertis par défaut en sauts de ligne avec retour de chariot. Ces valeurs par défaut peuvent être modifiées en définissant [Special] SMTPChunkingInbound=Yes/No, SMTPChunkingOutbound=Yes/No, et SMTPChunkingAllowBareLF=Yes/No dans \MDaemon\AppMDaemon .ini.
- Filtre de contenu Mise à jour de la liste des <u>pièces jointes interdites</u> a par défaut.

- Filtre du contenu Ajout d'une règle d'action pour <u>ajouter une pièce jointe au</u> <u>message.</u>
- Les entrées de démarrage et d'arrêt du Serveur ActiveSync sont écrites dans le journal du système de MDaemon.
- Clustering Ajout de la prise en charge de la synchronisation des rappels à partir des nœuds secondaires.
- Écran dynamique Ajout d'une option permettant de journaliser les emplacements en utilisant des codes ISO-3166 600 au lieu de noms.
- XMLAPI Ajout de la prise en charge du paramètre AlwaysSendMeetingUpdates d'ActiveSync.
- XMLAPI Ajout du support pour la création de fichiers sémaphores.
- XMLAPI Ajout du support pour rapporter/modifier les paramètres depuis Configuration/Paramètres de serveur/Journalisation.
- MDaemon Instant Messenger Amélioration de la fonctionnalité de discussion de groupe en ajoutant la possibilité de sélectionner plusieurs compagnons de discussion pour la discussion de groupe. Une option permettant d'accepter automatiquement les demandes de salle de discussion a également été ajoutée.
- <u>Filtrer par emplacement</u> also dispose d'une nouvelle option permettant de contrôler si l'en-tête X-MDOrigin-Country est ajouté ou non aux messages. Cette option est activée par défaut.
- Il existe désormais un paramètre des Comptes permettant d'autoriser ou non les utilisateurs à se connecter à l'aide d'alias : <u>Mon compte | Paramètres des</u> <u>comptes | Alias | Paramètres</u> [366]. Ce paramètre est activé par défaut.
- MDaemon Connector a été mis à jour vers la version 7.5.0.
- Le texte par défaut du message de confirmation de livraison (dans \MDaemon\ApplicationReceipt.dat) a été modifié pour utiliser la macro \$HEADER:X-RCPT-TO\$ au lieu de \$RECIPIENT\$ afin d'éviter de divulguer l'adresse électronique réelle à laquelle un alias se résout.

Notes de mise à jour du serveur MDaemon

Pour une liste complète des ajouts, modifications et corrections inclus dans la version 21.5 de MDaemon 21.5, consultez les Notes de mise à jour.

Nouveautés dans MDaemon Private Cloud 9.0.0

• MDaemon Private Cloud 9.0 inclut MDaemon 21.0.2 avec MDaemon Connector 7.0.4.

Pour une liste de tous les changements apportés à MDaemon, voir le document MDaemon 21.0.2 Release Notes.

Pour une liste de toutes les modifications apportées à MDaemon Connector, voir le document MDaemon Connector 7.0.4.

Nouveautés de MDaemon 21.0

Principales nouveautés

Salles de discussion permanentes 400

Le serveur XMPP de MDaemon prend désormais en charge les Salles de discussion permanentes, qui n'ont pas besoin d'être recréées à chaque fois que tous les utilisateurs quittent la salle. Vous pouvez les configurer à l'adresse suivante Serveur Web | Services Web et de messagerie instantanée | XMPP.

Rapport sur les erreurs de classification des virus/spams

Dans l'interface graphique de MDaemon, dans les écrans Quarantaine, Mauvais ou Piège à spam, une option de menu contextuel avec un clic droit a été ajoutée pour signaler à MDaemon.com les messages comme étant des faux positifs ou des faux négatifs. Des options similaires ont également été ajoutées à MDaemon Remote Admin. Les messages seront analysés et transmis à des fournisseurs tiers pour qu'ils prennent des mesures correctives.

Interface graphique du client ActiveSync Migration (ASMC)

Une interface graphique a été créée pour faciliter l'exécution d'ASMC(ASMCUI.exe dans le dossier \app\ de MDaemon). Elle vous permet de mémoriser vos options et de les rappeler ultérieurement. ASMC permet de migrer le courrier, les calendriers, les tâches, les notes et les contacts à partir de serveurs ActiveSync qui prennent en charge la version 14.1 du protocole. La documentation correspondante se trouve dans le dossier Docs de MDaemon, à l'adresse suivante : \NDemon\NDemon\NDemon\NDemon.com : \MDaemon\Docs\Client ActiveSync Migration.html.

Améliorations du thème mobile du webmail

Le thème mobile pour les utilisateurs de Webmail a été considérablement étendu et amélioré. Voir RelNotes.html situé dans le dossier MDaemon's \Docs\Npour une liste complète des nombreuses fonctionnalités qui ont été ajoutées.

Améliorations du clustering 431

Un grand nombre d'améliorations ont été apportées au service de cluster de MDaemon :

- Ajout d'une option de routage de courrier multi-nœuds 430, où les files d'attente sont partagées entre les nœuds de la grappe. Dans ce cas, les files d'attente sont partagées entre les nœuds du cluster. Le fait que plusieurs machines traitent et distribuent les messages permet de répartir le travail plus équitablement et d'éviter que les messages ne restent bloqués dans les files d'attente des machines en panne.
- Les certificats SSL sont désormais répliqués des nœuds primaires aux nœuds secondaires.

- Les files d'attente sur les nœuds secondaires sont gelées pendant la réplication initiale des données, ce qui améliore la réactivité lors du démarrage.
- La réplication est interrompue dès le début de l'arrêt de MDaemon, ce qui élimine les retards liés à l'arrêt des clusters.
- Les nœuds de la grappe peuvent être ajoutés à l'aide d'une adresse IP ou d'un nom DNS.
- Les chemins d'accès au réseau partagé peuvent désormais être gérés plus facilement à partir du nouvel écran Chemins d'accès au réseau partagé.
- Des outils de journalisation et de diagnostic sont fournis dans le nouvel écran Diagnostics.

Autres nouveautés et changements

MDaemon Remote Admin (MDRA)

Des dizaines d'options ont été ajoutées à l'interface d'Administration de MDaemon Remote Admin. Pour une liste complète de ces options et des autres modifications apportées à MDRA, voir RelNotes.html situé dans le dossier MDaemon's \Docs\N.

Filtre de contenu

Possibilité de <u>Chercher des fichiers restreints à l</u> contrainers des fichiers compressés 7-Zip.

<u>Répondeurs automatiques</u>

Les autorépondeurs prennent désormais en charge l'Unicode (UTF-8), ce qui permet au texte d'être rédigé dans n'importe quelle langue.

Filtres IMAP 789

Les règles de filtrage IMAP peuvent désormais rechercher un texte particulier dans le corps du message.

Webmail

- Vous pouvez désormais joindre un événement à un Nouvel e-mail en cliquant avec le bouton droit de la souris sur l'événement et en choisissant l'option "Envoyer" dans les thèmes LookOut et WorldClient, et à partir de l'aperçu de l'événement dans le thème Mobile.
- Toutes les fonctionnalités de création de Nouveaux comptes ont été supprimées.
- Lorsque vous publiez un calendrier (partagez un lien d'accès public vers celuici), de nouvelles options vous permettent de définir sa vue calendrier par défaut (par exemple, mois/semaine/jour) et de publier un lien de calendrier libre/occupé.
- Ajout d'une option permettant d'ignorer la vérification de la persistance de l'IP pour chaque utilisateur. Dans MDRA, modifiez un compte utilisateur, allez dans

Services Web et cochez "Ignorer la vérification de la persistance IP pour les sessions Webmail".

- Dans la recherche avancée, il est désormais possible d'effectuer une recherche dans le champ CC.
- Ajout du <u>Nombre max de messages envoyés par jour</u> [784] aux quotas affichés.

Interface utilisateur

- Configuration | Gestion des terminaux mobiles a été supprimée et remplacée par la boîte de dialogue Gestion des terminaux mobiles à Configuration | ActiveSync.
- L'écran Paramètres du client ActiveSync a été supprimé. Filtrez les paramètres des clients dans les écrans Tuning, Domaines, Groupes, Comptes et Clients.
- L'écran Types ActiveSync Client a des commandes de menu pour mettre les types de clients sur liste blanche et sur liste noire.
- Des écrans ont été cherchés dans Configuration | Indexation des messages pour la configuration de la maintenance en temps réel et nocturne des index de recherche utilisés par Webmail, ActiveSync, et MDaemon Remote Admin.
- Plusieurs plugins partagent désormais un écran commun de configuration des diagnostics.
- Les systèmes d'aide par navigateur MDRA et Webmail ont été mis à jour avec un nouveau thème réactif, afin de les rendre plus utilisables sur différents types d'appareils.

API XML

- L'apparence du portail de documentation de l'API XML peut être personnalisée globalement et par domaine. Voir les "Changements et notes de développement" dans le portail d'aide (c'est-à-dire http[s]://ServerName[:MDRAPort]/MdMgmtWS) ou consulter le fichier \MDaemon\Docs\API\XML API\Help_Readme.xml sur le disque à l'aide d'Internet Explorer pour plus d'informations. Un exemple de répertoire company.mail est fourni à l'adresse \MDaemon\Docs\API\XML API\Samples\Branding.
- Ajout d'une opération Alias pour simplifier la gestion des alias, résoudre et signaler les alias.
- Ajout de l'opération FolderOperation Chercher pour rechercher des messages.
- Ajout de la prise en charge du service de cluster dans QueryServiceState et ControlServiceState.

Archivage 128

- Si un message est envoyé entre des comptes locaux, des copies d'archive "in" et "out" seront créées si les options "Archiver en entrée" et "Archiver en sortie" sont activées.
- L'option permettant d'archiver les spams, qui avait été supprimée dans la version 20.0, est de retour.
- Les messages spams distribués par le piège à spams sont archivés.

Mises à jour des composants

- MDaemon Connector a été mis à jour vers la version 7.0.0.
- Filtre anti-spam : mise à jour vers SpamAssassin 3.4.4. et suppression des paramètres obsolètes dans local.cf.
- AntiVirus : ClamAV mis à jour à la version 0.103.0, et Cyren AV engine mis à jour à la version 6.3.0.2.
- Serveur XMPP : Mise à jour de la base de données avec la version SQLite 3.33.0.

Notes de mise à jour du serveur MDaemon

Dans une liste complète des ajouts, changements et corrections inclus dans MDaemon 21.0, voir les notes de mise à jour.

Nouveautés dans MDaemon Private Cloud 8.0.0

 MDaemon Private Cloud 8.0 inclut MDaemon 20.0.2 avec MDaemon Connector 6.5.2.

Pour une liste de tous les changements apportés à MDaemon, voir le document Notes de mise à jour de MDaemon 20.0.2.

Pour une liste de tous les changements apportés à MDaemon Connector, voir le document MDaemon Connector 6.5.2.

Nouveau dans MDaemon 20.0

Service de cluster MDaemon 431

Le nouveau service de cluster de MDaemon est conçu pour partager votre configuration entre deux ou plusieurs serveurs MDaemon sur votre réseau. Cela vous permet d'utiliser du matériel ou des logiciels d'équilibrage de charge pour répartir la charge de votre messagerie sur plusieurs serveurs MDaemon, ce qui peut améliorer la vitesse et l'efficacité en réduisant la congestion et la surcharge du réseau et en maximisant les ressources de votre messagerie. Cela permet également d'assurer la redondance de vos systèmes de messagerie en cas de défaillance matérielle ou logicielle de l'un de vos serveurs. Voir : <u>Service de cluster</u> [431], pour plus d'informations sur la mise en place d'un cluster de serveurs MDaemon sur votre réseau.

Nouvelles extensions SMTP

REQUIRETLS (RFC 8689) 628

L'effort de RequireTLS dans l'IETF est enfin terminé, et le support a été implémenté. RequireTLS vous permet de marquer les messages qui **doivent être** envoyés en utilisant TLS. Si TLS n'est pas possible (ou si les paramètres de l'échange de certificats TLS sont inacceptables), les messages seront renvoyés plutôt que délivrés de manière non sécurisée. RequireTLS est activé par défaut, mais les seuls messages soumis au processus RequireTLS sont les messages spécifiquement marqués par une règle du Filtre de contenu à l'aide de la nouvelle <u>action du Filtre de</u> <u>contenu</u>, "Marquer le message pour REQUIRETLS...", ou les messages envoyés à <local-part>+requiretls@domain.tld (par exemple,

arvel+requiretls@mdaemon.com). Tous les autres messages sont traités comme si le service était désactivé. En outre, plusieurs conditions doivent être remplies pour qu'un message puisse être envoyé à l'aide de RequireTLS. Dans le cas où l'une d'entre elles échouerait, le message serait renvoyé au lieu d'être envoyé en clair. Pour plus d'informations sur ces conditions et sur la manière de configurer RequireTLS, voir : Extensions SMTP [22]. Pour une description complète de RequireTLS, voir : <u>RFC 8689 : SMTP Require TLS</u>.

SMTP MTA-STS (RFC 8461) - Sécurité stricte du transport

L'effort MTA-STS dans l'IETF est terminé, et le support pour ceci a été implémenté. SMTP MTA Strict Transport Security (MTA-STS) est un mécanisme permettant aux fournisseurs de services de messagerie (SP) de déclarer leur capacité à recevoir des connexions SMTP sécurisées par Transport Layer Security (TLS) et de spécifier si les serveurs SMTP d'envoi doivent refuser de livrer aux hôtes MX qui n'offrent pas TLS avec un certificat de serveur de confiance. La prise en charge de MTA-STS est activée par défaut. Voir : <u>SMTP Extensions</u> pour plus d'informations sur la configuration, et MTA-STS est entièrement décrit dans la <u>RFC 8461 : SMTP MTA</u> <u>Strict Transport Security (MTA-STS)</u>.

Rapports TLS SMTP (RFC 8460) 630

Les Rapports TLS permettent aux domaines utilisant MTA-STS d'être notifiés de tout échec de récupération de la politique MTA-STS ou de négociation d'un canal sécurisé à l'aide de STARTTLS. Lorsque cette option est activée, MDaemon envoie un rapport quotidien à chaque domaine compatible STS auquel il a envoyé (ou tenté d'envoyer) du courrier ce jour-là. Plusieurs options permettent de configurer les informations contenues dans les rapports. Le Rapports TLS est désactivé par défaut et discuté dans la <u>RFC 8460 : SMTP TLS ReportingSMTP</u>.

Chiffrement de MDPGP à l'échelle d'un domaine ou d'une entreprise avec une seule clé

MDPGP [677] prend désormais en charge le chiffrement des messages entre domaines à l'aide d'une clé de chiffrement unique pour tous les utilisateurs. Exemple : supposons que "Tous les domaines" et "Tous les domaines" souhaitent crypter tous les e-mails envoyés entre eux, mais ne souhaitent pas configurer et gérer des clés de cryptage individuelles pour chaque compte d'utilisateur au sein du domaine. Il est désormais possible de procéder comme suit :

Chiffrer avec une clé publique avec clé publique. Exemple : ils peuvent s'envoyer les clés par e-mail en cliquant avec le bouton droit de la souris sur une clé publique existante dans l'interface utilisateur de MDPGP et en sélectionnant "Exporter et envoyer la clé par e-mail". S'ils souhaitent créer de nouvelles clés à cette fin, ils peuvent cliquer sur le bouton "Créer des clés pour un utilisateur spécifique" et choisir l'élément "_Domain Key (domain.tld)_ <anybody@domain.tld>" qui a été mis en place à cet effet (bien que n'importe quel élément puisse fonctionner). Une fois que chaque partie a reçu la clé de l'autre, elle clique sur le bouton "Importer la clé du domaine" dans l'interface utilisateur de MDPGP et saisit le nom du domaine vers lequel tous les courriels seront

cryptés à l'aide de la clé fournie. Dans la liste déroulante, le système ne crée pas de clé pour chacun de vos domaines. Vous pouvez utiliser la clé fournie pour tous les domaines ou créer vous-même des clés spécifiques à chaque domaine si vous le souhaitez.

Si l'une des parties dispose déjà d'une clé publique qu'elle souhaite utiliser et qu'elle se trouve déjà sur le porte-clés, elle peut cliquer avec le bouton droit de la souris sur la clé dans l'interface utilisateur de MDPGP et sélectionner "Set as a Domain's Key" (Définir comme clé de domaine). Cependant, n'utilisez pas une clé pour laquelle vous possédez également la clé privée correspondante. Si vous le faites, MDPGP cryptera un message, puis constatera immédiatement que la clé de décryptage est connue et décryptera rapidement ce même message.

À ce stade, MDPGP crée un Règles du Filtre de contenu appelé "Encrypt all mail to <domain>" qui invoquera l'opération de cryptage sur chaque e-mail envoyé à ce domaine. L'utilisation du Filtre de contenu signifie que vous pouvez contrôler ce processus en activant ou en désactivant la règle du Filtre de contenu. Vous pouvez également modifier la règle pour affiner les critères que vous souhaitez utiliser avant que les messages ne soient cryptés (par Exemple, vous voulez peut-être faire la même chose mais pour deux domaines ou seulement pour certains destinataires au sein du domaine). Le filtre de contenu offre la souplesse nécessaire pour y parvenir.

Chiffrement du courrier sortant en fonction de l'adresse IP de réception

MDPGP [677] dispose d'une nouvelle case à cocher et d'un bouton de configuration permettant d'associer des adresses IP à des clés de chiffrement spécifiques. Toute session SMTP sortante délivrant un message à l'une de ces adresses IP cryptera d'abord le message à l'aide de la clé associée juste avant la transmission. Si le message est déjà crypté à l'aide d'une autre clé, aucun travail n'est effectué. Cette fonction est utile (par exemple) lorsque vous souhaitez vous assurer que tous les messages envoyés à certains partenaires clés, fournisseurs, affiliés, etc. sont toujours cryptés.

Macros pour les messages de listes de diffusion

L'écran <u>"Routage" de l'éditeur de listes de diffusion</u> we comporte de nouvelles options qui permettent d'utiliser des macros dans le corps du message des messages de la liste. Cela vous permettra (par Exemple) de personnaliser chaque message de liste. Les macros sont prises en charge depuis longtemps dans les fichiers d'en-tête et de pied de page des messages de liste, mais elles ne l'ont jamais été dans le corps du message. Dans la mesure où les macros sont liées à des membres individuels de la liste, cette option n'est compatible qu'avec les listes configurées pour "*Distribuer le courrier individuellement à chaque membre*". En outre, à des fins de sécurité, vous pouvez demander que le mot de passe de la liste soit fourni afin d'utiliser les macros dans le corps du message. Si vous choisissez de ne pas exiger de mot de passe, tout membre de la liste autorisé à poster dans la liste pourra les utiliser. Voir l'écran <u>Routage des</u> <u>listes de diffusion</u> we plus d'informations et pour la liste des macros qui peuvent être utilisées.

Amélioration du système de détection des détournements

Le système<u>de Détection détournement de compte</u> as dispose de nouvelles options qui permettent d'éviter que des comptes soient utilisés pour envoyer du spam suite au vol de leur mot de passe. Une caractéristique commune aux e-mails de spam est que les

messages sont souvent envoyés à un grand nombre de destinataires non valides, parce que le spammeur tente de les envoyer à d'anciennes adresses électroniques ou d'en deviner de nouvelles. Dans ce cas, si un compte MDaemon commence à envoyer des messages à un nombre important de destinataires non valides en peu de temps, c'est une bonne indication que le compte a été piraté et qu'il est utilisé pour envoyer du spam. Pour éviter cela, MDaemon peut désormais suivre le nombre de fois qu'un utilisateur authentifié tente d'envoyer un e-mail à un destinataire non valide. Si cela se produit trop souvent dans un laps de temps trop court, vous pouvez demander à MDaemon de figer le compte (le postmaster recevra un e-mail à ce sujet et pourra répondre pour réactiver le compte). Cela permet d'arrêter automatiquement un compte piraté avant qu'il ne fasse trop de dégâts. **Remarque :** dans le cadre de ce travail, les options de Modification de l'en-tête <u>From</u> [611] ont été déplacées vers leur propre page de <u>Filtrage de l'en-tête From</u> [611], pour faire de la place aux nouvelles options de Détection de détournement.

File Distribution Messages différée et Rappel de message amélioré

Afin d'améliorer l'efficacité du système de Rappel des messages et la prise en charge des en-têtes de Distribution différée, MDaemon dispose désormais d'une file d'attente dédiée aux messages différés. Auparavant, la File Distribution différée pouvait être encombrée de messages différés, ce qui pouvait ralentir la Distribution du courrier non différé. La nouvelle file Distribution différée permet de résoudre ce problème. Les messages dans la File Distribution Différée sont placés par le système et la date à laquelle ils doivent quitter la file d'attente est encodée dans le nom du fichier. MDaemon vérifie la file d'attente une fois par minute et lorsqu'il est temps pour les messages de quitter la file d'attente, ils sont déplacés dans la file d'attente des messages entrants et sont soumis au traitement et à la distribution normaux des messages.

De plus, MDaemon suit désormais les Message-ID du dernier e-mail envoyé par chaque utilisateur local authentifié, ce qui signifie que les utilisateurs peuvent désormais se rappeler le dernier message qu'ils ont envoyé (mais uniquement le dernier message qu'ils ont envoyé) simplement en mettant RECALL (seul) comme Objet du message envoyé au compte système mdaemon@. Il n'est pas nécessaire de trouver et de coller le Message ID du message que vous souhaitez rappeler lorsqu'il s'agit du dernier message envoyé. Pour rappeler un autre message, il faut toujours que l'ID du message soit inclus dans l'Objet ou dans le message d'origine du dossier SENT de l'utilisateur joint à la demande de rappel.

Dans la mesure où MDaemon se souvient du dernier e-mail envoyé par chaque utilisateur authentifié, il se souvient également de l'emplacement et de l'ID du message des 1000 derniers e-mails envoyés par tous les utilisateurs authentifiés. Il est donc possible de rappeler des messages directement depuis les boîtes aux lettres de l'utilisateur, même après qu'ils aient été livrés. Si les messages sont rappelés, ils disparaîtront des clients de messagerie et des téléphones des utilisateurs. **Send note :** ceci n'est bien sûr possible que pour les messages envoyés à d'autres utilisateurs locaux ; une fois que MDaemon a délivré un message à un autre serveur, il n'est plus sous le contrôle de MDaemon et ne peut donc pas être rappelé.

Pas de journalisation des échecs d'authentification

Il existe un nouveau fichier journal des échecs d'authentification qui contient une seule ligne avec des détails pour chaque tentative de journalisation SMTP, IMAP et POP qui

échoue. Les informations comprennent le protocole utilisé, l'identifiant de session afin de pouvoir effectuer des recherches dans d'autres journaux, l'adresse IP du contrevenant, la valeur de connexion brute qu'il a essayé d'utiliser (il s'agit parfois d'un alias) et le compte qui correspond à la connexion (ou "aucun" si aucun compte ne correspond).

Authentification lors du transfert/acheminement du courrier

MDaemon permet désormais d'ajouter des informations d'authentification à plusieurs options d'acheminement. Cela signifie que plusieurs fichiers du dossier \APP\ (par exemple, forward.dat, gateways.dat, MDaemon.ini et tous les fichiers .grp des listes de diffusion) peuvent contenir des données de connexion et des mots de passe obscurcis dans un état faiblement crypté. Comme toujours, vous devez donc utiliser les outils du système d'exploitation à votre disposition, ainsi que toute autre mesure de votre choix, pour sécuriser la machine et la structure des répertoires de MDaemon contre tout accès non autorisé. Des options d'authentification ont été ajoutées à : Courrier inconnu 102, Routage des listes de diffusion 308, Éditeur de passerelle » Transfert de courrier 274, Éditeur de passerelle » Mise en file d'attente 275, et Éditeur de compte » Transfert 780.

Authentification de l'hôte

L'Écran Authentification de l'hôte est un nouvel écran dans lequel vous pouvez configurer les valeurs de port, de connexion et de mot de passe pour n'importe quel hôte. Lorsque MDaemon envoie du courrier SMTP à cet hôte, les informations d'identification associées sont utilisées. Notez que ces informations d'identification sont une solution de repli et ne sont utilisées que lorsque d'autres informations d'identification plus spécifiques à une tâche ne sont pas disponibles. Exemple, si vous configurez un mot de passe AUTH à l'aide des nouvelles options <u>Editeur de compte »</u> <u>Transfert</u> [760] ou <u>Gestionnaire de comptes » Mise en file d'attente</u> [275], ces informations d'identification sont utilisées et remplacent ce qui est configuré ici. Cette fonctionnalité ne fonctionne qu'avec les noms d'hôte (pas avec les adresses IP).

Amélioration des Files personnalisées et du Routage des messages

Vous pouvez désormais spécifier un Hôte, une connexion, un mot de passe, un Port SMTP et un port pour n'importe quelle File distante. Si ces informations sont fournies, tous les messages de la file d'attente sont distribués en utilisant ces nouveaux paramètres. Toutefois, par conception, il est toujours possible que les messages individuels de la file d'attente aient leurs propres données de distribution, qui auront la priorité sur ces nouveaux paramètres. En outre, vous pouvez désormais créer autant de files d'attente distantes que vous le souhaitez, y filtrer le courrier à l'aide du Filtre de contenu en fonction des critères de votre choix, attribuer à chaque file d'attente son propre calendrier de distribution et faire en sorte qu'un routage complètement différent soit effectué en fonction de vos souhaits.

Partage de domaine amélioré

Depuis un certain temps, le Partage de domaine effectue des recherches sur les valeurs SMTP MAIL de l'expéditeur en fonction des besoins. Cependant, les messages étaient souvent refusés avec la mention "Authentification requise", alors qu'il n'existe aucun moyen de procéder à une authentification lorsque le compte de l'expéditeur réside sur un autre serveur. Ce problème a été résolu et MDaemon peut accepter du courrier sans requérir d'authentification requise de la part de comptes se trouvant sur d'autres serveurs. Cette fonction peut être désactivée à l'aide d'une nouvelle option du gestionnaire de sécurité : <u>Authentification de l'expéditeur » Authentification SMTP</u> si vous préférez ne pas effectuer de recherche de Partage de domaines sur l'expéditeur SMTP MAIL, vous pouvez désactiver complètement cette fonction à l'aide d'une option Partage de domaines.

Le Partage de domaine comporte également une nouvelle option qui permet d'activer le partage des listes de diffusion. Lorsqu'un message arrive pour une liste de diffusion, une copie est créée pour chaque hôte du Partage de domaine qui conserve également une version de cette liste (une requête est effectuée pour vérifier). Lorsque ces hôtes reçoivent leur copie, ils la transmettent à tous les membres de la liste qu'ils desservent. De cette manière, les listes de diffusion peuvent être réparties sur plusieurs serveurs sans perte de fonctionnalité. Pour que cela fonctionne, chaque hôte du Partage de domaine doit inclure les adresses IP des autres hôtes dans sa configuration des <u>IP</u> <u>autorisées</u>

Enfin, le Partage de domaine dispose d'un bouton Avancé qui ouvre un fichier dans lequel vous pouvez configurer les Noms de domaines autorisés à utiliser le Partage de domaine. Si ce fichier ne contient rien (le cas par défaut), tous les domaines peuvent utiliser le Partage de domaine. Voir les instructions en haut du fichier pour plus d'informations.

Transférer le message à d'autres utilisateurs ! TRANSFÉRER LE MESSAGE !

Préférences » Divers a une nouvelle option qui permet aux administrateurs d'empêcher le Transfert courrier à ce domaine d'envoyer des e-mails en dehors du domaine. Si un utilisateur configure le transfert de courrier de son compte pour l'envoyer à un domaine étranger, le message sera placé dans la file d'attente des messages erronés. Ce paramètre ne s'applique qu'aux messages qui sont transférés à l'aide des options de transfert de courrier du compte.

Nouveau<u>compte » Redirection »</u> ⁷⁸⁰ dispose d'un nouveau bouton *Horaire* qui permet aux comptes de configurer un horaire pour le démarrage et l'arrêt de la redirection. Cette fonction est également incluse dans l'écran <u>Modèles de comptes</u> ¹⁸⁶ correspondant. Ces paramètres permettent de configurer la date et l'heure de début de la réexpédition ainsi que la date et l'heure d'arrêt, mais la réexpédition ne se fera que les jours de la semaine que vous aurez sélectionnés.

Le champ Adresse de réexpédition dans le <u>Modèle de Nouveaux comptes</u> [446] fonctionne désormais avec les macros de comptes. Par contre, les seules macros avec des données au moment de la création d'un nouveau compte sont celles liées au nom complet de l'utilisateur, au domaine, à la boîte aux lettres et au mot de passe. Si (par exemple) vous souhaitez que chaque nouveau compte soit redirigé vers la même adresse électronique, mais dans un domaine différent, vous pouvez indiquer ceci dans le champ "Adresse de redirection" : <code>\$MAILBOX\$@example.com</code>. Les macros fonctionnent également dans les champs *Send As, Utilisateur AUTH et Mot de passe* AUTH.

Transférer un message met désormais à jour l'heure du dernier accès du compte qui le transmet. Cela signifie que les comptes qui ne font rien d'autre que transférer du courrier ne sont plus susceptibles d'être supprimés pour cause d'inactivité. **Note :** Le transfert doit effectivement avoir lieu et ne pas être entravé par d'autres options de configuration telles que des restrictions sur l'endroit où le transitaire peut envoyer du

courrier ou le fait d'être "hors horaire". Le simple fait d'avoir une adresse de transfert configurée n'indiquera pas automatiquement que le compte est actif.

Authentification SMTP améliorée

L'option<u>" Authentification de l'expéditeur » de l'authentification SMTP</u> alispose de deux nouvelles options. Tout d'abord, l'option "*Ne pas autoriser l'authentification sur le Port SMTP*" désactive complètement le support AUTH sur le Port SMTP. AUTH ne sera pas proposé dans la réponse EHLO et sera traité comme une commande inconnue s'il est fourni par le client SMTP. Cette option ajoutera à l'Écran Dynamique al' l'adresse IP de tout client qui tente de s'authentifier alors que AUTH est désactivé. La connexion sera également immédiatement interrompue. Ces paramètres sont utiles dans les configurations où tous les comptes légitimes utilisent le port Mon (ou autre) pour soumettre du courrier authentifié. Dans de telles configurations, on suppose que toute tentative d'authentification sur le Port SMTP doit provenir d'un attaquant.

Gestion des comptes améliorée

Les options de filtrage du Gestionnaire des comptes ont été étendues. Vous pouvez désormais choisir d'afficher les comptes selon qu'ils sont activés ou non, qu'ils utilisent Activer MultiPOP, qu'ils sont proches du quota (70 %), qu'ils sont proches du quota (90 %) ou qu'ils n'effectuent pas de transfert. Vous pouvez également chercher dans le champ Description du compte le texte de votre choix et sélectionner les comptes en fonction de celui-ci. En outre, le menu contextuel/clic droit comporte de nouvelles options permettant d'ajouter ou de supprimer tous les comptes sélectionnés de ou vers des listes de diffusion et des groupes. Il comporte également une option permettant de copier un compte existant afin d'en créer un nouveau. Tous les paramètres du compte existant sont copiés dans le nouveau compte, à l'exception du Nom complet, de la Boîte aux lettres, du Mot de passe et du Dossier courrier. Enfin, l'écran <u>Filtres IMAP</u> de l'Éditeur de comptes comporte un nouveau bouton appelé Publier qui permet d'ajouter une nouvelle règle au compte en cours de modification et à tous les autres comptes du domaine de ce compte. Cela peut faire gagner du temps lorsqu'une nouvelle règle est nécessaire pour tout le monde.

Activer "Ne Ne pas déranger" pour le Domaine entier

L'écran Nom hôte & IP 187 du Gestionnaire de domaines dispose d'un nouveau paramètre qui vous permet d'activer la fonction "Ne pas déranger" pour un domaine. Lorsqu'il est actif, le domaine refusera toutes les connexions de tous les utilisateurs pour tous les services, mais il acceptera toujours les messages entrants du monde extérieur. De plus, vous pouvez programmer le début et la fin de la fonction "Ne pas déranger". Exemple : Si vous configurez la période du 1er mai 2020 au 30 juin 2020 de 17h00 à 7h00, du lundi au vendredi, cela signifie qu'aucun service de messagerie ne sera disponible pour les utilisateurs de ce domaine les jours de la semaine commençant à 17h00 et reprenant à 7h01, tant que la date du jour se situe entre le 1er mai et le 30 juin 2020. Le fait de supprimer la date de début programmée désactive la programmation et a pour effet de **mettre le domaine en mode "Ne pas déranger" pour toujours.**

Archivage amélioré

Le système d'archivage des messages de MDaemon a été modifié pour être plus efficace et plus cohérent. L'archivage fonctionne maintenant comme suit : Si un message est distribué depuis le(s) Dossier(s) d'attente local(aux) vers le dossier

courrier d'un utilisateur, une copie de l'archive sera créée à ce moment-là (dans le dossier 'IN' du destinataire, s'il a été configuré). Si un message est récupéré dans la (les) file(s) distante(s) en vue d'une livraison SMTP (que la livraison réussisse ou non), une copie de l'archive sera créée à ce moment-là (dans le dossier "OUT" de l'expéditeur, s'il a été configuré à cet effet). Vous verrez des lignes comme "ARCHIVE message : pgp5001000000172.msg" dans le journal de routage ou vous pourriez voir des lignes comme "* Archivé : (archives)

\company.test\infrank@company.test\arc500100000023.msg" dans le journal de routage lorsque le courrier local et distant est traité. Dans le même temps, une file d'attente 'ToArchive' existe désormais en tant que file d'attente système (non visible dans l'interface utilisateur). Cette file d'attente est vérifiée à intervalles réguliers pour les messages qui y ont été déposés (manuellement, ou par un plugin, ou autrement). Lorsque des messages y sont trouvés, ils sont immédiatement archivés et supprimés. Si des messages non éligibles à l'archivage sont trouvés, ils sont alors simplement supprimés. Votre nom de file d'attente est \MDaemon\Queuesues\ToArchive\. L'écran/le journal de Routage affiche des détails chaque fois gu'un message est archivé avec succès. Par ailleurs, l'archivage des messages cryptés est maintenant géré de manière plus cohérente. Par défaut, des copies non chiffrées des messages chiffrés sont stockées dans l'archive. Si un message ne peut pas être décrypté, la forme cryptée sera stockée à la place. Si vous préférez que les versions cryptées soient stockées, une option vous permet de le faire. En outre, il existe maintenant une option permettant d'archiver les messages envoyés à des adresses d'envoi de dossiers publics, qui est activée par défaut. Enfin, les types de messages suivants ne sont jamais archivés : Le trafic des listes de diffusion, les spams (l'option permettant de le faire a été dépréciée et supprimée), les messages contenant des virus, les messages au niveau du système et les autorépondeurs.

Pas de journalisation plus efficace

MDaemon ne crée plus de fichiers journaux vides. Lorsque des éléments sont désactivés dans l'écran Paramètres, le fichier journal correspondant n'est pas créé au démarrage. Les Fichiers journaux qui peuvent déjà exister lorsqu'un élément est désactivé sont laissés en place (et non supprimés). Si un fichier journal est manquant lorsqu'un élément est activé, le fichier journal requis sera créé instantanément. Cette modification s'applique à tous les fichiers journaux gérés par le moteur principal de MDaemon. Les fichiers journaux pour l'Écran dynamique, la Messagerie instantanée, XMPP, WDaemon et WebMail sont gérés en dehors de MDaemon et n'ont donc pas été modifiés. Plusieurs autres changements liés à la journalisation ont été apportés : les journaux de session ATRN sont désormais corrects, les couleurs de tous les journaux sont cohérentes, de même que la manière dont ils enregistrent les Identifiants de session et les Identifiants enfant, et le serveur MultiPOP n'interrompt plus les sessions pour les comptes qui ont déjà dépassé leur quota, ce qui évite toute perte de journalisation dans ces cas-là. Enfin, le journal du routeur ne journalisait que l'analyse des messages des files d'attente INBOUND et LOCAL. Désormais, il enregistre également l'analyse de la file d'attente REMOTE lorsque des tentatives de livraison sont effectuées. Ainsi, il n'est plus nécessaire de chercher dans le journal du routeur et dans le journal SMTP(out) pour savoir quand un message a été traité.

Amélioration de l'intégration avec Active Directory

Vous pouvez désormais configurer l'intégration de MDaemon à Active Directory de manière à ce qu'un compte MDaemon soit créé lorsque vous ajoutez un utilisateur à un groupe Active Directory, et que le compte MDaemon correspondant soit désactivé

(mais pas supprimé) lorsque vous supprimez un utilisateur d'un groupe Active Directory. Pour utiliser cette fonctionnalité, vous devez utiliser un autre filtre de recherche Active Directory. Voir : <u>Active Directory » Authentification</u>, pour plus d'informations.

Dans l'écran d' <u>authentification d'</u> Active Directory, il existe désormais une option distincte "*Filtre recherche contacts*" pour les recherches de contacts. Auparavant, la recherche de contacts s'effectuait à l'aide du filtre de recherche de l'utilisateur. Il y a également un bouton de test séparé pour le filtre de recherche de contacts. Les recherches dans Active Directory ont été optimisées de sorte que lorsque les filtres de recherche sont identiques, une seule requête met à jour toutes les données. Lorsqu'ils sont différents, deux requêtes distinctes sont nécessaires.

Les champs suivants ont été ajoutés aux modèles de fichiers ActiveDS.dat, de sorte qu'ils sont inclus dans les enregistrements de contact lorsque le contrôle Active Directory crée ou met à jour les carnets d'adresses : abTitle=%personalTitle%, abMiddleName=%middleName%, abSuffix=%generationQualifier%, abBusPager=% pager%, abBusIPPhone=%ipPhone%, et abBusFax=%FacsimileTelephoneNumber%.

Les contacts des Dossiers publics sont désormais supprimés par défaut lorsque le compte associé est supprimé d'Active Directory. Toutefois, le contact n'est supprimé que s'il a été créé par la fonction d'intégration d'Active Directory. Le paramètre permettant de contrôler cela se trouve dans l'écran de <u>surveillance d'Active</u> <u>Directory</u>.

Dans le cas où le système de surveillance d'Active Directory crée ou met à jour un compte et trouve une valeur de boîte aux lettres trop longue pour tenir dans l'espace limité de MDaemon pour la valeur de boîte aux lettres, il tronque la valeur de boîte aux lettres comme auparavant, mais maintenant il crée également un Alias en utilisant la valeur de boîte aux lettres de taille normale. En outre, lorsqu'un compte ou un alias est créé, la section des notes de l'écran <u>Rôles d'administration</u> [812] du compte est mise à jour à des fins d'audit.

L'écran <u>Active Directory</u> [315] du gestionnaire de listes de diffusion vous permet désormais de saisir un attribut Active Directory pour le champ du nom complet des membres de la liste.

Les modifications apportées aux propriétés d'un compte dans Active Directory peuvent déclencher la recréation d'un compte MDaemon, même si le compte a été précédemment supprimé dans MDaemon. Pour éviter que les comptes ne soient recréés de cette manière, une nouvelle option a été ajoutée à la <u>surveillance d'Active</u> <u>Directory</u> [387]. Non (par défaut), les comptes ne seront pas recréés s'ils ont été supprimés manuellement dans MDaemon.

Amélioration du filtrage de l'en-tête FROM

Les options"Modification de l'en-tête From" ont été déplacées de l'écran Hijack Detection vers leur propre écran <u>En-tête From Screening</u> [61], et de nouvelles options ont été ajoutées. Par nom, le filtrage de l'en-tête peut désormais vérifier les noms d'affichage de l'en-tête "From :" à la recherche de tout ce qui ressemble à une adresse électronique. Si une adresse est trouvée et qu'elle ne contient pas l'adresse e-mail actuelle, l'adresse affichée peut être remplacée par l'adresse e-mail actuelle. Exemple : si vous utilisez cette fonction et que l'en-tête "From :" ressemble à ceci : "From : 'Frank Thomas <friend@friend.test>' <enemy@enemy.test>", il sera modifié en : "From : 'Frank Thomas <enemy@enemy.test>' <enemy@enemy.test>".

Vérification des mots de passe compromis

MDaemon peut désormais vérifier le mot de passe d'un utilisateur par rapport à une liste de mots de passe compromis provenant d'un service tiers. Si le mot de passe d'un utilisateur figure sur la liste, cela ne signifie pas que le compte a été piraté. Cela signifie que quelqu'un, quelque part, a utilisé les mêmes caractères que son mot de passe et que celui-ci est apparu dans une violation de données. Les mots de passe publiés peuvent être utilisés par des pirates dans des attaques par dictionnaire, mais les mots de passe uniques qui n'ont jamais été utilisés ailleurs sont plus sûrs. Voir <u>Mots de passe publiés</u> pour plus d'informations.

Dans les Paramètres de sécurité de l'écran <u>Mots de passe</u> [915], MDaemon dispose désormais d'une option permettant d'empêcher que le mot de passe d'un compte soit défini sur un mot de passe figurant dans la liste des mots de passe compromis. Il peut également vérifier le mot de passe d'un utilisateur tous les jours lorsqu'il se connecte, et si c'est le cas, envoyer une notification par e-mail à l'utilisateur et au postmaster. Les messages d'alerte peuvent être personnalisés en modifiant les fichiers de modèles de messages dans le dossier Destinataire des messages d'alerte. Dans la mesure où les instructions relatives à la manière dont un utilisateur doit modifier son mot de passe peuvent dépendre du fait que le compte utilise un mot de passe stocké dans MDaemon ou qu'il utilise l'authentification Active Directory, il existe deux fichiers modèles, CompromisedPasswordMD.dat et CompromisedPasswordAD.dat. Des macros peuvent être utilisées pour personnaliser le message, modifier l'objet, changer les destinataires, etc.

Fonctionnalités supplémentaires et améliorations

Avec plus de 250 nouvelles fonctionnalités et améliorations incluses dans MDaemon 20, il y en a beaucoup qui ne sont pas répertoriées dans cette section. Dans une liste complète des ajouts, modifications et corrections inclus dans MDaemon 20.0, consultez les notes de mise à jour.

Voir cette section :

<u>Introduction</u> 14 <u>Mise à jour vers MDaemon 25.0.0</u> ໜີ <u>L'écran principal de MDaemon</u> 70

1.4 Mise à jour vers MDaemon 25.0.0

Vous trouverez ci-dessous une liste de considérations et de remarques particulières à prendre en compte lors de la mise à jour d'une version précédente vers la version 25.0.0 de MDaemon. Dans une liste complète des ajouts, changements et corrections inclus dans MDaemon 25.0.0, consultez les Notes de mise à jour.

Version 25.0.0

• Le thème **Lite** de MDaemon Webmail a été supprimé des nouvelles installations de MDaemon, et il ne sera plus mis à jour dans les installations existantes.

- cadre-ancêtres: Non(par défaut) a été ajouté à l'en-tête Content-Security-Policy pour les serveurs Webmail et MDaemon Remote Admin par défaut. Si les utilisateurs accèdent à Webmail ou à MDaemon Remote Admin via un cadre sur un site intranet, cela peut poser des problèmes. Vous pouvez modifier les Fichiers d'en-tête en éditant les fichiers INI correspondants, ou vous pouvez les modifier à l'intérieur de MDaemon Remote Admin : <u>En-tête | Paramètres de</u> <u>MDaemon Webmail | Serveur</u>[339] Web et <u>En-tête | Paramètres de MDaemon</u> <u>Remote Admin | Settings</u>[377], sous En-têtes de réponse HTTP.
- ClamAV 1.4 n'est pas compatible avec Windows Server 2008 R2 ou Windows 7. ClamAV n'est donc pas installé sur ces versions de Windows. Si vous avez un ClamAV plus ancien installé par une version précédente de MDaemon, vous pouvez continuer à l'utiliser avec MDaemon 25.

Version 24.5.0

 Il n'y a pas de considérations particulières propres à MDaemon 24.5.0 lors d'une mise à jour à partir de la version précédente. Si vous effectuez une mise à jour à partir d'une version antérieure, veuillez consulter les notes spéciales cidessous pour toutes les versions publiées depuis cette version.

Version 24.0.0

 L'API XML refuse désormais par défaut l'accès aux IP qui ne sont pas spécifiquement autorisées. Ceci peut être modifié dans l'interface de l'application : <u>Configuration | Service API XML | Restrictions d'adresses</u> [517].

Version 23.5.0

 Il n'y a pas de considérations particulières propres à la version 23.5.0 de MDaemon lors d'une mise à jour à partir de la version précédente. Si vous effectuez une mise à jour à partir d'une version antérieure, veuillez consulter les notes spéciales ci-dessous pour toutes les versions distribuées depuis cette version.

Version 23.0.2

 La Protection instantanée a été rétablie. Veuillez vérifier vos <u>paramètres de</u> <u>Protection instantanée</u>, car ils peuvent avoir été réinitialisés à leurs valeurs par défaut.

Version 23.0.1

 Cyren Anti-Virus a été remplacé par IKARUS Anti-Virus. Cyren a récemment annoncé son intention de <u>cesser ses activités</u> sans préavis. Il nous a donc fallu trouver un nouveau partenaire pour l'antivirus. Après une évaluation approfondie, IKARUS Anti-Virus s'est distingué par son excellent taux de détection et sa rapidité. Il offre une protection fiable contre les programmes malveillants et potentiellement hostiles, et combine les méthodes traditionnelles de défense antivirus avec les dernières technologies proactives. IKARUS Anti-Virus met automatiquement à jour ses définitions toutes les 10 minutes. L'analyse avec IKARUS est désactivée si votre licence AntiVirus a expiré.

- La Protection instantanée de Cyren a été supprimée. Cyren a récemment annoncé son intention de cesser ses activités sans préavis. Nous recherchons activement et considérons des technologies anti-spam viables comme des ajouts appropriés aux mécanismes anti-spam existants trouvés dans nos produits logiciels.
- La prise en charge des drapeaux de mots-clés IMAP peut désormais être activée ou désactivée via le paramètre [Special] IMAPKeywordFlags=Yes/No dans \MDaemon\App\MDaemon.ini. Les indicateurs de mots-clés IMAP sont désactivés par défaut lors de la mise à jour de MDaemon à partir d'une version antérieure à 23, afin d'éviter la perte potentielle des balises de messages dans les clients de messagerie Thunderbird. Lorsque Thunderbird se connecte à un serveur IMAP qui prend en charge les indicateurs de mots-clés, il remplace ses indicateurs de messages locaux par les indicateurs lus depuis le serveur, qui sont initialement vides. Les indicateurs de mots-clés IMAP sont activés par défaut pour les nouvelles installations et lors des mises à jour à partir de la version 23.0.0.

Version 22.0.0

- MDaemon 32 bits n'est plus utilisé. MDaemon 22.0 et les versions plus récentes ne seront disponibles qu'en 64 bits. Si vous utilisez actuellement une version 32 bits sur un système d'exploitation 64 bits pris en charge, vous pouvez simplement installer la version 64 bits par-dessus l'installation existante.
- La Longueur minimale des passe forts [915] doit maintenant être d'au moins 8 caractères. Si la longueur minimale était inférieure à 8 caractères avant la mise à jour vers MDaemon 22, elle passera à 8. La longueur minimale par défaut des mots de passe sécurisés pour les nouvelles installations est désormais de 10 caractères.
- MDaemon n'utilise plus les termes "liste blanche" et "liste noire". Dans la plupart des cas, il s'agit désormais de "liste d'autorisation" et de "liste de blocage". Les fonctionnalités qui disposaient d'une " liste blanche " pour exclure les IP, les adresses, etc., disposent désormais d'une " liste d'exclusion ". Les dossiers contacts du filtre anti-spam par utilisateur sont désormais nommés "Expéditeurs autorisés" et "Expéditeurs bloqués". Les dossiers de tous les comptes seront renommés au premier démarrage de MDaemon 22.

Version 21.5.0

- L'en-tête X-MDOrigin-Country, que le <u>Filtrage des emplacements</u> ajouter aux messages, contient désormais les codes de pays et de continents ISO 3166 à deux lettres au lieu des noms complets de pays et de continents. Veillez à mettre à jour tous les filtres dont vous disposez et qui recherchent des valeurs particulières dans cet en-tête.
- Le changement de nom du thème Webmail "Mobile" en "Pro" peut avoir un effet secondaire pour les utilisateurs qui utilisent le thème Mobile et dont l'option Se souvenir de moi est activée. Ces utilisateurs peuvent constater qu'ils ne peuvent pas ouvrir les pièces jointes. Pour résoudre ce problème, ils doivent simplement se déconnecter de leur compte Webmail et se reconnecter.

Version 21.0.2

 Les paramètres dans Configuration "Préférences " Divers pour copier toutes les notifications du postmaster générées par le système vers les administrateurs globaux et les administrateurs de domaine s'appliquent maintenant à plus de notifications, telles que Figer et Désactiver le compte, Pas d'utilisateur, Erreur de disque, Espace disque réduit, et Expiration de Beta et d'AV. Si vous estimez qu'il n'est pas opportun que vos administrateurs reçoivent ces notifications, vous devez désactiver ces paramètres.

Version 20.0.3

• MDaemon commente la ligne "AlertExceedsMax yes" dans le fichierclamd.conf de ClamAV, car elle provoque trop d'échecs d'analyse AV de type "Heuristics.Limits.Exceeded".

Version 20.0.1

- Les paramètres d'accès aux ressources réseau dans Configuration | Préférences | Service Windows configurent maintenant le service MDaemon (et les services Administration à distance et Serveur XMPP) pour qu'il s'exécute en tant que compte spécifié, au lieu de s'exécuter en tant que SYSTÈME et d'exécuter ensuite des processus et des threads spécifiques en tant que ce compte. Le programme d'installation mettra à jour les services pour qu'ils s'exécutent sous le compte spécifié lors de la mise à jour vers cette version.
- Dans la mesure où de nombreux paramètres de clamd.conf ont été modifiés et rendus obsolètes, le programme d'installation écrasera désormais les fichiers clamd.conf existants. Si vous avez personnalisé votre clamd.conf, il se peut que vous deviez revoir et apporter des modifications à clamd.conf après l'installation.

Version 20.0.0

- Veuillez lire attentivement la section des notes de mise à jour complète intitulée tâche [8930] car elle implique des changements dans le système d'intégration Active Directory et il se peut que des choses qui ne fonctionnaient pas dans le passé commencent à fonctionner. Veuillez prendre connaissance de tous les changements effectués dans ce domaine et lire attentivement cette section des notes de mise à jour.
- MDaemon 20.0 nécessite Windows 7, Server 2008 R2 ou une version plus récente.
- Préférences | Divers 535 comporte deux nouvelles cases à cocher qui permettent de contrôler si les e-mails de notification générés par le système et envoyés périodiquement à l'alias Postmaster doivent également être envoyés aux administrateurs des niveaux Global et Domaine. Non (par défaut), ces options sont toutes deux activées. Les administrateurs de domaine ne reçoivent que les courriels concernant leur domaine et les notes de mise à jour. Les administrateurs globaux reçoivent tout, y compris le rapport de synthèse de la file d'attente, le rapport de statistiques, les notes de mise à jour, le message "No Such User" (pour tous les domaines), les notifications d'erreurs de disque,

les notifications de gel et de désactivation des comptes pour tous les domaines (qu'ils peuvent, comme les administrateurs de domaine, débloquer et réactiver), les avertissements concernant les licences et les versions de test bêta sur le point d'expirer, et peut-être d'autres encore. Si vous estimez qu'il n'est pas opportun que vos administrateurs reçoivent ces notifications, vous devez désactiver ces paramètres.

- La façon dont les autorépondeurs sont stockés a changé. Le Texte de l'autorépondeur d'un compte est désormais stocké sous forme de fichiers OOF.MRK dans le Dossier DATA du compte, qui est un nouveau sous-dossier dans le Dossier courrier racine du compte. Les fichiers de script du répondeur automatique ne sont plus conservés dans le dossier APP et ne sont pas partagés entre les comptes. Lorsque Mon compte démarre pour la première fois, il migre tous les fichiers et paramètres de l'autorépondeur vers les emplacements appropriés pour chaque compte. Le fichier AUTORESP. DAT est obsolète et sera supprimé en même temps que tous les fichiers.RSP spécifiques à un compte (OutOfOffice.RSP et les fichiers non spécifiques à un compte seront conservés à titre de référence et d'exemple). Si vous souhaitez affecter rapidement une seule configuration d'autorépondeur à plusieurs comptes, vous pouvez utiliser le nouveau bouton Publier qui se trouve dans Paramètres des comptes | Autorépondeur mi. Ce bouton copiera le Texte de l'autorépondeur existant et tous les paramètres du compte actuel vers d'autres comptes que vous sélectionnerez. Il existe également un boutonModifier fichier autorépondeur mil qui vous permet de modifier le script autorépondeur par défaut (OutOfOffice.rsp). Ce script par défaut est copié dans le fichier OOF.MRK d'un compte si le fichier OOF.MRK est manguant ou vide.
- Le mode de stockage des fichiers de signature des comptes a été modifié. Les fichiers de signature sont désormais stockés sous le nom de SIGNATURE.MRK dans le dossier DATA du compte, qui est un nouveau sous-dossier du dossier courrier racine du compte. Lors du premier démarrage de MDaemon, tous les fichiers de signatures existants sont déplacés vers les emplacements appropriés pour chaque compte. Le dossier racine Signatures de MDaemon ne contiendra plus les fichiers de signatures spécifiques à chaque compte, mais il reste en place car il peut encore contenir des éléments nécessaires à MDaemon Remote Admin et au Filtre de contenu. Le dossier Signatures d'origine a été sauvegardé dans \NBackup\20.0.0\Nsignatures\Navant la migration. Enfin, le fichier ADMINNOTES.MRK de chaque compte a été déplacé du dossier courrier racine du compte vers le nouveau sous-dossier DATA.
- Filtre anti-spam | Liste blanche (automatique) [739] a vu sa valeur par défaut modifiée en désactivée pour l'option "...only whitelist addresses that authentifient avec DKIM". Activer cette liste s'avère un peu restrictif pour beaucoup et empêche la Liste blanche du carnet d'adresses de fonctionner pour le courrier MultiPOP et DomainPOP. Si cela ne vous convient pas, réactivez le paramètre.
- L'option <u>Préférences | Interface utilisateur</u> pour "Centrer toutes les boîtes de dialogue de l'interface utilisateur" a été réinitialisée à un Non (par défaut) "activé" pour tout le monde. Si vous préférez, vous pouvez la désactiver. Cela permet d'éviter que des écrans soient créés partiellement hors cadre, mais cela peut occasionnellement rendre plus difficile la sélection de plusieurs écrans qui se chevauchent.

- <u>Gestionnaire de sécurité | Filtrage | Filtrage de la localisation (00)</u>] Le Non (par défaut) de cette fonction a été changé de désactivé à activé. Lorsque le filtrage des connexions est activé, le pays/région de connexion sera toujours journalisé (s'il est connu), même si le pays/région en question n'est pas activement bloqué. Ainsi, si vous ne souhaitez pas bloquer de pays, vous pouvez toujours activer le filtrage de localisation (sans sélectionner de pays à bloquer) afin que le pays/la région puisse être affiché(e) et journalisé(e). Non (par défaut) par défaut, il est conseillé de vérifier la configuration du filtrage de l'emplacement. MDaemon insère l'en-tête "x-MDOrigin-Country" qui indique le pays et la région à des fins de filtrage de contenu ou autres.
- La limite de taille fixe de 2 Mo codée en dur pour les analyses du Filtre antispam a été supprimée. Il n'y a désormais plus de limite théorique à la taille d'un message qui peut être analysé. Il est toujours possible, cependant, de configurer votre propre limite au cas où cela poserait un problème, mais l'utilisation de "0" dans l'option signifie désormais qu'il n'y a pas de limite. Vous devriez consulter l' écran<u>" Paramètres du Filtre anti-spam</u> [749] pour vous assurer que cette option est réglée sur la valeur souhaitée.
- Dans les écrans de files d'attente de l'interface principale, les colonnes "Domaine de l'expéditeur" et "Domaine du destinataire" ont été ajoutées. En conséquence, une réinitialisation unique des largeurs de colonnes sauvegardées a dû être effectuée. Une fois que vous aurez réglé les largeurs de colonnes à votre convenance, elles seront mémorisées.
- Non par défaut, l'Écran d'hôte est maintenant appliqué aux connexions MSA. Cette option se trouve à l'endroit suivant : Security Manager | Screening | Host Screen : <u>Gestionnaire de sécurité | Filtrer | Écran d'hôte</u> [60].
- Par défaut, les serveurs MDaemon IMAP, WebMail et ActiveSync ne donnent plus accès aux dossiers partagés des comptes désactivés. Vous pouvez modifier ce paramètre dans <u>Paramètres du serveur | Dossiers publics & partagés.</u>

Voir aussi :

Introduction 14 Nouveautés dans MDaemon 25.0 17 Affichage principal de MDaemon 70

1.5 Obtenir de l'aide

Options d'assistance

Le support est un élément essentiel de l'expérience client de MDaemon Technologies. Nous voulons que vous tiriez le meilleur parti de nos produits longtemps après l'achat et l'installation initiaux et nous nous engageons à veiller à ce que tous les problèmes soient résolus à votre satisfaction. Pour obtenir les dernières informations sur le service clientèle, les options d'assistance technique, les ressources d'auto-assistance, les informations sur les produits, etc. MDaemon Technologies à l'adresse suivante www.mdaemon.com/support/

Test bêta de MDaemon

MDaemon Technologies maintient des équipes de bêta-test actives pour ses produits. Si vous souhaitez obtenir des informations sur la façon de rejoindre l'équipe bêta de MDaemon, envoyez un message à <u>MDaemonBeta@mdaemon.com.</u>

> L'équipe bêta est destinée à ceux qui souhaitent obtenir les mises à jour de MDaemon avant leur sortie générale et participer à leur test ; il ne s'agit pas d'une alternative de support technique. Le support technique de MDaemon ne sera assuré que par les méthodes décrites à l'adresse suivante : www.mdaemon.com/support/.

Nous contacter

Heures d'ouverture

M-F 8:30 am - 5:30 pm Central Standard Time Exclut les week-ends et les jours fériés américains Customer Service or Sales U.S.Toll Free : 866-601-ALTN (2586) International : 817-601-3222 sales@helpdesk.mdaemon.com

Support technique www.mdaemon.com/support/

Formation training@mdaemon.com

Développement commercial/Alliances alliance@mdaemon.com

Médias/Analystes

press@mdaemon.com

Demandes de renseignements des distributeurs/revendeurs

Veuillez vous référer à la page des <u>partenaires de distribution</u> pour de plus amples informations.

Siège social

MDaemon Technologies

4550 State Highway 360, Suite 100 Grapevine, Texas 76051 Numéro vert aux États-Unis : 866-601-ALTN (2586) International : 817-601-3222 Fax : 817-601-3223

Marques déposées

Copyright @ 1996-2025 MDaemon Technologies. Alt-NR, MDaemonR, and RelayFaxR are trademarks of MDaemon Technologies.

Apple is a trademark of Apple Inc. Microsoft and Outlook are trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.



2 Interface principale de MDaemon

🧐 Alt-N MDaemon PRO - company.test - 10.10.50.235 [fe80::ec17:20:fd19:4833%11] (Configuration Session)
<u>E</u> ile <u>E</u> dit <u>S</u> etup Sec <u>u</u> rity <u>A</u> ccounts <u>C</u> atalogs <u>Q</u> ueues <u>W</u> indows <u>H</u> elp
] 🐼 🍞 🔍 🕹 🛃 🔈 🤽 😂 😂 😂 💭 🔛
Image: Statistics Image: Statistatistics Image: Statistics <
Stats System (Statistics (Routing) Security (Mail (WorldClient (Queues (Plug-ins (Active Directory (Sessions)

L'interface graphique principale de MDaemon vous donne des informations importantes sur les ressources, les statistiques, les sessions actives et le courrier en attente de traitement. Elle contient également des options permettant d'activer/désactiver facilement les différents serveurs de MDaemon. Les onglets de l'interface graphique vous tiennent au courant des performances du serveur et de ses connexions entrantes et sortantes.

Statistiques

Le volet Statistiques est le volet gauche par défaut de l'interface principale de MDaemon. Il contient quatre sections : Statistiques, Comptes, Files d'attente et Serveurs.

La section*Statistiques* contient des statistiques sur le nombre de messages envoyés et reçus par MDaemon, ainsi que des statistiques sur les sessions POP et IMAP, les Spam acceptés et refusés, les virus, etc. Ces statistiques sont comptabilisées à partir de l'Heure de début de MDaemon, et il existe un menu de raccourcis par clic droit qui peut être utilisé pour effacer les compteurs.



Lorsque vous cliquez sur l'option "Réinitialiser les compteurs du nœud racine", tous les compteurs sont réinitialisés, et pas seulement celui sur lequel vous avez cliqué avec le bouton droit de la souris. De plus, il existe une option dans Serveur"

70

Préférences | GUI qui peut être utilisée pour "*Préserver les compteurs de courrier du nœud racine à travers les redémarrages*", sinon ils seront réinitialisés chaque fois que le serveur sera redémarré.

La section*Comptes* contient des entrées pour MDaemon, MDaemon Connector et ActiveSync. Chaque entrée indique le nombre de comptes utilisés et le nombre de comptes restants, en fonction de la licence de votre produit.

La section*Files* contient une entrée pour chaque file d'attente de messages et le nombre de messages (le cas échéant) que chaque file contient. Vous pouvez cliquer avec le bouton droit de la souris sur chacune des entrées de file d'attente pour ouvrir un menu contextuel contenant une ou plusieurs des options suivantes, en fonction de la file d'attente sélectionnée :

- Afficher la file d'attente cette option fait basculer le volet principal vers l'onglet Files sélectionnées et affiche la file d'attente sélectionnée. Une liste de tous les messages que la file contient s'affiche, et vous pouvez cliquer avec le bouton droit de la souris sur n'importe quel message pour ouvrir un menu contextuel contenant de nombreuses options similaires à celles disponibles dans le Gestionnaire des files d'attente et des statistiques, telles que Copier, Déplacer, Modifier, etc.
- **Gestion des files d'attente et des** statistiques ouvre le Gestionnaire des files d'attente et des statistiques à la page des files d'attente avec la file sélectionnée affichée.
- Dans cette option remet en file d'attente tous les messages contenus dans la file d'attente et tente de les traiter normalement en vue de leur distribution. Si vous tentez de traiter les messages contenus dans la file d'attente Garder, file d'attente Mauvais, ou similaire, les messages peuvent rencontrer les mêmes erreurs que celles qui les ont placés dans la file d'attente et les renvoyer dans la même file d'attente.
- **Figer/dégeler file d'attente** met temporairement en pause le traitement de la file sélectionnée, ou continue le traitement s'il est actuellement en pause.
- **Distribuer**: distribue les messages de la file d'attente. MDaemon tentera de délivrer les messages quelles que soient les erreurs rencontrées - ils ne seront pas renvoyés dans la file d'attente même s'ils rencontrent les mêmes erreurs que celles qui les ont déplacés à l'origine.
- **Remettre en file d**'attente Cette option est disponible pour la file d'attente et a le même effet que l'option *Traiter maintenant* ci-dessus.
- Activer/désactiver la file d' attente active ou désactive la file d'attente. Lorsqu'elle est désactivée, les messages ne sont pas déplacés vers la file d'attente, quelles que soient les erreurs rencontrées.

La section*Serveurs* contient une entrée pour chaque serveur de MDaemon, et chaque entrée indique l'état actuel du serveur : "Actif" ou "Inactif". Sous l'entrée de chaque serveur se trouve une entrée pour chaque domaine (le cas échéant), ainsi que le port et l'adresse IP actuellement utilisés par ce serveur ou ce domaine. Le menu contextuel

71

permet de faire basculer chaque serveur entre l'état actif et l'état inactif. Lorsqu'un serveur est inactif, son icône devient rouge.

Journal des événements et journalisation

Le volet droit par défaut de l'interface principale contient un groupe d'onglets qui affichent les actions actuelles de MDaemon et l'état de ses différents serveurs et ressources, et ils sont continuellement mis à jour pour refléter les conditions actuelles du serveur. Chaque session active et chaque action sur le serveur sont consignées dans l'onglet approprié une fois que l'action est terminée. Les informations affichées dans ces onglets sont reprises dans les fichiers journaux conservés dans le répertoire Directory de journalisation, si vous avez choisi d'enregistrer ce type d'activité.

Le volet principal de l'interface graphique de MDaemon contient les onglets suivants :

- **Système** au démarrage du programme, l'onglet Système affiche un Pas de journalisation du processus d'initialisation, qui peut vous alerter sur d'éventuels problèmes liés à la configuration ou à l'état de MDaemon. Il affiche également les activités telles que l'activation/désactivation des différents serveurs de MDaemon.
- **Statistiques** cet onglet affiche un rapport de statistiques du serveur correspondant aux informations contenues dans les différents compteurs du nœud racine dans l'onglet Statistiques du volet Statistiques et outils. Si vous souhaitez modifier la police ou la taille de la police utilisée pour ce rapport, vous pouvez le faire en modifiant les clés suivantes dans le fichier MDaemon.ini :

```
[ReportWindow]
DefFontFace=Courier New
DefFontHeigh=15
DefFontWidth=7
```

En outre, chaque nuit à minuit, le Postmaster et toutes les adresses figurant sur l 'écran <u>Recipients</u> 714 du Filtrage de contenu recevront une copie de ce rapport par e-mail. Il s'agit du même rapport que celui qui est généré lorsque vous utilisez la commande "Status" listée dans <u>General Email Controls</u> 1. Si vous ne souhaitez pas que ce rapport soit envoyé, désactivez l'option "Envoyer*le résumé des statistiques au postmaster à minuit*" (*Envoyer le rapport de statistiques au postmaster à minuit*) située dans l' écran <u>Divers</u> 500 Préférences.

- **Routage** affiche les informations de routage (À, De, Message ID, etc.) pour chaque message analysé par MDaemon.
- **Sécurité** cliquez sur cet onglet et plusieurs autres onglets relatifs à la sécurité apparaîtront au-dessus.
 - **Filtre de contenu** Les opérations du<u>Filtre de contenu de</u> **DE** MDaemon sont listées dans cet onglet. Lorsqu'un message correspond aux critères d'une des Règles du Filtre des messages, les informations relatives à ce message et les actions entreprises sont journalisées ici.
 - AntiVirus Les opérations de l'<u>AntiVirus</u> sont répertoriées dans cet onglet. Lorsqu'un message est analysé à la recherche de virus, les informations pertinentes relatives à ce message et l'action entreprise sont consignées ici.
- **Anti-spam** affiche toutes les activités de<u>filtrage</u> [725] et de prévention du<u>spam</u> <u>de</u> [725] MDaemon .
- MDSpamD affiche toutes les activités du <u>Daemon anti-spam</u> (MDSpamD) <u>de MDaemon</u> (736).
- **SPF** affiche toutes les activités de<u>Sender Policy Framework.</u>
- **DKIM** liste toutes les activités de DomainKeys Identified Mail. 563
- **DMARC** liste toutes les activités <u>DMARC</u> 573.
- **VBR** cet onglet affiche les activités de<u>Certification VBR</u>
- **MDPGP** cet onglet affiche les activités<u>MDPGP</u> [677].
- Screening cet onglet affiche les activités Tarpitting [941] et Écran dynamique. [603]
- Auth Failures (Échecs d'authentification) Cet onglet (et le fichier journal correspondant) contient une entrée détaillée pour chaque tentative d'authentification SMTP, IMAP et POP qui échoue. Les informations comprennent le protocole utilisé, l'ID de la session (afin de pouvoir effectuer des recherches dans d'autres journaux), l'IP de l'auteur de l'infraction, la valeur brute de la connexion qu'il a essayé d'utiliser (il s'agit parfois d'un alias) et l'Identifiantiant de compte qui correspond à la connexion (ou 'aucun' si aucun compte ne correspond).Vous pouvez faire un clic droit sur une ligne dans cet onglet pour ajouter l'Adresse des Comptes Bloqués.
- **MTA-STS** Affiche toute l'activité liée au protocole SMTP MTA Strict Transport Security (MTA-STS).
- **Courrier** cliquez sur cet onglet et plusieurs autres onglets relatifs au courrier apparaîtront au-dessus.
 - SMTP (in) Cet onglet affiche toute l'activité des sessions entrantes utilisant le protocole SMTP.
 - SMTP (out) toutes les sessions sortantes utilisant le protocole SMTP sont affichées dans cet onglet.
 - **IMAP** -les sessions de messagerie utilisant le protocole IMAP sont consignées dans cet onglet.
 - **POP3** -lorsque les Actifs collectent du courrier électronique à partir de MDaemon en utilisant le protocole POP3, cette activité est journalisée ici.
 - Collecte **MultiPOP** -cet onglet affiche les activités de Collecte de courrier MultiPOP de MDaemon.
 - **DomainPOP** -cet onglet affiche l'activité DomainPOP de MDaemon.
 - LDAP affiche l'activité du serveur LDAP.
 - Minger affiche l'activité du serveur Minger 923.
 - **RAW** L'activité des messages RAW ou générés par le système est consignée dans cet onglet.
 - **MDaemon Connector** affiche toutes les activités de<u>MDaemon Connector</u> 4091.

Webmail

Webmail - affiche les activités de messagerie de MDaemon Webmail.

ActiveSync - cet onglet affiche l'activité d'ActiveSync.

- **Messages et files d'attente** cet onglet donne accès à une autre rangée d'onglets au-dessus de lui avec un onglet correspondant à chaque file d'attente de messages, tels que : LOCAL & REMOTE, Mise en attente, Quarantaine, Spam bayésien, et ainsi de suite.
- **Plug-ins** affiche toutes les activités liées aux plug-ins de MDaemon.

Active Directory - affiche toutes les activités liées à Active Directory.

Sessions - cliquez sur cet onglet et plusieurs autres onglets apparaîtront audessus. Ces onglets affichent une entrée pour chaque connexion active à MDaemon. Dans le cas d'une connexion SMTP en entrée ou en sortie, POP en entrée ou en sortie, IMAP, Webmail ou ActiveSync, des informations sur chaque session active sont affichées ici. Double-cliquez sur une session active pour afficher une fenêtre de session sont les 1, qui affiche la transcription de la session SMTP au fur et à mesure de son déroulement.



Menu contextuel de la fenêtre de suivi des événements

Si vous cliquez avec le bouton droit de la souris sur l'un des onglets de la fenêtre de suivi des événements, un menu contextuel s'ouvre. Ce menu propose diverses options permettant de sélectionner, copier, supprimer ou enregistrer le contenu d'un onglet donné. L'option Imprimer/Copierdu menu ouvre le texte sélectionné dans le Blocnotes, qui peut alors être utilisé pour imprimer les données ou les enregistrer dans un fichier. L' option Supprimer permet d'effacer le texte sélectionné. L' optionChercher ouvre une fenêtre dans laquelle vous pouvez spécifier un mot ou une phrase à rechercher dans les fichiers journaux. MDaemon cherchera la chaîne de texte dans tous les fichiers journaux, puis toutes les transcriptions de session contenant cette chaîne seront regroupées dans un seul fichier et ouvertes dans le Bloc-notes pour que vous puissiez les consulter. Une utilisation pratique de cette fonctionnalité consisterait à rechercher un Message ID particulier, ce qui permettrait d'obtenir une compilation de tous les journaux de toutes les transcriptions de session contenant ce Message ID. Certains onglets proposent également des options permettant de signaler à MDaemon.com les messages qui ont été classés par erreur comme étant du spam ou contenant un virus, ou qui auraient dû être classés comme tels (c'est-à-dire les faux positifs et les faux négatifs). Les messages signalés seront analysés et transmis à des fournisseurs tiers pour qu'ils prennent des mesures correctives.



La disposition de l'interface graphique de MDaemon n'est pas limitée aux positions par défaut décrites ci-dessus. Vous pouvez changer leur position en cliquant sur Windows | Changer de panneau dans la barre de menu.

Pas de journalisation composite

Dans le menu Windows de la barre de menus de MDaemon se trouve l'option Journalisation composite. En cliquant sur cette option, vous ajoutez une fenêtre à l'interface graphique qui combine les informations affichées dans un ou plusieurs onglets du panneau principal. Dans l'écranJournal composite Journalisation, les options permettent de désigner les informations qui apparaîtront dans cette fenêtre.

Compteurs de performances

MDaemon prend en charge les compteurs de performance Windows, qui permettent aux logiciels de surveillance de suivre l'état de MDaemon en temps réel. Il existe des compteurs pour le nombre de sessions actives pour les différents protocoles, le nombre de messages dans les files d'attente, les états actif/inactif du serveur, le temps de fonctionnement de MDaemon et les statistiques sur les sessions et les messages.

Pour utiliser les compteurs de performance, démarrez System Monitor en allant dans Panneau de configuration | Outils d'administration | Performance, ou en exécutant "perfmon". Cliquez sur Ajouter des compteurs, sélectionnez l'objet de performance MDaemon, puis sélectionnez et ajoutez les compteurs que vous souhaitez voir. Pour voir les compteurs de performance de MDaemon s'exécutant sur une autre machine, vous devez avoir activé le service "Registre à distance" et avoir accès à travers les pare-feux.

Voir :

<u>Fenêtre de session</u> ଛୀ <u>Icône de la barre d'état système</u> ଛୀ <u>Menu contextuel</u> ୡୀ <u>Pas de journalisation composite</u> 170

2..1 Service d'autodécouverte

MDaemon prend en charge le service AutoDiscovery, qui permet aux utilisateurs de configurer leurs clients de messagerie pour qu'ils se connectent à leurs comptes en fournissant uniquement leur adresse e-mail et leur mot de passe, sans avoir à connaître d'autres détails de configuration tels que les noms des serveurs de messagerie et les ports. La plupart des clients prennent en charge ce service, bien que certains ne le prennent en charge que de manière limitée. Le service AutoDiscovery est activé par défaut, mais vous pouvez l'activer ou le désactiver manuellement à partir de l'interface principale de MDaemon. Dans le volet Stats, sous **Serveurs**, cliquez avec le bouton droit de la souris sur **Service de découverte automatique**, puis cliquez sur **Activer/Désactiver le service de découverte automatique**.

75

Les clients dans lesquels le service AutoDiscovery est entièrement pris en charge utiliseront le nom de domaine figurant dans les adresses électroniques de l'utilisateur pour rechercher le type de service _autodiscover._tcp dans les enregistrements du service DNS (SRV) et se connecteront à ce serveur pour obtenir des informations supplémentaires. Par conséquent, pour prendre en charge AutoDiscovery, vous devez créer des enregistrements DNS SRV pour AutoDiscovery et les services qu'il prend en charge. L'implémentation du service AutoDiscovery par MDaemon prend en charge les services suivants <u>ActiveSync</u> [41] (airsync), IMAP, POP, SMTP, DAV et XMPP.

_autodiscovertcp	SRV C) ()	443 adsc.example.com.
_airsynctcp	SRV (0 (443 eas.example.com.
_imaptcp	SRV (0 (0 imap4.example.com.
_poptcp	SRV (0 (0 pop3.example.com.
_smtptcp	SRV (0 (0 msa.example.com.
_caldavtcp	SRV (0 (0 dav.example.com.
_carddavtcp	SRV (0 (0 dav.example.com.
xmpp-client. tcp	SRV () ()	0 chat.example.com.

Remarque : certains clients consultent toujours en premier lieu autodiscover. {domaine}.{tld}. Par conséquent, le fait que l'enregistrement du service de découverte automatique pointe vers un serveur nommé autodiscover.{domaine}. {tld} peut s'avérer utile à cet égard. Dans l'exemple suivant, le serveur de découverte automatique est adsc.example.com.

Exemple :

Nom de domaine : exemple.com

L'administrateur doit mettre en place un enregistrement de service _tcp pour le type de service _autodiscover

autodiscover. tcp SRV 0 0 443 adsc.example.com.

Dans ce cas, il pointe vers adsc.example.com, qui a un enregistrement A pointant vers 192.168.0.101

Le client se connectera alors à ce serveur et demandera des informations sur le point de connexion pour certains protocoles spécifiques : ActiveSync, IMAP, XMPP, SMTP, DAV, etc...

Le service AutoDiscovery recherche alors les protocoles demandés et renvoie les noms de serveur appropriés pour ces protocoles. Par exemple, pour ActiveSync, il renvoie le nom de serveur défini dans l'enregistrement de service _tcp _airsync, qui, dans cet exemple, serait eas.{domaine}.{tld}.

Si Outlook appelait AutoDiscovery, il renverrait les Serveurs IMAP et SMTP, représentés pour les enregistrements de service _tcp de _imap et _msa, ce qui donnerait les serveurs imap4.example.com et msa.example.com.

Voici un exemple de configuration correcte des services de découverte automatique. Votre nom doit être unique pour chaque protocole, mais il peut facilement être adapté à un nom commun, tel que mail.example.com.

;

; Fichier de base de données example.com.dns pour la zone example.com.

;	
	ovider.org. nostmaster.mydnsprovider.org. (
4 ; numero c	e serre
900 ; rairai	
600 ; reessa	.1
86400 ; expi	ration
3600) ; 1111	, par defaut
;	
; Enregistrements NS	de la zone
;	
0 NS dns.mydns	provider.org
;	
; Enregistrements de	zone
;	
@ A192.	168.0.100
adsc	A192.168.0.101
www	A 192.168.0.102
imap4	A 192.168.0.103
pop3 entrant	A192.168.0.104
msa	A192.168.0.105
eas	A 192.168.0.106
api	A 192.168.0.107
autodiscover	A192.168.0.108
dav	A192.168.0.109
chat	A 192.168.0.110
inbound A 192.	168.0.111
MX 10	inbound.exemple.com.
;	
; Enregistrements de	e service
;	
autodiscover. tcp	SRV 0 0 443 adsc.example.com.
airsync. tcp	SRV 0 0 443 eas.example.com.
imap. tcp	SRV 0 0 0 imap4.example.com.
pop. tcp	SRV 0 0 0 pop3.example.com.
smtp. tcp	SRV 0 0 0 msa.example.com.
caldav. tcp	SRV 0 0 0 dav.example.com.
carddav. tcp	SRV 0 0 0 dav.example.com.
xmpp-client. tcp	SRV 0 0 0 chat.example.com.
_xmpp crrencccb	SKV 0 0 Chatterampie.com.

Voir :

Pour plus d'informations générales sur AutoDiscover, voir le document Microsoft : <u>Autodiscover pour Exchange</u>.

2.2 Suivi des événements et journalisation

🧐 Alt-N MDaemon PRO - company.test - 10.10.50.235 [fe80::ec17:20:fd19:4833%11] (Configuration Session)				
<u>File Edit Setup Security Acc</u>	ounts <u>C</u> atalogs <u>Q</u> ueues <u>W</u> indows <u>H</u> elp			
J 😒 📚 🌪 🔍 🚳 🚹	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$			
Statistics	Tue 2017-03-14 00:00:28.138: SecurityPlus AntiVirus processing c:\mdaemon\queues\local\md75000000323.msg Tue 2017-03-14 00:00:28.138: Message troum-path: MD aemon@mail.company.test Tue 2017-03-14 00:00:28.138: Message trom: MD aemon@mail.company.test Tue 2017-03-14 00:00:28.138: Message to: mAL aemon@mail.company.test Tue 2017-03-14 00:00:28.138: Message subject: Mail Statistics Summary - mail company.test - Mon, 13 Mar 2017 Tue 2017-03-14 00:00:28.138: Stat SecurityPlus AntiVirus results Tue 2017-03-14 00:00:28.138: Stat SecurityPlus AntiVirus results Tue 2017-03-14 00:00:28.156: "Total attachments disinfected: 0 Tue 2017-03-14 00:00:28.156: "Total attachments disinfected: 0 Tue 2017-03-14 00:00:28.156: "Total attachments disinfected: 0 Tue 2017-03-14 00:00:28.156: "Total attachments removed : 0 Tue 2017-03-14 00:00:28.156: "Total attachments for sommary.test Tue 2017-03-14 00:00:28.156: "Total attachments disinfected: 0 Tue 2017-03-14 00:00:28.156: "Total attachments removed : 0 Tue 2017-03-14 00:00:28.156: "Total attachments removed : 0 Tue 2017-03-14 15:34:12.319: Message trom: Postmaster@company.test Tue 2017-03-14 15:34:12.319: "Message to: SF Update: mail.company.test - Tue, 14 Mar 2017 15:34:09-0500 Tue 2017-03-14 15:34:12.319: "Message to: SF Update: mail.company.test - Tue, 14 Mar 2017 15:34:09-0500 Tue 2017-03-14 15:34:12.319: "Message to: SF Update: mail.company.test - Tue, 14 Mar 2017 15:34:09-0500 Tue 2017-03-14 15:34:12.2319: "Message to: SF Update: mail.company.test - Tue, 14 Mar 2017 15:34:09-0500 Tue 2017-03-14 15:34:12.2319: "Message to: SF Update: mail.company.test - Tue, 14 Mar 2017 15:34:09-0500 Tue 2017-03-14 15:34:12.2319: "Total attachments scanned : 1 (including multipat/alternatives and message body) Tue 2017-03-14 15:34:12.2319: Total attachments scanned :			
Stats/	System & Statistics & Routing & Security & Mail & WorldClient & Queues & Plug-ins & Active Directory & Sessions			
company.test 10.10.50.235 [fe80::ec1]	7:20 fd19:/ v17.0.0 rc2 32 bit Active: 0 Buf: 0/0 SMTP: 0/0 POP3: 0/0 IMAP: 0 Time left: 1:15 Up: 5 days 6 hr			

L'interface graphique principale de MDaemon vous donne des informations importantes sur les ressources, les statistiques, les sessions actives et le courrier en attente de traitement. Elle contient également des options permettant d'activer/désactiver facilement les différents serveurs de MDaemon. Les onglets de l'interface graphique vous tiennent au courant des performances du serveur et de ses connexions entrantes et sortantes.

Statistiques

Le volet Statistiques est le volet gauche par défaut de l'interface principale de MDaemon. Il contient quatre sections : Statistiques, Comptes, Files d'attente et Serveurs.

La section*Statistiques* contient des statistiques sur le nombre de messages envoyés et reçus par MDaemon, ainsi que des statistiques sur les sessions POP et IMAP, les Spam acceptés et refusés, les virus, etc. Ces statistiques sont comptabilisées à partir de l'Heure de début de MDaemon, et il existe un menu de raccourcis par clic droit qui peut être utilisé pour effacer les compteurs.

Lorsque vous cliquez sur l'option "Réinitialiser les compteurs du nœud racine", tous les compteurs sont réinitialisés, et pas seulement celui sur lequel vous avez cliqué avec le bouton droit de la souris. De plus, il existe une option dans Serveur" Préférences | GUI qui peut être utilisée pour "*Préserver les*

78

compteurs de courrier du nœud racine à travers les redémarrages", sinon ils seront réinitialisés chaque fois que le serveur sera redémarré.

La section*Comptes* contient des entrées pour MDaemon, MDaemon Connector et ActiveSync. Chaque entrée indique le nombre de comptes utilisés et le nombre de comptes restants, en fonction de la licence de votre produit.

La section*Files* contient une entrée pour chaque file d'attente de messages et le nombre de messages (le cas échéant) que chaque file contient. Vous pouvez cliquer avec le bouton droit de la souris sur chacune des entrées de file d'attente pour ouvrir un menu contextuel contenant une ou plusieurs des options suivantes, en fonction de la file d'attente sélectionnée :

- Afficher la file d'attente cette option fait basculer le volet principal vers l'onglet Files sélectionnées et affiche la file d'attente sélectionnée. Une liste de tous les messages que la file contient s'affiche, et vous pouvez cliquer avec le bouton droit de la souris sur n'importe quel message pour ouvrir un menu contextuel contenant de nombreuses options similaires à celles disponibles dans le Gestionnaire des files d'attente et des statistiques, telles que Copier, Déplacer, Modifier, etc.
- **Gestion des files d'attente et des** statistiques ouvre le Gestionnaire des files d'attente et des statistiques à la page des files d'attente avec la file sélectionnée affichée.
- Dans cette option remet en file d'attente tous les messages contenus dans la file d'attente et tente de les traiter normalement en vue de leur distribution. Si vous tentez de traiter les messages contenus dans la file d'attente Garder, file d'attente Mauvais, ou similaire, les messages peuvent rencontrer les mêmes erreurs que celles qui les ont placés dans la file d'attente et les renvoyer dans la même file d'attente.
- **Figer/dégeler file d'attente** met temporairement en pause le traitement de la file sélectionnée, ou continue le traitement s'il est actuellement en pause.
- **Distribuer**: distribue les messages de la file d'attente. MDaemon tentera de délivrer les messages quelles que soient les erreurs rencontrées ils ne seront pas renvoyés dans la file d'attente même s'ils rencontrent les mêmes erreurs que celles qui les ont déplacés à l'origine.
- **Remettre en file d**'attente Cette option est disponible pour la file d'attente et a le même effet que l'option *Traiter maintenant* ci-dessus.
- Activer/désactiver la file d' attente active ou désactive la file d'attente. Lorsqu'elle est désactivée, les messages ne sont pas déplacés vers la file d'attente, quelles que soient les erreurs rencontrées.

La section*Serveurs* contient une entrée pour chaque serveur de MDaemon, et chaque entrée indique l'état actuel du serveur : "Actif" ou "Inactif". Sous l'entrée de chaque serveur se trouve une entrée pour chaque domaine (le cas échéant), ainsi que le port et l'adresse IP actuellement utilisés par ce serveur ou ce domaine. Le menu contextuel permet de faire basculer chaque serveur entre l'état actif et l'état inactif. Lorsqu'un serveur est inactif, son icône devient rouge.

79

Journal des événements et journalisation

Le volet droit par défaut de l'interface principale contient un groupe d'onglets qui affichent les actions actuelles de MDaemon et l'état de ses différents serveurs et ressources, et ils sont continuellement mis à jour pour refléter les conditions actuelles du serveur. Chaque session active et chaque action sur le serveur sont consignées dans l'onglet approprié une fois que l'action est terminée. Les informations affichées dans ces onglets sont reprises dans les fichiers journaux conservés dans le répertoire Directory de journalisation, si vous avez choisi d'enregistrer ce type d'activité.

Le volet principal de l'interface graphique de MDaemon contient les onglets suivants :

- **Système** au démarrage du programme, l'onglet Système affiche un Pas de journalisation du processus d'initialisation, qui peut vous alerter sur d'éventuels problèmes liés à la configuration ou à l'état de MDaemon. Il affiche également les activités telles que l'activation/désactivation des différents serveurs de MDaemon.
- **Statistiques** cet onglet affiche un rapport de statistiques du serveur correspondant aux informations contenues dans les différents compteurs du nœud racine dans l'onglet Statistiques du volet Statistiques et outils. Si vous souhaitez modifier la police ou la taille de la police utilisée pour ce rapport, vous pouvez le faire en modifiant les clés suivantes dans le fichier MDaemon.ini :

```
[ReportWindow]
DefFontFace=Courier New
DefFontHeigh=15
DefFontWidth=7
```

En outre, chaque nuit à minuit, le Postmaster et toutes les adresses figurant sur l 'écran <u>Recipients</u> 714 du Filtrage de contenu recevront une copie de ce rapport par e-mail. Il s'agit du même rapport que celui qui est généré lorsque vous utilisez la commande "Status" listée dans <u>General Email Controls</u> 1. Si vous ne souhaitez pas que ce rapport soit envoyé, désactivez l'option "Envoyer*le résumé des statistiques au postmaster à minuit*" (*Envoyer le rapport de statistiques au postmaster à minuit*) située dans l' écran <u>Divers</u> 500 Préférences.

- **Routage** affiche les informations de routage (À, De, Message ID, etc.) pour chaque message analysé par MDaemon.
- **Sécurité** cliquez sur cet onglet et plusieurs autres onglets relatifs à la sécurité apparaîtront au-dessus.
 - **Filtre de contenu** Les opérations du<u>Filtre de contenu de</u> **DE** MDaemon sont listées dans cet onglet. Lorsqu'un message correspond aux critères d'une des Règles du Filtre des messages, les informations relatives à ce message et les actions entreprises sont journalisées ici.
 - AntiVirus Les opérations de l'<u>AntiVirus</u> sont répertoriées dans cet onglet. Lorsqu'un message est analysé à la recherche de virus, les informations pertinentes relatives à ce message et l'action entreprise sont consignées ici.
 - Anti-spam affiche toutes les activités de<u>filtrage</u> 725 et de prévention du<u>spam</u> <u>de</u> 725 MDaemon.

- MDSpamD affiche toutes les activités du <u>Daemon anti-spam</u> (MDSpamD) <u>de MDaemon</u> (736).
- **SPF** affiche toutes les activités de<u>Sender Policy Framework.</u>
- **DKIM** liste toutes les activités de DomainKeys Identified Mail. 563
- DMARC liste toutes les activités DMARC 573.
- **VBR** cet onglet affiche les activités de<u>Certification VBR</u>
- **MDPGP** cet onglet affiche les activités<u>MDPGP</u> [77].
- Screening cet onglet affiche les activités<u>Tarpitting</u> and et Écran dynamique.
- Auth Failures (Échecs d'authentification) Cet onglet (et le fichier journal correspondant) contient une entrée détaillée pour chaque tentative d'authentification SMTP, IMAP et POP qui échoue. Les informations comprennent le protocole utilisé, l'ID de la session (afin de pouvoir effectuer des recherches dans d'autres journaux), l'IP de l'auteur de l'infraction, la valeur brute de la connexion qu'il a essayé d'utiliser (il s'agit parfois d'un alias) et l'Identifiantiant de compte qui correspond à la connexion (ou 'aucun' si aucun compte ne correspond). Vous pouvez faire un clic droit sur une ligne dans cet onglet pour ajouter l'Adresse des Comptes Bloqués.
- **MTA-STS** Affiche toute l'activité liée au protocole SMTP MTA Strict Transport Security (MTA-STS).
- **Courrier** cliquez sur cet onglet et plusieurs autres onglets relatifs au courrier apparaîtront au-dessus.
 - **SMTP (in)** Cet onglet affiche toute l'activité des sessions entrantes utilisant le protocole SMTP.
 - **SMTP (out)** toutes les sessions sortantes utilisant le protocole SMTP sont affichées dans cet onglet.
 - **IMAP** -les sessions de messagerie utilisant le protocole IMAP sont consignées dans cet onglet.
 - **POP3** -lorsque les Actifs collectent du courrier électronique à partir de MDaemon en utilisant le protocole POP3, cette activité est journalisée ici.
 - Collecte **MultiPOP** -cet onglet affiche les activités de Collecte de courrier MultiPOP de MDaemon.
 - **DomainPOP** -cet onglet affiche l'activité DomainPOP de MDaemon.
 - LDAP affiche l'activité du serveur LDAP.
 - Minger affiche l'activité du serveur Minger 923.
 - **RAW** L'activité des messages RAW ou générés par le système est consignée dans cet onglet.

MDaemon Connector - affiche toutes les activités de <u>MDaemon Connector</u> 409.

Webmail

Webmail - affiche les activités de messagerie de MDaemon Webmail.

ActiveSync - cet onglet affiche l'activité d'ActiveSync.

- **Messages et files d'attente** cet onglet donne accès à une autre rangée d'onglets au-dessus de lui avec un onglet correspondant à chaque file d'attente de messages, tels que : LOCAL & REMOTE, Mise en attente, Quarantaine, Spam bayésien, et ainsi de suite.
- **Plug-ins** affiche toutes les activités liées aux plug-ins de MDaemon.
- Active Directory affiche toutes les activités liées à Active Directory.
- Sessions cliquez sur cet onglet et plusieurs autres onglets apparaîtront audessus. Ces onglets affichent une entrée pour chaque connexion active à MDaemon. Dans le cas d'une connexion SMTP en entrée ou en sortie, POP en entrée ou en sortie, IMAP, Webmail ou ActiveSync, des informations sur chaque session active sont affichées ici. Double-cliquez sur une session active pour afficher une fenêtre de session structures, qui affiche la transcription de la session SMTP au fur et à mesure de son déroulement.



Les informations affichées dans ces onglets n'ont aucune incidence sur la quantité de données réellement stockées dans les fichiers journaux. Dans ce cas, MDaemon offre une grande flexibilité en ce qui concerne la quantité et le type d'informations enregistrées dans ces fichiers. Voir la boîte de dialogue<u>Journalisation</u> (106) pour plus d'informations sur les options de journalisation.

Menu contextuel de la fenêtre de suivi des événements

Si vous cliquez avec le bouton droit de la souris sur l'un des onglets de la fenêtre de suivi des événements, un menu contextuel s'ouvre. Ce menu propose diverses options permettant de sélectionner, copier, supprimer ou enregistrer le contenu d'un onglet donné. L'option Imprimer/Copierdu menu ouvre le texte sélectionné dans le Blocnotes, qui peut alors être utilisé pour imprimer les données ou les enregistrer dans un fichier. L' option Supprimer permet d'effacer le texte sélectionné. L' optionChercher ouvre une fenêtre dans laquelle vous pouvez spécifier un mot ou une phrase à rechercher dans les fichiers journaux. MDaemon cherchera la chaîne de texte dans tous les fichiers journaux, puis toutes les transcriptions de session contenant cette chaîne seront regroupées dans un seul fichier et ouvertes dans le Bloc-notes pour que vous puissiez les consulter. Une utilisation pratique de cette fonctionnalité consisterait à rechercher un Message ID particulier, ce qui permettrait d'obtenir une compilation de tous les journaux de toutes les transcriptions de session contenant ce Message ID. Certains onglets proposent également des options permettant de signaler à MDaemon.com les messages qui ont été classés par erreur comme étant du spam ou contenant un virus, ou qui auraient dû être classés comme tels (c'est-à-dire les faux positifs et les faux négatifs). Les messages signalés seront analysés et transmis à des fournisseurs tiers pour qu'ils prennent des mesures correctives.



La disposition de l'interface graphique de MDaemon n'est pas limitée aux positions par défaut décrites ci-dessus. Vous pouvez changer leur position en cliquant sur Windows | Changer de panneau dans la barre de menu.

Pas de journalisation composite

Dans le menu Windows de la barre de menus de MDaemon se trouve l'option Journalisation composite. En cliquant sur cette option, vous ajoutez une fenêtre à l'interface graphique qui combine les informations affichées dans un ou plusieurs onglets du panneau principal. Dans l'écranJournal composite Journalisation, les options permettent de désigner les informations qui apparaîtront dans cette fenêtre.

Compteurs de performances

MDaemon prend en charge les compteurs de performance Windows, qui permettent aux logiciels de surveillance de suivre l'état de MDaemon en temps réel. Il existe des compteurs pour le nombre de sessions actives pour les différents protocoles, le nombre de messages dans les files d'attente, les états actif/inactif du serveur, le temps de fonctionnement de MDaemon et les statistiques sur les sessions et les messages.

Pour utiliser les compteurs de performance, démarrez System Monitor en allant dans Panneau de configuration | Outils d'administration | Performance, ou en exécutant "perfmon". Cliquez sur Ajouter des compteurs, sélectionnez l'objet de performance MDaemon, puis sélectionnez et ajoutez les compteurs que vous souhaitez voir. Pour voir les compteurs de performance de MDaemon s'exécutant sur une autre machine, vous devez avoir activé le service "Registre à distance" et avoir accès à travers les pare-feux.

Voir :

<u>Fenêtre de session</u> ଛୀ <u>Icône de la barre d'état système</u> ଛୀ <u>Menu contextuel</u> ୡୀ <u>Pas de journalisation composite</u> 170

2.4 Icône de la zone de notification

Dans le cas où le serveur MDaemon est en cours d'exécution, son icône est visible dans la barre d'état système. Cependant, en plus de vous indiquer si le serveur est en cours d'exécution, l'icône est également dynamique et change de couleur en fonction de l'état actuel du serveur. Voici une liste des indicateurs de l'icône :

Tout va bien. Pas de courrier dans les files d'attente locales ou distantes.
Tout va bien. Files d'attente locales ou distantes occupées par du courrier.

	L'espace disque disponible est inférieur au seuil (voir Configuration Préférences <u>Disque</u> [527]).
	Le réseau est en panne, l'accès à distance a échoué ou le disque est plein.
Icône clignotant e	Une version plus récente de MDaemon est disponible.

Des informations supplémentaires sur le serveur sont disponibles dans l'info-bulle de l'icône. Placez le pointeur de la souris au-dessus de l'icône et la bulle d'aide apparaîtra, affichant le nombre de messages en file d'attente et la session active.



Menu des raccourcis

Cliquez avec le bouton droit de la souris sur l'icône de MDaemon dans la barre des tâches pour ouvrir le menu contextuel. Ce menu vous permet d'accéder rapidement à pratiquement tous les menus de MDaemon sans avoir à ouvrir l'interface utilisateur principale.

Cliquez sur l'icône "À propos de MDaemon..." dans la partie supérieure du menu contextuel pour en savoir plus sur MDaemon ou sur MDaemon Technologies.

Dans la section suivante, cliquez sur "Rechercher les mises à jour de MDaemon..." pour voir si une version plus récente de MDaemon est disponible au téléchargement.

Dans la troisième section, vous pouvez accéder aux menus MDaemon suivants : Configuration, Sécurité, Comptes et Files d'attente. Chacun de ces menus en cascade est identique au menu du

About Alt-N MDaemon	
About Alt NIT-shares and	
About Alt-N Technologies	
Check for MDaemon Updates	
Setup	►
Security	►
Accounts	►
Catalogs	►
Queues	•
Open Account Manager	
Process all Queues Now	
Queue and Stats Manager	
Lock Server	
Unlock Server	
Open MDaemon	
Close configuration session	

même nom situé dans la barre de menus de l'interface principale.

La quatrième section comporte des options permettant d'ouvrir le Gestionnaire des comptes et le Gestionnaire de files d'attente et de statistiques, ainsi qu'une option qui entraîne le traitement de toutes les files d'attente de MDaemon.

Ensuite, il y a des commandes pour verrouiller et déverrouiller l'interface de MDaemon (voir "Verrouiller/déverrouiller l'interface principale de MDaemon" cidessous), suivies de la sélection de menu"Ouvrir MDaemon...", utilisée pour ouvrir/restaurer l'interface de MDaemon lorsqu'elle est minimisée dans la barre d'état système.

La dernière option est "Fermer la session de configuration", qui ferme l'interface de MDaemon. Fermer la session de configuration n'arrête pas le service MDaemon.

Verrouillage/déverrouillage de l'interface principale de MDaemon

Pour verrouiller l'interface utilisateur, minimisez MDaemon, cliquez sur l'élément de menu"Verrouiller le serveur..." puis saisissez un mot de passe dans la boîte qui s'ouvre. Après avoir confirmé le mot de passe en le saisissant une seconde fois, l'interface utilisateur de MDaemon sera verrouillée. Il n'est pas possible de l'ouvrir ou de la visualiser, mais MDaemon continuera à fonctionner normalement. Vous pourrez cependant toujours utiliser l'option de raccourci"Traiter toutes les files d'attente maintenant..." pour traiter les files d'attente manuellement. Pour déverrouiller MDaemon, ouvrez la boîte de dialogue"Déverrouiller MDaemon" en double-cliquant sur l'icône de la barre des tâches, ou en cliquant avec le bouton droit de la souris sur l'icône et en choisissant "Déverrouiller le serveur..." Saisissez ensuite le mot de passe que vous avez créé lors du verrouillage.

2.5 Fenêtre de session

Lorsque vous double-cliquez sur une session active dans l'un des <u>onglets Session</u> ⁷² de l'interface graphique principale, la fenêtre de session correspondant à cette entrée s'ouvre. La fenêtre de session affiche la transcription SMTP de cette session au fur et à mesure qu'elle progresse. Vous pouvez cliquer sur Déconnecter dans cette fenêtre si vous souhaitez interrompre et déconnecter la session en cours.

SMTP inbound from WorldClient (session 956:2)	×
Tue 2008-06-03 00:17:49: → 220 example.com ESMTP MD aemon 10.0.0g; Tue, 03 Jun 2008 00:17:49 +0100 Tue 2008-06-03 00:17:49: → 250 example.com Hello WorldClient, pleased to meet you Tue 2008-06-03 00:17:49: → 250-example.com Hello WorldClient, pleased to meet you Tue 2008-06-03 00:17:49: → 250-example.com Hello WorldClient, pleased to meet you Tue 2008-06-03 00:17:49: → 250-example.com Hello WorldClient, pleased to meet you Tue 2008-06-03 00:17:49: → 250-AUTH +LOGIN Tue 2008-06-03 00:17:49: → 250-801TMINE Tue 2008-06-03 00:17:49: → 250-801TMINE Tue 2008-06-03 00:17:49: → 250 SIZE 0 Tue 2008-06-03 00:17:49: → 250 SUZE 0 Tue 2008-06-03 00:17:49: → 250 Authentication successful Tue 2008-06-03 00:17:49: → 250 Authentication successful Tue 2008-06-03 00:17:49: → 250 Chrimk@example.com > SIZE=86273839 Tue 2008-06-03 00:17:49: → 250 Chrimk@example.com > Ine 2008-06-03 00:17:49: → 250 Chrimk@example.com > Recipient ok Tue 2008-06-03 00:17:49: → 250 Chrimk@e	hbXBsZ! Q2MWI=
	>
Disc	connect

2.6 Flux SMTP de MDaemon

Lorsqu'une connexion SMTP entrante est établie, MDaemon passe par une série complexe d'étapes de traitement pour déterminer s'il faut accepter le message et ce qu'il faut en faire une fois qu'il est accepté. Le diagramme suivant est une représentation graphique de ce flux de travail pour les messages SMTP entrants.

> Le degré d'exécution de ces étapes dépend de votre configuration particulière. Une ou plusieurs étapes peuvent être ignorées si une fonction donnée est désactivée dans votre configuration.



Section

3 Menu Configuration

3.1 Paramètres du serveur

3.1.1 Paramètres du serveur

3.1.1.1 Serveurs

90

|--|

Serveur SMTP.

Activer VRFY

Cliquez sur ce commutateur si vous souhaitez répondre aux commandes SMTP VRFY. Cette commande est parfois utilisée par des serveurs qui utilisent une fonction de renvoi d'appel ou de rappel SMTP pour tenter de confirmer la validité des adresses électroniques sur votre serveur. Elle est désactivée par défaut.

Activer EXPN

Cochez cette case si vous souhaitez que MDaemon accepte les commandes EXPN.

Activer APOP et CRAM-MD5

Par défaut, les serveurs MDaemon(POP, IMAP, etc.) n'acceptent pas les méthodes d'authentification APOP et CRAM-MD5. Dans ce type d'authentification, les mots de passe doivent être stockés en utilisant un cryptage réversible, ce qui n'est pas

recommandé à des fins de sécurité, afin de protéger les mots de passe contre le décryptage par MDaemon, l'administrateur ou un éventuel attaquant. Par conséquent, cette option n'est pas compatible avec l'<u>option Mots de passe</u> "*Stocker les mots passe boîtes aux lettres en utilisant un chiffrement non réversible*", ni avec l'authentification Active Directory. Si, toutefois, vous n'utilisez pas SSL/TLS, APOP et CRAM-MD5 pourraient fournir une sécurité supplémentaire en permettant aux utilisateurs d'être authentifiés sans envoyer de mots de passe en texte clair.

Rejeter les valeurs RCPT en double

Activez cette option si vous souhaitez que le serveur SMTP ignore les destinataires en double dans la même session SMTP. MDaemon acceptera puis rejettera les destinataires en double. Cette option est désactivée par défaut.

Refuser les messages qui ne respectent pas les standards RFC

Activez cette option si vous souhaitez rejeter, au cours du processus SMTP, les messages qui ne sont pas conformes aux normes Internet RFC. Pour passer le test de conformité, le message doit

- 1. Avoir une taille supérieure à 32 octets (taille minimale nécessaire pour inclure toutes les parties requises).
- 2. Avoir un En-tête FROM : ou SENDER :.
- 3. Ne pas comporter plus d'un en-tête FROM :.
- Ne pas avoir plus d'un en-tête SUBJECT :, bien qu'aucun en-tête de sujet ne soit requis.

Les messages utilisant des sessions authentifiées ou provenant de domaines ou d'adresses IP autorisés sont exemptés de cette exigence.

Les échecs de négociation SSL sont suivis de nouveaux essais sans SSL pendant une heure maxi

Cette option vous permet de réessayer temporairement les IP hôtes sans SSL lorsqu'elles rencontrent une erreur SSL au cours d'une session SMTP sortante. Cette option est réinitialisée toutes les heures.

Activer le pipeline de commandes sortantes

Par défaut, MDaemon prend en charge l'extension de service SMTP pour le pipelining de commandes (RFC 2920), ce qui signifie qu'il envoie les commandes MAIL, RCPT et DATA par lots plutôt qu'individuellement, ce qui améliore les performances sur les liaisons réseau à forte latence. Le SMTP pipelining est toujours utilisé pour les connexions en entrée, et il est activé par défaut pour les connexions en sortie. Décochez cette case si vous ne souhaitez pas l'utiliser pour les connexions sortantes.

Refuser les messages supérieurs à [xx] Ko (0=pas de limite)

Par taille, MDaemon n'acceptera ni ne traitera les messages dépassant une certaine taille. Dans ce cas, MDaemon tente d'utiliser la commande ESMTP SIZE spécifiée dans la RFC-1870. Si l'agent d'envoi prend en charge cette extension SMTP, MDaemon déterminera la taille du message avant sa distribution et le refusera immédiatement. Si l'agent d'envoi ne supporte pas cette extension SMTP, MDaemon

devra commencer à accepter le message, suivre sa taille périodiquement pendant le transfert, et enfin refuser de délivrer le message une fois la transaction terminée. Utilisez "0" dans cette option si vous ne souhaitez pas fixer de taille limite. Si vous souhaitez exempter les sessions authentifiées des contrôles de taille, utilisez l'option "...sauf si SMTP AUTH est utilisé avec succès" ci-dessous.

... Sauf si SMTP AUTH est utilisé avec succès

Cochez cette case si vous souhaitez exempter les messages de la limitation de taille lorsque la session SMTP est authentifiée.

Nbre max. de commandes RCPT autorisées

Utilisez cette option si vous souhaitez limiter le nombre de commandes RCPT pouvant être envoyées par message. Utilisez "0" si vous ne souhaitez pas fixer de limite.

Fermer la session si la valeur est atteinte

Cochez cette case si vous souhaitez Fermer la session immédiatement si le nombre maximum de commandes RCPT autorisées est atteint.

Paramètres serveur

Le serveur POP supprime le courrier après la commande DELE

Cochez cette option si vous souhaitez que MDaemon supprime les messages immédiatement lorsqu'ils sont récupérés et que la commande DELETE est reçue, même si la session POP ne se termine pas correctement.

Le serveur IMAP prend en charge la commande COMPRESS

Cochez cette case si vous souhaitez prendre en charge l'extension IMAP COMPRESS (RFC 4978), qui compresse toutes les données envoyées vers et depuis le client. COMPRESS augmente l'utilisation de l'unité centrale et de la mémoire par session IMAP.

Autoriser les mots de passe en texte clair

Cette option détermine si MDaemon accepte ou non les mots de passe envoyés en texte clair aux serveurs SMTP, IMAP ou POP3. Si elle est désactivée, les commandes POP3 USER, POP3 PASS, IMAP LOGIN, IMAP AUTH LOGIN et SMTP AUTH LOGIN renverront une erreur, sauf si la connexion utilise SSL.

Autoriser les connexions à partir de ses propres adresses IP des serveurs

Lorsque cette option est activée, MDaemon peut se connecter à lui-même.

Les serveurs POP et IMAP autorisent toujours les connexions provenant de cette IP

Les serveurs POP et IMAP acceptent toujours les connexions provenant de cette IP, quels que soient les paramètres de filtrage et de Bouclier.

3.1.1.2 Distribution

🧐 Server Settings - Delivery		×
 Servers & Delivery Servers Delivery Sessions Timeouts Unknown Mail DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging 	Message Routing Send all outbound email directl Send all outbound email directl Send all email directly first, and Default Smart Host Default smart host Use at default smart host as don User name Password Allow per-account authentication Use the Domain Manager to config Otherwise, these defaults may be u Delivery Settings Abort delivery if SMTP RCPT of Bounce message on 5% error Bounce message on 5% error	ly to the recipient's mail server mart host I then to smart hosts if there are problems in name and deliver to its MX hosts Perform a POP check Host or IP User name User name Sure these values for individual domains. used. command receives a 5X error domain has no MX records rs from any of receiving domain's MX hosts rs from smart hosts
	Ok	Cancel Apply Help

Routage des messages

Envoyer tout le courrier sortant directement au serveur destinataire

Lorsque cette option est choisie, MDaemon tente de distribuer le courrier directement au lieu de le transmettre à un autre hôte. MDaemon place les messages non distribuables dans son système de relance et continue d'essayer de les distribuer en fonction des paramètres et des intervalles de temps que vous avez définis dans l' écran<u>File d'attente de relance de</u> al la boîte de dialogue Files d'attente de courrier.

Envoyer tout le courrier sortant à un hôte de relais

Sélectionnez cette option si vous souhaitez que le courrier sortant, quel que soit son domaine de destination, soit envoyé vers un autre hôte ou serveur pour être distribué. Si cette option est sélectionnée, les e-mails sortants seront envoyés au *Non (par défaut Hôte relais*) spécifié ci-dessous. En règle générale, cette fonction est utile pendant les périodes de volume élevé, lorsque la livraison directe des messages entraînerait une taxation excessive des ressources du serveur. Si un message ne peut pas être distribué au serveur désigné, il sera placé dans le système de relance et MDaemon continuera d'essayer de le distribuer en fonction des paramètres et des intervalles de temps que vous avez définis dans l'écran<u>Fileur de relance de [932</u>] la boîte de dialogue Files d'attente de messagerie.

Envoyer les e-mails directement, puis aux hôtes de relais en cas de problème

Cette option est une combinaison des deux options de distribution précédentes. Si MDaemon tente d'abord de distribuer le courrier sortant directement sur le serveur, mais s'il n'y parvient pas, il l'envoie à l'*Hôte de relais par défaut spécifié ci-dessous*. Le courrier non distribuable est un courrier destiné à des hôtes qui n'ont pas pu être résolus en adresse IP réelle (comme une passerelle non enregistrée vers un réseau distant) ou un courrier destiné à un hôte qui a été résolu correctement mais qui n'a pas pu être connecté directement ou qui refuse les connexions directes. Plutôt que de renvoyer ce type de courrier à son expéditeur, cette option permet à MDaemon de transmettre le message à un MTA plus puissant. Il arrive que le système de messagerie de votre fournisseur d'accès dispose de méthodes de distribution du courrier auxquelles votre serveur local n'a pas forcément un accès direct. Si un message ne peut pas être distribué à l'hôte intelligent désigné, il sera placé dans le système de relance et MDaemon continuera d'essayer de le distribuer en fonction des paramètres et des intervalles de temps que vous avez définis dans l'écranFile de relais [32] de la boîte de dialoque Files d'attente. À chaque nouvelle tentative de distribution, MDaemon essaiera d'abord de distribuer le message directement à son destinataire, puis à l'hôte intelligent désigné.

Hôte de relais par défaut

Non Hôte de relais par défaut

Indiquez ici le Nom d'hôte & IP de votre FAI ou de votre hébergeur de messagerie. Il s'agit généralement du Serveur SMTP de votre FAI.



Traiter le Domaine Hôte default par défaut comme un nom de domaine et distribuer à ses hôtes MX

Activez cette option si vous souhaitez que MDaemon traite le <Domain *default default Hôte* > comme un nom de domaine, en interrogeant son enregistrement DNS et en distribuant le courrier à ses hôtes MX.

Utiliser l'authentification SMTP

Cochez cette case et entrez vos identifiants de connexion ci-dessous si l'*Hôte intelligent* par défaut requiert une authentification. Ces identifiants seront utilisés pour tous les messages SMTP sortants envoyés à l'Hôte de relais. Si vous choisissez d'utiliser l' option *Autoriser l'authentification par compte* ci-dessous, MDaemon s'authentifiera auprès de l'hôte séparément pour chaque message, en utilisant les informations d'*accès à l'hôte intelligent* du compte d'envoi désignées dans l'écran<u>Services de messagerie</u>

Nom d'utilisateur

Saisissez ici votre nom d'utilisateur ou votre login.

Mot de passe

Utilisez cette option pour spécifier votre mot de passe Identifiant de l'hôte relais.

Effectuer d'abord une vérification POP

Si votre Hôte de relais doit effectuer un contrôle POP3 avant d'accepter vos messages, cochez cette case et entrez les informations d'identification requises cidessous.

Hôte ou IP

Saisissez l'hôte ou l'Adresse IP à laquelle vous souhaitez vous connecter.

Nom d'utilisateur

Il s'agit de l'identifiant ou du nom du comptePOP.

Mot de passe

Ils'agit dumot de passe du compte POP.

Autoriser l'authentification par compte

Cochez cette case si vous souhaitez utiliser l'authentification par compte pour les messages SMTP sortants envoyés au *Hôte par défaut* spécifié ci-dessus. Au lieu d'utiliser les identifiants *Nom d'utilisateur* et *Mot de passe* fournis ici, les identifiants *Accès Hôte relais de* chaque compte, désignés dans l' écran<u>Services de messagerie</u> seront utilisés à la place. Si aucun identifiant Hôte de relais n'a été désigné pour un compte donné, les identifiants ci-dessus seront utilisés à la place.

Si vous souhaitez configurer *l'authentification par compte de* manière à utiliser le *mot de passe Mot de passe de* chaque compte au lieu du *mot de passe Hôte de relais* facultatif, modifiez la clé suivante dans le fichierMDaemon.ini :

[AUTH] ISPAUTHUsePasswords=Yes (Non (par défaut))



L'activation de l'option ISPAUTHUsePasswords=Yes aura pour effet, au fil du temps, de communiquer les mots de passe du courrier local de tous vos comptes à votre Hôte de relais. Cela peut présenter un risque pour la sécurité de la messagerie, puisque des informations sensibles sont communiquées à un autre serveur. Vous ne devez pas utiliser cette option, sauf si vous utilisez un Hôte de relais en qui vous avez une confiance absolue et si vous pensez qu'il est nécessaire de le faire. En outre, vous devez savoir que si vous utilisez cette option et donnez à vos utilisateurs la permission de modifier leur *mot de* passe de messagerie par l'intermédiaire de la Webmail ou par un autre moyen, le fait de modifier le mot de passede la *messagerie* modifiera également le *mot de passe de l'hôte* relais. Cela peut entraîner l'échec de l'authentification de l'hôte intelligent pour un compte lorsque son *mot de passe de messagerie* est modifié localement, mais que le *mot de passe de l'hôte intelligent* correspondant n 'est pas modifié dans votre hôte intelligent.

Abandonner la distribution si la commande SMTP RCPT reçoit une erreur 5XX

Activez cette option si vous souhaitez que MDaemon interrompe sa tentative de distribution d'un message lorsqu'il reçoit une erreur fatale 5xx en réponse à la commande SMTP RCPT. Cette option est désactivée par défaut.

Renvoyer le message si le domaine destinataire ne possède pas d'enregistrements MX

En règle générale, lorsque MDaemon vérifie les enregistrements DNS du domaine destinataire, il recherche les enregistrements MX, puis un enregistrement A si aucun enregistrement MX n'est trouvé. Si aucun n'est trouvé, le message est renvoyé à l'expéditeur car il n'est pas distribuable. Cliquez sur cette option si vous souhaitez que MDaemon renvoie immédiatement le message lorsqu'aucun enregistrement MX n'est trouvé, au lieu de l'autoriser à rechercher un enregistrement A également. Cette option est Non (par défaut).

Renvoyer à l'expéditeur dès qu'un hôte MX envoie une erreur 5XX

Lorsque cette case est cochée, MDaemon renvoie le message lorsqu'il reçoit une réponse d'erreur fatale 5xx d'un hôte MX. Par conséquent, il ne continuera pas à essayer de distribuer le message aux hôtes MX suivants qui pourraient être désignés pour le domaine du destinataire. Si cette option est désactivée, MDaemon ne renverra pas le message tant qu'au moins un des hôtes MX renvoie une réponse d'erreur non fatale 4xx. Cette option est activée par défaut.

Renvoyer le message en cas d'erreur 5XX des hôtes relais

Utilisez cette option si vous souhaitez renvoyer/rebondir un message lorsqu'il reçoit une réponse d'erreur fatale 5xx de la part de vos hôtes intelligents.

Voir :

<u>File de relance</u> ସେଥି <u>Services de messagerie</u> 7ତ୍ରୀ

3.1.1.3 Sessions

Server Settings - Sessions	
 Servers & Delivery Servers Delivery Sessions Timeouts Unknown Mail DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging 	SMTP Maximum concurrent SMTP outbound sessions 30 Maximum concurrent SMTP inbound sessions 50 Maximum concurrent MSA inbound sessions 50 Max SMTP outbound messages spooled per session 0 (0 = unlimited) Cache SMTP connection failures for this many minutes 5 (0 = never) Maximum simultaneous connections from any single IP 0 (0 = unlimited) Maximum simultaneous connections to any single IP 0 (0 = unlimited) Maximum simultaneous connections to any single IP 0 (0 = unlimited) Maximum simultaneous connections to any single IP 0 (0 = unlimited) Maximum simultaneous connections to any single IP 0 (0 = unlimited) Maximum simultaneous connections to any single IP 0 (0 = unlimited) Maximum simultaneous connections to any single IP 0 (0 = unlimited) Maximum simultaneous connections to any single IP 0 (0 = unlimited) Maximum simultaneous connections to any single IP 0 (0 = unlimited) Maximum simultaneous connections to any single IP 0 (0 = unlimited)
	Try delivering to all A records before moving on to the next MX host POP3 & IMAP Maximum concurrent MultiPOP outbound sessions Maximum concurrent POP3 inbound sessions 100 Maximum concurrent IMAP sessions 130

SMTP

Nombre maximal de sessions SMTP sortantes simultanées

La valeur saisie ici représente le nombre maximal de sessions SMTP sortantes qui seront créées au moment de l'envoi du courrier sortant. Chaque session enverra des messages sortants jusqu'à ce que la file d'attente soit vide ou que le paramètre*Maximum SMTP outbound messages spooled per session* soit atteint. Exemple : si la file d'attente du courrier sortant contient vingt messages en attente au moment de l'envoi et que la valeur de ce paramètre est de cinq, cinq sessions seront créées simultanément et chacune d'entre elles enverra consécutivement quatre messages.

Dans cette option, la valeur par défaut est 30, mais vous pouvez expérimenter avec le nombre de sessions afin de trouver le paramètre qui vous permettra d'obtenir les meilleures performances en fonction de votre bande passante. Il est possible de spécifier un si grand nombre de sessions que votre bande passante sera surchargée ou que votre machine Windows manquera de ressources et que vous perdrez en efficacité de distribution. N'oubliez pas que chaque session SMTP créée par MDaemon délivre les messages consécutivement et que, par conséquent, quatre sessions délivrant deux messages chacune peuvent être plus performantes et plus rapides que huit threads délivrant un seul message chacun. De cinq à dix threads pour un modem 56k et de vingt à trente pour un modem à large bande constituent un bon point de départ.

Nombre maximal de sessions SMTP entrantes simultanées

Cette valeur détermine le nombre de sessions SMTP entrantes simultanées que le serveur acceptera avant de répondre par un message "Serveur trop occupé". La valeur par défaut est 50.

Nombre maximal de sessions MSA entrantes simultanées

Cette option permet de définir le nombre maximal de sessions entrantes simultanées de l'agent de soumission du courrier (MSA).

Nombre maximal de messages SMTP sortants spoliés par session

Ce paramètre limite le nombre de messages individuels que chaque session peut envoyer avant d'arrêter la distribution du courrier et de se libérer de la mémoire. En règle générale, vous devez laisser ce paramètre à zéro, ce qui signifie que chaque session continuera à envoyer des messages jusqu'à ce que la file d'attente soit vide.

Mettre en cache les échecs de connexion SMTP pendant ce nombre de minutes (0 = jamais)

Dans le cas d'un échec de connexion SMTP à un hôte donné, MDaemon cesse d'essayer de se connecter à cet hôte pendant le nombre de minutes spécifié dans cette option. Cela permet d'éviter que MDaemon n'essaie inutilement de se connecter à un hôte problématique à plusieurs reprises lorsque, par Exemple, il a plusieurs messages destinés à cet hôte et qu'il découvre qu'il est en panne lors de la première tentative de livraison. Le paramètre (par défaut) est de "5" minutes. Utilisez "0" si vous ne souhaitez pas mettre en cache les échecs SMTP.

Nombre maximal de connexions simultanées à partir d'une même IP (0 = illimité) Il s'agit du nombre maximal de connexions simultanées autorisées à partir d'une seule adresse IP avant qu'elle ne soit bloquée. Utilisez "0" si vous ne souhaitez pas fixer de limite.

Nombre maximal de connexions simultanées à une seule adresse IP (0 = illimité) Cette option permet de limiter le nombre de connexions simultanées autorisées à partir d'une seule adresse IP pendant la distribution du courrier. Utilisez "0" si vous ne souhaitez pas limiter les connexions simultanées.

Cette option est utile pour éviter d'établir un trop grand nombre de connexions simultanées à diverses adresses IP. Si, lors de la distribution, un message nécessite une connexion à une adresse IP qui dépasse cette limite, la connexion est ignorée et l'hôte MX suivant (ou l'hôte intelligent) est utilisé. Si aucun hôte supplémentaire n'est disponible, le message est mis en attente pour le prochain cycle de distribution. Non (par défaut), cette option est désactivée, ce qui préserve le comportement existant.

...inclure les IP autorisées

Par défaut, les connexions aux adresses IP autorisées sont exemptées de l' option "*Maximum de connexions simultanées à une même IP*". Cochez cette case si vous souhaitez l'appliquer également aux IP autorisées.

...inclure les IP réservées

Toujours par défaut, les connexions aux adresses IP réservées à l'usage de l'intranet sont exemptées de cette fonction. Il s'agit des adresses127.0.0.*,

192.168.*.*, 10.*.*.* et 172.16.0.0/12. Cochez cette case si vous souhaitez l'appliquer également aux adresses IP réservées.

Utiliser plusieurs commandes RCPT pour l'envoi de courrier

Non par défaut, MDaemon utilise un spooling intelligent, c'est-à-dire qu'il utilise plusieurs commandes RCPT pour l'envoi courrier. Décochez cette case si vous souhaitez n'utiliser qu'une seule commande RCPT par session.

Liste des exceptions

Ce bouton permet d'ouvrir la liste des Exceptions de mise en file d'attente intelligente. Lorsque MDaemon envoie des messages à des domaines figurant dans cette liste, il n'utilise PAS le spooling intelligent ; une seule commande RCPT est utilisée par session.

Essayez de distribuer à tous les enregistrements A avant de passer à l'hôte MX suivant En cas d'erreur ou d'échec de livraison, MDaemon tente par défaut de livrer tous les enregistrements A d'un hôte MX avant de passer à l'hôte MX suivant. Désactivez cette option si vous souhaitez que MDaemon passe à l'hôte MX suivant immédiatement après avoir rencontré une erreur, plutôt que d'essayer d'abord tous les enregistrements A.

POP3 & IMAP

Nombre maximum de sessions sortantes MultiPOP simultanées

La valeur saisie ici représente le nombre maximum de sessions POP sortantes qui seront créées au moment de la collecte du courrier MultiPOP. Chaque session collectera ce type de messages jusqu'à ce que tous les serveurs Collecte MultiPOP aient été traités et que tout le courrier ait été collecté. Exemple : s'il y a quinze sessions MultiPOP parmi tous vos utilisateurs et que la valeur de ce paramètre est fixée à trois, chaque session collectera le courrier de cinq sources MultiPOP.

Nous vous conseillons de faire des essais avec le nombre de sessions afin de déterminer le nombre qui vous permettra d'obtenir les meilleures performances pour votre bande passante. Il est possible de spécifier un si grand nombre de sessions que votre bande passante sera surchargée, ou que votre machine Windows manquera de ressources et que vous perdrez en efficacité de traitement. N'oubliez pas que chaque session POP créée par MDaemon collectera du courrier jusqu'à ce que toutes les sources soient épuisées. Par conséquent, quatre sessions collectant du courrier provenant de vingt sources peuvent être plus performantes et plus rapides que vingt sessions collectant du courrier provenant d'une seule source.

Nombre maximal de sessions POP3 entrantes simultanées

Cette valeur contrôle le nombre maximum de sessions POP entrantes simultanées que le serveur acceptera avant de répondre par un message "Serveur trop occupé".

Nombre maximal de sessions IMAP simultanées

Cette valeur détermine le nombre maximal de sessions IMAP simultanées que le serveur acceptera avant de répondre par un message "Serveur trop occupé".

3.1.1.4 Temporisateurs

100

Server Settings - Timeouts		
 Servers & Delivery Servers Delivery Sessions Timeouts Unknown Mail DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging 	Timeouts Wait 30 seconds for sockets to connect Wait 60 seconds for protocol dialog to start Wait 10 seconds for MX responses Wait 10 seconds for A/AAAA responses Wait 10 seconds for Minger responses SMTP and POP3 sessions timeout after Wait on response to SMTP DATA command for IMAP sessions timeout after	10 inactive minutes 10 minutes 30 inactive minutes
	Ok Cance	Apply Help

Délais

Attendre [xx] secondes pour que les sockets se connectent

Après avoir initié une demande de connexion, MDaemon attendra ce nombre de secondes pour que le système distant accepte la connexion. Si le système distant ne répond pas dans ce délai, MDaemon envoie le message à un *hôte intelligent* spécifié ou le place dans le système de relance, selon l'option que vous avez choisie dans l'écranDélivrance de serveur.

De [xx] secondes pour le démarrage du dialogue de protocole

Une fois la connexion établie avec un Hôte distant, MDaemon attendra pendant un certain nombre de secondes que l'hôte distant entame la boîte de dialogue du protocole SMTP ou POP3. Si l'hôte distant ne démarre pas la session de protocole dans ce délai, MDaemon enverra le message à un *hôte intelligent*spécifié ou le placera dans le système de relance, selon l'option que vous avez choisie dans l' écran<u>Délivrance de sal</u> la boîte de dialogue Paramètres du serveur.

Attendre [xx] secondes pour les réponses MX

Lorsque MDaemon utilise les services DNS pour résoudre les hôtes 'MX' de domaines distants, il attend les réponses à ses requêtes'MX' pendant ce nombre de secondes. Si le serveur DNS ne répond pas dans ce délai, MDaemon tente de distribuer le

message à l'adresse IP spécifiée dans l'enregistrement DNS 'A' de l' hôte distant. Si cette tentative échoue, MDaemon enverra le message à un *Hôte* relais spécifié ou le placera dans le système de relance, en fonction de l'option que vous avez choisie dans l' écran<u>Livraison de</u> al boîte de dialogue Paramètres du serveur.

Attendre [xx] secondes pour les réponses A/AAAA

Ce délai détermine la durée d'attente de MDaemon lors d'une tentative de résolution de l'adresse IP d'un hôte distant.Si la tentative échoue, MDaemon envoie le message à un *Hôte de relais*spécifié ou le place dans le système de relance, selon l'option que vous avez choisie dans l' écranLivraison de solution de lore de dialogue Paramètres du serveur.

Attendre [xx] secondes pour les réponses de Minger

Il s'agit du nombre de secondes pendant lesquelles MDaemon attendra une réponse d'un serveur<u>Minger</u> [323].

Les sessions SMTP et POP3 expirent au bout de [xx] minutes inactives.

Si une session connectée et opérationnelle reste inactive (pas d'entrées/sorties) pendant ce laps de temps, MDaemon interrompt la transaction. MDaemon réessayera au prochain intervalle de traitement programmé.

Attendre la réponse à la commande SMTP DATA pendant [xx] minutes

Cette option détermine la durée pendant laquelle MDaemon attend la réponse "250 Ok" après l'envoi de la commande DATA au cours du processus SMTP. Comme certains serveurs de réception effectuent de longues opérations anti-spam, antivirus ou d'autres opérations nécessaires à ce moment-là, cette option peut être utilisée pour leur donner le temps de terminer ces tâches. La valeur par défaut est de 10 minutes.

Les sessions IMAP expirent après [xx] minutes inactives.

Si une session IMAP n'est pas active pendant ce nombre de minutes, MDaemon la ferme.

3.1.1.5 Courrier inconnu

102

Server Settings - Unknown Mail	
 Servers & Delivery Servers Delivery Sessions Timeouts Unknown Mail DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging 	What to do with Local Queue mail addressed to unknown users? Normally, mail sent to unknown users will be rejected long before it reaches the local queue however there are configurations in which this is not possible. Mail queued for unknown users should be
	Ok Cancel Apply Help

Les Files d'attente pour les utilisateurs inconnus doivent être...

...renvoyé à l'expéditeur avec un avertissement "aucun utilisateur de ce type".

Lorsque cette option est activée, les messages qui arrivent sur le serveur à destination d'utilisateurs inconnus mais supposés locaux seront renvoyés à l'expéditeur du message. Si vous souhaitez personnaliser le contenu du message d'avertissement "No Such User", vous pouvez le faire en créant un fichier texte appelé "NoShUser.dat" et en le plaçant dans le dossier "MDaemon\\".

...envoyés à l'alias "Postmaster

Par défaut, les messages qui arrivent sur le serveur et qui sont destinés à des utilisateurs inconnus mais supposés locaux seront transférés à l'utilisateur qui a été désigné comme alias 'Postmaster'. Désactivez cette option si vous ne souhaitez pas envoyer ces messages au Postmaster.

... envoyés dans le dossier des mauvais messages

Par défaut, les messages qui arrivent au serveur à destination d'utilisateurs inconnus mais supposés locaux seront routés vers la file d'attente des messages erronés. Décochez cette case si vous ne souhaitez pas envoyer ces messages dans la file d'attente des mauvais messages.

...transféré vers un autre serveur de messagerie

Utilisez cette option si vous souhaitez Transférer les messages à un autre serveur de messagerie lorsqu'ils sont adressés à des utilisateurs locaux inconnus.

Nom d'hôte ou IP

Indiquez le nom hôte ou l'adresse IP vers lequel vous souhaitez Transférer les messages.

Ce qui suit s'applique globalement partout dans MDaemon où vous êtes autorisé à spécifier un hôte vers lequel transférer, copier ou envoyer du courrier électronique. Si vous mettez l'hôte entre parenthèses (par exemple [exemple.com]), MDaemon ne consultera pas l'enregistrement MX lorsqu'il distribuera à cet hôte. Exemple : si cette option contient "exemple.com", les recherches MX seront effectuées normalement. Si, par contre, cette option contient" [exemple.com]", seule la recherche de l'enregistrement A sera effectuée.

Mot de passe AUTH

Saisissez les informations d'identification nécessaires pour le serveur de messagerie vers lequel vous transférez les messages adressés à des utilisateurs inconnus.

Valeur SMTP 'MAIL' (en anglais)

Cette adresse sera utilisée dans la commandeSMTP "Mail From :", utilisée lors de l'établissement de la session avec l'hôte acceptant le message. Dans cette partie de l'enveloppe SMTP, c'est normalement l'expéditeur du message qui est utilisé. Si vous avez besoin d'une commande vide (MAIL FROM<>), entrez" [poubelle]" dans cette option.

Port (par défaut = 25)

Il s'agit du port TCP que MDaemon utilisera pour envoyer les messages. La valeur par défaut est le port 25.

3.1.2 DNS & IPs

3.1.2.1 DNS

🧐 Server Settings - DNS	×
Servers & Delivery DNS & IPs DNS Ports IPv6 Binding IP Cache Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging	DNS Servers Use Windows DNS servers Detect Reload DNS servers hourly Use EDNS0 (Extension mechanisms for DNS) UDP packet size 1280 Manually configured DNS servers: Image: Configured DNS servers: Up Down Down New Local Cache Files Itel thosts file Edit MX cache file Edit HOSTS file
	Ok Cancel Apply Help

Serveurs DNS

Utiliser les serveurs DNS de Windows

Lorsque cette option est sélectionnée, MDaemon utilise tous les serveurs DNS présents dans la configuration TCP/IP de Windows. MDaemon essaiera chaque serveur DNS une fois par opération de recherche et dans l'ordre jusqu'à ce qu'il épuise la liste complète des serveurs DNS ou trouve le premier qui fonctionne. Si vous incluez des serveurs DNS supplémentaires dans l'option*Serveurs DNS configurés manuellement* ci-dessous, MDaemon essaiera également ces serveurs. Enfin, au démarrage, le Pas de journalisation affichera chaque serveur DNS et indiquera sa source (c.-à-d. configuré manuellement ou provenant de Windows).

Recharger les serveurs DNS toutes les heures

Cochez cette case si vous souhaitez recharger le serveur DNS toutes les heures. Cette option est désactivée par défaut.

Utiliser EDNS0 (Extension Mechanisms for DNS)

Par défaut, MDaemon prend en charge les mécanismes d'extension pour le DNS (voir <u>RFC 2671go to</u>). Décochez cette case si vous ne souhaitez pas les prendre en charge.

Taille des paquets UDP

Cette option contrôle la Taille des paquets UDP. La taille par défaut est de 1280 octets.

Serveurs DNS configurés manuellement

MDaemon utilisera tous les serveurs DNS spécifiés ici lorsqu'il effectuera des recherches DNS. MDaemon essaiera chaque serveur une fois par opération de recherche et dans l'ordre jusqu'à ce qu'il épuise la liste complète des serveurs DNS ou qu'il trouve le premier qui fonctionne. Si vous activez l' option*Utiliser les serveurs DNS de Windows* ci-dessus, MDaemon interrogera également tous les serveurs DNS présents dans votre configuration TCP/IP Windows. Enfin, au démarrage, le Pas de journalisation affiche chaque serveur DNS et indique sa source (c'est-à-dire s'il a été configuré manuellement ou s'il provient de Windows).

Fichier du cache local

Fichier HOSTS...

Avant d'interroger les serveurs DNS, MDaemon tente d'abord de résoudre une adresse en traitant le fichier HOSTS de Windows. Si ce fichier contient l'adresse IP du domaine en question, MDaemon n'aura pas besoin d'interroger le serveur DNS.

Vous devez saisir le chemin d'accès complet et le nom du fichier, et non pas uniquement le nom du fichier. MDaemon tentera d'utiliser la valeur suivante comme emplacement par défaut de ce fichier :

[lecteur]:\Nwindows\system32\Ndrivers\etc\hosts

Le fichier HOSTS est un fichier Windows qui contient l'enregistrement A ou l'adresse IP principale des noms de domaine. MDaemon vous permet également de spécifier les adresses IP des enregistrements MX dans un fichier appelé MXCACHE.DAT. Ce fichier se trouve dans le dossier MDaemon\APP\ dans le dossier MDaemon. Cliquez sur **Modifier Ie fichier de cache MX** ci-dessous et lisez les commentaires en haut du fichier pour plus d'informations.

Modifier le fichier cache MX

Cliquez sur ce bouton pour afficher ou modifier le fichier MXCACHE.DAT.

Modifier le fichier HOSTS

Cliquez sur ce bouton pour afficher ou éditer le fichier HOSTS.

3.1.2.2 Ports

 Servers & Delivery DNS & IPs DNS Ports IPv6 Binding IP Cache Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging 	🧐 Server Settings - Ports				×
 Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging 	Servers & Delivery DNS & IPs DNS Ports IPv6 Binding IP Cache Domain Sharing	SMTP, ODMR, & MSA F SMTP inbound port MSA inbound port SMTP SSL port POP & IMAP Ports POP inbound port	Ports 25 587 465 110	SMTP outbound port ODMR inbound port POP outbound port	25 366
Return port settings to defaults Bind to new port values now	Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP	IMAP inbound port POP SSL port Other Ports DNS outbound port Remote Admin port	143 995 53 1000	IMAP SSL port LDAP port Minger port	993 389 4069
	in RAS in Logging	Return port settings to	defaults	Bind to new	w port values now

Port SMTP, ODMR et MSA

Port SMTP entrant

MDaemon surveille ce port TCP pour les connexions entrantes des clients SMTP. Il s'agit du port SMTP principal qui, dans la plupart des cas, doit être laissé au paramètre par défaut (port = 25).

Port SMTP sortant

Ce port est utilisé lorsque le courrier est envoyé à d'autres serveurs SMTP.

Port MSA entrant

Il s'agit d'un port MSA (Message Submission Agent) qui peut être utilisé par vos utilisateurs à la place du *port SMTP entrant* spécifié ci-dessus. La transmission sur ce port requiert une authentification requise. Les utilisateurs qui envoient des messages sur ce port doivent donc configurer leurs clients de messagerie de manière à s'assurer que leurs connexions sont authentifiées. En outre, comme certains fournisseurs de services Internet bloquent le port 25, vos utilisateurs distants peuvent contourner cette restriction en utilisant le port MSA à la place. Si vous ne souhaitez pas désigner de port MSA, définissez la valeur "0" pour le désactiver.



Les connexions au port MSA sont exemptées des recherches PTR et inversées, de l'Écran d'hôte et d'IP, du Bouclier IP et du Tarpitting. Les connexions au port MSA continuent d'utiliser la limitation de connexion par attaque dictionnaire.

Port ODMR entrant

MDaemon surveille ce port pour les connexions ODMR (On-Demand Mail Relay) entrantes, telles que les ATRN des domaines de la passerelle.

Port SMTP SSL

Il s'agit du port dédié aux sessions de messagerie SMTP utilisant une connexion sécurisée (SSL). Voir <u>SSL & Certificats appendict</u> pour plus d'informations.

Ports POP & IMAP

Port POP entrant

MDaemon surveille ce port pour les connexions entrantes provenant de clients POP distants.

Port POP sortant

Ce port sera utilisé lorsque MDaemon récupérera le courrier des serveurs POP.

Port IMAP entrant

MDaemon surveille ce port pour les requêtes IMAP entrantes.

Port SSL POP

Il s'agit du port dédié aux clients de messagerie POP utilisant une connexion sécurisée (SSL). Voir <u>SSL et certificats</u> pour plus d'informations.

Port IMAP SSL

Il s'agit du port dédié aux clients de messagerie IMAP utilisant une connexion sécurisée (SSL). Voir <u>SSL & Certificats and pour plus d'informations</u>.

Autres ports

Port DNS sortant

Entrez le port que vous souhaitez que MDaemon utilise pour envoyer et recevoir des datagrammes vers le serveur DNS.

Port LDAP

MDaemon enverra les informations de la base de données et du carnet d'adresses à votre serveur LDAP sur ce port.

Voir : Prise en charge du carnet d'adresses LDAP

Port MDaemon Remote Admin

Il s'agit du port que MDaemon surveille pour les connexions deMDaemon <u>Remote</u> <u>Admin.</u>

Port Minger

Il s'agit du port que le serveur<u>Port Minger</u> surveillera pour les connexions.

Restaurer les paramètres par défaut des ports

Ce bouton permet de rétablir les valeurs par défaut de tous les paramètres des ports.

Appliquer ces nouvelles valeurs

Lorsque vous modifiez les valeurs de l'un des paramètres de port, vous devez appuyer sur ce bouton pour que vos modifications prennent effet immédiatement. Dans le cas contraire, vos modifications ne seront appliquées qu'au prochain démarrage du serveur.


3.1.2.3 IPv6

Server Settings - IPv6	IPv6 (Dual stack available) MDaemon's SMTP/PDP/IMAP Servers
	Ok Cancel Apply Help

Non (par défaut), MDaemon détecte le niveau de capacité IPv6 pris en charge par votre système d'exploitation et effectue une double pile lorsque cela est possible. Sinon, MDaemon surveille IPv4 et IPv6 de manière indépendante.

IPv6

Les Serveurs SMTP/POP3/IMAP de MDaemon...

...acceptent uniquement les connexions IPv4

Choisissez cette option si vous souhaitez accepter uniquement les connexions IPv4.

...acceptent uniquement les connexions IPv6

Choisissez cette option si vous souhaitez accepter uniquement les connexions IPv6.

...acceptent les connexions IPv4 ou IPv6

Choisissez cette option si vous souhaitez accepter les connexions IPv4 et IPv6. Non (par défaut), MDaemon donnera la priorité aux connexions IPv6 sur les connexions IPv4 dans la mesure du possible.

Se connecter à des hôtes IPv6 sortants lorsque c'est possible

Activez cette option si vous souhaitez que MDaemon se connecte aux hôtes IPv6 en sortie chaque fois que cela est possible.

Lorsque MDaemon se connecte à un hôte IPv6, il doit utiliser une adresse IPv6 locale qui lui est propre. L'adresse IPv6 est désignée dans l'<u>écran Gestionnaire de domaines | Nom hôte ou</u> <u>IP.</u> [187] Si nécessaire, une adresse pour la liaison des sockets sortants peut être spécifiée dans l' écran <u>Liaison</u> [10].

Voir :

Liaison 110

Gestionnaire de domaines | Nom d'hôte ou IP 187

3.1.2.4 Liaison

Paramètres de liaison sortante

Activer la liaison d'IP sortante

Lorsque cette option est cochée, MDaemon lie toujours les sockets sortants. Pour les domaines dont l' option <u>Ce domaine ne reconnaît que les connexions effectuées</u>

<u>vers ces IP</u> [187] est cochée dans l'écran <u>Nom hôte ou IP</u> [187], MDaemon utilise l'IP configurée du domaine. Sinon, il utilise les paramètres (par défaut) par défaut pour lier les sockets sortants spécifiés ci-dessous.

Non (par défaut) par défaut pour la liaison des sockets sortants : Adresse IPv4/IPv6 Il s'agit des adresses IP qui seront utilisées pour la liaison de la prise sortante pour les domaines qui ne sont pas déjà liés à des adresses IP spécifiques sur l'écran Nom hôte & IP du Gestionnaire de domaines.

Paramètres de liaison entrante

Deuxième adresse IP pour la liaison de socket entrante: Adresse IPv4/IPv6 Utilisez cette option si vous souhaitez désigner un deuxième jeu d'adresses IP pour la liaison de socket entrante 1871.

Voir :

Gestionnaire de domaines | Nom de l'hôte ou IP IPv6

3.1.2.5 Cache IP

🧐 Server Settings - IP Cache	
Servers & Delivery DNS & IPs DNS & IPs Ports Ports IPv6 Binding IP Cache Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging	MDaemon consults the IP Cache before making DNS queries.
	Ok Cancel Apply Help

Dans le but d'accélérer la distribution des messages et de réduire le temps de traitement du courrier, MDaemon met en cache les adresses IP de tous les hôtes avec

lesquels il entre en contact. Ces adresses IP sont stockées, puis le cache est vérifié chaque fois que MDaemon a besoin d'une résolution DNS pour un nom d'hôte. Si le Nom d'hôte nécessitant une résolution est trouvé dans le cache IP, la recherche DNS est ignorée, ce qui peut faire gagner un temps de traitement considérable. Dans cette fenêtre, les paramètres de fonctionnement du cache sont définis. Vous pouvez également ajouter ou supprimer des entrées manuellement, d'utiliser ou non DNSSEC, de définir la taille maximale du cache et de déterminer la durée pendant laquelle les entrées resteront dans le cache. Le Cache IP est accessible à partir de la sélection de menu"Configuration | Paramètres de serveur | Cache IP".

Pas de cache IP

Hôte

Entrez l'hôte que vous souhaitez ajouter au Cache IP.

IP

Entrez l'adresse IP que vous souhaitez ajouter au cache IP.

DNSSEC

Cochez cette case pour DNSSEC.

Ajouter

Une fois que vous avez saisi manuellement un hôte et une adresse IP, cliquez sur ce bouton pour l'ajouter au cache.

Supprimer

Si vous souhaitez supprimer une adresse IP mise en cache de la liste, sélectionnez l'entrée, puis cliquez sur ce bouton.

Effacer

Ce bouton permet de supprimer toutes les entrées du cache.

Pas de cache

Cliquez sur ce bouton pour afficher une liste de noms de domaine ou d'adresses IP que vous ne souhaitez pas que MDaemon ajoute au Cache IP.

Paramètres

Mettre les domaines automatiquement en cache

Cette option régit lemoteur interne de mise en cache automatique deMDaemon. Si vous souhaitez que MDaemon mette automatiquement les domaines en cache, activez cette option. Si vous souhaitez construire le Cache IP vous-même, décochez cette case.

Vider le cache à chaque intervalle de traitement

Si cette option est sélectionnée, l'intégralité du contenu du cache sera vidée au début de chaque session de courrier. Cela permet d'actualiser le cache à chaque intervalle de traitement.

Durée de vie par défaut (en minutes)

Il s'agit de la valeur par défaut, en minutes, pendant laquelle une entrée restera dans le Cache IP. Dans ce cas, MDaemon supprime l'entrée. Si vous souhaitez définir une entrée permanente dans le Cache IP, fixez la valeur de*Non (par défaut)* à 9999.

Nombre maximal d'entrées dans le cache

Cette valeur détermine la taille du cache. Lorsque ce nombre est atteint, l'entrée suivante est supprimée du cache.

3.1.3 Partage de domaine

	 Server Settings - Domain Sharing Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging 	Domain Sharing allows you to split a domain's accounts and mailing lists across multiple servers. Please see HELP for complete configuration instructions. Minger queries are made to each host listed here to find whether the account exists and where. Messages are then accepted and routed accordingly. Enable Domain Sharing Image: I
--	---	---

Le partage de domaine permet de répartir plusieurs utilisateurs d'un domaine sur plusieurs serveurs. Il est ainsi possible d'avoir des serveurs MDaemon fonctionnant à différents endroits, utilisant tous les mêmes noms de domaine mais avec des comptes utilisateurs différents. Une partie des comptes utilisateurs de vos domaines est hébergée sur un serveur tandis qu'une autre partie est hébergée sur un ou plusieurs autres serveurs. La boîte de dialogue Partage de domaine permet de spécifier l'emplacement de chacun de ces autres serveurs. Dans ce cas, lorsqu'un message entrant arrive pour un utilisateur local qui n'a pas de boîte aux lettres locale, le Partage de domaine utilisera Mon compte pour interroger les autres serveurs afin de découvrir si cet utilisateur possède ou non un compte sur l'un d'entre eux. Si l'adresse est valide, MDaemon acceptera le message et le routera vers le serveur où se trouve le compte. Exemple : vous pouvez avoir des bureaux dans plusieurs villes et choisir d'utiliser le Partage de domaine pour permettre à chaque employé d'avoir une adresse électronique se terminant par "@example.com". Le MDaemon de chaque bureau hébergerait une partie de l'adresse électroniqued'example.com, avec des comptes uniquement pour les employés locaux qui travaillent dans ce bureau. Ensuite, chaque bureau serait configuré pour utiliser le Partage de domaine, afin que les messages de chacun soient routés vers le bon bureau.

Comme le Partage de domaine utilise Minger 23 pour vérifier les adresses, Minger doit être activé et correctement configuré sur chaque serveur pour que les requêtes fonctionnent. Si, toutefois, une erreur survient lors d'une requête Minger, par exemple lorsque l'un des serveurs est temporairement indisponible, MDaemon répondra par un code d'erreur temporaire "451" afin que le serveur d'envoi puisse réessayer de délivrer le message ultérieurement. En outre, une fois qu'une adresse a été vérifiée, elle est mise en cache pendant cinq jours, de sorte que MDaemon peut immédiatement accepter les futurs messages pour cette adresse et commencer à essayer d'acheminer ces messages vers l'hôte approprié.

Enfin, pour éviter les problèmes qui pourraient survenir si un même compte était créé sur plusieurs serveurs, MDaemon interroge tous les serveurs de Partage de domaine avant de créer un nouveau compte.

Il existe une option appelée "*Les vérifications Minger déclenchent également les vérifications Partage de domaine*", située dans l'écran Paramètres de l'éditeur de passerelle. Cette option permet à MDaemon d'interroger les hôtes du Partage de domaine lorsque la <u>vérification Minger 270</u> est utilisée par une passerelle.

Activer Partage de domaine

Cochez cette case pour activer le Partage de domaine. Après avoir activé le Partage de domaine et ajouté tous les hôtes ou adresses IP du Domaine à la liste, assurezvous d'avoir également activé et configuré <u>Minger</u> afin de pouvoir répondre aux requêtes de ces hôtes lorsqu'ils tentent de vérifier vos adresses locales.

Supprimer

Pour supprimer l'une de vos entrées de Partage de domaine, sélectionnez-la dans la liste et cliquez sur ce bouton.

Avancé

Ce bouton ouvre un fichier dans lequel vous pouvez configurer les noms de domaines autorisés à utiliser le Partage de domaine. Si ce fichier ne contient rien (le cas par défaut), tous les domaines peuvent utiliser le Partage de domaine. Voir les instructions en haut du fichier pour plus d'informations.

Hôte ou IP

Utilisez ce champ pour entrer le Domaine ou l'adresse IP qui partage un ou plusieurs de vos domaines. Vous pouvez ajouter deux points et un port (par exemple mail.example.com:2525) si vous souhaitez utiliser un port spécifique, Non par

défaut, lors de l'envoi de messages SMTP à l'hôte (ce n'est pas la même chose que le Port Minger ci-dessous).

Port Minger

Il s'agit du port que Minger utilisera pour interroger cet hôte. Le port par défaut est 4069.

Mot passe Minger (facultatif)

Si l'hôte que vous ajoutez requiert un mot de passe Minger, entrez-le ici. Paramètres de passe Minger (facultatif) est recommandé.

Ajouter

Après avoir saisi l'hôte ou le domaine IP, le port et le mot de passe, cliquez sur ce bouton pour ajouter la nouvelle entrée du Partage de domaine à la liste.

Ne pas envoyer le courrier du partage de domaine aux hôtes de relais à la suite d'erreurs de distribution

Si cette option est activée, si MDaemon rencontre une erreur lors d'une tentative de distribution du courrier électronique du Partage de domaine (par exemple, lorsque l'hôte du Partage de domaine est hors ligne), le courrier sera conservé dans la <u>file</u> <u>d'attente</u> plutôt qu'envoyé à l'<u>hôte intelligent</u> . L'envoi de ces e-mails à l'hôte intelligent peut souvent conduire à une boucle de courrier. Cette option est activée par défaut.

Vérifier les expéditeurs auprès des hôtes du partage de domaine

Par défaut, MDaemon accepte le courrier provenant de comptes qui existent sur d'autres hôtes du Partage par défaut - Domaine. Si vous préférez ne pas effectuer de recherche de Partage de domaine sur l'expéditeur du SMTP MAIL, désactivez cette option.

Partager les posts de liste de diffusion avec les hôtes du Partage de domaine

Activer cette option si vous souhaitez partager les listes diffusion avec les hôtes du Partage de domaine. Lorsqu'un message arrive pour une liste de diffusion, une copie est créée pour chaque hôte du Partage de domaine qui maintient également une version de cette liste (une requête est effectuée pour vérifier). Lorsque ces hôtes reçoivent leur copie, ils distribuent le message à tous les membres de la liste qu'ils desservent. De cette manière, les listes de diffusion peuvent être réparties sur plusieurs serveurs sans perte de fonctionnalité. Pour que cela fonctionne, chaque hôte du Partage de domaine doit inclure les IP des autres hôtes dans sa configuration d'<u>IP autorisées</u> (564). Dans le cas contraire, les messages de la liste risquent d'être refusés et d'afficher le message d'erreur "L'expéditeur n'est pas membre de la liste".

Voir :

<u>Minger</u> ब्रिटेडो <u>Gestionnaire de domaines</u> 1841

3.1.4 Dossiers publics et partagés

MDaemon prend en charge les Dossiers publics publics et partagés IMAP. Les Dossiers publics (gérés à partir du <u>Gestionnaire des dossiers publics</u> (serés à partir du <u>Gestionnaire des dossiers publics</u>) sont des dossiers supplémentaires qui n'appartiennent à aucun compte particulier mais qui peuvent être mis à la disposition de plusieurs utilisateurs IMAP. Les Dossiers utilisateurs sont des dossiers IMAP qui appartiennent à des comptes MDaemon individuels. Chaque dossier partagé, qu'il soit public ou utilisateur, doit être associé à une liste d'utilisateurs MDaemon, et seuls les membres de cette liste peuvent y accéder par le biais de MDaemon Webmail ou un client de messagerie IMAP.

Lorsque les utilisateurs IMAP accèdent à leur liste de Dossiers publics & partagés, ils voient également les Dossiers publics et partagés utilisateurs auxquels ils ont été autorisés à accéder. De cette manière, certains dossiers courrier peuvent être partagés par plusieurs utilisateurs tout en nécessitant les identifiants de connexion individuels de chacund'entre eux.Par ailleurs, avoir accès à un dossier ne signifie pas nécessairement avoir un accès complet en lecture/écriture ou un accès administratif à ce dossier. Des droits d'accès spécifiques peuvent être accordés à des utilisateurs individuels, ce qui vous permet de définir différents niveaux d'accès pour chacun d'entre eux. Exemple : vous pouvez autoriser certains utilisateurs à supprimer des messages et en restreindre l'accès à d'autres.

Une fois qu'un dossier IMAP public ou utilisateur a été créé, vous pouvez utiliser le Filtre de contenu pour définir les critères selon lesquels certains messages sont déplacés dans ce dossier. Exemple : il peut être utile d'établir une règle de filtrage pour que les messages contenant support@example.com dans l'en-tête TO : soient déplacés dans le Dossier public Support. Les <u>actions du Filtre de contenu</u> m "Déplacer le message dans les Dossiers publics..." et "Copier le message dans un dossier..."permettent d'effectuer cette opération. Pour les dossiers d'utilisateurs partagés, vous pouvez utiliser vos <u>filtres IMAP personnels</u> [789] pour acheminer des messages spécifiques vers ces dossiers. Dans le cas des dossiers partagés, vous pouvez utiliser vos propres filtres IMAP pour acheminer des messages spécifiques. Dans le cas des dossiers partagés, vous pouvez non seulement utiliser les Filtres de contenu et les filtres IMAP, mais aussi associer un compte spécifique à un dossier partagé de sorte que les messages destinés à cette "Adresse d'envoi" soient automatiquement acheminés vers le dossier partagé. Toutefois, seuls les utilisateurs ayant reçu l'autorisation de "poster" dans le dossier pourront envoyer des messages à cette adresse.

Pour plus de commodité, l'éditeur Liste des dossiers contient également un écran <u>Dossiers publics</u> [314] qui vous permet de configurer un dossier public à utiliser avec une liste particulière. Si vous activez cette fonction, une copie de chaque message de la liste sera placée dans le dossier public spécifié. Tous les dossiers publics sont stockés dans le répertoire _{Dossiers} publics de la hiérarchie des répertoires de MDaemon.

Dossiers de documents du webmail

Les thèmes du Webmail permettent de partager des documents en utilisant des Dossiers IMAP partagés. Les dossiers de documents disposent d'une <u>Liste de Contrôle</u> <u>d'Accès (ACL)</u> wittotale, comme les autres dossiers partagés. comme les autres dossiers partagés, ce qui permet de définir les autorisations et les règles de partage, et tous les types de fichiers peuvent être partagés par l'intermédiaire du système. Les utilisateurs duwebmail peuvent télécharger des fichiers dans leurs dossiers de documents à l'aide des outils intégrés. Lorsqu'ils utilisent le thème LookOut, les navigateurs qui prennent en charge l'API HTML5 Drag and Drop, tels que Chrome et Firefox, peuvent également télécharger des fichiers en les faisant glisser du bureau vers la fenêtre du navigateur. Les noms de fichiers peuvent être recherchés et renommés, et les fichiers peuvent être joints aux nouveaux messages en cours de composition.

Vous pouvez activer/désactiver les dossiers documents (et autres dossiers partagés) par domaine et par utilisateur en modifiant le fichier \WorldClient\Domains.ini et les fichiers \Users\..\WCuser.ini individuels respectivement. Vous pouvez configurer à la fois les paramètres par défaut et les paramètres personnalisés, qui remplaceront les paramètres par défaut. Exemple :

```
[Non (par défaut)]
NomDossierDocuments=Documents
ActiverDocuments=Oui
Exemple : [Exemple.com:UserDefaults]
DocumentsFolderName=Documents de l'Exemple
EnableDocuments=Oui
[superControllingDomain.gov:UserDefaults]
EnableDocuments=No
EnableDocuments=No
EnableCalendar=No
EnableNotes=Non
EnableTasks=No
```

Définition d'une taille maximale de fichier

Vous pouvez limiter la taille des fichiers individuels qui peuvent être téléchargés dans les dossiers de documents en ajoutant cette clé au fichier domains.ini :MaxAttachmentSize=<valeur en KB> La valeur par défaut est 0, ce qui signifie qu'il n'y a pas de limite.

Bloquer ou autoriser des types de fichiers

Pour empêcher certains types de fichiers d'être téléchargés dans le dossier documents, ajoutez la clé BlockFileTypes= au fichierdomains.ini, en listant les types de fichiers que vous souhaitez bloquer, séparés par un espace ou une virgule. Exemple : "BlockFileTypes=exe dll js".

Pour autoriser uniquement certains types de fichiers à être téléchargés dans le dossier documents, ajoutez la clé AllowFileTypes= au fichierdomains.ini, en listant les types de fichiers que vous souhaitez autoriser, séparés par un espace ou une virgule. Exemple : "AllowFileTypes=jpg png doc docx xls xlsx".

Lorsque les deux clés sont utilisées, la priorité est donnée aux fichiers bloqués en cas de conflit ; si une extension figure dans les deux listes, elle sera bloquée. Si une clé est utilisée sans valeur (c'est-à-dire sans liste d'extensions), cette clé ne sera pas utilisée. Les extensions de fichiers peuvent inclure un "." (par exemple .exe .dll), mais ce n'est pas obligatoire.

Voir :

Dossiers publics & partagés 118 Gestionnaire des dossiers publics 25 Contrôle d'accès 27 Éditeur de dossier partagé | Dossiers partagés 796 Liste des dossiers | Dossiers publics 314

3.1.4.1 Dossiers publics et partagés

<u>μ</u>

Pour accéder à l'écran Dossiers publics & partagés, cliquez sur "Configuration | Paramètres du serveur | Dossiers publics & partagés".

Activer les dossiers publics

Cochez cette case si vous souhaitez permettre aux utilisateurs d'accéder aux Dossiers publics. Les utilisateurs qui peuvent y accéder et le niveau d'accès accordé sont désignés sous chaque dossier dans le <u>Gestionnaire Dossiers publics</u> cette case à cocher si vous souhaitez masquer les Dossiers publics à tous les utilisateurs.

Préfixe des dossiers publics IMAP (ex. : 'Public/')

Les dossiers publics sont préfixés par une séquence de 20 caractères maximum, telle que "#" ou "Dossiers publics/". Cela permet aux utilisateurs de distinguer facilement les Dossiers publics des Dossiers privés à partir de leur client de messagerie. Utilisez cette zone de texte pour spécifier la série de caractères que vous souhaitez utiliser pour désigner les Dossiers publics.

Créer les dossiers Contacts, Calendrier, Tâches, Journal et Notes pour tous les domaines Cochez cette case si vous souhaitez que ces dossiers existent pour tous les domaines. Chaque fois qu'un <u>domaine</u> est ajouté à MDaemon, ces dossiers seront créés.

Maintenir les dossiers de contacts à jour avec les données du compte MDaemon Si cette option est activée, MDaemon gardera les dossiers de contacts synchronisés avec sa liste de comptes.

Ajouter/supprimer les contacts lorsque les comptes sont activés/désactivés

Par défaut, lorsque vous désactivez un compte, celui-ci est supprimé du dossier des contacts publics du domaine. Si vous réactivez le compte activé, il sera à nouveau ajouté aux contacts. Cette option est activée par défaut pour éviter que les comptes désactivés n'apparaissent dans le système d'auto-complétion du Webmail.

Supprimer les dossiers publics du domaine lorsque celui-ci est supprimé

Cochez cette case si vous souhaitez supprimer les dossiers publics d'un domaine lorsque celui-ci est supprimé.

Activer les dossiers partagés

Cochez cette case si vous souhaitez autoriser les utilisateurs IMAP à partager l'accès à leurs dossiers IMAP. Les utilisateurs qui peuvent y accéder et le niveau d'accès accordé sont désignés sous chaque dossier dans l'écran<u>Dossiers</u> <u>partagés</u> de l'Éditeur Comptes (Comptes | Gestionnaire de comptes | [Compte utilisateur] | Dossiers partagés). Cochez cette case si vous souhaitez empêcher les utilisateurs de partager l'accès à leurs dossiers et empêcher l'apparition de l'écran Dossiers partagés susmentionné dans l'Éditeur de comptes.



Préfixe des dossiers IMAP partagés (ex. : 'Partage/')

Les dossiers utilisateurs partagés sont préfixés par une séquence de 20 caractères maximum, telle que "Dossiers publics et partagés/ ". Cela permet aux utilisateurs de distinguer facilement les Dossiers partagés des dossiers privés à partir de leur client de messagerie. Utilisez cette zone de texte pour spécifier la série de caractères que vous souhaitez utiliser pour désigner les Dossierssiers utilisateurs partagés.

Aucun accès aux dossiers partagés lorsque le compte est désactivé

Par défaut, les serveurs IMAP, Webmail et ActiveSync de MDaemon n'autorisent pas l'accès aux dossiers partagés des comptes désactivés. Décochez cette case si vous souhaitez autoriser l'accès aux dossiers partagés des comptes lorsque le compte est désactivé.

Voir :

Dossiers publics - Vue d'ensemble 116 Gestionnaire des dossiers publics 325 Liste de contrôle d'accès 327 Éditeur de compte | Dossiers partagés 736 Liste des dossiers | Dossiers publics 314

3.1.5 Rappel de message

Système de rappel de message

MDaemon dispose d'un système de rappel des messages que vous pouvez utiliser pour retarder de 0 à 15 minutes les messages entrants envoyés par des utilisateurs locaux authentifiés, ce qui donne aux utilisateurs un court laps de temps pendant lequel ils peuvent tenter d'empêcher la distribution d'un message. Pendant ce délai, les messages

sont placés dans une file Distribution différée plutôt que d'être envoyés directement dans la file d'attente du courrier entrant. Dans la file Distribution différée, la date à laquelle les messages doivent quitter la file d'attente est encodée dans le nom du fichier. MDaemon vérifie la file d'attente une fois par minute et lorsqu'il est temps pour un message de quitter la file d'attente, il est déplacé dans la file d'attente des messages entrants et soumis au traitement et à la distribution normaux des messages. L'activité est Pas de journalisation dans l'onglet Routage et dans le fichier journal.

Vous pouvez régler le délai sur "0" si vous le souhaitez, mais cela augmente la possibilité qu'un message qu'un utilisateur souhaite rappeler ait déjà été délivré. Il est donc recommandé de fixer un délai d'au moins 1 ou 2 minutes pour que les utilisateurs aient le temps de se rendre compte qu'ils veulent rappeler un message, d'envoyer la demande de rappel et d'avoir le temps restant pour que MDaemon traite la demande. Cependant, comme MDaemon est capable de retirer les messages rappelés de la ou des files d'attente Remote, où il peut déjà y avoir un délai, certains administrateurs peuvent trouver cette temporisation de livraison différée inutile.

Rappel de message

Les utilisateurs peuvent rappeler un message de plusieurs manières.

- 1. Dans MDaemon Webmail, cliquez sur le bouton Rappel de message qui s'affiche lors de l'affichage d'un message récemment envoyé dans le dossier Éléments envoyés. Si vous cliquez sur ce bouton avant l'expiration du délai de rappel, le MDaemon Webmail enverra un message de RAPPEL à MDaemon.
- Envoyez un message au Compte système mdaemon@example.com, avec le mot "RAPPEL" (sans les guillemets) comme Objet du message. Cela rappellera le dernier message que vous avez envoyé. Il ne rappellera que le dernier message.
- Dans le dossier Pièces jointes, localisez le message que vous souhaitez rappeler, choisissez l'option "Transférer en pièce jointe" et envoyez le message au compte du système mdaemon@example.com, en utilisant le mot "RAPPEL" comme Objet du message.
- Afficher les messages en-tête, copier l'en-tête "Message-ID : <valeur ID du message>" et créer un nouveau message avec "RAPPEL Message ID : <valeur ID du message>" dans l'objet (sans les guillemets).

Quelle que soit la méthode de rappel choisie, MDaemon enverra un e-mail à l'utilisateur pour lui indiquer si le rappel a réussi ou non. Si un message est rappelé avec succès, MDaemon le supprime de la file d'attente comme s'il n'avait jamais été envoyé. Si l' option *Supprimer les messages rappelés des dossiers de courrier* du *compte* est activée, MDaemon tente également de supprimer le message rappelé du dossier de courrier de l'utilisateur local où il a peut-être déjà été distribué. Les messages envoyés à plusieurs destinataires seront tous rappelés par une seule demande. Enfin, le système de Rappel de message ne fonctionne pas sans l' en-tête X-Authenticated-Sender pour assurer la sécurité et empêcher d'autres personnes de rappeler des messages dont elles ne sont pas à l'origine. Par conséquent, l'<u>option</u> <u>de désactivation de cet en-tête</u> [530] sera annulée si le Rappel de message est activé.

Rappel de message

Activer le rappel de message

Cochez cette case pour activer le système de rappel de messages. L'option est désactivée par défaut.

Supprimer les messages rappelés des dossiers de messagerie du compte

Cochez cette case si vous souhaitez également supprimer les messages rappelés des dossiers courrier de vos comptes MDaemon locaux s'ils ont déjà été distribués avant le rappel du message. Cela peut entraîner la disparition des messages des clients de messagerie et des téléphones des utilisateurs locaux. L'option est désactivée par défaut.

Distribution différée des messages pendant ce nombre de minutes [xx] (0-15 minutes)

Il s'agit du nombre de minutes pendant lesquelles MDaemon mettra en attente les messages entrants des utilisateurs locaux authentifiés. Si un message RECALL est reçu pendant ce délai, MDaemon supprime le message référencé avant toute tentative de distribution. Cette option peut être réglée entre 0 et 15 minutes. Le Nonètres par défaut est de 1 minute.

Ne pas différer les messages si le destinataire possède une boîte aux lettres sur ce serveur

Cochez cette case si vous ne souhaitez pas différer les messages lorsque la boîte aux lettres du destinataire se trouve sur le même serveur MDaemon que l'expéditeur. Remarque : lorsque vous utilisez l'option"*Supprimer les messages rappelés des dossiers messagerie du compte*" ci-dessus, même les messages qui ont déjà été distribués peuvent être rappelés et supprimés de la boîte aux lettres d'un utilisateur.

Les derniers messages authentifiés [xx] envoyés sont éligibles pour rappel.

MDaemon se souvient de l'ID et de l'emplacement d'un nombre spécifié des derniers e-mails envoyés par les utilisateurs authentifiés. Les tentatives échouées si le message rappelé ne fait pas partie de ce groupe de messages. Par conséquent, lorsque l'on utilise l' option*Supprimer les messages rappelés des dossiers de messagerie compte* ci-dessus, il est possible de rappeler des messages directement à partir des boîtes aux lettres de l'utilisateur, même après qu'ils ont été livrés. Non (Paramètres par défaut), cette option est fixée à 1000 messages.

Distribution différée

L'option Distribution différée autorise les clients authentifiés à envoyer des messages qui seront distribués à une date et une heure programmées. Le webmail inclut cette option, permettant aux utilisateurs de cliquer sur "Envoyer plus tard" et de spécifier la date et l'heure d'envoi du message. Le message comprend l'en-têteDistribution différée contenant la date et l'heure de la tentative de remise du message. Si l'option Rappel de message est activée et qu'une demande de rappel est reçue pour un message dont la distribution est différée, MDaemon tentera de supprimer le message rappelé.

Activer la distribution différée

Activer cette option si vous souhaitez permettre aux clients authentifiés d'utiliser l' en-tête Distribution différée pour programmer la distribution différée des messages. Dans le cas où cette option est activée, les utilisateurs du Webmail disposeront de l'option**Envoyer plus tard** dans les thèmes WorldClient et Lookout. L'option est désactivée par défaut.

Remplacer 'Date:' par la date à laquelle le message est distribué

Activez cette option si vous souhaitez remplacer l'en-tête 'Date:' par la date et l'heure actuelles lorsqu'un message est libéré de la File Distribution Différée. Cette option est désactivée par défaut.

3.1.6 Authentification de l'hôte

Server Settings - Host Authentication	
 Server Settings - Host Authentication Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging 	Host Authentication Host Authentication Logon and password, and port values for use when sending mail. Logon and passwords are not shown here. This uses host names (not IPs). To edit an entry remove and recreate it.
	Host Add AUTH Logon AUTH Password Port 0 (0 = use system default)

Authentification de l'hôte

Cet écran permet de configurer les valeurs de connexion, de mot de passe et de port pour n'importe quel hôte. Lorsque MDaemon envoie du courrier SMTP à cet hôte, les informations d'identification associées sont utilisées. Notez que ces informations d'identification sont une solution de repli et ne sont utilisées que lorsque des informations d'identification plus spécifiques à une tâche ne sont pas disponibles. Exemple : si vous configurez des paramètres de connexion et de mot de passe pour les options de transfert de l'Éditeur de comptes ou les options de mise en file d'attente du Gestionnaire de comptes, ou tout autre paramètre spécifique à une tâche, ces informations d'identification sont utilisées et remplacent toutes les informations configurées ici. Cette fonction ne fonctionne qu'avec les noms d'hôte (pas avec les adresses IP).

3.1.7 Courrier prioritaire

🧐 Server Settings - Priority Mail	
 Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging 	Priority mail is delivered immediately regardless of any existing delivery schedule and is defined as mail with any of the header/value combinations specified below.
	Value Add Exceptions
	Ok Cancel Apply Help

L'écran Courrier prioritaire est accessible à partir de la sélection de menu "Setup | Serveur Paramètres de serveur | Courrier prioritaire". Il permet de définir ce qui constitue le Courrier prioritaire sur votre système. Le Courrier prioritaire est distribué immédiatement par MDaemon, indépendamment des intervalles de traitement du courrier programmés. Lorsqu'un nouveau message arrive, MDaemon inspecte ses en-têtes à la recherche d'un ensemble de combinaisons en-tête/valeur que vous avez spécifiées dans cette boîte de dialogue. Si c'est le cas, il considère le message comme hautement prioritaire et tente de le distribuer immédiatement.

Moteur de courrier prioritaire

Activer le moteur de vérification du courrier prioritaire

Cochez cette case pour activer la fonctionnalité Courrier prioritaire. MDaemon inspectera les messages entrants pour déterminer leur statut de priorité.

En-tête From: : TO

Dans ce champ, entrez l'en-tête du message. N'incluez pas les deux-points de fin.

Valeur

Dans ce champ, entrez la valeur qui doit se trouver dans l'en-tête spécifié pour que le message soit considéré comme hautement prioritaire.

Activer l'option même si la valeur est une sous-chaîne

Lors de la saisie d'un nouveau paramètre de Courrier prioritaire, vous pouvez sélectionner cette fonction pour activer la correspondance prioritaire d'une partie (ou d'une sous-chaîne) d'une valeur dans l'en-tête. Exemple : vous pouvez créer un paramètre de Courrier prioritaire pour l'en-tête"À" avec la valeur "Boss". Ainsi, tout courriel contenant "Boss@anything" dans l'en-tête sera considéré comme du Courrier prioritaire. Si une entrée est créée sans que cette fonction soit activée, la valeur de l'en-tête doit correspondre exactement à l'entrée ; la correspondance d'une partie seulement ne suffira pas.

Ajouter

Après avoir saisi les informations En-tête/Valeur dans les zones de texte spécifiées, et après avoir spécifié si cette entrée s'appliquera aux sous-chaînes, cliquez sur le bouton*Ajouter* pour créer la nouvelle entrée Courrier prioritaire.

Supprimer

Cliquez sur ce bouton pour supprimer une entrée sélectionnée dans la fenêtre *Paramètres actuels du Courrier prioritaire.*

Exceptions

Cette option vous permet de définir des combinaisons champ/valeur qui feront qu'un message sera considéré comme une exception aux paramètres du Courrier prioritaire. Vous disposez ainsi d'un contrôle plus souple sur cette fonction.

3.1.8 Conversion d'en-tête

126

Server Settings - Header Translation	
 Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging 	Header translation replaces text within the headers of outbound messages sent from local accounts. All headers are searched and each occurrence of the specified text is replaced. Header Translation Remove Exceptions Exceptions Existing header text New header text Add
	Translate headers in forwarded messages Translate headers in gateway messages forwarded to host or IP Ok Cancel Apply Help

La fonction de Conversion d'en-tête permet de remplacer toute portion de texte trouvée dans un en-tête par une nouvelle valeur chaque fois qu'est détecté un message qui doit quitter votre domaine à destination d'un hôte distant. Vous devez spécifier le Texte à rechercher et la valeur de remplacement correspondante. MDaemon cherchera alors dans tous les en-têtes du message et effectuera les remplacements. Vous pouvez également spécifier des en-têtes que MDaemon **ne**doit **pas** modifier (comme les en-têtes "Subject :" ou "Received :") en cliquant sur le bouton*Exceptions* de cette boîte de dialogue.

Cette fonctionnalité est nécessaire pour certaines configurations de MDaemon dans lesquelles le nom de domaine local est fictif ou différent du nom de domaine qui doit apparaître sur le Courrier sortant. Dans ce cas, la Conversion d'en-tête peut être utilisée pour remplacer chaque occurrence de "@localdomain" par "@RemoteDomain".

Conversion d'en-tête TO :

Cette liste contient les portions de texte que MDaemon recherchera dans les en-têtes des messages sortants, ainsi que le texte qui sera substitué en cas de correspondance.

Supprimer

Sélectionnez une entrée dans la liste Conversion d'en-tête actuelle, puis cliquez sur ce bouton pour la supprimer de la liste.

Exceptions

Cliquez sur ce bouton pour ouvrir la boîte de dialogue<u>Exceptions de conversion en-</u> <u>tête</u> 127]. Cette boîte de dialogue permet de spécifier les en-têtes qui ne doivent pas être pris en compte dans le processus de conversion d'en-tête.

Texte d'en-tête existant : Ce texte en-tête TO

Remplacer le texte dans l'en-tête d'un message sortant.

Nouveau texte d'en-tête From : Ce texte sera substitué au texte d'en-tête existant.

Ce texte remplacera celui que vous avez indiqué dans le champEn-tête existant.

Ajouter

Cliquez sur ce bouton pour ajouter les paramètres de texte ci-dessus à la liste*Conversion d'en-tête*.

Convertir les en-têtes des messages transférés

Cochez cette case pour que les conversions d'en-têtes s'appliquent également aux messages transférés automatiquement d'un domaine local à un domaine non local.

Convertir les en-têtes des messages de passerelle transférés à un hôte ou une IP Cochez cette case si vous voulez que les en-têtes soient traduits dans le courrier de la passerelle transféré vers un domaine. Pour plus d'informations, voir l' écran<u>Redirection</u> [274] de l'éditeur de passerelle.

3.1.8.1 Exceptions de la conversion d'en-tête

Exceptions	×
Ne pas convertir ces en-	êtes
En-tête	Ajouter
En-têtes non convertis—	
RECEIVED: SUBJECT: X-MS-TNEF-Co	Supprimer
	OK Annuler

Ne pas convertir les valeurs dans ces en-têtes

Valeur d'en-tête From: : Dans l'en-tête FROM: :.

Saisissez tout en-tête que vous souhaitez omettre dans le processus de<u>Conversion</u> <u>d'en-tête : FROM</u> [126].

Ajouter

Cliquez sur ce bouton pour ajouter un nouvel en-tête à la liste.

Excepté ces en-têtes From : TO : MDaemon n'analysera pas ces en-têtes.

MDaemon n'analysera pas ces en-têtes lorsqu'il remplacera le Texte d'en-tête.

Supprimer

Sélectionnez un en-tête dans la liste et cliquez sur ce bouton pour le supprimer.

3.1.9 Archivage

	Archive to Folder
	Boot archive mail folder:
⊞ DNS & IPs	
Domain Sharing	TWDT-MIKE (MD aemon varchives \E mail\ Browse
Public & Shared Folders	Archive inbound mailarchive based on recipient address
Message Recall	Archive outbound mailarchive based on sender address
Host Autnentication Priority Mail	Provide separate archives for each MD aemon domain
Header Translation <mark>Archiving</mark> Pruning	Send copies of all inbound and outbound mail to these addresses:
Signatures	Separate multiple email addresses with a comma character.
🗄 - RAS	Include local mailing list messages
🛓 Logging	Include MultiPOP collected messages
	Insert "(Archive Copy)" into message Subject header
	Archive Settings
	Archive encrypted messages in decrypted (readable) form
	Archive public folder submissions
	Archive span messages
	Archive forwarded messages (requires content filter processing)
	Improve server performance, protect against lost data, and save on storage space using a fully featured email archiving product. Visit the Email Archiving page to learn more.

Cette fonction permet d'archiver tous les messages entrants ou sortants dans un dossier. L'emplacement par défaut de ce dossier est C:MDaemon\Archives\Email\, mais vous pouvez le définir dans le dossier de votre choix. Vous pouvez choisir d'archiver les messages entrants adressés à vos utilisateurs locaux, les messages sortants de vos utilisateurs locaux ou les deux. Les listes de diffusion, les messages relayés, les messages de niveau système et les répondeurs automatiques ne sont jamais archivés. Il en va de même pour les messages de spam ou les messages contenant des virus.

Les messages entrants et sortants seront stockés respectivement dans les sousdossiers NInN et NOutN. Ils peuvent être subdivisés en utilisant les options ... selon l'adresse du destinataire et ... selon l'adresse de l'expéditeur ci-dessous. Il est également possible de créer des archives distinctes pour chaque domaine en utilisant l' option*Créer des archives distinctes pour chaque domaine MDaemon.*

Les messages archivés sont sauvegardés dans l'état final dans lequel ils apparaissent dans le Dossier courrier de l'utilisateur local, ou dans l'état " prêt à être distribué " pour les messages sortants. Cela signifie que si, par exemple, vous demandez au filtre de contenu d'apporter une modification à un message, telle que l'ajout d'un en-tête, le message archivé contiendra cette modification.

Pour parcourir le dossier d'archivage, utilisez l'un de vos comptes de messagerie (ou créez-en un nouveau) et faites pointer son <u>Dossier courrier</u> [766] sur le même dossier que celui utilisé pour l'archivage. Si plusieurs personnes doivent avoir accès à l'archive, connectez-vous au compte d'archivage et <u>partagez</u> [766] les dossiers souhaités à l'aide de la <u>Liste de contrôle d'accès</u> [327].

Il existe une file d'attente cachée, située à l'adresse suivante

:"\MDaemon\Queuesues\ToArchive\". Cette file d'attente est vérifiée à intervalles réguliers pour les messages qui y ont été placés manuellement, par un plugin ou autrement. Lorsqu'un message y est trouvé, il est immédiatement archivé et supprimé. Si des messages non éligibles à l'archivage sont trouvés, ils sont alors simplement supprimés. L'écran/le journal de Routage affichera des détails chaque fois qu'un message est archivé avec succès.

Archivage dans un dossier

Désignez ici votre Dossier Archivage dans courrier :. Par défaut, il est défini sur C:MDaemon\Archives\Email\, mais vous pouvez le définir sur n'importe quel dossier de votre choix.

Archiver le courrier entrant

Cochez cette case pour enregistrer une copie de tous les messages destinés à un utilisateur local. Les messages de listes de diffusion et les messages contenant un virus ne sont pas archivés. Voir relnotes txt.

... selon l'adresse du destinataire

Cliquez sur cette option si vous souhaitez que l'archive du courrier entrant soit classée en fonction de l'adresse électronique dudestinataire.

Archiver le courrier sortant

Cochez cette case pour enregistrer une copie de tous les messages provenant d'un utilisateur local. Les messages de listes de diffusion et les messages contenant un virus ne sont pas archivés. Voirnotes relnotes.

... selon l'adresse de l'expéditeur

Cliquez sur cette option si vous souhaitez que l'archive du courrier sortant soit classée en fonction de l'adresse e-mail de l'expéditeur.

Créer des archives distinctes pour chaque domaine MDaemon

Cliquez sur cette option si vous souhaitez conserver des archives distinctes pour chaque domaine.

Liste des exceptions

Cliquez sur ce bouton pour ouvrir la liste Exceptions de l'archivage. Vous pouvez y répertorier les adresses "à" et "de" que vous souhaitez exempter de l'archivage.

Envoyer des copies de tous les messages entrants et sortants à ces adresses

Saisissez une ou plusieurs adresses auxquelles vous souhaitez envoyer des messages d'archivage. Les adresses multiples doivent être séparées par une virgule. Vous pouvez spécifier des adresses locales et distantes, ainsi que des alias d'adresses.

Inclure les messages locaux de listes de diffusion

Lorsque cette option est activée, des copies des messages de la Liste liste de diffusion locale seront également envoyées à ces adresses.

Inclure les messages collectés par MultiPOP

Activez cette option si vous souhaitez envoyer des messages collectés via la fonctionnalité MultiPOP deMDaemon.

Insérer "(Copie d'archive)" dans l'objet du message

Dans cette option, " (Copie d'archive) " sera inséré dans l'objet : de l'en-tête des messages envoyés.

Paramètres d'archivage

Archiver les messages chiffrés sous forme déchiffrée (lisible)

Non (par défaut), les copies non chiffrées des messages chiffrés sont stockées dans l'archive. Si, toutefois, un message ne peut pas être décrypté, la forme cryptée sera stockée à la place. Désactivez cette option si vous préférez stocker les versions cryptées même lorsque le décryptage est possible.

Archiver les envois aux dossiers publics

Par défaut, les messages envoyés aux dossiers publics sont archivés. Désactivez cette option si vous ne souhaitez pas archiver ces messages.

Archiver les spams

Activez cette option si vous souhaitez que les archives et les copies envoyées incluent les messages marqués comme spams.

Archiver les messages transférés

Activez cette option si vous souhaitez que les archives et les copies envoyées incluent les messages transférés. Par défaut, ces messages ne sont pas archivés.

3.1.10 Nettoyage

Nettoyage des dossiers publics

Supprimer les messages de plus de [xx] jours (0 = jamais)

Spécifiez un nombre de jours dans cette option si vous souhaitez que les anciens messages soient supprimés des <u>Dossiers publics</u> [116].

Nettoyage du Filtre Antivirus de contenu - de l'antivirus

Supprimer les fichiers en quarantaine

Cliquez sur cette option si vous souhaitez que toutes les pièces jointes en quarantaine soient supprimées chaque nuit.

...mais seulement s'ils sont plus anciens que ce nombre de jours [xx] (0 = tous les fichiers)

Non (par défaut) les fichiers en quarantaine seront tous supprimés. Spécifiez un nombre de jours dans cette option si vous ne souhaitez supprimer que les fichiers dont l'ancienneté est supérieure à cette valeur.

Supprimer les messages en quarantaine

Cliquez sur cette option si vous souhaitez que tous les messages en quarantaine soient supprimés chaque nuit.

...mais seulement s'ils sont plus anciens que ce nombre de jours [xx] (0 = tout) Par défaut, tous les messages en guarantaine seront supprimés. Spécifiez un

nombre de jours dans cette option si vous souhaitez uniquement supprimer les messages plus anciens que cette valeur.

Supprimer les pièces jointes bloquées

Cliquez sur cette option si vous souhaitez que toutes les pièces jointes interdites soient supprimées chaque nuit.

...mais seulement si elles sont plus anciennes que ce nombre de jours [xx] (0 = tout) Non (par défaut) les pièces jointes interdites seront supprimées. Spécifiez un nombre de jours dans cette option si vous souhaitez supprimer uniquement les pièces jointes interdites plus anciennes que cette valeur.

3.1.11 Signatures

3.1.11.1 Signatures par défaut

🧐 Server Settings - Default Signatures	
 Server Settings - Default Signatures Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures 	A domain signature is a block of text which MDaemon will append to all messages sent by users of a particular domain. Each domain can have its own signature. Domains without their own signature will have the default signatures appended. Plain text signature:
Default Signatures	<
DomainPOP	
KAS inclosed	HTML signature (cut-and-paste from your favorite HTML editor): Note: (BDDY) (HTML), and their closing tags will be removed
i i i i i i i i i i i i i i i i i i i	Plain text signature will be created from HTML when only HTML is given.
	< > ×
	Ok Cancel Apply Help

Utilisez cet écran pour ajouter une signature à tous les messages envoyés par les utilisateurs de MDaemon. Utilisez l'écran <u>Signatures</u> [210] du Gestionnaire de domaines si vous souhaitez utiliser des signatures différentes pour les utilisateurs de domaines spécifiques - lorsqu'une signature spécifique à un domaine existe, elle sera utilisée à la place de la Signature par défaut. Les signatures sont ajoutées au bas des messages, sauf pour les messages de listes de diffusion utilisant un <u>pied de page</u> [311], auquel cas le

pied de page est ajouté sous la signature. Vous pouvez également utiliser la fonction<u>Signature de</u> a) l'éditeur de compte pour ajouter des signatures individuelles pour chaque compte. Les signatures de compte sont ajoutées juste avant les Signatures par défaut ou Domaine - Domaine.

Signature en texte brut

Cette zone permet d'insérer une signature en texte brut. Si vous souhaitez désigner une signature html correspondante à utiliser dans la partie texte/html des messages multipartites, utilisez la zone de*signature HTML* ci-dessous. Si une signature est incluse dans les deux zones, MDaemon utilisera la signature appropriée pour chaque partie du message multipart. Si aucune signature HTML n'est spécifiée, la signature en texte brut sera utilisée dans les deux parties.

Signature HTML (copier-coller à partir de votre éditeur HTML préféré)

Dans cette zone, vous pouvez insérer une signature HTML à utiliser dans la partie texte/html des messages multipartites. Si une signature est incluse ici et dans la zone*Signature en texte brut* ci-dessus, MDaemon utilisera la signature appropriée pour chaque partie du message multipart. Si aucune signature en texte brut n'est spécifiée, la signature html sera utilisée pour en créer une.

Pour créer votre signature html, saisissez le code html manuellement ou copiez-collez-le directement à partir de votre éditeur HTML préféré. Si vous souhaitez inclure des images en ligne dans votre signature HTML, vous pouvez le faire en utilisant la macro\$ATTACH INLINE:path to image file\$.

Exemple :

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
\Nimages\r t and arnold.jpg$">
```

Il existe également plusieurs façons d'insérer des images en ligne dans les signatures à partir de MDaemon. dans les signatures à partir de l'interface web de l'<u>Administration</u> <u>Remote Admin de</u> MDaemon :

- Dans l'écran Signatures par défaut dans l'administration à distance, cliquez sur le bouton "Image" de la barre d'outils de l'éditeur HTML et sélectionnez l'onglet upload.
- Dans l'écran Dans l'écran Signatures par défaut de l'administration à distance, cliquez sur le bouton "Ajouter une image" de la barre d'outils de l'éditeur HTML.
- Glissez-déposez une image dans la barre d'outils HTML de l'écran Signatures par défaut de l'administration à distance. l'éditeur HTML de l'écran Signatures par défaut avec Chrome, FireFox, Safari ou MSIE 10+.
- Copier et coller une image du presse-papiers dans l'éditeur HTML de l'écran Signatures par défaut. Non (par défaut) par défaut dans l'éditeur HTML de l'écran Signatures par défaut avec Chrome, FireFox, Safari ou MSIE 11+.



Les balises <body></body> et <html></html> ne sont pas autorisées dans les signatures et seront supprimées lorsqu'elles seront trouvées.

Macros de signature

Les signatures MDaemon prennent en charge les macros qui insèrent dans la signature les Informations de contact de l'expéditeur, extraites du contact de l'expéditeur situé dans le Dossier public de son domaine. Cela permet de personnaliser les signatures par défaut et par domaine avec les informations de l'expéditeur. Par exemple, \$CONTACTFULLNAME\$ insère le nom complet de l'expéditeur et \$CONTACTEMAILADDRESS\$ insère l'adresse électronique de l'expéditeur. Utilisez Webmail, MDaemon Connector ou ActiveSync pour modifier les contacts publics. Des valeurs vides sont utilisées si aucun contact n'existe pour l'expéditeur. Les macros disponibles sont listées ci-dessous.

Les utilisateurs peuvent contrôler l'emplacement des signatures MDaemon dans leurs courriers électroniques en plaçant l'une des macros**du Sélecteur de signature** dans un message, à l'endroit où ils souhaitent que la signature apparaisse.

Sélecteur de signature	
\$SYSTEMSIGNATURE\$	Place la <u>Signature par défaut</u> [132] ou la <u>Signature du</u> <u>domaine</u> [210] dans un message. Si les deux existent, c'est la signature de domaine qui est utilisée.
SIGNATURE DU CLIENT	Place la <u>Signature client par défaut</u> [138] ou la <u>Signature client par domaine dans</u> [216] un message. Si les deux existent, c'est la Signature client du domaine qui est utilisée.
\$ACCOUNTSIGNATURE\$	Place la <u>signature du compte</u> l ^{®7} l dans le message.
Par noms et identifiants	
Votre nom complet	\$CONTACTFULLNAME\$\$ (NOM DE LA PERSONNE À CONTACTER)
Votre nom	\$CONTACTFIRSTNAME\$ (PRÉNOM DU CONTACT)
Deuxième prénom	\$CONTACTMIDDLENAME\$,
Votre nom	NOM DE FAMILLE \$CONTACTLASTNAME\$
Titre	TITRE \$CONTACTTITLE
Suffixe	SUFFIXE \$CONTACTSUFFIX\$
Surnom	NOM DE FAMILLE DU CONTACT
Votre nom	PRÉNOM DE YOMI \$CONTACTYOMIFIRSTNAME

Votre nom\$ \$contactyomifirstname\$ \$contactyomilastname	NOM DE FAMILLE \$CONTACTYOMILASTNAME\$
Nom du compte	NOM DU COMPTE \$CONTACTACCOUNTNAME\$
ID du client	\$CONTACTCUSTOMERID\$ (IDENTIFIANT DU CLIENT)
Identifiant du gouvernement	ID DU GOUVERNEMENT \$CONTACTGOVERNMENTID
Fichier comme	FICHIER EN TANT QUE \$CONTACTFILEAS\$
Adresses électroniques	
Adresse électronique	ADRESSE ÉLECTRONIQUE \$CONTACTEMAILADDRESS
Cette adresse électronique [2	ADRESSE DE COURRIEL 2\$ \$CONTACTEMAILADDRESS2
Cette adresse électronique 3	\$CONTACTEMAILADDRESS3\$ (ADRESSE DE COURRIER ÉLECTRONIQUE)
Numéros de téléphone et de fax	
Téléphone portable	TÉLÉPHONE PORTABLE \$CONTACTHOMEMOBILE
Téléphone portable 2	\$CONTACTMOBILE2
Téléphone de voiture	\$CONTACTNUMÉRODEVOITURE
Téléphone fixe	\$CONTACT TÉLÉPHONE DOMICILE
Téléphone fixe 2	\$CONTACTHOMEPHONE2\$ \$CONTACTHOMEPHONE3\$ \$CONTACTHOMEPHONE4
Fax à domicile	\$CONTACTHOMEFAX
Autre téléphone	\$CONTACTAUTRETÉLÉPHONE
Messagerie instantanée et Web	
Adresse IM	ADRESSE DE MESSAGERIE INSTANTANÉE \$CONTACTTIMADDRESS
Adresse de messagerie instantanée 2	ADRESSE DE MESSAGERIE INSTANTANÉE 2\$ \$CONTACTIMADDRESS2
Adresse IM 3	\$CONTACTIMADDRESS3
Adresse MMS	ADRESSE MMS\$ \$CONTACTMMSADDRESS
Adresse web du domicile	ADRESSE WEB DU DOMICILE \$CONTACTHOMEWEBADDRESS

Adresse de la maison		
Adresse du domicile	\$CONTACTHOMEADDRESS	
Ville du domicile	\$CONTACTHOMECITY\$	
État du domicile	ÉTAT DU DOMICILE \$CONTACTHOMESTATE	
Code postal du domicile	CODE POSTAL DU DOMICILE \$CONTACTHOMEZIPCODE	
Pays d'origine	PAYS DU DOMICILE \$CONTACTHOMECOUNTRY	
Autre adresse	\$CONTACTAUTREADRESSE	
Autre ville	\$CONTACTOTHERCITY\$ (AUTRE VILLE)	
Autre état	\$CONTACTAUTREÉTAT\$ AUTRE CODE POSTAL	
Autre code postal	\$CONTACTOTHERZIPCODE\$ AUTRE CODE POSTAL	
Autre pays	\$CONTACTOTHERCOUNTRY	
Entreprise		
Nom de l'entreprise	\$CONTACTBUSINESSCOMPANY\$ (EN ANGLAIS)	
Nom de l'entreprise Votre nom	\$CONTACTYOMICOMPANYNAME\$ (NOM DE L'ENTREPRISE)	
Titre de l'entreprise	TITRE DE L'ENTREPRISE \$CONTACTBUSINESSTITLE	
Bureau de l'entreprise	BUREAU DE L'ENTREPRISE \$CONTACTBUSINESSOFFICE\$	
Département de l'entreprise	DÉPARTEMENT DE L'ENTREPRISE \$CONTACTBUSINESSDEPARTMENT	
Chef d'entreprise	CONTACT MANAGER D'ENTREPRISE \$CONTACTBUSINESSMANAGER	
Assistant(e) commercial(e)	ASSISTANT COMMERCIAL \$CONTACTBUSINESSASSISTANT	
Téléphone de l'assistant commercial	TÉLÉPHONE DE L'ASSISTANT D'AFFAIRES \$CONTACTBUSINESSASSISTANT\$	
Téléphone principal de l'entreprise	TÉLÉPHONE PRINCIPAL DE L'ENTREPRISE \$CONTACTBUSINESSMAINPHONE\$	
Téléphone de l'entreprise	TÉLÉPHONE PRINCIPAL \$CONTACTBUSINESSMAINPHONE\$ TÉLÉPHONE PROFESSIONNEL \$CONTACTBUSINESSMAINPHONE\$ TÉLÉPHONE PROFESSIONNEL \$CONTACTBUSINESSMAINPHONE	

Téléphone professionnel 2	TÉLÉPHONE PROFESSIONNEL 2\$ \$CONTACTBUSINESSPHONE2	
Téléphone IP professionnel	TÉLÉPHONE IP PROFESSIONNEL \$CONTACTBUSINESSIPPHONE	
Fax professionnel	FAX PROFESSIONNEL \$CONTACTBUSINESSFAX	
Téléavertisseur professionnel	TÉLÉAVERTISSEUR D'ENTREPRISE \$CONTACTBUSINESSPAGER	
Radio professionnelle	RADIO PROFESSIONNELLE \$CONTACTBUSINESSRADIO\$	
Adresse professionnelle	ADRESSE DE L'ENTREPRISE \$CONTACTBUSINESSADDRESS	
Ville de l'entreprise	VILLE DE L'ENTREPRISE \$CONTACTBUSINESSCITY	
État de l'entreprise	ÉTAT DE L'ENTREPRISE \$CONTACTBUSINESSSTATE\$	
Code postal de l'entreprise	CODE POSTAL DE L'ENTREPRISE \$CONTACTBUSINESSZIPCODE\$	
Pays de l'entreprise	PAYS DE L'ENTREPRISE \$CONTACTBUSINESSCOUNTRY	
Adresse web de l'entreprise	ADRESSE WEB DE L'ENTREPRISE \$CONTACTBUSINESSWEBADDRESS	
Autre		
Conjoint	\$CONTACTCONJOINT\$	
Enfants	\$CONTACTENFANTS\$	
Catégories	CATÉGORIES\$ DE CONTACT	
Commentaire	COMMENTAIRE\$CONTACT	

Voir :

<u>Gestionnaire de domaines | Signatures</u> 210 <u>Mon compte | Signature</u> ଛମ

3.1.11.2 Signatures client par défaut

Server Settings - Default Client Signatures	
Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall	This signature can be pushed to Webmail and MDaemon Connector. In Webmail it's called the "System" signature. Each domain can have its own signature. Domains without their own signature will use the default signature. Plain text signature:
Host Authentication Priority Mail Header Translation Archiving Pruning Funing Signatures	\$CONTACTFULLNAME\$ \$CONTACTEMAILADDRESS\$
Default Signatures Default Client Signatures Default Client Signatures PomainPOP RAS Dogging	HTML signature (cut-and-paste from your favorite HTML editor): Note: <bddy>, <html>, and their closing tags will be removed. Plain text signature will be created from HTML when only HTML is given.</html></bddy>
	< >
	Ok Cancel Apply Help

Utilisez cet écran pour créer une signature client par défaut que vous pouvez envoyer vers MDaemon Webmail [365] et MDaemon Connector [428], et qui sera utilisée par vos utilisateurs lors de la rédaction de messages électroniques. Vous pouvez utiliser les <u>macros</u> [139] listées ci-dessous pour personnaliser la signature, afin qu'elle soit unique pour chaque utilisateur, en incluant des éléments tels que le nom de l'utilisateur, son adresse e-mail, son numéro de téléphone, etc. Utilisez l' écran <u>Signatures clients</u> [216] dans le Gestionnaire de domaines si vous souhaitez utiliser une signature différente pour les utilisateurs de domaines spécifiques. Lorsqu'une signature spécifique à un domaine existe, elle sera utilisée à la place de la Signature client par défaut. Utilisez l'option <u>Transmettre</u> [366] la signature client si vous souhaitez transmettre la signature client à Webmail et l' option<u>Transmettre la signature client à Outlook</u> [428] si vous souhaitez la transmettre à MDaemon Connector. Dans les options de composition de Webmail, la signature client transmise est appelée "Système". Pour MDaemon Connector, vous pouvez désigner un nom pour la signature qui apparaîtra dans Outlook.

Signature en texte clair

Cette zone permet d'insérer une signature en texte brut. Si vous souhaitez désigner une signature html correspondante à utiliser dans la partie text/html des messages multipart, utilisez la zone de*signature HTML* ci-dessous. Si une signature est incluse dans les deux zones, MDaemon utilisera la signature appropriée pour chaque partie du message multipart. Si aucune signature HTML n'est spécifiée, la signature en texte brut sera utilisée dans les deux parties.

Signature HTML (copier-coller à partir de votre éditeur HTML préféré)

Dans cette zone, vous pouvez insérer une signature HTML à utiliser dans la partie texte/html des messages multipartites. Si une signature est incluse à la fois dans cette zone et dans la zone de*signature en texte brut* ci-dessus, MDaemon utilisera la signature appropriée pour chaque partie du message multipart. Si aucune signature en texte brut n'est spécifiée, la signature html sera utilisée pour en créer une.

Pour créer votre signature html, saisissez le code html manuellement ou copiez-collez-le directement à partir de votre éditeur HTML préféré. Si vous souhaitez inclure des images en ligne dans votre signature HTML, vous pouvez le faire en utilisant la macro\$ATTACH_INLINE:path_to_image_file\$.

Exemple :

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
\images\mr t and arnold.jpg$">
```

Il existe également plusieurs façons d'insérer des images en ligne dans les signatures à partir de l'interface web d'<u>Administration de articles</u> MDaemon <u>Remote Admin : articles</u>

- Dans l'écran Signature client par défaut de MDaemon Remote Admin, cliquez sur le bouton "Image" de la barre d'outils de l'éditeur HTML et sélectionnez l'onglet upload.
- Dans l'écran Signature client par défaut de l'administration à distance, cliquez sur le bouton "Ajouter une image" de l'éditeur HTML.
- Glisser-déposer une image dans l'éditeur HTML de l'écran Signatures client défaut avec Chrome, FireFox, Safari ou MSIE 10+.
- Copier et coller une image du presse-papiers dans l'éditeur HTMLde l'écran Signatures client par défaut avec Chrome, FireFox, MSIE 11+.



Les balises <body></body> et <html></html> ne sont pas autorisées dans les signatures et seront supprimées lorsqu'elles seront trouvées.

Macros de signature

Les signatures MDaemon prennent en charge les macros qui insèrent dans la signature les Informations de contact de l'expéditeur, extraites du contact de l'expéditeur situé dans le Dossier public de son domaine. Cela permet de personnaliser les signatures par défaut et par domaine avec les informations de l'expéditeur. Par exemple, \$CONTACTFULLNAME\$ insère le nom complet de l'expéditeur et \$CONTACTEMAILADDRESS\$ insère l'adresse électronique de l'expéditeur. Utilisez Webmail, MDaemon Connector ou ActiveSync pour modifier les contacts publics. Des valeurs vides sont utilisées si aucun contact n'existe pour l'expéditeur. Les macros disponibles sont listées ci-dessous.

Les utilisateurs peuvent contrôler l'emplacement des signatures MDaemon dans leurs

courriers électroniques en plaçant l'une des macros**du Sélecteur de signature** dans un message, à l'endroit où ils souhaitent que la signature apparaisse.

Sélecteur de signature	
\$SYSTEMSIGNATURE\$	Place la <u>Signature par défaut (132</u>) ou la <u>Signature du</u> <u>domaine (210)</u> dans un message. Si les deux existent, c'est la signature de domaine qui est utilisée.
SIGNATURE DU CLIENT	Place la <u>Signature client par défaut</u> [138] ou la <u>Signature client par domaine dans</u> [216] un message. Si les deux existent, c'est la Signature client du domaine qui est utilisée.
\$ACCOUNTSIGNATURE\$	Place la <u>signature du compte</u> 1007 dans le message.
Par noms et identifiants	
Votre nom complet	\$CONTACTFULLNAME\$\$ (NOM DE LA PERSONNE À CONTACTER)
Votre nom	\$CONTACTFIRSTNAME\$ (PRÉNOM DU CONTACT)
Deuxième prénom	\$CONTACTMIDDLENAME\$,
Votre nom	NOM DE FAMILLE \$CONTACTLASTNAME\$
Titre	TITRE \$CONTACTTITLE
Suffixe	SUFFIXE \$CONTACTSUFFIX\$
Surnom	NOM DE FAMILLE DU CONTACT
Votre nom	PRÉNOM DE YOMI \$CONTACTYOMIFIRSTNAME
Votre nom\$ \$contactyomifirstname\$ \$contactyomilastname	NOM DE FAMILLE \$CONTACTYOMILASTNAME\$
Nom du compte	NOM DU COMPTE \$CONTACTACCOUNTNAME\$
ID du client	\$CONTACTCUSTOMERID\$ (IDENTIFIANT DU CLIENT)
Identifiant du gouvernement	ID DU GOUVERNEMENT \$CONTACTGOVERNMENTID
Fichier comme	FICHIER EN TANT QUE \$CONTACTFILEAS\$
Adresses électroniques	
Adresse électronique	ADRESSE ÉLECTRONIQUE \$CONTACTEMAILADDRESS
Cette adresse électronique [2	ADRESSE DE COURRIEL 2\$ \$CONTACTEMAILADDRESS2

Cette adresse électronique 3	\$CONTACTEMAILADDRESS3\$ (ADRESSE DE COURRIER ÉLECTRONIQUE)	
Numéros de téléphone et de	fax	
Téléphone portable	TÉLÉPHONE PORTABLE \$CONTACTHOMEMOBILE	
Téléphone portable 2	\$CONTACTMOBILE2	
Téléphone de voiture	\$CONTACTNUMÉRODEVOITURE	
Téléphone fixe	\$CONTACT TÉLÉPHONE DOMICILE	
Téléphone fixe 2	\$CONTACTHOMEPHONE2\$ \$CONTACTHOMEPHONE3\$ \$CONTACTHOMEPHONE4	
Fax à domicile	\$CONTACTHOMEFAX	
Autre téléphone	\$CONTACTAUTRETÉLÉPHONE	
Messagerie instantanée et Web		
Adresse IM	ADRESSE DE MESSAGERIE INSTANTANÉE \$CONTACTTIMADDRESS	
Adresse de messagerie instantanée 2	ADRESSE DE MESSAGERIE INSTANTANÉE 2\$ \$CONTACTIMADDRESS2	
Adresse IM 3	\$CONTACTIMADDRESS3	
Adresse MMS	ADRESSE MMS\$ \$CONTACTMMSADDRESS	
Adresse web du domicile	ADRESSE WEB DU DOMICILE \$CONTACTHOMEWEBADDRESS	
Adresse de la maison		
Adresse du domicile	\$CONTACTHOMEADDRESS	
Ville du domicile	\$CONTACTHOMECITY\$	
État du domicile	ÉTAT DU DOMICILE \$CONTACTHOMESTATE	
Code postal du domicile	CODE POSTAL DU DOMICILE \$CONTACTHOMEZIPCODE	
Pays d'origine	PAYS DU DOMICILE \$CONTACTHOMECOUNTRY	
Autre adresse	\$CONTACTAUTREADRESSE	
Autre ville	\$CONTACTOTHERCITY\$ (AUTRE VILLE)	
Autre état	\$CONTACTAUTREÉTAT\$ AUTRE CODE POSTAL	
Autre code postal	\$CONTACTOTHERZIPCODE\$ AUTRE CODE POSTAL	

Autre pays	\$CONTACTOTHERCOUNTRY
Entreprise	
Nom de l'entreprise	\$CONTACTBUSINESSCOMPANY\$ (EN ANGLAIS)
Nom de l'entreprise Votre nom	\$CONTACTYOMICOMPANYNAME\$ (NOM DE L'ENTREPRISE)
Titre de l'entreprise	TITRE DE L'ENTREPRISE \$CONTACTBUSINESSTITLE
Bureau de l'entreprise	BUREAU DE L'ENTREPRISE \$CONTACTBUSINESSOFFICE\$
Département de l'entreprise	DÉPARTEMENT DE L'ENTREPRISE \$CONTACTBUSINESSDEPARTMENT
Chef d'entreprise	CONTACT MANAGER D'ENTREPRISE \$CONTACTBUSINESSMANAGER
Assistant(e) commercial(e)	ASSISTANT COMMERCIAL \$CONTACTBUSINESSASSISTANT
Téléphone de l'assistant commercial	TÉLÉPHONE DE L'ASSISTANT D'AFFAIRES \$CONTACTBUSINESSASSISTANT\$
Téléphone principal de l'entreprise	TÉLÉPHONE PRINCIPAL DE L'ENTREPRISE \$CONTACTBUSINESSMAINPHONE\$
Téléphone de l'entreprise	TÉLÉPHONE PRINCIPAL \$CONTACTBUSINESSMAINPHONE\$ TÉLÉPHONE PROFESSIONNEL \$CONTACTBUSINESSMAINPHONE\$ TÉLÉPHONE PROFESSIONNEL \$CONTACTBUSINESSMAINPHONE
Téléphone professionnel 2	TÉLÉPHONE PROFESSIONNEL 2\$ \$CONTACTBUSINESSPHONE2
Téléphone IP professionnel	TÉLÉPHONE IP PROFESSIONNEL \$CONTACTBUSINESSIPPHONE
Fax professionnel	FAX PROFESSIONNEL \$CONTACTBUSINESSFAX
Téléavertisseur professionnel	TÉLÉAVERTISSEUR D'ENTREPRISE \$CONTACTBUSINESSPAGER
Radio professionnelle	RADIO PROFESSIONNELLE \$CONTACTBUSINESSRADIO\$
Adresse professionnelle	ADRESSE DE L'ENTREPRISE \$CONTACTBUSINESSADDRESS
Ville de l'entreprise	VILLE DE L'ENTREPRISE \$CONTACTBUSINESSCITY

État de l'entreprise	ÉTAT DE L'ENTREPRISE \$CONTACTBUSINESSSTATE\$
Code postal de l'entreprise	CODE POSTAL DE L'ENTREPRISE \$CONTACTBUSINESSZIPCODE\$
Pays de l'entreprise	PAYS DE L'ENTREPRISE \$CONTACTBUSINESSCOUNTRY
Adresse web de l'entreprise	ADRESSE WEB DE L'ENTREPRISE \$CONTACTBUSINESSWEBADDRESS
Autre	
Conjoint	\$CONTACTCONJOINT\$
Enfants	\$CONTACTENFANTS\$
Catégories	CATÉGORIES\$ DE CONTACT
Commentaire	COMMENTAIRE\$CONTACT

Voir :

Signatures par défaut 132 Gestionnaire de domaines | Signatures 210 Gestionnaire de domaines | Signatures des clients 216 Mon compte | Signature 807 Paramètres de MDaemon Webmail 365 Paramètres du client MC | Signature 428

3.1.12 MultiPOP

🧐 Server Settings - MultiPOP	
 Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures MultiPOP RAS Logging 	☑ Enable MultiPOP MultiPOP collects mail from POP servers and stores it in local mailboxes. ☐ MultiPOP always deletes mail from all servers after collection This option overrides the 'Leave a copy of message on POP3 server' setting for all MultiPOP users. ☑ Send notification email after this many failures 5 Do not notify again for this many days 7 MultiPOP OAuth Register your MD aemon with Google or Microsoft to allow OAuth 2.0 usage when collecting mail from them. Users must authorize their accounts in Webmail, which requires permission to edit MultiPOP settings. Use the Redirect URI when setting up the application. Gmail
	Ok Cancel Apply Help

Activer MultiPOP

Cochez cette case pour activer le serveur MultiPOP. MultiPOP collecte le courrier sur les serveurs POP pour le compte de vos utilisateurs et le stocke dans leurs boîtes locales. La fonction MultiPOP vous permet de créer un nombre illimité de combinaisons hôte/utilisateur/mot de passe POP3 pour la Collecte de courrier en provenance de plusieurs sources. Cette fonction est utile pour les utilisateurs qui possèdent des comptes de messagerie sur plusieurs serveurs, mais qui préfèrent collecter et regrouper tous leurs messages électroniques en un seul endroit. Avant d'être placé dans laboîte aux lettres de l'utilisateur, le courrier collecté par MultiPOP est d'abord placé dans la File locale afin qu'il puisse être traité comme les autres courriers auxquels sont appliqués des répondeurs automatiques et des filtres de contenu. Les options de planification pour MultiPOP se trouvent à l'adresse suivante : Configuration | Programmation d'événements | Programmation du courrier | Collecte MultiPOP 406].

Supprimer le courrier des serveurs après la collecte

Cochez cette case si vous souhaitez ignorer l'option *Laisser une copie du message sur le* serveur POP3 (située sur la page*d*'accueil). *POP3* (située dans l' écran<u>MultiPOP</u> red) de l'Éditeur de compte) pour tous les utilisateurs. Tous les messages seront supprimés de chaque serveur MultiPOP après leur collecte.
Envoyer un e-mail de notification après ce nbre d'échecs

Non (par défaut), MDaemon envoie un e-mail de notification après plusieurs échecs lors de la vérification d'un compte MultiPOP. Comme les échecs temporaires peuvent être fréquents, cette option vous permet de spécifier le nombre d'échecs consécutifs nécessaires pour déclencher la notification, et l'option ci-dessous vous permet de choisir le nombre de jours d'attente entre ces notifications. Le contenu et les destinataires des E-mails de notification peuvent être personnalisés en modifiant le fichier \MDaemon\App\MPOPFailureNotice.dat. Par défaut, les notifications sont envoyées au propriétaire du compte MultiPOP après 5 échecs, au maximum une fois tous les 7 jours.

Ne pas renvoyer de notification pendant (jours)

Par défaut, les notifications d'échec de MultiPOP sont envoyées au maximum une fois tous les sept jours. Utilisez cette option si vous souhaitez modifier cet intervalle.

OAuth pour MultiPOP

OAuth 2.0 est une méthode d'authentification moderne que Gmail et Microsoft (Office) 365 exigent désormais (ou exigeront bientôt), car ils désactivent la prise en charge de l'authentification héritée/de base. Dans le but que la fonctionnalité MultiPOP de MDaemon utilise OAuth 2.0 pour collecter le courrier de Gmail ou d'Office 365 au nom de vos utilisateurs, vous devez enregistrer votre serveur MDaemon auprès de Google ou de Microsoft, respectivement, en créant une application OAuth 2.0 à l'aide de la Console API de Google ou de l'Azure Active Directory de Microsoft. Cette procédure est similaire à celle requise pour utiliser l'<u>Intégration avec Dropbox</u> 352 de MDaemon pour vos utilisateurs de Webmail.

Pour configurer MultiPOP afin de collecter le courrier de Gmail ou de Microsoft (Office) 365 pour vos utilisateurs :

- 1. Activez l' option**Activer MultiPOP** ci-dessus.
- 2. Suivez les instructions ci-dessous pour <u>créer et lier votre application</u> OAuth 46 pour<u>MultiPOP</u> 46 pour Gmail ou Office 365.
- 3. Sur la <u>page MultiPOP de l'éditeur de compte</u>, **Activer MultiPOP** pour chaque utilisateur que vous souhaitez autoriser à utiliser MultiPOP pour récupérer des emails depuis Gmail ou Office 365.
- 4. Ajoutez le compte Gmail (pop.gmail.com:995) ou Office 365 (outlook.office365.com:995) pour chacun des utilisateurs, et activez l 'option Utiliser OAuth. En option, vous pouvez demander à vos utilisateurs d'effectuer eux-mêmes cette étape dans le Webmail 333. Remarque : pour les comptes Gmail, chaque compte Gmail doit être ajouté aux utilisateurs de test dans votre application Gmail OAuth (voir la note sur le statut de publication dans les instructions<u>Création et liaison de votre application OAuth pour</u> <u>MultiPOP</u> 1461 ci-dessous).
- 5. Sur la page<u>Services Web de l'éditeur de compte</u> [771], activez l'option "...modifier les paramètres MultiPOP" pour chacun de ces utilisateurs.
- 6. Chaque utilisateur doit se connecter à Webmail, aller sur sa page **Boîtes aux lettres** sous Options, ajouter son compte Gmail ou Office 365 (si vous ne l'avez

pas déjà fait pour lui), puis cliquer sur **Autoriser** pour se connecter à son compte Gmail ou Office 365 et suivre les étapes pour autoriser MDaemon à collecter son courrier à partir de cet emplacement.

Gmail/Office 365

ID client

Il s'agit de l'ID client unique attribué à votre appli OAuth pour MultiPOP 2.0 lorsque vous la créez dans la console API de Google ou sur le portail Microsoft Azure Active Directory. Après avoir créé votre app, copiez son ID client et collez-le ici.

Code secret client

Il s'agit du Code client unique attribué à votre application OAuth 2.0 MultiPOP lorsque vous la créez dans la console API de Google ou sur le portail Microsoft Azure Active Directory. Après avoir créé votre app, copiez son Code secret client et collez-le ici. **Remarque :** lorsque vous créez le Code secret client pour une app Azure, vous devez le copier lors de la création de l'app, car il ne sera plus visible par la suite. Si vous ne le copiez pas à ce moment-là, vous devez alors supprimer le secret et en créer un nouveau.

URI de redirection

Vous devez spécifier un URI de redirection lors de la création de votre app OAuth 2.0 pour Gmail ou Office 365. L'URI de redirection affiché sur l'écran MultiPOP est un exemple construit à partir du <u>nom d'hôte SMTP</u> [187] <u>***</u> [187] <u>de votre Domaine défaut -</u> <u>Domaine - Domaine [184]</u>, qui devrait fonctionner pour les utilisateurs de ce domaine lorsqu'ils se connectent à Webmail. Vous devez ajouter d'autres Connexions à MDaemon Webmail à votre application pour tous les autres domaines de MDaemon auxquels vos utilisateurs accèdent lorsqu'ils se connectent à Webmail. Exemple : "https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Office365" fonctionnera pour tous les utilisateurs qui se connectent à mail.example.com lorsqu'ils se connectent à Webmail. Voir : **Création et liaison de votre application OAuth pour MultiPOP** ci-dessous pour plus d'informations.

Exemple d'URI de redirection :

```
https://mail.example.com/WorldClient.dll?
View=OAuth&AuthRequest=Gmail
https://mail.example.com/WorldClient.dll?
View=OAuth&AuthRequest=Office365
```

Création et liaison de votre application OAuth pour MultiPOP

Instructions étape par étape pour créer votre application OAuth pour MultiPOP pour MultiPOP 2.0.

Pour Google Gmail

Suivez les étapes ci-dessous pour créer une application Google permettant à MultiPOP de s'authentifier à l'aide d'OAuth 2.0 lors de la collecte de courrier à partir de Gmail pour vos utilisateurs.

1. Dans votre navigateur, accédez à la <u>console API Google</u>.

- Si vous êtes dans la liste des projets, cliquez sur NOUVEAU PROJET, ou si vous êtes dans la <u>page Gérer les ressourcesPage Gérer les</u>, cliquez sur (+) CRÉER UN PROJET.
- Saisissez un nom de projet, puis cliquez sur Modifier si vous souhaitez modifier l'identifiant du projet ou le laisser à sa valeur par défaut. Remarque : l 'identifiant du projet ne peut pas être modifié après la création du projet.
- 4. Dans le volet de gauche, allez dans **APIs & Services | OAuth consent** screen.
- 5. Sélectionnez External (Externe) et cliquez sur Create (Créer).
- 6. Saisissez le nom de l'application (par exemple, OAuth pour MultiPOP 2.0 pour Gmail), une adresse e-mail d'assistance à laquelle les utilisateurs peuvent s'adresser et une adresse e-mail de développeur à laquelle Google peut s'adresser en cas de modification de votre projet. C'est tout ce qui est requis sur cette page pour la configuration, mais en fonction de votre organisation particulière ou des exigences de vérification, vous pouvez également saisir le logo de votre entreprise et les liens vers vos conditions d'utilisation automatiquement lorsque vous ajouterez les URI de redirection dans une étape ultérieure. Remarque : ces informations sont utilisées pour l'écran de consentement qui sera présenté aux utilisateurs pour autoriser Collecte MultiPOP à collecter des données à partir de Gmail.
- 7. Cliquez sur Enregistrer et continuer.
- Cliquez sur ADD OR REMOVE SCOPES (ajouter ou supprimer des champs d'application) et, sous "Manually add scopes" (ajouter manuellement des champs d'application), entrez https://mail.google.com/. Cliquez sur AJOUTER À LA TABLE, puis sur Mettre à jour.
- 9. Cliquez sur Enregistrer et continuer.
- Sous Test Users (Utilisateurs de test), cliquez sur ADD USERS (Ajouter des utilisateurs), saisissez chaque compte Gmail à partir duquel vous collecterez du courrier, puis cliquez sur ADD (voir la note ci-dessous concernant le statut de publication de 148 votre application).
- 11. Cliquez sur **Enregistrer et continuer**.
- 12. Dans Résumé, cliquez sur **RETOUR AU TABLEAU DE BORD** en bas de la page.
- 13. Dans le volet de gauche, cliquez sur **Credentials**, cliquez sur **(+) Create Credentials**, et sélectionnez **OAuth client ID**.
- 14. Dans la liste déroulante "Type d'application", sélectionnez **Application Web**, et sous "URI de redirection autorisés", cliquez sur **+ AJOUTER DES URI**. Saisissez l'URI de redirection. L'URI de redirection affiché sur l'écran MultiPOP est un exemple construit à partir du <u>nom d'hôte SMTP</u> [187] *** [187] de votre Domaine <u>défaut Domaine Domaine</u> [184], qui devrait fonctionner pour les utilisateurs de ce domaine lorsqu'ils se connectent à Webmail. Vous devez ajouter d'autres Connexions à MDaemon Webmail à votre application pour tous les autres domaines de MDaemon auxquels vos utilisateurs accèdent lorsqu'ils se connectent à Webmail. Exemple : "https://mail.example.com/WorldClient.dll?

View=OAuth&AuthRequest=Gmail" fonctionnera pour tous les utilisateurs qui se connectent à mail.example.com lorsqu'ils se connectent à Webmail.

- 15. Cliquez sur **CRÉER**.
- 16. Copiez les valeurs des champs**Votre ID client** et **Votre Code secret client** dans les champs ID client Gmail et Code secret client de la page MultiPOP.

État de la publication - Ces instructions concernent la création d'une application Google dont l'état de la publicationPlus d'informations est défini sur "Test". Pour ce faire, vous devez ajouter chaque compte Google spécifique qui utilisera l'application pour collecter son courrier à partir de Gmail, et ce nombre est limité à 100 utilisateurs. Dans le Webmail, lorsqu'il est demandé aux utilisateurs d'autoriser MDaemon à collecter leur courrier dans Gmail, un message d'avertissement s'affiche "pour confirmer que l'utilisateur a un accès de test à votre projet, mais qu'il doit tenir compte des risques associés à l'accès à ses données par une application non vérifiée". Cette autorisation expire au bout de sept jours, ce qui signifie que chaque utilisateur doit réautoriser la collecte de son courrier dans Gmail toutes les semaines.

Si vous souhaitez supprimer ces exigences et limitations, vous devez alors changer votre statut en "**En production**", ce qui peut vous obliger ou non à passer par un processus de vérification. Pour plus d'informations sur la vérification des applications et le statut de publication, consultez les articles suivants de Google : <u>Filtrerpar</u> <u>l'écran de consentement Google</u> et <u>FAQ sur la vérification de l'API</u> <u>Google</u>.

Pour Microsoft (Office) 365

- Suivez les étapes ci-dessous pour créer une application Microsoft Azure afin de permettre à Collecte MultiPOP de s'authentifier à l'aide d'OAuth 2.0 lors de la collecte des courriels Office 365 pour vos utilisateurs.
- Accédez à la page <u>Microsoft AzureMicrosoft</u> du portail Azure et cliquez sur Enregistrements d'applications dans le volet de gauche (vous devez vous inscrire à un compte Azure gratuit ou payant si vous n'en avez pas déjà un).
- 2. Cliquez sur + New Registration.
- 3. Dans le champ**À nom,**entrez un nom d'application (par exemple, "Nom Boîte Boîte OAuth pour Office 365").
- Pour "Types de comptes pris en charge", sélectionnez Comptes dans n'importe quel répertoire organisationnel (Tout répertoire Azure AD -Multitenant).
- 5. Pour "URI de redirection", sélectionnez web, puis saisissez votre URI de redirection Office 365. L'URI de redirection affiché sur l'écran MultiPOP est un exemple construit à partir du <u>nom d'hôte SMTP</u> [187] *** [187] de votre Domaine <u>défaut Domaine Domaine</u> [184], qui devrait fonctionner pour les utilisateurs de

ce domaine lorsqu'ils s'inscrivent à Webmail. Vous devez ajouter d'autres Connexions à MDaemon Webmail à votre application pour tous les autres domaines de MDaemon auxquels vos utilisateurs accèdent lorsqu'ils se connectent à Webmail. Exemple : "https://mail.example.com/WorldClient.dll? View=OAuth&AuthRequest=Office365" fonctionnera pour tous les utilisateurs qui se connectent à mail.example.com lorsqu'ils se connectent à Webmail.

- 6. Cliquez sur **Enregistrer**.
- Notez l'ID de l'application (client) (un bouton "copier dans le presse-papiers" se trouve à côté). Vous pourrez retrouver cet identifiant plus tard en cliquant sur Vue d'ensemble dans le volet de gauche.
- Si vous devez ajouter des URI de redirection supplémentaires, cliquez sur le lien web Redirect URIs : 1 à droite. Cliquez sur Ajouter un URI et saisissez l'URI, en répétant l'opération si nécessaire, puis cliquez sur Enregistrer.
- 9. Cliquez sur **API Permissions** dans le volet de gauche.
- 10. Cliquez sur + Ajouter une autorisation.
- 11. Cliquez sur Microsoft Graph.
- 12. Cliquez sur Delegated Permissions (Autorisations déléguées).
- 13. Faites défiler l'écran jusqu'à **POP** et sélectionnez **POP.AccessAsUser.All**, puis sous **User** select et **User.Read** (User.Read est déjà sélectionné par défaut).
- 14. Cliquez sur **Ajouter des autorisations**.
- 15. Dans le volet de gauche, cliquez sur **Certificats & Secrets**.
- 16. Cliquez sur + Nouveau Code secret client.
- 17. Saisissez une description (par exemple, "Secret client pour Office 365 OAuth pour MultiPOP app").
- 18. Sélectionnez le délai d'expiration du secret client.
- 19. Cliquez sur **Ajouter**.
- 20. Notez le secret client généré dans le champ Valeur (il y a un bouton copier dans le presse-papiers à côté). REMARQUE : le secret client ne sera plus visible sur cette page il y aura une icôneSupprimer à côté de l'entrée pour que vous puissiez la supprimer et créer un nouveau secret client si nécessaire.
- 21. Saisissez les valeurs de l'ID de l'application (client) et du Code secret client dans les champs**ID client** et **Code secret client de la** section Office 365 de la page MultiPOP de MDaemon, sous Paramètres du serveur.

Voir :

Mon compte | MultiPOP 792 Collecte de courrier MultiPOP | Collecte MultiPOP 406

3.1.13 DomainPOP

Utilisez DomainPOP Mail Collection ("Configuration | Paramètres du serveur | DomainPOP") pour configurer MDaemon afin qu'il télécharge le courrier d'une boîte aux lettres POP distante pour le redistribuer à vos utilisateurs. Cette fonctionnalité utilise le protocole POP3 pour télécharger tous les messages trouvés dans laboîte aux lettres POP du FAIassociée à l'identifiant spécifié. Si les messages sont collectés, ils sont analysés en fonction des paramètres fournis dans cette boîte de dialogue, puis placés dans les boîtes aux lettres des utilisateurs ou dans la file d'attente du courrier distant pour que MDaemon les distribue, comme s'ils étaient arrivés sur le serveur par le biais de transactions SMTP classiques.

Il est important de noter que les messages stockés dans les boîtes aux lettres et récupérés à l'aide du protocole POP3 seront dépourvus des importantes informations de routage (parfois appelées"enveloppe" dumessage) qui seraient normalement fournies si les messages avaient été distribués à l'aide du protocole SMTP, plus puissant. Dans ces conditions, MDaemon est obligé de "lire" le message et d'examiner les en-têtes pour tenter de déterminer à qui le message était destiné à l'origine. Le moins que l'on puisse dire, c'est qu'il ne s'agit pas d'une science exacte. Les en-têtes des messages sont parfois connus pour leur manque d'informations suffisantes pour déterminer le destinataire. Cette absence de ce qui semble être une caractéristique fondamentale d'un E-mail du destinataire peut paraître surprenante, mais il faut garder à l'esprit que le message n'a jamais été destiné à être remis à son destinataire par le biais du protocole POP. Avec le SMTP, le contenu du message n'a pas d'importance puisque le protocole lui-même dicte spécifiquement au serveur, pendant la transaction de courrier, le destinataire du message.

Afin de permettre la récupération et la distribution des messages POP de manière fiable et cohérente, MDaemon utilise un ensemble puissant d'options de traitement des entêtes. Lorsque MDaemon télécharge un message à partir d'une source POP distante, il analyse immédiatement tous les en-têtes pertinents de ce message et constitue une collection de destinataires potentiels. Cette adresse e-mail dans les en-têtes TO : MDaemon analyse immédiatement tous les en-têtes pertinents de ce message et crée une liste de destinataires potentiels.

Une fois ce processus terminé, lacollection de destinataires de MDaemon() est divisée en deux groupes : les destinataires locaux et les destinataires distants. De plus, toutes les adresses analysées et placées dans la collection de destinataires potentiels sont traitées par le traducteur<u>Alias</u> avant d'être divisées en ensembles locaux et distants. Chaque membre de l'ensemble local (les adresses dont le domaine correspond à l'un des domaines locaux de MDaemon) recevra une copie du message. Ce qu'il advient de l'ensemble distant est régi par les paramètres de cette boîte de dialogue. Vous pouvez choisir d'ignorer simplement ces adresses, d'en Transférer une liste sommaire au postmaster, ou de les honorer - dans ce cas, MDaemon délivrera effectivement une copie du message au destinataire distant. Ce n'est que dans de rares cas qu'il est nécessaire de délivrer ces messages à des destinataires distants.

Il faut veiller à éviter les messages en double ou les cycles de distribution du courrier en boucle. Un problème courant résultant de la perte de l'enveloppe SMTP se manifeste avec le courrier des listes de diffusion. En règle générale, les messages distribués par une liste de diffusion ne contiennent pas, dans le corps du message, de référence aux adresses des destinataires. Par nom, le moteur de liste insère simplement le nom de la liste de diffusion dans le champ λ :. Cela pose un problème immédiat : si le champ TO : contient le nom de la liste de diffusion, MDaemon peut télécharger ce message, analyser le champTo : (qui indiquera le nom de la liste de diffusion), puis renvoyer le message à la même liste. Dans ce cas, une autre copie du même message serait envoyée à la boîte aux lettres POP à partir de laquelle MDaemon a téléchargé le message original, De sorte que tout le cycle recommence. Pour faire face à de tels problèmes, les administrateurs de messagerie doivent veiller à utiliser les outils et les paramètres fournis par MDaemon pour supprimer le courrier de la Liste d'alias ou pour l'aliaser de manière à ce qu'il soit distribué au(x) destinataire(s) local(aux) approprié(s). Vous pouvez également utiliser les Règles de routage ou les Filtres de contenu pour délivrer le message au(x) bon(s) destinataire(s).

D'autres problèmes liés à l'utilisation de ce type de système de collecte de courrier concernent la question de la duplication des messages non désirés. Il est très facile pour le courrier distribuéen SMTP MAIL' par le FAIde générer des doublons indésirables, une fois qu'il a été collecté à l'aide de DomainPOP. Exemple : supposons qu'un message soit envoyé à une personne de votre domaine et qu'une copie carbone soit envoyée à une autre personne du même domaine. Dans cette situation, le SMTP livrera deux copies du même message à laboîte aux lettres de votre FAI- une pour chaque destinataire. Dans chacun des deux fichiers de message, les **deux** destinataires seront mentionnés, l'un dans le champ A : et l'autre dans le champ cc :. MDaemon collectera chacun de ces deux fichiers de messages identigues et analysera les deux adresses de chacun d'entre eux. Les deux destinataires recevront donc un message en double non désiré. Pour éviter ce type de duplication, MDaemon utilise un contrôle qui vous permet de spécifier un en-tête que MDaemon utilisera pour vérifier s'il y a duplication. Le champ Message ID est idéal pour cela. Dans l'Exemple ci-dessus, les deux messages sont identiques et contiennent donc la même valeur dans le champMessage ID. MDaemon peut utiliser cette valeur pour identifier et supprimer le second message pendant la phase de téléchargement, avant qu'il ne soit analysé pour en extraire les informations relatives à l'adresse.

Enfin, pour éviter les messages doubles et les cycles de distribution en boucle, MDaemon utilise un moyen de détecter le nombre de voyages ou de "sauts" effectués par un message dans le système de transport. Chaque fois qu'un serveur SMTP traite un message, il l'estampille avec un en-tête "Received". MDaemon compte tous ces entêtes lorsqu'il rencontre un message pour la première fois. Si le nombre total de serveurs de messagerie dépasse une valeur donnée, il est probable que le message soit pris dans une boucle de distribution du courrier et qu'il doive être retiré du flux de courrier et déplacé dans le bad message directory. Cette valeur peut être configurée sous <u>File de relance</u>

Voir :

 Filtres de contenu

 Listes de diffusion

3.1.13.1 Hôte & Paramètres

152

Server Settings - Host & Settings	Enable DomainPOP
DNS & IPs	Host name or IP Extra hosts
 Drives & Derivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP Host & Settings Parsing Processing Routing Foreign Mail Name Matching Archive RAS Logging 	Logon name
	Download small messages before large ones Over Quota Check Warn account holder and delete over quota message Warn account holder and forward over quota message to Postmaster
	Ok Cancel Apply Help

Propriétés de l'hôte DomainPOP

Activer le moteur de collecte de courrier DomainPOP

Si cette option est sélectionnée, MDaemon utilisera le paramètre fourni dans cet écran pour collecter le courrier d'un hôte DomainPOP en vue d'une redistribution locale.

Nom d'hôte ou IP

Entrezici le Nom d'hôte ou l'adresse IP devotre DomainPOP.

Hôtes suppl.

Cliquez sur ce bouton pour ouvrir le fichierDpopXtra.dat, dans lequel vous pouvez désigner des Hôtes suppl. à partir desquels collecter le courrier DomainPOP. Voir le contenu de ce fichier pour plus d'informations.

Votre nom identifiant

Entrez votre login du compte POP utilisé par DomainPOP.

Mot de passe

Entrez ici le mot de passe ducompte POP ou APOP.

Utiliser APOP

Cochez cette case si vous souhaitez utiliser la commande APOP et l'authentification CRAM-MD5 lors de la récupération de votre courrier. Ce texte permet de s'authentifier sans devoir envoyer des mots de passe en clair.

Collecte des messages

Laisser les messages sur le(s) hôte(s) DomainPOP Si cette option est sélectionnée, MDaemon téléchargera mais ne supprimera pas les messages de votre hôte DomainPOP.

...jusqu'à ce qu'ils aient atteint ce nombre de jours (0 = ne jamais supprimer) Il s'agit du nombre de jours pendant lesquels un message peut rester sur l'hôte DomainPOP avant d'être supprimé. Utilisez "0" si vous ne souhaitez pas supprimer les messages plus anciens.



Certains hôtes peuvent limiter la durée pendant laquelle vous êtes autorisé à stocker des messages dans votre boîte aux lettres.

Ne pas télécharger les messages de plus de [xx] Ko (0 = pas limite) (0 = pas de limite) Les messages supérieurs ou égaux à cette taille ne seront pas téléchargés depuis votre hébergeur DomainPOP. Saisissez "0" si vous souhaitez que MDaemon télécharge les messages quelle que soit leur taille.

Supprimer les messages volumineux des hôtes DomainPOP et MultiPOP

Activez cette option pour que MDaemon supprime les messages dont la taille est supérieure à celle indiquée ci-dessus. Les messages seront simplement supprimés des hôtes DomainPOP et MultiPOP et ne seront pas téléchargés.

Destinataire des messages d'alerte des messages DomainPOP de grande taille Dans cette option, MDaemon enverra une notification au postmaster chaque fois qu'un message volumineux sera découvert dans la boîte aux lettres DomainPOP.

Télécharger les petits messages avant les grands

Activez cette case à cocher si vous souhaitez que l'ordre de téléchargement des messages soit basé sur leur taille - en commençant par le plus petit et en continuant par le plus grand.



Cette option permet de récupérer plus rapidement les petits messages, mais nécessite un tri et un traitement internes plus importants.

Vérification du dépassement de quota

Avertir le titulaire du compte et supprimer le message hors quota.

Lorsque cette option est sélectionnée et qu'un message est collecté pour un compte dont le quota est dépassé (indiqué dans l 'écranQuotas real de l'éditeur de compte),

MDaemon supprime le message, puis envoie un message au titulaire du compte indiquant que le quota est dépassé.

Expéditeur des messages d'alerte et Transférer le message MESSAGE !

Lorsque cette option est choisie et qu'un message est collecté pour un compte dont le quota est dépassé, MDaemon transmet le message au Postmaster et envoie une notification à l'utilisateur pour l'informer que son quota est dépassé.

3.1.13.2 Analyse

🧐 Server Settings - Parsing	
 Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP Host & Settings Parsing Processing Routing Foreign Mail Name Matching Archive RAS Logging 	Parse these headers for email addresses X-POP3.RCPT: Remove RESENT-TO: Default TO: Default CC: APPARENTLY-TO: X-APPARENTLY-TO: X-APPARENTLY-TO: New header Mexicon address ENVELOPE-TO: Add Parse 'Subject:' header for address inside "(" and ")" characters Parse 'Subject:' headers for email addresses Skip over the first 0 'Received:' headers Stop parsing if 'Received:' yields a local address Send postmaster a warning when no email addresses are found
	Ok Cancel Apply Help

Rechercher les adresses électroniques inscrites dans ces en-têtes

Dans cette zone sont répertoriés les en-têtes que MDaemon analysera pour tenter d'en extraire des adresses. Tous les en-têtes listés ici sont analysés pour en extraire les adresses.

Supprimer

Ce bouton permet de supprimer les entrées sélectionnées de la liste d'en-tête.

Non (par défaut)

Ce bouton efface le contenu actuel de la liste d'en-têtes et ajoute laliste d'en-têtes par défaut deMDaemon. Les en-têtes par défaut sont généralement suffisants pour extraire toutes les adresses du message.

Nouvel en-tête From : TO : Dans l'en-tête FROM

Saisissez l'en-tête que vous souhaitez ajouter à la liste d'en-têtes.

Ajouter

Après avoir spécifié un en-tête dans l'option*Nouvel en-tête*, cliquez sur ce bouton pour l'ajouter à la liste.

Rechercher les doublons à l'aide de l'en-tête

Si cette option est sélectionnée, MDaemon se souviendra de la valeur de l'en-tête spécifié et ne traitera pas les messages supplémentaires collectés dans le même cycle de traitement qui contiennent une valeur identique. L'en-têteMessage ID est l'en-tête par défaut utilisé par cette option.

En-tête From: : Rechercher les adresses inscrites parenthèses dans l'en-tête "Subject Subject :" pour l'adresse à l'intérieur des caractères "(" et ")".

Dans le cas où cette option est sélectionnée et que MDaemon trouve une adresse contenue dans les caractères "()" dans l'en-tête "Subject :" d'un message, cette adresse sera ajoutée à laliste des destinataires dumessageavec toutes les autres adresses analysées.

Rechercher les adresses électroniques dans les en-têtes "Received"

Il est possible de stocker dans les en-têtes "Received" du message les informations sur le destinataire qui ne se trouvent habituellement que dans l'enveloppe du message. Cela permet aux personnes qui analysent le message d'obtenir l'adresse réelle du destinataire en inspectant simplement les en-têtes "Received" par la suite. Cochez cette case si vous souhaitez analyser les adresses trouvées dans tous les en-têtes "Received" du message.

Ne pas tenir compte des premiers en-têtes [xx] en-têtes "Received"

Dans certaines configurations de serveur, il se peut que vous souhaitiez analyser les en-têtes "Received" mais que vous deviez ignorer les premiers d'entre eux. Ce paramètre vous permet d'entrer le nombre d'en-têtes "Received" que MD ignorera avant de commencer son analyse.

Stopper recherche si "Received" correspond à une adresse locale trouvée

Si MDaemon détecte une adresse locale valide lors de l'analyse d'un en-tête "Received", ce paramètre interrompt l'analyse et MDaemon ne recherche pas d'autres adresses de livraison potentielles dans le message.

Envoyer une notification au postmaster si aucune adresse électronique n'est trouvée

Par défaut, MDaemon envoie un e-mail d'avertissement au postmaster lorsqu'aucune adresse n'est trouvée par le processus d'analyse. Décochez cette case si vous ne souhaitez pas envoyer cette notification.

3.1.13.3 Traitement



Remplacement de nom de domaine

Activer le moteur de remplacement de nom de domaine

Cette option peut être utilisée pour réduire le nombre d'alias dont votre site pourrait avoir besoin. Lorsqu'un message est téléchargé, tous les noms de domaine de toutes les adresses analysées à partir de ce message seront convertis en nom de domaine spécifié ici.

Filtrage d'adresse

Extraire toujours le texte suivant des adresses analysées

Certains hôtes apposent sur chaque message une ligne indiquant le destinataire du message, ainsi que des informations de routage ajoutées à l'adresse à gauche ou à droite. Ce cachet serait parfait pour analyser l'adresse du destinataire, sauf que les informations de routage supplémentaires rendent cette opération impossible sans un grand nombre d'alias de comptes. Dans ce cas, MDaemon extraira ce texte de toutes les adresses analysées.

Ignorer les adresses locales inconnues trouvées dans les messages

Comme indiqué ci-dessus, la fonctionnalité Remplacement du Nom de Domaine modifie le nom de domaine de toutes les adresses électroniques analysées à partir d'un message, en le convertissant en celui que vous indiquez dans cet écran. Cela peut créer des adresses qui n'ont pas de compte correspondant sur votre serveur. Par conséquent, MDaemon considère que ces adresses sont celles d'utilisateurs locaux inconnus. Ce type de courrier génère généralement un message "No Such User". Cochez cette case si vous souhaitez empêcher le moteur de Remplacement du Nom de Domaine de générer ces messages.

3.1.13.4 Routage

 Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP Host & Settings Parsing Processing Foreign Mail Name Matching Archive RAS Logging 	Existing Rules Image: Second state st
---	---

Règles existantes

Cette liste présente les règles que vous avez créées et qui seront appliquées à vos messages.

Supprimer

Sélectionnez une règle dans la liste et cliquez ensuite sur ce bouton pour la supprimer.

Effacer tout

Ce bouton permet de supprimer toutes les règles existantes.

Nouvelle règle

(1) Si l'adresse trouvée...

Est égale à, n'est pas égale à, contient, ne contient pas

Il s'agit du type de comparaison qui sera effectué lorsqu'une adresse sera comparée à cette règle de routage. MDaemon cherchera dans chaque adresse le texte contenu dans l'option" ...ce texte" ci-dessous, puis procédera en fonction du paramètre de cette option : letexte complet de l'adressecorrespond-il exactement, ne correspond-il pas exactement, contient-il le texte ou ne le contient-il pas du tout ?

(2) ... ce texte :

Saisissez le texte que vous souhaitez que MDaemon recherche lors de l'analyse des adresses.

(3) ... then do this :

Cette option répertorie les actions disponibles qui peuvent être exécutées si le résultat de la règle est vrai. Vous pouvez choisir parmi les actions suivantes :

Ne pas livrer à cette adresse livrer à cette adresse - En sélectionnant cette action, le message ne sera pas livré à l'adresse spécifiée.

Envoyer à l'utilisateur ou au groupe d'utilisateurs - La sélection de cette action ouvre une boîte de dialogue dans laquelle vous pouvez désigner une liste d'adresses e-mail qui doivent recevoir une copie du message en cours de traitement.

Ajouter une règle

Après avoir défini les paramètres de la Nouvelle règle, cliquez sur *Ajouter une règle* pour l'ajouter à la liste des règles.

3.1.13.5 Courrier étranger



Lorsque du courrier est destiné à des adresses non locales...

...être résumées dans un e-mail envoyé au postmaster.

Si cette option est sélectionnée, MDaemon enverra une seule copie du message au postmaster, accompagnée d'un résumé des adresses non locales que le moteur d'analyse a extraites à l'aide de l'ensemble actuel d'en-têtes et de règles d'analyse.

... envoyer une copie du message à chaque destinataire

Si cette option est sélectionnée, MDaemon remettra une copie de ce message à tous les destinataires non locaux qu'il trouvera dans les en-têtes FROM :.

... ignorer le message

Si cette option est sélectionnée, MDaemon supprimera de la liste des destinataires toute adresse non locale. Si MDaemon n'a jamais analysé les adresses distantes dans le message téléchargé, c'est comme si MDaemon n'avait jamais analysé les adresses distantes.



Les boutons*Exclure...* et *Sauf...* vous permettent de définir les adresses qui seront traitées comme des exceptions à l'option sélectionnée.

3.1.13.6 Correspondance de noms



La fonction de Correspondance de noms n'est active que conjointement avec le moteur de collecte de courrier DomainPOP. Si vous souhaitez utiliser cette fonction, vous devez vous assurer que DomainPOP est activé. DomainPOP est accessible à partir du menu "Configuration | Paramètres de serveur | DomainPOP ".

Moteur de correspondance de noms réels

Activer la correspondance de noms réels

Cette fonctionnalité permet à MDaemon de déterminer qui doit recevoir un message collecté par DomainPOP en se basant non pas sur l'adresse électronique analysée mais sur le texte inclus dans l'adresse. Il s'agit généralement du Nom réel du destinataire.

Exemple : l'en-tête TO d'un messagepourrait être le suivant : TO : "Michael Mason" :

TO : "Michael Mason" <user01@example.com>

ou

TO : Michael Mason <user01@example.com>

La Correspondance Nom ignore la partie "user01@example.com" de l'adresse. Elle extrait la partie "Michael Mason" et vérifie s'il s'agit d'un utilisateur de MDaemon. Si une correspondance est trouvée avec lenom réel d'un compte, l'adresse e-mail locale dece compteest utilisée pour la livraison. Si ce n'est pas le cas, MDaemon renvoie le message à l'adresse électronique trouvée dans les données (user01@example.com dans cet Exemple).



Votre Nom réel ne contient pas de virgule, de point-virgule ou de deux-points.

Activer cette fonctionnalité seulement si l'adresse correspond à

Cette option vous permet de spécifier une adresse électronique qui doit être présente dans les données extraites pour que le processus de correspondance du Nom réel puisse avoir lieu. Cela vous permet de contrôler dans une certaine mesure le moment où la fonction de Correspondance de noms sera utilisée. Exemple : vous pouvez spécifier une adresse telle que "user01@example.com" et seules les adresses correspondant à cette valeur seront candidates à la Correspondance de noms.

Exemple : vous spécifiez "user01@example.com" dans cette option. Cela signifie que "TO : 'Michael Mason' <user01@example.com>" sera candidat à la Correspondance de noms, alors que "TO : 'Michael Mason' <user02@example.com>" ne le sera pas.

3.1.13.7 Archivage

Server Settings - Archive	×.
 Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP Host & Settings Parsing Processing Routing Foreign Mail Name Matching Archive RAS Logging 	This feature will place a copy of each downloaded messages into a folder of your choice. Messages are placed there exactly as they are received and are not processed by MD aemon at all.
	Ok Cancel Apply Help

Archive

Conserver une copie de tous les messages téléchargés dans ce dossier

Il s'agit d'une fonction de sécurité qui permet de s'assurer que vousne perdez pas de courrier en raison d'erreurs imprévues d'analyse ou d'autres erreurs susceptibles de se produire lors du téléchargement de courrier en masse. Cochez cette case si vous souhaitez enregistrer une copie de chaque message téléchargé dans le dossier que vous indiquez. Ces copies sont placées dans le dossier exactement comme elles ont été reçues et ne sont pas du tout traitées par MDaemon.

3.1.14 Paramètres de connexion RAS

3.1.14.1 Connexion RAS

 Server Settings - RAS Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation 	Enable RAS dialup/dialdown engine Dialup only if remote mail is waiting in outbound queue Notify Postmaster when dialup attempts fail Make this many attempts to establish a session 1 After dialing, wait this many seconds for a valid connection 60
Pruning Signatures DomainPOP RAS Logon Processing C.Logging	Connection Keep-alive Once established, MD aemon will not close the RAS session Keep sessions alive for at least minutes (0 = immediate close) If applicable, you should use the option that has MD aemon leave RAS sessions open. If you need to close the session based on inactivity use the settings for this provided by Windows itself.
	Ok Cancel Apply Help

Cliquez sur le menu "Configuration | Paramètres de serveur | RAS" pour configurer vos paramètres de connexion RAS. Cette boîte de dialogue n'est disponible que si les Services d'accès à distance sont installés sur votre système. Elle est utilisée par MDaemon lorsque vous devez appeler votre fournisseur d'accès à Internet juste avant un événement de traitement de courrier distant.

Activer le moteur de numérotation et de déconnexion RAS

Lorsque cette option est activée, MDaemon utilise les paramètres spécifiés ici pour établir une connexion avec un hôte distant avant d'envoyer ou de recevoir du courrier distant.

Connexion uniquement si le courrier distant est en attente dans la file sortante

Dans cette option, MDaemon ne compose pas le numéro du fournisseur d'accès à moins qu'un courrier distant ne soit en attente dans la File distante. Cela peut s'avérer utile dans certaines circonstances, mais sachez que si MDaemon ne compose pas de numéro, il ne peut pas non plus**collecter de**courrier (sauf s'il est distribué sur le réseau local).

Notifier [adresse] en cas de tentatives échouées.

Si cette option est sélectionnée, MDaemon enverra un message à l'adresse spécifiée lorsqu'une tentative de connexion échoue à cause d'une erreur.

Nombre de tentatives pour établir une session

MDaemon tentera de se connecter à l'Hôte distant autant de fois que nécessaire avant d'abandonner.

Après avoir composé le numéro, attendre ce nombre de secondes pour une connexion valide

Cette valeur détermine le temps pendant lequel MDaemon attendra que l'ordinateur distant réponde et termine la connexion RAS.

Maintien de la connexion

Une fois la connexion établie, MDaemon ne ferme pas la session RAS

Dans le cas d'une connexion créée, MDaemon la ferme par défaut dès que toutes les transactions de courrier sont terminées et que la session n'est plus utilisée. Tout en sélectionnant cette option, la connexion restera ouverte même après la fin de toutes les transactions.



MDaemon ne fermera jamais une connexion qu'il n'a pas créée.

Maintenir les sessions en vie pendant au moins [xx] minutes

Si cette option est activée, une session RAS créée par MDaemon restera ouverte pendant au moins le nombre de minutes spécifié ou jusqu'à ce que toutes les transactions de courrier soient terminées.

3.1.14.2 Identifiant

🧐 Server Settings - Logon			×
 Server Settings - Logon Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logon Processing Logging 	RAS Profile Use any currently active dia Logon name Logon password Hangup now	Iup session Use this RAS dialup profile	
	0	Ik Cancel Apply H	Help

Profil RAS

Utiliser n'importe quelle session d'accès à distance active

Cochez cette case si vous souhaitez que MDaemon puisse utiliser d'autres profils de connexion lorsqu'il détecte qu'un profil est actif. Si le moment est venu de composer un numéro, MDaemon vérifiera d'abord s'il existe une connexion active qu'il peut utiliser plutôt que de composer un numéro.

Votre nom Identifiant

La valeur spécifiée ici est l'identification de l'utilisateur ou le nom d'ouverture de session qui sera transmis à l'hôte distant lors du processus d'authentification.

Mot de passe de connexion

La valeur spécifiée ici est le mot de passe qui sera transmis à l'hôte distant au cours de la procédure d'authentification.

Utiliser ce profil de connexion RAS

Cette liste déroulante vous permet de sélectionner un profil de session qui a été défini précédemment dans les fenêtres Dialup Networking ou Remote Access Services Setup.

Nouveau profil

Cliquez sur ce bouton pour créer un nouveau profil de mise en réseau à distance ou de services d'accès à distance.

Modifier le profil

Cliquez sur ce bouton pour modifier le profil de mise en réseau à distance ou de services d'accès à distance actuellement sélectionné.

Raccrocher maintenant

Ce bouton ferme la connexion avec le fournisseur d'accès. Ce bouton n'est actif que lorsque MDaemon a initié la session RAS.

3.1.14.3 Traitement

🧐 Server Settings - Processing	
 Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logon Processing Logging 	Post Connection Process Once connected, run this process: Browse Use these settings if you wish MD aemon to run a program immediately after a RAS connection has been established. This is useful when your ISP requires a FINGER program or other process in order to release your mail to you. Pause server for -1 seconds (-1 = infinite, 0 = no waiting) MDaemon's main execution thread can be paused for a specified interval to give the program you want to run time to do its thing. Force process to shutdown after pause interval has elapsed Use this switch if you wish to ensure that the program shuts down after the specified time interval has elapsed. Some programs Do not exit on their own and must be forced to terminate. This switch does not work when the pause interval is set to -1.
	Ok Cancel Apply Help

Processus post-connexion

Une fois connecté, exécutez ce processus

Si un programme est spécifié ici, MDaemon lance un thread et exécute le processus. Ceci est utile pour ceux qui ont besoin de Finger ou d'un autre programme pour déverrouillerla boîte aux lettres du fournisseur d'accès.

Mettre le serveur en pause pendant [xx] secondes (-1 = infini, 0=pas d'attente)

Si la commande*Une fois connecté, exécuter ce processus* contient une entrée valide, le serveur interrompt ses opérations pendant le nombre de minutes spécifié ici en attendant le retour du processus en cours d'exécution. En entrant "-1", le serveur attendra indéfiniment le retour du processus.

Forcer l'arrêt du processus après l'expiration de l'intervalle de pause

Dans certains cas, le programme que vous devez exécuter ne peut pas se terminer une fois qu'il est arrivé à son terme ; certains programmes nécessitent l'intervention de l'utilisateur pour être fermés. Cette situation n'est pas acceptable lorsque le logiciel doit fonctionner sans surveillance. Si cette option est sélectionnée, MDaemon forcera le processus à se terminer après le nombre de secondes spécifié dans l'option *Mettre le serveur en pause pendant [xx] secondes*. Cette fonction ne fonctionne pas lorsque le serveur est configuré pour attendre indéfiniment le retour du processus.

3.1.15 Paramètres duxy

 Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures MultiPOP DomainPOP RAS Proxy Settings Logging 	Configure firewall/proxy settings. Use proxy Hostname Port Authorization required Use NTLM authentication Use custom authentication Username Password
	Ok Cancel Apply Help

Paramètres du proxy

Si MDaemon fonctionne derrière un pare-feu ou un serveur proxy, vous pouvez utiliser cette boîte de dialogue pour configurer MDaemon de manière à ce qu'il utilise le proxy

pour effectuer diverses requêtes http, par exemple lors de la vérification des mises à jour de l'antivirus et de l'exécution d'autres tâches de maintenance normales. Mises à jour AntiVirus et d'autres tâches de maintenance normales. La boîte de dialogue Paramètres du proxy propose des options pour entrer le nom d'hôte et le port du serveur proxy, et si une authentification est requise, vous pouvez choisir d'utiliser l'authentification Windows NTLM ou une authentification personnalisée, en entrant un nom d'utilisateur et un mot de passe.

3.1.16 Journalisation

3.1.16.1 Mode de journalisation

 Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging Composite Log Statistics Log Windows Event Log Maintenance Settings
More Settings

Cliquez sur la sélection de menu "Configuration | Paramètres du serveur | Journalisation" pour configurer vos paramètres de journalisation. La journalisation est un outil utile pour diagnostiquer les problèmes et voir ce que le serveur a fait sans surveillance.

> Dans la boîte de dialogue Préférences, plusieurs options régissent la quantité de données de journalisation pouvant être affichées dans le volet Suivi des événements de l'interface

principale de MDaemon. Pour plus d'informations, voir <u>Préférences</u> <u>Interface utilisateur</u> <u>ser</u>.

Mode de journalisation et emplacement

Pas de journalisation

En choisissant cette option, vous désactivez toute la journalisation. Les Fichiers journaux seront toujours créés, mais aucune donnée de journalisation n'y sera écrite.

Nous ne recommandons pas l'utilisation de cette option. Sans journalisation, il peut être extrêmement difficile, voire impossible, de diagnostiquer ou de déboguer tout problème potentiel lié au courrier électronique que vous pourriez rencontrer.

Pas de journalisation dans un seul fichier dans un seul fichier journal (MDaemon-all.log). Choisissez cette option si vous souhaitez tout enregistrer dans un seul fichier séparé nommé MDaemon-all.log.

Fichier journal dans des fichiers distincts en fonction de la date

Si cette option est sélectionnée, un fichier journal distinct sera généré chaque jour. Le Nom du fichier correspondra à la date de création.

Enregistrer les sessions de courrier détaillées

Une transcription complète de chaque session de transaction de courrier sera copiée dans le fichier journal lorsque cette option est activée.

Pas de journalisation des sessions de courrier résumées

Cette option permet de copier dans le fichier journal une transcription résumée de chaque session de transaction de courrier.

Fichier journal de chaque service dans un fichier journal distinct

Cochez cette case pour que MDaemon conserve des journaux séparés par service plutôt que dans un seul fichier. Exemple : si cette option est activée, MDaemon enregistre l'activité SMTP dans le fichier MDaemon-SMTP.log et l'activité IMAP dans le fichierMDaemon-IMAP.log. Dans une session de configuration ou une instance Terminal Services de l'interface MDaemon, cette option doit être sélectionnée pour que les onglets de l'interface affichent les informations journalisées.

Placer les Fichiers journaux dans ce dossier :

Utilisez cette option si vous souhaitez désigner un chemin d'accès spécifique pour vos fichiers journaux.

Le fichier BadAddress.txt

Dansles Fichiers journaux, MDaemon conserve le fichierBadAddress.txt dans le dossier logs. Dans le cas où la livraison à une adresse résulte en une erreur 5xx, l'adresse est ajoutée au fichier. Cela peut vous aider, par exemple, à identifier les mauvaises adresses dans vos listes de diffusion plus rapidement qu'en cherchant dans les journaux SMTP sortants. Ce fichier est automatiquement supprimé à minuit chaque nuit pour éviter qu'il ne devienne trop volumineux.

3.1.16.2 Journal détaillé

 Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging Statistics Log Windows Event Log Maintenance Settings More Settings 	The composite log is a special log th services you are interested in. Include the following in the Compo System log activity Routing log activity SMTP activity IMAP activity MultiPOP activity DomainPOP activity	at you can configure to include only the site Log Content Filter activity Content Filter activity DAP activity SPF/DKIM activity Plug-in activity Plug-in activity
--	--	---

Journal composite

Cochez les cases des services à inclure dans le journal

Dans le menuWindowsde la barre de menus de MDaemonse trouve l' optionJournalisation composite. En cliquant sur cette option, vous ajoutez une fenêtre à l'affichage principal de MDaemonqui combine les informations affichées dans unou plusieursonglets duSuivi des événements.Utilisez les contrôles de cette section pour désigner les informations desonglets à combiner dans cette fenêtre. Les informations contenues dans les onglets suivants peuvent être combinées :

Système - Affiche l'activité du système de MDaemon, comme l'initialisation des services et l'activation/désactivation de l'un des différents serveurs de MDaemon.

- **Routage Affiche**les informations de routage (À, De, Message ID, etc.) pour chaque message analysé par MDaemon.
- **SMTP Toute**activation de session d'envoi/réception utilisant le protocole SMTP est affichée.
- **POP3 Lorsque les**Actifs collectent du courrier électronique à partir de MDaemon en utilisant le protocole POP3, cette activité est journalisée.
- **IMAP**: les sessions de**messagerie**utilisant le protocole IMAP sont journalisées.
- **RAW-L**'activité des messages**RAW**ou générés par le système est journalisée.
- Collecte **MultiPOP : affiche**les activités de Collecte de courrier MultiPOP de MDaemon.
- DomainPOP : affiche l'activité DomainPOP de MDaemon.
- **Webmail/HTTP/IM : affiche**toutes les activités de Webmail et de messagerie instantanée.
- Filtre de contenu -Les opérations du filtre de contenu de MDaemonsont listées.
- Filtre anti-spam Affichetoute l'activité du Filtre anti-spam.
- **LDAP Affiche**l'activité LDAP.
- AntiVirus-Les opérations anti-virus sont affichées dans la vue composite.
- SPF/DKIM : affichetoutes les activités de Sender Policy Framework et DKIM.
- MDaemon Connector : affichetoute l'activité de MDaemon Connector.
- Activité du plugin : enregistre les activités du plugin MDaemon dans le journal composite.

Activer le journal composite

Dansl'interface principale de MDaemon, cliquez sur ce bouton pour lancer la fenêtre du journal composite. Elle peut également être activée à partir du menuWindows de labarre de menu de MDaemon.

3.1.16.3 Journal de statistiques

Server Settings - Statistics Log		×
 Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging Log Mode Composite Log Statistics Log Windows Event Log Maintenance Settings More Settings 	Statistics Log □ Create 'Statistics' comma delimited file ☑ Create 'Statistics' database file (required for reporting) During nightly maintenance: ☑ Remove database records older than ☑ Compact database every ☑ Compact database every ☑ Current size of statistics database: 0.04 MB Compact database now	
	Ok Cancel Apply He	lp

Statistiques de journalisation

Créer un fichier de statistiques délimité par des virgules

Utilisez cette option si vous souhaitez conserver un fichier de statistiques délimité par des virgules, contenant des données sur le nombre de messages entrants et sortants traités, des statistiques sur le spam, des statistiques sur l'antivirus, etc. Cette option est désactivée par défaut.

Créer un fichier de base de données "Statistiques" (nécessaire pour l'établissement de rapports)

Cochez cette case si vous souhaitez enregistrer des informations statistiques sur l'activité de MDaemon dans un fichier de base de données SQLite. La base de données contient des données sur l'utilisation de la bande passante de MDaemon, le nombre de messages entrants et sortants, les statistiques sur le spam, etc. Par défaut, cette base de données est stockée dans le dossier"MDaemon\StatsDB" et 30 jours de données sont sauvegardés, mais vous pouvez ajuster la durée de conservation des données si vous souhaitez conserver plus ou moins de données que les 30 jours par défaut. Les données plus anciennes que la limite fixée seront supprimées lors de la maintenance chaque nuit. Vous pouvez également spécifier la fréquence à laquelle MDaemon compacte la base de données pour économiser de l'espace. La page Rapports dans la section de l'interface web de l'Administration Remote de MDaemon utilise cette base de données pour générer divers rapports accessibles aux Administrateurs Globaux. Pour chaque rapport, les données peuvent être générées pour plusieurs plages de dates prédéfinies, ou l'administrateur peut spécifier une plage de dates personnalisée. Les administrateurs peuvent choisir parmi les rapports suivants :

- Rapports améliorés sur la bande passante
- Messages entrants vs. Sortants
- Corrects vs Indésirables (pourcentage d'e-mails qui sont des spams ou des virus)
- Messages entrants traités
- Premiers destinataires par nombre de messages
- Premiers destinataires par taille de message
- Messages sortants traités
- Premières sources de spam (domaines)
- Premiers destinataires du spam
- Virus bloqués, par heure
- Virus bloqués, par nom

Durant la maintenance chaque nuit : :

Les options ci-dessous déterminent les tâches liées à la base de données que MDaemon effectuera pendant la maintenance chaque nuit.

Supprimer les enregistrements de la base de données datant de plus de [xx] jours

Utilisez cette option pour indiquer le nombre de jours d'enregistrements statistiques de la base de données que vous souhaitez conserver. Non (par défaut), cette option est activée et définie sur 30 jours.

Compresser la base de données tous les [xx] jours

Utilisez cette option si vous souhaitez compacter périodiquement la base de données pour économiser de l'espace. Non par défaut, cette option est activée et définie pour compacter la base de données tous les 7 jours.

Taille actuelle de la base de données statistiques :

La taille actuelle de votre base de données statistiques est indiquée ici.

Compacter base données maintenant

Cliquez sur ce bouton pour compacter immédiatement la base de données.

174

3.1.16.4 Journaux d'événements Windows

🧐 Server Settings - Windows Event Log	×
 Servers & Delivery DNS & IPs Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Logging Log Mode Composite Log Statistics Log Windows Event Log Maintenance Settings More Settings 	MD aemon logs data into the Application section of the Windows Event Log SMS gateway email address First checkbox means send notification about event to SMS email address. Second checkbox means log event to Windows event log. [SMS] [Log] the following events: Second checkbox means log event to Windows event log. [SMS] [Log] the following events: Second checkbox means log event to Windows event log. [SMS] [Log] the following events: Second checkbox means log event to Windows event log. [SMS] [Log] the following events: Second checkbox means log event to Windows event log. [SMS] [Log] the following events: Second checkbox means log event to Windows event log. [SMS] [Log] the following events: Second checkbox means log event to Windows event log. [SMS] [Log] the following events: Second checkbox means log event to Windows event log. [SMS] [Log] the following events: Second checkbox means log event to Windows event log. [SMS] [Log] the following events: Second checkbox means log event to Windows event log. [SMS] [Log] the following events: Second checkbox means log event to Windows event log. [SMS] [Log] the following events: Second checkbox means log event to Windows event log. [SMS] Event sub-system or socket failures Second checkbox sub-system o
	Ok Cancel Apply Help

Enregistrer dans le Journal des événements Windows

Cochez cette case si vous souhaitez enregistrer les erreurs système critiques, les avertissements et certains autres événements dans la section Application du Journal des événements Windows.

Adresse e-mail passerelle SMS [Cette adresse e-mail est facultative.

Utilisez cette option si vous souhaitez envoyer les données relatives à l'un des événements désignés ci-dessous à un périphérique dans un message SMS (texte). Pour ce faire, indiquez l'adresse électronique de la passerelle SMS (message texte) de votre opérateur téléphonique, comme celle de Verizon, qui est

PhoneNumber@vtext.com (par exemple 8175551212@vtext.com). Dans la colonne SMS ci-dessous, utilisez les cases à cocher pour spécifier les événements que vous souhaitez envoyer à l'appareil.

SMS | Journal des événements suivants : Enregistrer les événements suivants :

Utilisez les options SMS pour désigner les événements que vous souhaitez envoyer à un appareil par message texte. Utilisez les Options journalisation pour désigner les événements que vous souhaitez enregistrer dans la section Application du Journal des événements Windows. Pour envoyer des messages SMS, vous devez spécifier l'adresse électronique de la passerelle e-mail-SMS de votre opérateur téléphonique dans l'option ci-dessus. En outre, tout événement qui déclenche l'envoi d'un message de notification à la passerelle SMS entraînera le traitement de la file distante ; les notifications seront traitées comme des courriels "urgents".

L'option SMS pour les événements de*démarrage et d'arrêt du serveur* n'enverra un message e-mail vers SMS que pour les événements de démarrage, pas pour les événements d'arrêt.

3.1.16.5 Maintenance

Maintenance

Taille maximale d'un fichier journal [xx] KB

Il s'agit de la taille maximale en kilo-octets qu'un fichier journal peut atteindre. Une fois cette taille atteinte, le fichier journal est copié dans "LOGFILENAME.01.OLD" et un nouveau journal est démarré. Si LOGFILENAME.01.OLD existe déjà, l'ancien fichier sera soit supprimé, soit renommé en "LOGFILENAME.02.OLD", en fonction de la valeur définie dans "*Nombre maximum de journaux .OLD à conserver*" ci-dessous. Utilisez "O" dans cette option si vous ne voulez pas limiter la taille du fichier. Cette option est réglée sur "O" par défaut.

Nombre maximal de journalisations .OLD à conserver (1-99)

Lorsque vous utilisez l'option ci-dessus pour limiter la taille des fichiers journaux, cette option détermine le nombre d'itérations d'un fichier journal.oldonné qui seront conservées avant que la plus ancienne ne soit supprimée. Ces fichiers sauvegardés sont nommés "LOGFILENAME.01.OLD", "LOGFILENAME.02.OLD", et ainsi de suite, le fichier le plus récent étant toujours listé en premier. Exemple : SMTP(out).log.01.old contient des données plus récentes que SMTP(out).log.02.old, etc. Lorsque le nombre maximal est atteint, le fichier le plus ancien est supprimé lors de la création d'un nouveau fichier.

Nombre maximal de jours de journalisation des mises à jour de l'AV (0=pas de limite) Cette option régit le nombre maximal de jours pendant lesquels le journal des mises à jour de l'Antivirus (c'est-à-dire avupdate.log) conservera des données. Chaque nuit à minuit, ainsi qu'à chaque démarrage de MDaemon après une mise à jour, les données les plus anciennes sont supprimées du fichier. Utilisez "0" dans cette option si vous ne souhaitez pas fixer de limite de temps. Non (par défaut), les Derniers 30 jours sont conservés.

> Le journal des mises à jour de l'AV est conservé par défaut et sa taille est limitée à 5120 Ko. Si vous souhaitez modifier sa limite de taille ou désactiver la pas journalisation des mises à jour AV, les options de journalisation se trouvent dans la boîte de dialogue<u>Configurer l'utilitaire de mise à jour AV</u> l'23 située à l'adresse suivante **Sécurité | AntiVirus | Mises à jour antivirus | Configurer la mise à jour | Mises à jour diverses "**

Archivage

Archiver les fichiers journaux de plus de [xx] jours (0 = jamais)

Cliquez sur cette option si vous souhaitez que MDaemon archive chaque fichier journal dont l'âge dépasse le nombre de jours indiqué. Dansce cas, chaque jour à minuit, MDaemon archive les anciens fichiers *.log et *.old et les place dans le sous-dossier\Logs\NOldLogs\N (en supprimant les fichiers d'origine). Ce processus n'archive pas et ne supprime pas les fichiers en cours d'utilisation. Il n'archive pas non plus les fichiers lorsque l'option "*Fichier tout dans un fichier journal séparé (MDaemon-all.log)*" est sélectionnée dans l'écran Mode journalisation.

Supprimer les archives datant de plus de [xx] jours (0=jamais)

Utilisez cette option si vous souhaitez que MDaemon supprime automatiquement les fichiers journaux archivés lorsque leur âge dépasse le nombre de jours spécifié ici. Utilisez "0" dans cette option si vous ne souhaitez pas supprimer les archives automatiquement. La suppression des archives a lieu lors du nettoyage quotidien de minuit.

Archiver maintenant

Cliquez sur ce bouton pour archiver les fichiers journaux immédiatement plutôt que d'attendre que MDaemon les archive automatiquement à minuit.

3.1.16.6 Paramètres

	Select Data to Log	
DNS & IPs	🗹 Create 'All' log	Log Scheduler activity
 DNS & IPS Domain Sharing Public & Shared Folders Message Recall Host Authentication Priority Mail Header Translation Archiving Pruning Signatures DomainPOP RAS Log Mode Composite Log Statistics Log Windows Event Log Maintenance Settings More Settings 	Cleate All rog Cleate All rog Clog SMTP activity Clog POP3 activity Clog DomainPOP activity Clog MultiPOP activity Clog IMAP activity Clog RAS activity Clog Screening activity Clog System activity Clog Active Directory activity Clog Artive Directory activity Clog SPF activity Clog SPF activity Clog SPF activity Clog DKIM activity Clog DMARC activity Clog VBR activity Clog VBR	 Log Scheduler activity Log full Webmail/HTTP/IM activity Log AntWirus activity Log Spam Filter activity Log DNS block list activity Log content filter activity Log MDaemon Connector activity Log MDaemon Connector activity Log SMTP 'probes' Log authentication failures Log MDaemon msg tasks Log LDAP activity activity but only when DNS data is found
	Select all Unselect all	

Sélectionner les données à journaliser

Pas de journalisation

Cliquez sur cette option si vous souhaitez que soit généré le fichier"*-all.log", qui contient une synthèse de toutes les activités journalisées.

Consigner l'activité SMTP

Activez cette option si vous souhaitez journaliser toutes lesactivités d'envoi/réception SMTP deMDaemon.

Pas de journalisation de l'activité POP3

Cochez cette case pour enregistrer toutes les activités liées au courrier POP. Cela permet d'enregistrer les sessions de collecte de courrier POP de vosutilisateurs.

Enregistrer l'activité DomainPOP

Cochez cette case pour enregistrer toutes les activités de courrier DomainPOP.

Consigner l'activité MultiPOP

Cochez cette case pour consigner toutes les activités de collecte de courrier MultiPOP devos utilisateurs.

Consigner l'activité IMAP

Si vous activez cette option, toutes les sessions IMAP de vosutilisateurs seront incluses dans les fichiers journaux de MDaemon.

Pas de journalisation de l'activité des plugins

Cette option permet de journaliser toutes les activités liées aux plugins.

Enregistrer l'activité RAS

Cliquez sur ce bouton si vous souhaitez que MDaemon copie les activités de connexion et de déconnexion RAS dans le fichier journal. Ces informations sont utiles pour diagnostiquer les problèmes de connexion.

Filtrer par l'activité de journalisation

Cochez cette case si vous souhaitez que les activités de Screening de MDaemon soient incluses dans le fichier journal de MDaemon.

Enregistrer l'activité Minger

Cochez cette case pour enregistrer les activités du serveur Minger.

Consigner l'activité du système

Cette option permet de journaliser les activités du système.

Consigner l'activité de journalisation

Cette option permet de journaliser toutes les activités d'analyse des files d'attente entrantes, locales et distantes.

Consigner l'activité Active Directory

Cette option permet de journaliser les activités de l'Active Directory liées à MDaemon.

Pas de journalisation de l'activité Rapports MTA-STS/TLS

Cette optionpermet de journaliser toutes les activités liées à SMTP MTA Strict Transport Security (MTA-STS).

Consigner l'activité du planificateur

Activez cette case à cocher si vous souhaitez journaliser toute l'activité $de \frac{Programmation d'événement d}{405}$ '.

Enregistrer toute l'activité Webmail/HTTP/IM

Cochez cette option si vous souhaitez journaliser toute l'activité des messageries Web, HTTP et MDaemon Webmail. Si cette option est désactivée, les journaux Webmail et HTTP seront toujours créés et indiquerontles heures de démarrage et d'arrêt deMDaemon Webmail, mais les autres activités Webmail/HTTP/IM ne seront pas journalisées.

Pas de journalisation de l'activité AntiVirus

Cette option permet de journaliser les activités de l'antivirus.

Consigner l'activité du Filtre anti-spam

Cette option permet de journaliser toutes les activités du Filtre anti-spam.

Pas de journalisation du DNS Liste de blocage DNS

Cette option permet à MDaemon d'enregistrer les activités de la liste de blocage DNS. L'utilisation de cette option vous permettra de retrouver facilement les sites qui ont été enregistrés comme bloqués.

Enregistrer les activités de journalisation des messages

MDaemon effectue périodiquement un grand nombre d'analyses de messages pour déterminer à qui un message doit être délivré. Activez ce commutateur si vous souhaitez que ces informations soient incluses dans le fichier journal.

Enregistrer l'activité du filtre de contenu

Cochez cette case si vous souhaitez inclure l'activité du Filtre de contenu dans le fichier journal.

Pas de journalisation de l'activité de MDaemon Connector

Cette option détermine si les activités du MDaemon Connector sont consignées ou non dans le journal.

Pas de journalisation des "sondes"SMTP

Cliquez sur cette option pour journaliser les sessions SMTP lorsqu'aucune donnée de message n'est transmise par le serveur d'envoi (c'est-à-dire lorsque le serveur d'envoi n'utilise pas la commande DATA).

Pas de journalisation des échecs d'authentification

Cliquez sur cette option pour consigner les échecs d'authentification.

Pas de journalisation de l'activité RAW

Pas de journalisation de l'activité des messages RAW de MDaemon.

Pas de journalisation des tâches liées aux messages de MDaemon

Consigne les tâches liées aux messages.

Consigner l'activité LDAP

Pasalisation de toute l'activité LDAP.

Consigner l'activité SPF

Cochez cette case si vous souhaitez journaliser toutes les activités de recherche du Sender Policy Framework.

...mais seulement lorsque des données DNS sont trouvées

Si vous enregistrez les activités SPF, cochez cette case si vous souhaitez n'enregistrer que les consultations pour lesquelles des données SPF ont été trouvées lors de la consultation DNS, au lieu d'enregistrer toutes les consultations SPF.

Pas de journalisation des activités DKIM

Cliquez sur cette option si vous souhaitez journaliser l'activité DomainKeys Identified Mail (DKIM).

...mais uniquement lorsque des données DNS sont trouvées

Cochez cette case si vous enregistrez l'activité DKIM mais que vous souhaitez enregistrer uniquement les cas où des données DNS sont trouvées au lieu d'enregistrer toute l'activité.

Pas de journalisation de l'activité DMARC

Cochez cette option si vous souhaitez journaliser l'activité DMARC.

...mais uniquement lorsque des données DNS sont trouvées

Cochez cette case si vous enregistrez l'activité DMARC mais que vous souhaitez enregistrer uniquement les cas où des données DNS sont trouvées au lieu d'enregistrer toute l'activité.

Pas de journalisation de l'activité VBR

...mais uniquement lorsque des données DNS sont trouvées

Si vous enregistrez l'activité de certification des messages, cochez cette case si vous souhaitez l'enregistrer uniquement lorsque des données de certification réelles sont trouvées lors de la recherche DNS.
3.1.16.7 Plus de paramètres

|--|

Sélectionner les données à journaliser

Enregistrer toutes les activités locales de MDSpamD (Pas de journalisation de débogageperformance)

Cette option permet de journaliser toutes les activités locales de MDSpamD (voir Attention ci-dessous).

Enregistrer les sessions en temps réel (Pas de journalisation de débogage - perte de performance)

Dans la plupart des cas, les informations relatives à la session sont consignées une fois la session terminée afin d'économiser les ressources. Cliquez sur cette option si vous souhaitez que les informations relatives à la session soient consignées au fur et à mesure.

Dans l'utilisation de l'une ou l'autre des deux options de journalisation précédentes, il se peut que vous constatiez une baisse des performances de votre système de messagerie, en fonction de votre système et du niveau d'activité. En règle générale, vous ne devez utiliser ces options qu'à des fins de débogage. **Enregistrer les réponses du protocole multiligne (comme UIDL et LIST)** Parfois, les réponses aux demandes de protocole nécessitent plus d'une ligne d'information. Cochez cette case si vous souhaitez consigner ces lignes supplémentaires.

> L'activation de ce commutateur peut potentiellement augmenter considérablement la quantité d'informations journalisées. Par taille, le nombre de lignes d'une réponse ne peutêtre déterminé à l'avance, et parce que certaines réponses risquent fort de "remplir" votre fichier journal d'informations éventuellement inutiles (POP TOP, par exemple, énumère le contenu réel du message), nous vous déconseillons d'utiliser cette fonction si la taille ou la verbosité du fichier journal vous préoccupe.

Enregistrer la chaîne ID dans les journaux de session de messagerie

Cochez cette case si vous souhaitez inclure les chaînes de caractères d'identification [%d:%d] dans les journaux de session.

Utiliser des couleurs lors de l'affichage des journaux de session de messagerie (Redémarrez MDaemon en cours)

Activez cette option si vous souhaitez coloriser le texte affiché dans plusieurs des onglets<u>Suivi des événements et Journalisation de les les des activation de les des activation</u> de MDaemon. Cette option est désactivée par défaut, et son activation/désactivation nécessite un Redémarrage de MDaemon avant que la modification ne prenne effet. Pour plus d'informations, voir : "Journaux de session colorisés" ci-dessous.

Toujours filtrer à l'écran

Cliquez sur cette option si vous souhaitez que les données journalisées soient copiées dans l'interface graphique de MDaemon, même lorsqu'elle est réduite ou exécutée dans la barre d'état système.

Dans ce cas, les données du journal ne sont pas copiées dans le volet Suivi des événements lorsque MDaemon est exécuté dans la barre d'état système. Par conséquent, l'activité la plus récenten'apparaît dans aucun des onglets du volet Suivi des événements lorsque MDaemon est ouvert pour la première fois. Il commencera à afficher les informations nouvellement journalisées à partir de ce moment-là.

Journaux de session colorisés

Dans <u>l'interface utilisateur de MDaemon</u> ⁷²], les onglets qui affichent les activités Routage, SMTP-in, SMTP-out, IMAP, POP, MultiPOP et DomainPOP peuvent être colorés pour aider à distinguer visuellement les événements au cours d'une session. Cette fonctionnalité est désactivée par défaut, mais peut être activée via l'option *"Utiliser des couleurs lors de l'affichage des journaux de session de messagerie*" située à l'adresse suivante : <u>Pas de journalisation | Autres paramètres</u> ^[16] et <u>préférences |</u> <u>Interface utilisateur</u> ^[52]. Les couleurs de texte par défaut peuvent être modifiées en éditant la section [Couleurs] du fichierLogColors.datdans le dossier\APP\de MDaemon. Voir le tableau ci-dessous pour une liste des couleurs par défaut.

Si vous souhaitez utiliser des couleurs mais ne pas coloriser un ou plusieurs des éléments listés, définissez la valeur de chacun de ces éléments à zéro (par Exemple, SpamFilter=0). Cela aura pour effet d'utiliser les paramètres Non par défaut pour les éléments choisis . Pour Background et SelectedBackground, cependant, la mise à zéro de leurs valeurs ne fonctionne pas. Si vous souhaitez modifier l'un ou l'autre de ces éléments, vous devrez fournir une nouvelle valeur de couleur. Les valeurs de couleur sont spécifiées en hexadécimal sous la forme suivante : "0xbbggrr", où "bb" représente l'intensité relative du bleu, "gg" celle du vert et "rr" celle du rouge. Exemple : "Error=0x0000ff" met le texte d'erreur en rouge. **Remarque : il** s'agit de l'ordre inverse de l'ordre traditionnel des codes de couleur, qui est généralement "rrggbb". Si vous modifiez les couleurs, vous devez redémarrer MDaemon ou créer un fichier appelé COLORS.SEM et le placer dans le dossier\APP\ de MDaemon .

Arrière-plan=0x000000	Couleur d'arrière-plan ; noir
SelectedBackground=0xff0000	Couleur de l'arrière-plan sélectionné ; bleu
Non (par défaut)=0xffffff	Non (par défaut texte) ; blanc
Traitement=0x00ffff	Traitement interne et activité d'analyse ; Non (par défaut) jaune
DataIn=0x008040	Données entrantes en provenance d'un autre serveur ; la couleur par défaut est le vert foncé.
DataOut=0x00ff00	Données envoyées à un autre serveur ; par défaut en vert clair
Error=0x0000ff	Messages d'erreur ; par défaut en rouge
TCPIP=0xff8000	Activité liée à TCP/UDP/DNS/PTR ; bleu clair par défaut
SpamFilter=0x0080ff	Filtre anti-spam ; par défaut en orange
AntiVirus=0xdda0dd	Traitement de l'antivirus ; la valeur par défaut est prune.
DKIM=0xff00ff	Activité DKIM ; la valeur par défaut est fuchsia
VBR=0x40c0ff	Activité Vouch by Reference ; la valeur par défaut est orange clair
SPF=0x808080	Activité du Sender Policy Framework ; la valeur par défaut est le gris.
Plugins=0x0080c0	Tout message envoyé par un plugin ; Non (par défaut) marron

Pas de journalisation par défaut

Localq=0x00ffff	Acheminement de la file locale ; la valeur par défaut est jaune.
Spam=0x0080ff	Routage des messages de spam ; la valeur par défaut est l'orange.
Restreint=0x40c0ff	Routage des messages restreints ; par défaut en orange clair
BlackList=0x808080	Routage des messages en liste bloquée ; la valeur par défaut est le gris.
Gateway=0x00ff00	Routage des messages de la passerelle ; par défaut en vert clair
Inboundq=0xff8000	Routage des messages entrants ; la valeur par défaut est bleu clair
PublicFolder=0xdda0dd	Routage des messages du Dossier public ; la valeur par défaut est prune.

3.2 Gestionnaire de domaines

🗾 Domain Manager - Domain Manager		×
Domain Manager Domain M	Domain Management New domain Delete domain Rename domain Copy domain	
	Currently selected default domain: company.test	
	The default domain can not be deleted or renamed.	
	Select a domain to delete or rename it. Double-click to edit domain properties.	
	Make the currently selected domain the new default domain Count: 2	
	company, test example, com	
	Ok Cancel Apply He	elp

MDaemon prend en charge plusieurs domaines, administrés à l'aide du Gestionnaire de domaines. Vous pouvez y gérer les noms de domaine, les adresses IP, les paramètres d'élagage des comptes et des messages, les paramètres de Webmail et d'autres options spécifiques à vos domaines.

MDaemon prend en charge les adresses IP uniques ou multiples, et les adresses IP peuvent être propres à chaque domaine ou partagées entre eux. De plus, plusieurs fonctionnalités clés telles que les Comptes, les Listes de diffusion et certains Paramètres de sécurité, sont disponibles pour chaque domaine. Lorsque vous créez un compte, par exemple, vous devez spécifier le domaine auquel le nouveau compte appartient. Il en va de même pour les Listes de diffusion. Cela signifie également que des fonctions telles que l'Écran IP [508] et le Bouclier IP [505] sont liées à des domaines individuels.

Certaines fonctions, telles que la <u>Correspondance des noms</u> fuel sous <u>DomainPOP</u> fuel, sont liées exclusivement au Domaine par défaut. Le Domaine par défaut est également le domaine affiché par défaut dans diverses options, notamment lors de la création de nouveaux comptes ou de listes de diffusion. En outre, pour faciliter la gestion des messages système par MDaemon, les <u>alias</u> alias alias par défaut suivants font pointer plusieurs noms de boîtes aux lettres réservées vers le domaine par défaut de MDaemon plutôt que vers ses autres domaines :

```
MDaemon@$LOCALDOMAIN$ = MDaemon@<Domaine par défaut>.
listserv@$LOCALDOMAIN$ = MDaemon@<DomaineParDéfaut>
listserver@$LOCALDOMAIN$ = MDaemon@<Domainepardéfaut>.
```

Enfin, afin de prendre en charge plusieurs domaines, MDaemon demande par défaut aux utilisateurs d'utiliser leur adresse e-mail complète (par exemple, "user01@example.com") comme valeur de connexion plutôt que d'utiliser uniquement la partie boîte aux lettres de l'adresse (par exemple, "user01"). Toutefois, certains clients de messagerie très anciens ne permettent pas d'utiliser "@" dans le champ À :. Par conséquent, pour satisfaire ces clients, vous pouvez spécifier un autre caractère dans l' écran Préférences <u>- Système.</u> Est En outre, cette valeur peut comporter jusqu'à 10 caractères, ce qui permet de fournir une chaîne de caractères servant de délimiteur au lieu d'un seul caractère tel que "\$". Exemple : l'utilisation de '.at.' vous permettra de définir des valeurs de connexion telles que "user02.at.example.com". Vous pouvez également désactiver l'exigence relative à l'adresse électronique complète, ce qui permet d'utiliser uniquement la partie boîte aux lettres de l'adresse comme valeur de connexion, mais cela n'est pas recommandé et peut poser des problèmes lorsque vous avez plus d'un domaine.

Liste des domaines

La zone située à gauche de cette boîte de dialogue contient la liste de vos domaines, avec des liens vers chaque écran utilisé pour configurer les différents paramètres spécifiques au domaine. Le Domaine par défaut - Domaine est listé en premier et tous les autres domaines sont listés par ordre alphabétique. La liste de droite est utilisée pour supprimer et renommer des domaines, ainsi que pour désigner le Domaine par défaut. Vous pouvez double-cliquer sur un domaine dans cette liste pour passer au domaine et configurer ses paramètres.

Gestion de domaines

Nouveau domaine

Pour créer un nouveau domaine : cliquez sur *Nouveau domaine*, entrez le nom du domaine dans la boîte de dialogue Créer/Mettre à jour un domaine, puis cliquez sur *OK*.

Créer/renommer domaine	×
Entrer un nouveau nom de do	omaine :
	OK Annuler

En règle générale, la valeur saisie ici sera le nom de domaine Internet enregistré qu'un serveur DNS résout en adresse IP de la machine locale exécutant le serveur, ou un alias qualifié de ce nom. Vous pouvez également choisir d'utiliser un nom de domaine interne ou non valide et non public (tel que "company.mail") pour votre nom de domaine. En configurant votre serveur de cette manière, il peut être nécessaire d'utiliser la fonction de <u>Conversion d'en-tête</u> [126], et/ou le <u>moteur de</u> <u>Remplacement de nom de domaine</u> [156], pour permettre une distribution correcte du courrier.

Supprimer un domaine

Pour supprimer un domaine : sélectionnez le domaine dans la liste ci-dessous, cliquez sur *Supprimer le domaine*, puis confirmez votre décision de supprimer le domaine en cliquant sur *Oui*.

Vous ne pouvez pas supprimer ou renommer le Domaine par défaut Domaine. Si vous souhaitez le supprimer ou le renommer, vous devez d'abord désigner un autre domaine comme domaine par défaut.

Renommer un domaine

Pour modifier le nom d'un domaine : sélectionnez un domaine dans la liste cidessous, cliquez sur *Renommer le domaine*, tapez le nouveau nom de domaine dans la boîte de dialogue Créer/Mettre à jour un domaine, puis cliquez sur *OK*.

Copier un domaine

Si vous souhaitez créer un nouveau domaine dont les paramètres correspondent à ceux d'un autre domaine, sélectionnez un domaine dans la liste, cliquez sur ce bouton, puis indiquez un nom pour le nouveau domaine. Les Nouveaux comptes, les listes, etc. ne seront pas copiés dans le nouveau domaine.

Faire du domaine actuellement sélectionné le nouveau domaine par défaut

Si vous souhaitez changer le domaine par défaut de MDaemon, sélectionnez le domaine souhaité dans la liste ci-dessous et cliquez sur ce bouton.

Voir aussi :

Préférences - Système 525

3.2.1 Nom d'hôte et IP

🛽 Domain Manager - Host Name & IP		×
Domain Manager company.test Host Name & IP Smart Host MDIM Calendar Webmail Dequeuing Signatures Client Signatures Settings ActiveSync example.com	Host Name & IP Disable domain (Cloud only) Warning: Disabled domains are treated as if they do not exist. Domain users will be unable to send or receive mail and MD aemon will not accept incoming messages for the disabled domain. Enable Do Not Disturb (connections from users are refused but incoming mail to the domain is accepted) Schedule SMTP host name mail.company.test Fully qualified domain name for this host used by SMTP server and in many auto-generated emails. You may also use an IP literal enclosed within brackets. Examples: mail.domain.com or [10.20.30.40] IPv4 address 10.20.50.122 Detect IPv6 address fe80::bd80:5431:a808:3675% Detect This domain recognizes only connections made to these IPs. The MD aemon Private Cloud (MDPC) edition offers features for cloud service providers. Customers who want hosted email support can buy directly from MD aemon Technologies or its affiliated partners. Click here to learn more about all MD aemon cloud email options.	
	Ok Cancel Apply H	lelp

Nom d'hôte ou IP

Désactiver le domaine (Cloud uniquement)

Cochez cette case si vous souhaitez désactiver le domaine. Les domaines désactivés sont traités par MDaemon comme s'ils n'existaient pas. Les utilisateurs du domaine ne pourront pas envoyer ou recevoir de courrier et MDaemon n'acceptera pas de courrier entrant pour le domaine. Cette option est uniquement disponible dans MDaemon Private Cloud.

Activer "Ne pas déranger

Utilisez cette option pour activer Ne pas déranger pour un domaine. Lorsqu'elle est active, le domaine refusera toutes les connexions de tous les utilisateurs pour tous les services, mais il acceptera toujours les messages provenant des domaines externes.

Planifier

Cliquez sur ce bouton pour planifier le démarrage et l'arrêt de De Ne pas déranger. Exemple : si vous configurez la période du 1er mai 2020 au 30 juin 2020 de 17 h à 7 h, du lundi au vendredi, cela signifie qu'aucun service de messagerie ne sera disponible pour les utilisateurs de ce domaine ces jours-là, à partir de 17 h et jusqu'à 7 h 01, tant que la date actuelle tombe le 1er mai ou entre le 1er mai et le 30 juin 2020. Le fait de supprimer la date de début programmée désactive la programmation et a pour effet de **mettre le domaine en mode "Ne pas déranger" pour toujours.**

Nom d'hôte SMTP

Cette valeur est le nom de domaine entièrement qualifié (FQDN) qui sera utilisé dans l' instruction SMTP HELO/EHLO lors de l'envoi de courrier pour ce domaine. Pour les connexions entrantes, si l' option*Ce domaine reconnaît uniquement les connexions effectuées vers l'adresse IP de l'hôte* ci-dessous est utilisée, le domaine est lié à sa propre adresse IP et le FQDN approprié sera utilisé pour les connexions effectuées vers ce domaine. L'utilisation de cette option n'est cependant pas strictement nécessaire pour que cela fonctionne. Mais si deux domaines ou plus utilisent la même adresse IP non liée, le FQDN utilisé sera celui qui est associé au domaine qui vient en premier dans l'ordre alphabétique.

Dans la plupart des cas, le FQDN sera soit le *Nom du domaine*, soit un sous-domaine de celui-ci (par exemple, "mail.example.com"), mais une syntaxe IP littérale telle que "[192.0.2.0]" peut également être utilisée. Si aucune valeur FQDN n'est spécifiée, MDaemon utilise le FQDN du Domaine défaut - Domaine.

Adresse IPv4/IPv6

Entrez les adresses IPv4 et IPv6 à associer à ce domaine. Si une adresse IP est indiquée, MDaemon essaiera automatiquement de détecter une adresse destinataire.

Détection

Utilisez ces boutons pour détecter les adresses IPv4 et IPv6 qui peuvent être utilisées dans les options d'adresses IP correspondantes. Vous pouvez alors choisir parmi les adresses IP répertoriées.

Ce domaine ne reconnaît que les connexions faites à ces IPs

Cochez cette case si vous souhaitez limiter les connexions entrantes de ce domaine aux adresses IP spécifiées ci-dessus. Par défaut, cela ne s'applique qu'aux connexions entrantes. La liaison des sockets sortants est régie par une option sous "<u>Paramètres de serveur | Liaison</u> [110]".

Voir :

<u>Gestionnaire de domaines</u> 1841 <u>Préférences - Système</u> ସେଥି <u>Liaison</u> 110 <u>IPv6</u> 109

3.2.2 Hôte de relais

🛃 Domain Manager - Smart Host		x
Domain Manager company.test Host Name & IP Smart Host Accounts MDIM Calendar Webmail Dequeuing Signatures Client Signatures Settings ActiveSync example.com	Configure smart host for this domain Here you can configure a smart host which will receive all mail sent from this domain. Smart hosts would typically be the host name of your internet provider's SMTP server willing to accept mail from you for this domain. Smart host Image:	
	Ok Cancel Apply H	elp

Configurer un hôte de relais pour ce domaine

Si vous souhaitez acheminer le courrier sortant de ce domaine via un Hôte de relais spécifique plutôt que d'utiliser les options de<u>distribution</u> par défaut de MDaemon , cochez cette case et indiquez le Hôte de relais ci-dessous. Tous les courriers sortants du domaine seront acheminés vers cet hôte.

Hôte de relais

Indiquez ici le nom ou l'adresse IP de votre FAI ou de votre hôte de messagerie. Il s'agit généralement du Serveur SMTP de votre FAI.

Ne saisissez pas le Domaine par défaut - Domaine ouadresse IP deMDaemondans cette zone de texte. Il doit s'agir d'un FAI ou d'un autre serveur de messagerie qui peut relayer le courrier pour vous.

Utiliser le nom de domaine et distribuer à ses hôtes MX

Cochez cette case si vous souhaitez traiter l'hôte comme un nom de domaine plutôt que comme un serveur spécifique. MDaemon récupérera alors tous les hôtes MX associés au domaine et s'y connectera.

Utiliser l'authentification SMTP

Cochez cette case et entrez vos identifiants de connexion ci-dessous si le *Hôte* relais requiert une authentification. Ces identifiants seront utilisés pour tous les messages SMTP sortants envoyés à l'hôte relais. Si vous choisissez d'utiliser l' option *Autoriser l'authentification par compte* ci-dessous, MDaemon s'authentifiera auprès de l'hôte séparément pour chaque message, en utilisant les informations d'accès à *l'hôte intelligent* du compte d'envoi désignées dans l'écran<u>Services de</u> <u>messagerie</u> al l'Éditeur de compte.

Nom d'utilisateur

Saisissez ici votre nom d'utilisateur ou votre login.

Mot de passe

Utilisez cette option pour identifier votre mot de passe de l'hôte relais.

Autoriser l'authentification par compte

Cochez cette case si vous souhaitez utiliser l'authentification par compte pour les messages SMTP sortants envoyés à l'*Hôte relais* spécifié ci-dessus. Au lieu d'utiliser les identifiants *Nom d'utilisateur* et *Mot de passe* fournis ici, les identifiants *Accès Hôte relais de* chaque compte , désignés dans l' écran<u>Services de messagerie</u> seront utilisés à la place. Si aucun identifiant Hôte de relais n'a été désigné pour un compte donné, les identifiants ci-dessus seront utilisés à la place.

Si vous souhaitez configurer *l'authentification par compte de* manière à utiliser le *mot de passe Mot de passe de* chaque compte au lieu du *mot de passe Hôte de relais* facultatif, modifiez la clé suivante dans le fichierMDaemon.ini :

[AUTH] ISPAUTHUsePasswords=Yes (Non (par défaut))

L'activation de l'option ISPAUTHUsePasswords=Yes aura pour effet, au fil du temps, de communiquer les mots de passe du courrier local de tous vos comptes à votre Hôte de relais. Cela peut présenter un risque pour la sécurité de la messagerie, puisque des informations sensibles sont communiquées à un autre serveur. Vous ne devez pas utiliser cette option, sauf si vous utilisez un Hôte de relais en qui vous avez une confiance absolue et si vous pensez qu'il est nécessaire de le faire. En outre, vous devez noter que si vous utilisez cette option et donnez à vos utilisateurs la permission de modifier le *mot de passe de* leur *messagerie* via Webmail ou d'autres moyens, le changement du *mot de passe de la messagerie* modifiera également le mot de passe de l'hôte relais. Cela peut entraîner l'échec de l'authentification de l'hôte intelligent pour un compte lorsque son *mot de passe de messagerie* est modifié localement, mais que le *mot de passe de l'hôte intelligent* correspondant n 'est pas modifié dans votre hôte intelligent.

Voir :

Gestionnaire de domainesParamètres de serveur | DistributionMon compte | Services de messagerie

3.2.3 Comptes

🛃 Domain Manager - Accounts						×
Domain Manager company.test Host Name & IP Smart Host Accounts MDIM Calendar Webmail Dequeuing Signatures Client Signatures Settings ActiveSync example.com	Mailbox	Domain company.test company.test company.test company.test	Real name Bill Farmer Frank Thomas Michael Mason Randy Peterman Sir Smith	Forwarding No No No No	Groups Dept A (n/a) (n/a) (n/a)	Msg count 2 1563 14 18 1
	<					>
	Show more account	ts New	Edit Delete			
			[Ok Car	ncel Apply	Help

La page Comptes affiche la liste de tous les comptes MDaemon de ce domaine. Chaque entrée de la liste contient les icônes d'État du compte (voir ci-dessous), la boîte aux lettres, le " vrai nom " du titulaire du compte, les éventuels groupes auxquels le compte appartient, le nombre de messages, la dernière fois que le compte a été consulté et l'espace disque utilisé (en Mo). Cette liste peut être triée par ordre croissant ou décroissant selon la colonne de votre choix. Cliquez sur l'en-tête d'une colonne pour trier la liste par ordre croissant selon cette colonne. Cliquez à nouveau sur la colonne pour la trier par ordre décroissant.

Icônes de statut du compte



Ce compte est administrateur global ou de domaine.

- Compte à accès total. Les accès POP et IMAP sont activés.
- Compte à accès limité. L'accès POP, IMAP ou les deux sont désactivés.
- Le compte est figé. MDaemon accepte toujours le courrier pour ce compte, mais l'utilisateur ne peut ni envoyer ni consulter du courrier.
- Compte désactivé. Tous les accès au compte sont désactivés.

Nouveau

Cliquez sur ce bouton pour ouvrir l'<u>Éditeur de comptes</u> afin de créer un nouveau compte.

Modifier vos

Sélectionnez un compte dans la liste, puis cliquez sur ce bouton pour l'ouvrir dans l'<u>éditeur de compte</u> [765]. Vous pouvez également double-cliquer sur le compte pour l'ouvrir.

Supprimer

Sélectionnez un compte dans la liste et cliquez sur ce bouton pour le supprimer. Il vous sera demandé de confirmer votre décision de supprimer le compte avant que MDaemon ne procède à la suppression.

Afficher plus de comptes

La liste des comptes n'affiche que 500 comptes à la fois. Si le domaine que vous avez choisi compte plus de 500 comptes, cliquez sur ce bouton pour afficher les 500 suivants.

Voir :

<u>Gestionnaire des comptes</u> 7ରୀ <u>Mon compte</u> 7ରୌ <u>Nouveau Modèles de comptes</u> ୫୫

3.2.4 MDIM

💷 Domain Manager - MDIM		×
Domain Manager company.test Host Name & IP Smart Host Accounts MDIM Calendar Webmail Dequeuing Signatures Client Signatures Settings ActiveSync boozleberry.com example.com	MDaemon Instant Messenger (MDIM) MDIM provides quick access to email, folders, instant messages, and other services using Webmail and XMPP. Enable MDIM (enables Webmail) Enable instant messaging IM users see all MDaemon domains in their buddy lists Enable buddy list syncing IM reminders are sent 'From:' MDaemon	
	Cit Cancer	

Cet écran permet de contrôler divers aspects de <u>MDaemon Instant Messenger</u> (<u>MDIM</u> [335]) pour ce domaine. Les paramètres initiaux de cet écran sont déterminés par les paramètres <u>par défaut de MDaemon Instant Messenger</u> [346] situés dans la boîte de dialogue Services Web & IM. Les services MDIM peuvent être activés ou désactivés pour des comptes ou groupes spécifiques via les écrans<u>Services Web</u> [771] et <u>Propriétés</u> <u>du groupe</u> [336] respectivement.

MDaemon Instant Messenger (MDIM)

Activer MDIM (active le Webmail)

Activer cette option si vous souhaitez que les utilisateurs du domaine puissent télécharger MDaemon Instant Messenger par défaut à partir de Webmail. Ils peuvent le télécharger à partir de la page *Options* | *MDaemon Messagerie instantanée.* Le fichier d'installation téléchargé sera automatiquement personnalisé pour lecompte de chaque utilisateurafin de faciliter l'installation et la configuration. Cette option permet également à MDIM d'utiliser les fonctionnalités de Dossiers de courrier, ce qui permet aux utilisateurs de vérifier l'arrivée de nouveaux courriers électroniques et d'ouvrir le Webmail directement à partir du menu contextuel de MDIM. MDIM est activé par défaut.

Activer la messagerie instantanée

Par défaut, les comptes peuvent utiliser MDIM et des clients XMPP witiers pour envoyer des messages instantanés aux autres membres de leur domaine. Décochez

cette case si vous ne souhaitez pas autoriser les utilisateurs de ce domaine à utiliser la messagerie instantanée.

Les utilisateurs de la messagerie instantanée visualisent tous les domaines MDaemon et leurs listes de contacts.

Cochez cette option si vous souhaitez que les utilisateurs de ce domaine puissent ajouter par défaut des contacts à leur liste d'amis à partir de tous vos domaines MDaemon. Lorsque cette option est désactivée, les contacts doivent se trouver sur le même domaine. Exemple : si votre MDaemon ajoute des hôtes pour les domaines example.com et example.org, l'activation de cette option pour example.com signifie que les utilisateurs de example.com peuvent ajouter des contacts de messagerie instantanée provenant des deux domaines. Désactivés, les utilisateurs de example.com ne peuvent ajouter que d'autres utilisateurs de example.com. Cette option est désactivée par défaut.

Activer la synchronisation de la liste d'amis

Utilisez cette option pour remplir automatiquement les listes d'amis des utilisateurs pour le domaine.

Les rappels de la messagerie instantanée sont envoyés par 'From'

Lorsqu'un rendez-vous est programmé dans lecalendrier du MDaemon Webmail d'un utilisateur, l'événement peut être configuré pour envoyer un rappel à l'utilisateur à une heure spécifiée. Si le système de messagerie instantanée est actif pour ledomaine de l' utilisateur, le rappel sera envoyé dans un message instantané à l'utilisateur. Utilisez ce texte pour spécifier le nom que vous souhaitez voir apparaître dans le message :'De:'.

Voir :

 Gestionnaire de domaines
 IRA

 Webmail | MDIM
 MG

 Mon compte | Services web
 1711

 Propriétés du groupe
 R381

3.2.5 Calendrier

🛃 Domain Manager - Calendar		×
Domain Manager company.test	Calendar Settings Send calendar and task reminders even to MDaemon Connector users First day of calendar week Sunday Free/Busy Enable Free/Busy services (enables Webmail) To use Free/Busy with Outlook configure Outlook to query the following URL: http:// <webmail server=""> http:// Webmail Server> Paplace Webmail Server> The password The password 3 months worth of Free/Busy data</webmail>	
	Ok Cancel Apply I	Help

Cet écran permet de contrôler les fonctions de calendrier de MDaemon pour ce domaine. Les paramètres initiaux de cet écran sont filtrés par l'écran<u>Calendrier</u> at situé dans la boîte de dialogue Services Web & IM.

Paramètres de calendrier

Envoyer des rappels pour le calendrier et les tâches

Cochez cette case si vous souhaitez que les rappels du calendrier et des tâches du Webmailsoient envoyés à vos utilisateurs par courrier électronique et par la messagerie instantanée de MDaemon. MDaemon Instant Messenger.

... même aux utilisateurs MDaemon Connector

Si vous avez activé l'option "*Envoyer des rappels pour le calendrier et les tâches*" cidessus, cliquez sur cette option si vous souhaitez également activer les rappels pour les utilisateurs<u>MDaemon Connector</u> 409.

Premier jour de la semaine

Choisissez un jour dans la liste déroulante. Le jour sélectionné apparaîtra dans les calendriers comme le premier jour de la semaine.

Libre/occupé

MDaemon comprend un serveur Libre/occupé, qui permet à un organisateur de réunion de voir la disponibilité des participants potentiels à la réunion. Pour accéder

à cette fonctionnalité, cliquez sur Planification dans le Webmail lorsque vous créez un nouveau rendez-vous. Une fenêtre de planification s'ouvre alors, contenant la liste des participants et une grille de calendrier codée par couleur avec une ligne pour chacun d'entre eux.La ligne de chaque participantest codée par couleur pour indiquer les heures auxquelles il pourrait être disponible pour une réunion. Les couleurs correspondent à Occupé, Provisoire, Absent du bureau et Pas d'information. Il existe également un boutonAuto-Pick Next qui vous permet d'interroger le serveur pour connaître le prochain créneau horaire auquel tous les participants peuvent être disponibles. Lorsque vous avez terminé de créer le rendez-vous, une invitation est envoyée à tous les participants, qui peuvent alors l'accepter ou la refuser.

Le serveur Free/Busy deWebmailest également compatible avec Microsoft Outlook. Pour l'utiliser, configurez Outlook de manière à ce qu'il interroge l'URL mentionnée cidessous pour obtenir les données Free/Busy. Dans Outlook 2002, par exemple, les options Free/Busy se trouvent sous "Outils | Options | Options du calendrier... | Options Free/Busy..."

URL du serveur Free/Busy pour Outlook :

```
http://<Webmail><:Port>/Worldclient.dll?view=fbinfo&user=%NAME%0%
SERVER%
```

Remplacez"<Webmail>" par l'adresse IP ou le nom de domaine de votre serveur Webmail, et"<:Port>" par le numéro de port (si vous n'utilisez pas le port Web par défaut). Exemple :

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%0%
SERVER%.
```

Pour en savoir plus sur la manière d'utiliser lesfonctions Free/Busy duWebmailpour planifier vos rendez-vous, consultez le système d'aide en ligne du Webmail.

Activer les services de disponibilité (Webmail activé)

Cliquez sur cette option si vous souhaitez donner accès aux fonctionnalités du serveur Free/Busy aux utilisateurs.

Mot de passe Free/Busy

Si vous souhaitez demander un mot de passe lorsque les utilisateurs tentent d'accéder aux fonctionnalités du serveur Free/Busy via Outlook, indiquez le mot de passe ici. Ce mot de passe doit être ajouté à l'URL mentionnée ci-dessus (sous la forme : "&password=FBServerPass") lorsque les utilisateurs configurent leurs paramètres Free/Busy dans Outlook. Exemple :

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%0%
SERVER%&password=MyFBServerPassword
```

Permettre aux utilisateurs d'interroger X mois de données libres/occupés

Utilisez cette option pour indiquer le nombre de mois de données Free/Busy que vos utilisateurs peuvent consulter.

Voir :

Webmail | Calendrier 348

3.2.6 Webmail

📃 Domain Manager - Webmail		×
Domain Manager - Webmail	Webmail Settings Language en (English) Theme WorldClient Date format 2m/2d/2Y Date format 2m/2d/2Y Date format 2m/2d/2Y Macros Display time using AM/PM Send read confirmations? Empty trash on exit always Use advanced compose in ever Save messages to 'Sent' folder prompt Block HTML images use HTML editor when composing new messages Lanable password recovery Enable Remember Me Push client signature Allow user-created signatures Message listing shows this many messages per page 50 Message listing refresh frequency (in minutes) 10 Login failure 'Help' text (can contain HTML code): 10	
	Ok Cancal Applu L	
	UK Cancel Apply F	eih

Cet écran filtre les différentes options du client Webmail pour ce domaine. Lorsqu'un utilisateur se connecte au Webmail, ces options régissent le fonctionnement initial du Webmail pour cet utilisateur. La plupart de ces paramètres peuvent ensuite être personnalisés par l'utilisateur via les pages Options en page Webmail. Les paramètres par défaut de cet écran sont filtrés par l' écran<u>"Paramètres Webmail"</u> situé dans la boîte de dialogue Services web & IM.

Paramètres de MDaemon Webmail

Non (par défaut)

Ce bouton permet de réinitialiser un domaine aux <u>Paramètres par défaut du</u> <u>Webmail</u>

Langue

Utilisez la liste déroulante pour choisir la langue par défaut dans laquelle l'interface Webmail s'affichera lorsque vos utilisateurs se connecteront pour la première fois au domaine sélectionné. Dans la page de Connexion au Webmail, les utilisateurs peuvent modifier leurs paramètres de langue personnels, ainsi que par le biais d'une option dans Options | Personnaliser dans le Webmail.

Utiliser par défaut la langue du navigateur

Lorsque cette case est cochée, la langue des utilisateurs du Webmail sera celle de leur navigateur au lieu de la *langue*par défaut ci-dessus. **Note :** Cette option n'est disponible que dans <u>MDRA</u> [376].

Thème

Utilisez cette liste déroulante pour désigner le thème par défaut du Webmail à utiliser pour les utilisateurs du domaine sélectionnélorsqu'ils se connectent pour la première fois. Les utilisateurs peuvent personnaliser le thème à partir de Paramètres | Personnaliser dans le Webmail.

Format de la date

Utilisez cette zone de texte pour indiquer comment les dates seront formatées pour le domaine sélectionné. Dans le bouton*Macros*, vous pouvez afficher une liste de codes de macros qui peuvent être utilisés dans ce texte. Vous pouvez utiliser les macros suivantes dans cette commande :

- **%A** Nom complet du jour de la semaine
- %B Nom complet du mois
- %d Jour du mois (affiche "01-31")
- %m Mois (affiche "01-12")
- %y Année à 2 chiffres
- %Y Année à 4 chiffres

Exemple : "%m/%d/%Y" peut être affiché dans le Webmail comme "12/25/2011".

Macros

Cliquez sur ce bouton pour afficher la liste des codes macro pouvant être utilisés dans le *format Date*.

Envoyer des confirmations de lecture ?

Cette option régit la manière dont le Webmail répondra aux messages entrants qui contiennent une demande de confirmation de lecture.

toujours

Si cette option est sélectionnée, MDaemon enverra une notification à l'expéditeur indiquant que le message a été lu. L'utilisateur du Webmail qui a reçu le message ne verra aucune indication que la confirmation de lecture a été demandée ou a fait l'objet d'une réponse.

jamais

Choisissez cette option si vous souhaitez que le Webmail ignore les demandes de confirmation de lecture.

prompt

Choisissez cette option si vous souhaitez demander aux utilisateurs du Webmail s'ils doivent ou non envoyer une confirmation de lecture à chaque fois qu'un message qui en fait la demande est ouvert.

Afficher les horaires au format AM/PM

Cochez cette option si vous souhaitez qu'une horloge de 12 heures avec AM/PM soit utilisée dans le Webmail pour les heures affichées pour ce domaine. Décochez la case si vous souhaitez utiliser une horloge de 24 heures pour le domaine. Les utilisateurs individuels peuvent modifier ce paramètre via l'option "*Afficher mes heures au format AM/PM*" située sur la pageOptions | Calendrier dans le Webmail.

Vider la corbeille en quittant

Cette option permet devider la corbeille de l'utilisateurlorsqu'il se déconnecte de Webmail. Les utilisateurs individuels peuvent modifier ce paramètre à partir de la page Paramètres | MDaemon Webmail.

Utiliser la rédaction avancée

Cochez cette case si vous souhaitez que les utilisateurs du Domaine par défaut voient l'écran de composition avancée dans Webmail plutôt que l'écran de composition normal. Les utilisateurs individuels peuvent modifier ce paramètre à partir de Paramètres | Composer dans Webmail.

Enregistrer les messages dans le dossier "Envoyés

Cliquez sur cette option si vous souhaitez qu'une copie de chaque message envoyé soit enregistrée dans le dossier Envoyés de votreboîte aux lettres. Les utilisateurs individuels peuvent modifier ce paramètre à partir de la pageParamètres de MDaemon Webmail" Composer ".

Options de blocage des images

Les options de blocage d'images peuvent être utilisées pour contribuer à la sécurité et à la prévention du spam, car de nombreux messages de spam contiennent des images avec des URL spéciales qui peuvent aider l'expéditeur à identifier des éléments sur le destinataire, tels que la validité de son adresse e-mail, sa localisation, l'heure à laquelle le message a été consulté, la plate-forme utilisée, etc. **Note :** Ces options (à l'exception de "Bloquer les images HTML") ne sont*disponibles* que*dans MDRA.*

Bloquer les images HTML distantes dans les courriers indésirables et les messages qui échouent à l'authentification DMARC, DNSBL ou SPF.

Activez cette case à cocher si vous souhaitez empêcher l'affichage automatique des images distantes dans les messages électroniques HTML du Webmail lorsque le message a échoué à l'authentification DMARC, DNSBL ou SPF. Dans ce cas, l'utilisateur doit cliquer sur la barre qui apparaît au-dessus du message dans la fenêtre du navigateur pour voir les messages des files.

Bloquer les images HTML

Activez cette case à cocher si vous souhaitez empêcher l'affichage automatique des images distantes lors de la consultation des messages HTML dans le Webmail. Dans le but de voir les messages des files, l'utilisateur doit cliquer sur la barre qui apparaît

au-dessus du message dans la fenêtre du navigateur. Cette option est activée par défaut.

Toujours bloquer les images HTML distantes

Cette option est similaire à l'option"*Bloquer les images distantes HTML dans tous les messages*" ci-dessus, sauf que l'utilisateur n'a pas la possibilité d'afficher les messages. Dans le cas d'une réponse ou d'un transfert de message, elle empêche également l'affichage des images du message d'origine dans la vue de composition.

Conditions de Blocage des images

Note : Ces options ne sont disponibles que dans MDRA 3761.

... sauf lorsque l'en-tête From correspond à un contact figurant dans les listes d'Expéditeurs autorisés du domaine ou de l'utilisateur.

Cochez cette case si vous ne voulez pas que les options de blocage des images s'appliquent lorsque l'en-tête From du message correspond à un contact de la liste Expéditeurs autorisés du domaine ou de l'utilisateur. Toutefois, si l'option *"Toujours Bloquer les images HTML distantes"* est activée, les messages provenant d'adresses figurant dans la liste des Expéditeurs autorisés de l'utilisateur verront leurs images distantes bloquées ; cette exception ne s'appliquera qu'aux messages provenant d'une personne figurant dans la liste des Acteurs **Actifs. Remarque :** Cette option n'est disponible que dans <u>MDRA</u> **376**.

Bloquer également les images HTML intégrées

Utilisez cette option si vous souhaitez également appliquer les options de blocage d'images aux images en ligne/incorporées.

Désactivez les hyperliens dans les spams et les messages qui échouent à l'authentification DMARC, DNSBL ou SPF.

Non (par défaut), lorsqu'un message est signalé comme spam ou échoue à la vérification <u>DMARC</u> [560], <u>DNS-BL</u> [751] ou <u>SPF</u> [560], tous les hyperliens contenus dans le message sont désactivés. Décochez cette case si vous ne souhaitez pas désactiver les liens dans ces messages. **Remarque :** Cette option n'est disponible que dans <u>MDRA</u> [376].

...sauf lorsque l'en-tête From correspond à un contact figurant dans les listes d'Expéditeurs autorisés du domaine ou de l'utilisateur.

Cochez cette case si vous souhaitez exempter les messages marqués de la désactivation des hyperliens lorsque l'en-tête du message correspond à un contact figurant dans les listes d'Expéditeurs autorisés du domaine ou de l'utilisateur. **Note :** Cette option n'est disponible que dans MDRA 376.

Utiliser l'éditeur HTML pour la rédaction des messages

Cochez cette case si vous voulez que les utilisateurs du domaine voient l'éditeur de composition HTML par défaut dans le Webmail. Ils peuvent contrôler ce paramètre eux-mêmes à partir de Paramètres | Composer dans **Webmail**.

Activer la récupération de mot passe

Si cette option est activée, les utilisateurs du domaine qui ont le droit de <u>modifier</u> <u>leur mot de passe</u> [771] pourront entrer une autre adresse électronique dans Webmail, à laquelle ils pourront envoyer un lien pour réinitialiser leur mot de passe s'ils l'oublient. Pour configurer cette fonction, les utilisateurs doivent entrer l'adresse email de récupération du mot de passe et leur mot de passe actuel dans Webmail sur la page Options | Sécurité. Dans ce cas, le lien "Mot de passe oublié ?" sur la page de connexion au Webmail les conduira à une page de confirmation de l'adresse e-mail de secours. Si l'adresse est correctement saisie, un e-mail sera envoyé avec un lien vers une page de modification du mot de passe. Cette fonction est désactivée par défaut.

Vous pouvez activer ou désactiver cette option pour chaque utilisateur en ajoutant la clé suivante au fichier user.inid'un utilisateur de Webmail (par exemple : \Users\example.com\frank\WC\user.ini):

```
[Utilisateur]
EnablePasswordRecovery=Yes (ou "=No" pour désactiver l'option pour
l'utilisateur).
```

Autoriser l'option Se souvenir de moi pour l'authentification en deux étapes

Dans le cas où un utilisateur utilise l'authentification à deux facteurs (2FA) pour se connecter au Webmail ou à Remote Admin, une option "Se souvenir de moi" est généralement disponible sur la page d'authentification 2FA. Cette option empêche le serveur de redemander l'authentification à deux facteurs à cet utilisateur pendant un certain nombre de jours (voir l'option "Enable Se souvenir de moi" ci-dessous). Effacez cette case à cocher si vous ne souhaitez pas afficher l'option 2FA Se souvenir de moi, ce qui signifie que tous les utilisateurs dont l'authentification 2FA est activée devront saisir un code 2FA à chaque fois qu'ils se connectent. **Note :** Cette option n'est disponible que dans l' interface web de<u>MDaemon Remote Admin</u> (MDRA) [376].

Activer Se souvenir de moi

Cochez cette case si vous souhaitez qu'une case *Se souvenir de moi*apparaisse sur la page de connexion du MDaemon Webmail lorsque les utilisateurs du domaine se connectent via le port<u>https.</u> Si les utilisateurs cochent cette case au moment de la Connexion, leurs informations d'identification seront mémorisées pour ce périphérique. Dans ce cas, chaque fois qu'ils utiliseront ce périphérique pour se connecter au Webmail à l'avenir, ils seront automatiquement connectés, jusqu'à ce qu'ils se déconnectent manuellement de leur compte ou que leur jeton Se souvenir de moi expire.

Par défaut, les informations d'identification de l'utilisateur sont mémorisées pendant un maximum de 30 jours avant que l'utilisateur ne soit obligé de se connecter à nouveau. Si vous souhaitez augmenter le délai d'expiration, vous pouvez modifier la valeur de l'option *Expirer les jetons Se souvenir de moi après ce nombre de jours* dans l'interface Web de <u>MDaemon Remote Admin (MDRA)</u> (376). Vous pouvez également la modifier en modifiant la clé RememberUserExpiration=30 dans le fichier Domains.ini, situé dans le dossier \MDaemon\WorldClient\. La valeur d'expiration peut être fixée à un maximum de 365 jours. **Remarque :** L'authentification à deux facteurs [771] (2FA) possède sa propre clé d'expiration Se souvenir de moi(TwoFactorAuthRememberUserExpiration=30), située dans la section [Default:Settings] du fichier Domains.ini, situé dans le dossier\Daemon\WorldClient\N. Dans ce cas, l'option 2FA sera à nouveau requise à l'ouverture de session lorsque le jeton 2FA Se souvenir de moi expirera, même si le jeton normal est toujours valide.

L'option *Se souvenir de moi* est désactivée par défaut et ne s'applique qu'à ce domaine. L'option globale est filtrée par l'écran<u>Paramètres</u> MDaemon Webmail .

Le Paramètre *Se souvenir de moi* permet aux utilisateurs de bénéficier d'une connexion persistante sur plusieurs appareils. Il est conseillé de ne pas utiliser l'option *Se souvenir de moi* sur les réseaux publics. De plus, si vous soupçonnez une faille de sécurité dans un compte, MDRA dispose d'un bouton "*Réinitialiser Se souvenir de moi*" que vous pouvez utiliser pour réinitialiser les jetons Se souvenir de moi pour tous les utilisateurs. Tous les utilisateurs devront alors se connecter à nouveau.

Activer Dossier Documents du MDaemon Webmail

Cochez cette case pour activer le dossier Documents pour les utilisateurs de ce domaine. L'état par défaut de cette option est déterminé par l'option du même nom sur la page principale <u>des Paramètres Webmail.</u> Si vous modifiez ce paramètre spécifique au domaine, il remplacera le paramètre de l'option globale. **Note :** Cette option et les options Liens de Documents ci-dessous ne sont disponibles que dans l' interface web de<u>MDaemon Remote Admin (MDRA)</u> 376.

Permettre aux utilisateurs de créer des liens temporaires vers des documents personnels

Lorsque cette option est activée, les utilisateurs du domaine pourront créer des liens vers des documents personnels, qui peuvent être partagés avec n'importe qui. Les liens de plus de 30 jours sont automatiquement purgés.

Voir les Liens de Documents

Cliquez sur ce bouton pour afficher la pageLiens documents, qui contient une liste de tous les liens documents actifs pour ce domaine. A partir de cette page, vous pouvez révoquer les Liens de votre choix. Les liens datant de plus de 30 jours seront automatiquement révoqués.

Transmettre la signature client

Cochez cette case si vous souhaitez transmettre les <u>Signatures client</u> [216] aux utilisateurs du Webmail de ce domaine. Dans le Webmail, cela créera une signature appelée "Système" sous les options de signature à : **Options | Composer**. Les utilisateurs peuvent alors choisir d'insérer automatiquement cette signature dans l'Affichage du message lors de la rédaction d'un nouveau message. Si cette option est activée mais que vous n'avez pas créé de signature client dans l'écran Signatures client du Gestionnaire de domaines, l' option<u>Signatures client par</u> <u>défaut</u> [138] sera utilisée à la place. S'il n'y a pas non plus de signature client par défaut, il n'y aura pas d'option Signature du système dans le webmail.

Autoriser les signatures créées par l'utilisateur

Cochez cette case si vous souhaitez autoriser les utilisateurs de ce domaine à créer leurs propres signatures créées par l'utilisateur dans le Webmail. Les utilisateurs peuvent alors choisir la signature qu'ils souhaitent insérer automatiquement dans l'Affichage du message lors de la rédaction des messages. Lorsque vous n'autorisez pas les signatures créées par l'utilisateur, mais que l' option *Transmettre la signature client* ci-dessus est autorisée, seule la <u>Signature client</u> (138) (c'est-à-dire la signature du système dans le Webmail) peut être insérée automatiquement. Dans le Webmail, les options de signature se trouvent à l'adresse suivante : **Options | Composer**.

Autoriser les utilisateurs à modifier le nom d'affichage de leurs alias

Cochez cette case si vous souhaitez autoriser les utilisateurs à modifier le nom d'affichage de leurs alias associés à leur compte. Ils peuvent le faire en utilisant l' option *Modifier les noms d'affichage des alias*, située dans le thème Pro du Webmail, sous Paramètres | Composer. Cette option est désactivée par défaut. **Note :** Cette option n'est disponible que dans l' interface web de<u>MDaemon Remote Admin</u> (MDRA) [376].

Activer l'assistant IA pour les e-mails

Cochez cette case si vous souhaitez activer l'assistant pour les emails IA de MDaemon dans le MDaemon Webmail pour ce domaine ? L'état par défaut de cette option est hérité du paramètre du même nom situé dans la boîte de dialogue principale <u>Paramètres Webmail.</u> I a modification de ce paramètre spécifique au domaine aura pour effet de remplacer cette option par défaut. **Remarque :** Activer assistant IA pour les e-mails pour un domaine ne permet pas à tous les utilisateurs de ce domaine d'accéder à ces fonctions. Vous devez activer l' option *Activer les IA pour les e-mails dans* l'écran <u>Services Web</u> *Tri* de l'Éditeur de comptes pour tout utilisateur que vous souhaitez autoriser à les utiliser. Vous pouvez également utiliser les fonctions<u>Modèles de comptes</u> *messages AI du webmail Tri* ci-dessous pour des informations importantes et des mises en garde concernant l'utilisation de ces fonctionnalités.

Nombre de messages affichés par page

Il s'agit du nombre de messages qui seront affichés sur chaque page de la Liste des dossiers pour chacun de vos dossiers courrier. Si un dossier contient plus que ce nombre de messages, des contrôles situés au-dessus et au-dessous de la liste vous permettront de passer aux autres pages. Les utilisateurs individuels peuvent modifier ce paramètre à partir de Paramètres de MDaemon Webmail" Personnaliser ".

Fréquence d'actualisation de la liste de messages (en minutes)

Il s'agit du nombre de minutes que Webmail attendra avant d'actualiser automatiquement la liste des messages. Les utilisateurs peuvent modifier ce paramètre à partir de Paramètres | MDaemon Webmail.

Texte d'aide pour l'échec de la connexion (peut contenir du code HTML)

Vous pouvez utiliser cette option pour spécifier une phrase de texte (texte brut ou HTML) à afficher sur la page de connexion du Webmail lorsqu'un utilisateur rencontre un problème pour se connecter. Ce texte s'affiche en dessous du texte par défaut suivant : "Ouverture de session incorrecte, veuillezréessayer. Si vous avez besoin d'aide, veuillez contacter votre administrateur de messagerie" Ce texte peut être utilisé pour diriger les utilisateurs vers une page ou des informations de contact pour obtenir de l'aide concernant l'ouverture d'une session sur le Webmail.

Pour que cette fonction fonctionne correctement avec plusieurs domaines, un <u>Nom hôte SMTP</u> 187 valide est nécessaire pour chaque domaine, sinon le <u>texte du domaine par</u> <u>défaut sera utilisé.</u> 184 Par nom, par exemple, si vous avez plusieurs domaines mais que vous dirigez tous les utilisateurs de Webmail vers un seul nom d'hôte pour la connexion, le *texte d'aide* correct et spécifique au domaine pour l'*échec de la connexion peut ne pas être affiché.*

Paramètres de sécurité (Note : Les options de cette section ne sont disponibles que dans l' interface web de<u>MDaemon Remote Admin (MDRA</u>)).

Autoriser WebAuthn lors de la connexion

Cochez cette case si vous souhaitez autoriser les utilisateurs du MDaemon Webmail à se connecter en utilisant l'API d'authentification Web (également connue sous le nom de WebAuthn), qui leur offre une expérience de connexion sans mot passe sécurisée, en leur permettant d'utiliser la biométrie, les clés de sécurité USB, Bluetooth, etc. pour l'authentification. Non (par défaut).

Inviter les utilisateurs à enregistrer leur appareil à la première connexion

Cochez cette case si vous souhaitez inviter les utilisateurs à enregistrer leur appareil actuel (téléphone, données biométriques, etc.) pour la connexion sans passe lorsqu'ils se connectent pour la première fois à leur compte.

Permettre la connexion WebAuthn de contourner la page d'authentification à deux facteurs

WebAuthn étant déjà une forme d'authentification à plusieurs facteurs, l'utilisation d'une autre forme d'authentification à deux facteurs (2FA) après que quelqu'un a déjà utilisé WebAuthn pour se connecter pourrait être considérée comme redondante ou excessive par certains utilisateurs ou administrateurs. Vous pouvez donc cocher cette case si vous souhaitez ignorer l'authentification à deux facteurs lorsque quelqu'un utilise l'authentification par WebAuthn à l'ouverture de session. **Connexion :** Indépendamment de ce paramètre, lorsqu'un compte est spécifiquement configuré pour <u>requérir une authentification à deux</u> <u>facteurs</u> [771], ce compte ne pourra pas contourner l'authentification à<u>deux</u> <u>facteurs</u> [771], même s'il utilise WebAuthn pour se connecter.



Visitez : <u>webauthn.guide</u>, pour plus d'informations sur WebAuthn et son fonctionnement.

Activer la récupération de mot passe

Si cette option est activée, les utilisateurs du domaine qui ont la permission de modifier leur mot de passe [771] pourront entrer une autre adresse électronique dans le Webmail, à laquelle ils pourront envoyer un lien pour réinitialiser leur mot de passe s'ils l'oublient. Pour configurer cette fonction, les utilisateurs doivent entrer l'adresse e-mail de récupération du mot de passe et leur mot de passe actuel dans Webmail sur la page Options | Sécurité. Dans ce cas, le lien "Mot de passe oublié ?" sur la page de connexion au Webmail les conduira à une page de confirmation de l'adresse e-mail de secours. Si l'adresse est correctement saisie, un e-mail sera envoyé avec un lien vers une page de modification du mot de passe. Cette fonction est désactivée par défaut.

Vous pouvez activer ou désactiver cette option pour chaque utilisateur en ajoutant la clé suivante au fichier user.inid'un utilisateur de Webmail (par exemple, \Users\example.com\frank\WC\user.ini):

```
[Utilisateur]
EnablePasswordRecovery=Yes (ou "=No" pour désactiver l'option pour
l'utilisateur)
```

Autoriser les utilisateurs Active Directory à modifier leurs mots de passe via MDaemon Webmail

Lorsque cette case est cochée/activée, tous les utilisateurs de ce domaine dont le compte est configuré pour utiliser l'authentification Active Directory peuvent utiliser l'option "Modifier mot passe" de Webmail. Lorsque cette option est désactivée, seuls les utilisateurs dont les mots de passe sont définis dans MDaemon au lieu d'Active Directory peuvent modifier leur mot de passe à partir de Webmail.

Autoriser les utilisateurs à afficher les mots de passe saisis

Dans cette option, le champ mot de passe de la page de connexion à Webmail comporte une icône sur laquelle l'utilisateur peut cliquer pour rendre visible le mot de passe tapé. Décochez cette case si vous ne souhaitez pas autoriser la visibilité du mot de passe.

Autoriser les utilisateurs à recevoir par e-mail les codes de vérification de l'authentification en deux étapes

Par défaut, les utilisateurs sont autorisés à saisir une autre adresse e-mail dans le Webmail lors de la configuration de l'authentification à deux facteurs, afin qu'ils puissent recevoir les codes de vérification par e-mail plutôt que de devoir utiliser l'application Google authentification. Désactivez cette option si vous ne souhaitez pas autoriser les codes de vérification par e-mail pour ce domaine.

Le code de vérification de l'authentification en deux étapes envoyé par e-mail expire au bout de : [xx] minutes.

Lors de la réception de codes d'authentification à deux facteurs par email, il s'agit de la durée pendant laquelle l'utilisateur devra saisir le code avant qu'il n'expire. Non (par défaut), cette durée est fixée à **10** minutes.

Autoriser WebAuthn pour l'authentification à deux facteurs

Cochez cette case si vous souhaitez autoriser les utilisateurs du MDaemon Webmail à utiliser l'API WebAuthn pour l'authentification à deux facteurs. WebAuthn permet aux utilisateurs d'utiliser la biométrie, les clés de sécurité USB, Bluetooth, etc. pour l'authentification. Non (par défaut) pour l'authentification à deux facteurs, WebAuthn est autorisé.



Dans un souci de sécurité, vous ne pouvez pas utiliser la même méthode d'authentification pour la Connexion sans mot passe et l'authentification à deux facteurs. Par conséquent, si vous souhaitez utiliser à la fois l'authentification sans mot de passe et l'authentification à deux facteurs, choisissez une méthode d'authentification différente pour chacune d'entre elles.

Visitez : **webauthn.guide**, pour plus d'informations sur WebAuthn et son fonctionnement.

Autoriser l'option Se souvenir de moi pour l'authentification en deux étapes

Lorsque quelqu'un utilise l'authentification à deux facteurs (2FA) pour se connecter au Webmail ou à Remote Admin, l'utilisateur dispose généralement d'une option Se souvenir de moi sur la page d'authentification 2FA, qui empêchera le serveur de demander à nouveau l'authentification 2FA à cet utilisateur pendant un certain nombre de jours (voir l'option "Expirer les facteurs Paramètres à deux paramètres" cidessous). Effacez cette case à cocher si vous ne souhaitez pas afficher l'option 2FA Se souvenir de moi, ce qui signifie que tous les utilisateurs dont l'authentification 2FA est activée devront saisir un code 2FA à chaque fois qu'ils se connectent.

Fonctionnalités des messages IA du Webmail

Dans la version 23.5.0 de MDaemon, le thème Pro du client Webmail de MDaemon inclut diverses fonctionnalités d'intelligence artificielle (IA) pour aider vos utilisateurs à gérer leur courrier électronique et à augmenter leur productivité. Ces fonctionnalités sont facultatives et désactivées par défaut, mais peuvent être activées pour tout utilisateur de votre choix.

Grâce à ces fonctionnalités, dans le MDaemon Webmail, vous pouvez utiliser l IA pour :

- Vous donner un résumé du contenu d'un message électronique.
- Suggérer une réponse au message, selon plusieurs directives que vous pouvez demander à l'IA d'utiliser. Vous pouvez définir le *ton de* la réponse (professionnel, respectueux ou décontracté). La position à adopter dans la réponse peut être intéressée ou non, d'accord ou non, ou sceptique. L'attitude à adopter dans la réponse peut être confiante, enthousiaste, calme ou apologétique. Les derniers peuvent indiquer la *longueur de* la réponse, qui peut être très brève ou détaillée.
- Vous aider à composer un nouveau message électronique, sur la base d'un texte que vous avez déjà inclus. Comme pour l'option *Suggérer* ci-dessus, vous pouvez également définir le ton, la position, l'attitude et la longueur que l'IA utilisera pour rédiger le message.

L' option Activer les fonctions IA pour les messages de la boîte de dialogue principale Paramètres du Webmail (365) permet de déterminer si la prise en charge des fonctions IA est activée par défaut pour vos domaines. Une option du même nom située dans la boîte de dialogue du (197) Gestionnaire de domaines peut être utilisée pour remplacer ce paramètre principal pour des domaines spécifiques. **Remarque :** Activer assistant IA pour les e-mails pour un domaine ne permet pas à tous les utilisateurs de ce domaine d'accéder à ces fonctions. Vous devez activer l' option Activer les options IA pour les *e-mails dans* l'écran Services Web (771) de l'éditeur de compte pour tout utilisateur que vous souhaitez autoriser à les utiliser. Vous pouvez également utiliser les fonctions<u>Modèles de comptes</u> [847] et <u>Groupes</u> [836] pour affecter des utilisateurs à un groupe ayant accès aux fonctions de messages AI.

Activer les assistants IA pour les e-mails de MDaemon permet aux comptes d'envoyer et de recevoir des informations en provenance et à destination de services d'IA générative tiers, en particulier ChatGPT d'OpenAI. Les administrateurs et les utilisateurs doivent donc être conscients que cela introduit plusieurs problèmes potentiels de confidentialité en raison de la capacité de la fonctionnalité à traiter des données personnelles et à générer des informations potentiellement sensibles. Pour répondre à ces préoccupations, il est essentiel que les organisations forment leurs employés à une utilisation responsable de l'IA. **Remarque :** Les données soumises à/depuis l OpenAI ne sont pas stockées sur le serveur local ou sur notre réseau. Vous trouverez la politique d'utilisation de l'IA de MDaemon Technologies sur notre <u>page d'information sur l'intelligence</u> artificielle (IA)-la MDaemon. Sur cette même page, il y a également un lien vers les Conditions d'utilisation d'OpenAI.

Voir :

Webmail | Paramètres 365

3.2.7 Retrait de la file d'attente

🧐 Paramètres du serveur - Retrait de la file d'att	tente 💌
 Paramètres du serveur Distribution Serveurs Ports DNS IPv6 Liaison Temporisateurs Sessions Retrait de la file d'attente Archivage Nettoyage Courrier inconnu Rappel de message Partage de domaine Courrier prioritaire Cache IP Conversions d'en-têtes Signatures par défaut Dossiers publics et partagés DomainPOP Connexion RAS Journalisation 	Utilisez cette option pour que l'hôte distant distribue le courrier en attente. Cela s'effectue généralement en envoyant une commande ETRN/ATRN sur le port du courrier.
	OK Annuler Appliquer Aide

Retrait de file d'attente (Retrait de la file d'attente/ ETRN/ODMR/ATRN)

Activer le retrait file d'attente

Lorsqu'il s'agit de traiter du courrier distant, MDaemon peut se connecter à n'importe quel serveur sur n'importe quel port et envoyer n'importe quelle chaîne de caractères. C'est utile lorsque vous devez signaler à un serveur distant de libérer votre courrier en lui envoyant une chaîne de caractères. Exemple : ATRN, ETRN ou QSND. Vous pouvez également utiliser cette fonction lorsqu'une session FINGER ou TELNET est brièvement requise pour permettre à votre Hôte distant ou à votre FAI de déterminer que vous êtes en ligne.

Nom d'hôte ou IP

Il s'agit de l'hôte qui recevra le signal de libération de votre courrier.

Port

Entrez le port sur lequel vous souhaitez établir la connexion. Non par défaut = 25 (le port SMTP), qui convient à la méthode de signalisation ETRN ou QSND. Le port 366 est généralement utilisé pour ATRN, et le port 79 est utilisé pour FINGER.

Envoyer "EHLO" avant d'envoyer la chaîne de texte

Si vous activez cette case à cocher, vous devez vous connecter à un serveur SMTP pour signaler la libération de votre courrier. Ce commutateur lance une session SMTP

avec l'hôte spécifié et permet à la session de dépasser l'étapeSMTP "EHLO" avant d'envoyer la chaîne de déverrouillage.

Authentification avant l'envoi de la chaîne de texte (requise pour l'ATRN) Par mesure de sécurité, certains hôtes ou serveurs exigent que les clients s'authentifient à l'aide du protocole ESMTP AUTH avant de distribuer les messages en attente. Si c'est le cas pour votre hôte de messagerie, cochez cette case et saisissez les informations d'authentification requises ci-dessous.

> Aucune authentification requise n'est requise lors de l'utilisation de la commande ATRN pour la mise en file d'attente de votre courrier électronique.

Utilisateur AUTH

Saisissez ici le paramètre de connexion AUTH requis par votre hôte.

Mot passe AUTH

Saisissez ici le mot de passe AUTH.

Envoyer cette commande à l'hôte (laisser vide si une simple connexion suffit)

Dans cette commande, vous indiquez la chaîne de texte qui doit être envoyée pour que votre courrier soit libéré. Par Exemple, la méthodeETRN requiert le texte "ETRN" suivi du nom de domaine du site mis en file d'attente. D'autres méthodes nécessitent l'envoi d'un texte différent. Consultez votre FAI si vous avez besoin de plus d'informations sur ce qu'il faut envoyer pour débloquer votre file d'attente de courrier. Si vous avez le choix de la méthode à utiliser, nous vous recommandons d'utiliser le <u>Relais du courrier à la demande (ODMR)</u> ans la mesure du possible. L'ODMR nécessite l'utilisation de la commande ATRN dans cette option.

Le retrait de file attente lieu chaque [xx] fois que le courrier distant est traité (0=toujours) Non (par défaut), le signal de mise en file d'attente est envoyé chaque fois que le courrier distant est traité. La saisie d'un nombre dans cette commande empêchera l'envoi systématique du signal de mise en file d'attente. Il sera envoyé toutes les x fois désignées. Exemple : si cette valeur est fixée à "3", le signal sera envoyé toutes les trois fois que le courrier distant est traité.



Ce paramètre global s'applique à tous les domaines.

3.2.7.1 Relais du courrier à la demande (ODMR)

Lorsque vous avez besoin d'une méthode de file d'attente/dequeue pour l'hébergement et la libération de votre courrier électronique, nous vous recommandons d'utiliser le relais de courrier à la demande (ODMR) dans la mesure du possible. Cette méthode est supérieure à l'ETRN et à d'autres méthodes dans la mesure où elle requiert une authentification requise avant que le courrier ne soit libéré. De plus, elle utilise une commande ESMTP appelée ATRN qui ne nécessite pas que le client ait une adresse IP statique, car elle inverse immédiatement le flux de données entre le client et le serveur, en libérant les messages sans avoir à établir une nouvelle connexion pour ce faire (contrairement à l'ETRN).

MDaemon prend entièrement en charge l'ODMR du côté client en utilisant la commande ATRN et les contrôles d'authentification dans l' écran <u>Retrait</u> [275] <u>de la messagerie</u> [206], et du côté serveur en utilisant les fonctionnalités des passerelles de domaine dans l' écran<u>Mise en file d'attente de</u> [275] l'Éditeur de passerelles.

Certains serveurs de messagerie ne prennent pas en charge l'ODMR, il convient donc de vérifier auprès de votre fournisseur avant d'essayer de l'utiliser.

Voir :

Editeur de passerelle | Mise en file d'attente

3.2.8 Signatures

🗐 Domain Manager - Signatures		×
Domain Manager company.test Host Name & IP Smart Host Accounts MDIM Calendar Webmail Dequeuing Signatures Client Signatures Settings ActiveSync ActiveSync example.com	A domain signature is a block of text which MDaemon will append to all messages sent by users of a particular domain. Each domain can have its own signature. Domains without their own signature will have the default signatures appended. Plain text signature:	
	HTML signature (cut-and-paste from your favorite HTML editor): Note: (BDDY), (HTML), and their closing tags will be removed. Plain test signature will be created from HTML when only HTML is given.	>
		^
	<	>
	Ok Cancel Apply H	elp

Utilisez cet écran pour ajouter une signature à tous les messages envoyés par les utilisateurs de ce domaine. Si aucune signature n'est spécifiée ici, la <u>Signature par</u> <u>défaut</u> sera ajoutée à la place. Les signatures sont ajoutées au bas des messages, sauf pour les messages de listes de diffusion utilisant un <u>pied de page</u> suit, auquel cas le pied de page est ajouté sous la signature. Vous pouvez également utiliser la fonction<u>Signature de</u> a) l'éditeur de compte pour ajouter des signatures individuelles pour chaque compte. Les signatures de compte sont ajoutées juste avant les Signatures par défaut ou Domaine - Domaine.

Signature en texte brut

Cette zone permet d'insérer une signature en texte brut. Si vous souhaitez désigner une signature html correspondante à utiliser dans la partie texte/html des messages multipartites, utilisez la zone de*signature HTML* ci-dessous. Si une signature est incluse dans les deux zones, MDaemon utilisera la signature appropriée pour chaque partie du message multipart. Si aucune signature HTML n'est spécifiée, la signature en texte brut sera utilisée dans les deux parties.

Signature HTML (copier-coller à partir de votre éditeur HTML préféré)

Cette zone permet d'insérer une signature HTML, à rédiger en texte/html dans les messages multipart. Si une signature est incluse à la fois dans cette zone et dans la zone designature en texte brut ci-dessus, MDaemon utilisera la signature appropriée pour chaque partie du message multipart. Si aucune signature en texte brut n'est spécifiée, la signature html sera utilisée pour en créer une.

Pour créer votre signature html, saisissez le code html manuellement ou copiez-collez-le directement à partir de votre éditeur HTML préféré. Si vous souhaitez inclure des images en ligne dans votre signature HTML, vous pouvez le faire en utilisant la macro\$ATTACH_INLINE:path_to_image_file\$.

Exemple :

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
\images\mr t and arnold.jpg$">
```

Il existe également plusieurs façons d'insérer des images en ligne dans les signatures à partir de MDaemon. dans les signatures à partir de l'interface web de MDaemon Remote Admin : [376]

- Dans l'écran Signatures de MDaemon MDaemon Remote Admin, cliquez sur le bouton "Image" de la barre d'outils de l'éditeur HTML et sélectionnez l'onglet upload.
- Dans l'écran Signatures de l'administration à distance, cliquez sur le bouton "Ajouter une image" de la barre d'outils de l'éditeur HTML.
- Glisser-déposer une image dans l'éditeur HTML de l'écran Signatures avec Chrome, FireFox, Safari ou MSIE 10+.
- Copier et coller une image du presse-papiers dans l' éditeur HTMLde l'écran Signatures avec Chrome, FireFox, MSIE 11+.



Les balises <body></body> et <html></html> ne sont pas autorisées dans les signatures et seront supprimées lorsqu'elles seront trouvées.

Macros de signature

Les signatures MDaemon prennent en charge les macros qui insèrent dans la signature les Informations de contact de l'expéditeur, extraites du contact de l'expéditeur situé dans le Dossier public de son domaine. Cela permet de personnaliser les signatures par défaut et par domaine avec les informations de l'expéditeur. Par exemple, \$CONTACTFULLNAME\$ insère le nom complet de l'expéditeur et \$CONTACTEMAILADDRESS\$ insère l'adresse électronique de l'expéditeur. Utilisez Webmail, MDaemon Connector ou ActiveSync pour modifier les contacts publics. Des valeurs vides sont utilisées si aucun contact n'existe pour l'expéditeur. Les macros disponibles sont listées ci-dessous.

Les utilisateurs peuvent contrôler l'emplacement des signatures MDaemon dans leurs courriers électroniques en plaçant l'une des macros**du Sélecteur de signature** dans un message, à l'endroit où ils souhaitent que la signature apparaisse.

Sélecteur de signature		
\$SYSTEMSIGNATURE\$	Place la <u>Signature par défaut</u> [132] ou la <u>Signature du</u> <u>domaine</u> [210] dans un message. Si les deux existent, c'est la signature de domaine qui est utilisée.	
SIGNATURE DU CLIENT	Place la <u>Signature client par défaut</u> <u>Signature client par domaine dans</u> [216] un message. Si les deux existent, c'est la Signature client du domaine qui est utilisée.	
\$ACCOUNTSIGNATURE\$	Place la <u>signature du compte</u> l ^{®7} dans le message.	
Par noms et identifiants		
Votre nom complet	\$CONTACTFULLNAME\$\$ (NOM DE LA PERSONNE À CONTACTER)	
Votre nom	\$CONTACTFIRSTNAME\$ (PRÉNOM DU CONTACT)	
Deuxième prénom	\$CONTACTMIDDLENAME\$,	
Votre nom	NOM DE FAMILLE \$CONTACTLASTNAME\$	
Titre	TITRE \$CONTACTTITLE	
Suffixe	SUFFIXE \$CONTACTSUFFIX\$	
Surnom	NOM DE FAMILLE DU CONTACT	
Votre nom	PRÉNOM DE YOMI \$CONTACTYOMIFIRSTNAME	
Votre nom\$ \$contactyomifirstname\$ \$contactyomilastname	NOM DE FAMILLE \$CONTACTYOMILASTNAME\$	
Nom du compte	NOM DU COMPTE \$CONTACTACCOUNTNAME\$	

ID du client	\$CONTACTCUSTOMERID\$ (IDENTIFIANT DU CLIENT)	
Identifiant du gouvernement	ID DU GOUVERNEMENT \$CONTACTGOVERNMENTID	
Fichier comme	FICHIER EN TANT QUE \$CONTACTFILEAS\$	
Adresses électroniques		
Adresse électronique	ADRESSE ÉLECTRONIQUE \$CONTACTEMAILADDRESS	
Cette adresse électronique [2	ADRESSE DE COURRIEL 2\$ \$CONTACTEMAILADDRESS2	
Cette adresse électronique 3	\$CONTACTEMAILADDRESS3\$ (ADRESSE DE COURRIER ÉLECTRONIQUE)	
Numéros de téléphone et de fax		
Téléphone portable	TÉLÉPHONE PORTABLE \$CONTACTHOMEMOBILE	
Téléphone portable 2	\$CONTACTMOBILE2	
Téléphone de voiture	\$CONTACTNUMÉRODEVOITURE	
Téléphone fixe	\$CONTACT TÉLÉPHONE DOMICILE	
Téléphone fixe 2	\$CONTACTHOMEPHONE2\$ \$CONTACTHOMEPHONE3\$ \$CONTACTHOMEPHONE4	
Fax à domicile	\$CONTACTHOMEFAX	
Autre téléphone	\$CONTACTAUTRETÉLÉPHONE	
Messagerie instantanée et V	Veb	
Adresse IM	ADRESSE DE MESSAGERIE INSTANTANÉE \$CONTACTTIMADDRESS	
Adresse de messagerie instantanée 2	ADRESSE DE MESSAGERIE INSTANTANÉE 2\$ \$CONTACTIMADDRESS2	
Adresse IM 3	\$CONTACTIMADDRESS3	
Adresse MMS	ADRESSE MMS\$ \$CONTACTMMSADDRESS	
Adresse web du domicile	ADRESSE WEB DU DOMICILE \$CONTACTHOMEWEBADDRESS	
Adresse de la maison		
Adresse du domicile	\$CONTACTHOMEADDRESS	
Ville du domicile	\$CONTACTHOMECITY\$	

État du domicile	ÉTAT DU DOMICILE \$CONTACTHOMESTATE
Code postal du domicile	CODE POSTAL DU DOMICILE \$CONTACTHOMEZIPCODE
Pays d'origine	PAYS DU DOMICILE \$CONTACTHOMECOUNTRY
Autre adresse	\$CONTACTAUTREADRESSE
Autre ville	\$CONTACTOTHERCITY\$ (AUTRE VILLE)
Autre état	\$CONTACTAUTREÉTAT\$ AUTRE CODE POSTAL
Autre code postal	\$CONTACTOTHERZIPCODE\$ AUTRE CODE POSTAL
Autre pays	\$CONTACTOTHERCOUNTRY
Entreprise	
Nom de l'entreprise	\$CONTACTBUSINESSCOMPANY\$ (EN ANGLAIS)
Nom de l'entreprise Votre nom	\$CONTACTYOMICOMPANYNAME\$ (NOM DE L'ENTREPRISE)
Titre de l'entreprise	TITRE DE L'ENTREPRISE \$CONTACTBUSINESSTITLE
Bureau de l'entreprise	BUREAU DE L'ENTREPRISE \$CONTACTBUSINESSOFFICE\$
Département de l'entreprise	DÉPARTEMENT DE L'ENTREPRISE \$CONTACTBUSINESSDEPARTMENT
Chef d'entreprise	CONTACT MANAGER D'ENTREPRISE \$CONTACTBUSINESSMANAGER
Assistant(e) commercial(e)	ASSISTANT COMMERCIAL \$CONTACTBUSINESSASSISTANT
Téléphone de l'assistant commercial	TÉLÉPHONE DE L'ASSISTANT D'AFFAIRES \$CONTACTBUSINESSASSISTANT\$
Téléphone principal de l'entreprise	TÉLÉPHONE PRINCIPAL DE L'ENTREPRISE \$CONTACTBUSINESSMAINPHONE\$
Téléphone de l'entreprise	TÉLÉPHONE PRINCIPAL \$CONTACTBUSINESSMAINPHONE\$ TÉLÉPHONE PROFESSIONNEL \$CONTACTBUSINESSMAINPHONE\$ TÉLÉPHONE PROFESSIONNEL \$CONTACTBUSINESSMAINPHONE
Téléphone professionnel 2	TÉLÉPHONE PROFESSIONNEL 2\$ \$CONTACTBUSINESSPHONE2
Téléphone IP professionnel	TÉLÉPHONE IP PROFESSIONNEL \$CONTACTBUSINESSIPPHONE

Fax professionnel	FAX PROFESSIONNEL \$CONTACTBUSINESSFAX
Téléavertisseur professionnel	TÉLÉAVERTISSEUR D'ENTREPRISE \$CONTACTBUSINESSPAGER
Radio professionnelle	RADIO PROFESSIONNELLE \$CONTACTBUSINESSRADIO\$
Adresse professionnelle	ADRESSE DE L'ENTREPRISE \$CONTACTBUSINESSADDRESS
Ville de l'entreprise	VILLE DE L'ENTREPRISE \$CONTACTBUSINESSCITY
État de l'entreprise	ÉTAT DE L'ENTREPRISE \$CONTACTBUSINESSSTATE\$
Code postal de l'entreprise	CODE POSTAL DE L'ENTREPRISE \$CONTACTBUSINESSZIPCODE\$
Pays de l'entreprise	PAYS DE L'ENTREPRISE \$CONTACTBUSINESSCOUNTRY
Adresse web de l'entreprise	ADRESSE WEB DE L'ENTREPRISE \$CONTACTBUSINESSWEBADDRESS
Autre	
Conjoint	\$CONTACTCONJOINT\$
Enfants	\$CONTACTENFANTS\$
Catégories	CATÉGORIES\$ DE CONTACT
Commentaire	COMMENTAIRE\$CONTACT

Voir :

Signatures par défaut 132 Mon compte | Signature 807

3.2.9 Signatures clients

🛃 Domain Manager - Client Signatures		×
 Domain Manager def - company.test Host Name & IP Smart Host 	This signature can be pushed to Webmail and MDaemon Connector. In Webmail it's called the "System" signature. Each domain can have its own signature. Domains without their own signature will use the default signature.	
Accounts MDIM Calendar Webmail Dequeuing Signatures Client Signatures Settings ActiveSync example.com	CONTACTFULLNAME\$ \$CONTACTEMAILADDRESS\$	^
	<	>
	HTML signature (cut-and-paste from your favorite HTML editor): Note: <body>, <html>, and their closing tags will be removed. Plain text signature will be created from HTML when only HTML is given.</html></body>	
	<hp><!--</td--><td>~</td></hp>	~
	< 2	>
	Ok Cancel Apply H	elp

Utilisez cet écran pour créer une signature client pour ce domaine, que vous pouvez transmettre au <u>MDaemon Webmail</u> [197] et au <u>MDaemon Connector</u> [428], et qui sera utilisée par vos utilisateurs lors de la rédaction de messages électroniques. Vous pouvez utiliser les <u>macros</u> [217] listées ci-dessous pour personnaliser la signature, afin qu'elle soit unique pour chaque utilisateur, en incluant des éléments tels que le nom de l'utilisateur, son adresse e-mail, son numéro de téléphone, etc. Utilisez l' écran <u>Signatures client par</u> défaut [138] si vous souhaitez créer une signature différente qui sera utilisée lorsqu'aucune signature client spécifique à un domaine n'a été créée. Lorsqu'une signature spécifique au domaine existe, elle sera utilisée à la place de la Signature client par défaut. Utilisez l'option <u>Transmettre</u> [197] la signature client si vous souhaitez transmettre la signature client à Webmail et l' option<u>Transmettre la signature client à</u> <u>Outlook</u> [428] si vous souhaitez la transmettre à MDaemon Connector. Dans les options de composition de Webmail, la signature client transmise est appelée "Système". Pour MDaemon Connector, vous pouvez désigner un nom pour la signature qui apparaîtra dans Outlook.

Signature en texte clair

Cette zone permet d'insérer une signature en texte brut. Si vous souhaitez désigner une signature html correspondante à utiliser dans la partie text/html des messages multipart, utilisez la zone de*signature HTML* ci-dessous. Si une signature est incluse dans les deux zones, MDaemon utilisera la signature appropriée pour chaque partie du message multipart. Si aucune signature HTML n'est spécifiée, la signature en texte brut sera utilisée dans les deux parties.
Signature HTML (copier-coller à partir de votre éditeur HTML préféré)

Dans cette zone, vous pouvez insérer une signature HTML à utiliser dans la partie texte/html des messages multipart. Si une signature est incluse à la fois dans cette zone et dans la zone de*signature en texte brut* ci-dessus, MDaemon utilisera la signature appropriée pour chaque partie du message multipart. Si aucune signature en texte brut n'est spécifiée, la signature html sera utilisée pour en créer une.

Pour créer votre signature html, saisissez le code html manuellement ou copiez-collez-le directement à partir de votre éditeur HTML préféré. Si vous souhaitez inclure des images en ligne dans votre signature HTML, vous pouvez le faire en utilisant la macro\$ATTACH_INLINE:path_to_image_file\$.

Exemple :

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
\images\mr t and arnold.jpg$">
```

Il existe également plusieurs façons d'insérer des images en ligne dans les signatures à partir de l'interface web de l'<u>Administration de</u> **Barbing MDaemon Remote Admin** : **Barbing Remote Admin**

- Dans l'écran Signature client de MDaemon Remote Admin, cliquez sur le bouton "Image" de la barre d'outils de l'éditeur HTML et sélectionnez l'onglet upload.
- Dans l'écran Signature client de l'administration à distance, cliquez sur le bouton "Ajouter une image " de la barre d'outils de l'éditeur HTML.
- Glisser-déposer une image dans l'éditeur HTML de l'écran Signature client avec Chrome, FireFox, Safari ou MSIE 10+.
- Copier et coller une image du presse-papiers dans l'éditeur HTMLde l'écran Signature client avec Chrome, FireFox, MSIE 11+.



Les balises <body></body> et <html></html> ne sont pas autorisées dans les signatures et seront supprimées lorsqu'elles seront trouvées.

Macros de signature

Les signatures MDaemon prennent en charge les macros qui insèrent dans la signature les Informations de contact de l'expéditeur, extraites du contact de l'expéditeur situé dans le Dossier public de son domaine. Cela permet de personnaliser les signatures par défaut et par domaine avec les informations de l'expéditeur. Par exemple, \$CONTACTFULLNAME\$ insère le nom complet de l'expéditeur et \$CONTACTEMAILADDRESS\$ insère l'adresse électronique de l'expéditeur. Utilisez Webmail, MDaemon Connector ou ActiveSync pour modifier les contacts publics. Des valeurs vides sont utilisées si aucun contact n'existe pour l'expéditeur. Les macros disponibles sont listées ci-dessous.

Les utilisateurs peuvent contrôler l'emplacement des signatures MDaemon dans leurs courriers électroniques en plaçant l'une des macros**du Sélecteur de signature** dans

un message, à l'endroit où ils souhaitent que la signature apparaisse.

Sélecteur de signature	
\$SYSTEMSIGNATURE\$	Place la <u>Signature par défaut (132</u>) ou la <u>Signature du</u> <u>domaine</u> [210] dans un message. Si les deux existent, c'est la signature de domaine qui est utilisée.
SIGNATURE DU CLIENT	Place la <u>Signature client par défaut</u> [138] ou la <u>Signature client par domaine dans</u> [216] un message. Si les deux existent, c'est la Signature client du domaine qui est utilisée.
\$ACCOUNTSIGNATURE\$	Place la <u>signature du compte</u> [807] dans le message.
Par noms et identifiants	
Votre nom complet	\$CONTACTFULLNAME\$\$ (NOM DE LA PERSONNE À CONTACTER)
Votre nom	\$CONTACTFIRSTNAME\$ (PRÉNOM DU CONTACT)
Deuxième prénom	\$CONTACTMIDDLENAME\$,
Votre nom	NOM DE FAMILLE \$CONTACTLASTNAME\$
Titre	TITRE \$CONTACTTITLE
Suffixe	SUFFIXE \$CONTACTSUFFIX\$
Surnom	NOM DE FAMILLE DU CONTACT
Votre nom	PRÉNOM DE YOMI \$CONTACTYOMIFIRSTNAME
Votre nom\$ \$contactyomifirstname\$ \$contactyomilastname	NOM DE FAMILLE \$CONTACTYOMILASTNAME\$
Nom du compte	NOM DU COMPTE \$CONTACTACCOUNTNAME\$
ID du client	\$CONTACTCUSTOMERID\$ (IDENTIFIANT DU CLIENT)
Identifiant du gouvernement	ID DU GOUVERNEMENT \$CONTACTGOVERNMENTID
Fichier comme	FICHIER EN TANT QUE \$CONTACTFILEAS\$
Adresses électroniques	
Adresse électronique	ADRESSE ÉLECTRONIQUE \$CONTACTEMAILADDRESS
Cette adresse électronique [2	ADRESSE DE COURRIEL 2\$ \$CONTACTEMAILADDRESS2

Cette adresse électronique 3	\$CONTACTEMAILADDRESS3\$ (ADRESSE DE COURRIER ÉLECTRONIQUE)
Numéros de téléphone et de	e fax
Téléphone portable	TÉLÉPHONE PORTABLE \$CONTACTHOMEMOBILE
Téléphone portable 2	\$CONTACTMOBILE2
Téléphone de voiture	\$CONTACTNUMÉRODEVOITURE
Téléphone fixe	\$CONTACT TÉLÉPHONE DOMICILE
Téléphone fixe 2	\$CONTACTHOMEPHONE2\$ \$CONTACTHOMEPHONE3\$ \$CONTACTHOMEPHONE4
Fax à domicile	\$CONTACTHOMEFAX
Autre téléphone	\$CONTACTAUTRETÉLÉPHONE
Messagerie instantanée et V	Veb
Adresse IM	ADRESSE DE MESSAGERIE INSTANTANÉE \$CONTACTTIMADDRESS
Adresse de messagerie instantanée 2	ADRESSE DE MESSAGERIE INSTANTANÉE 2\$ \$CONTACTIMADDRESS2
Adresse IM 3	\$CONTACTIMADDRESS3
Adresse MMS	ADRESSE MMS\$ \$CONTACTMMSADDRESS
Adresse web du domicile	ADRESSE WEB DU DOMICILE \$CONTACTHOMEWEBADDRESS
Adresse de la maison	
Adresse du domicile	\$CONTACTHOMEADDRESS
Ville du domicile	\$CONTACTHOMECITY\$
État du domicile	ÉTAT DU DOMICILE \$CONTACTHOMESTATE
Code postal du domicile	CODE POSTAL DU DOMICILE \$CONTACTHOMEZIPCODE
Pays d'origine	PAYS DU DOMICILE \$CONTACTHOMECOUNTRY
Autre adresse	\$CONTACTAUTREADRESSE
Autre ville	\$CONTACTOTHERCITY\$ (AUTRE VILLE)
Autre état	\$CONTACTAUTREÉTAT\$ AUTRE CODE POSTAL
Autre code postal	\$CONTACTOTHERZIPCODE\$ AUTRE CODE POSTAL

Autre pays	\$CONTACTOTHERCOUNTRY
Entreprise	
Nom de l'entreprise	\$CONTACTBUSINESSCOMPANY\$ (EN ANGLAIS)
Nom de l'entreprise Votre nom	\$CONTACTYOMICOMPANYNAME\$ (NOM DE L'ENTREPRISE)
Titre de l'entreprise	TITRE DE L'ENTREPRISE \$CONTACTBUSINESSTITLE
Bureau de l'entreprise	BUREAU DE L'ENTREPRISE \$CONTACTBUSINESSOFFICE\$
Département de l'entreprise	DÉPARTEMENT DE L'ENTREPRISE \$CONTACTBUSINESSDEPARTMENT
Chef d'entreprise	CONTACT MANAGER D'ENTREPRISE \$CONTACTBUSINESSMANAGER
Assistant(e) commercial(e)	ASSISTANT COMMERCIAL \$CONTACTBUSINESSASSISTANT
Téléphone de l'assistant commercial	TÉLÉPHONE DE L'ASSISTANT D'AFFAIRES \$CONTACTBUSINESSASSISTANT\$
Téléphone principal de l'entreprise	TÉLÉPHONE PRINCIPAL DE L'ENTREPRISE \$CONTACTBUSINESSMAINPHONE\$
Téléphone de l'entreprise	TÉLÉPHONE PRINCIPAL \$CONTACTBUSINESSMAINPHONE\$ TÉLÉPHONE PROFESSIONNEL \$CONTACTBUSINESSMAINPHONE\$ TÉLÉPHONE PROFESSIONNEL \$CONTACTBUSINESSMAINPHONE
Téléphone professionnel 2	TÉLÉPHONE PROFESSIONNEL 2\$ \$CONTACTBUSINESSPHONE2
Téléphone IP professionnel	TÉLÉPHONE IP PROFESSIONNEL \$CONTACTBUSINESSIPPHONE
Fax professionnel	FAX PROFESSIONNEL \$CONTACTBUSINESSFAX
Téléavertisseur professionnel	TÉLÉAVERTISSEUR D'ENTREPRISE \$CONTACTBUSINESSPAGER
Radio professionnelle	RADIO PROFESSIONNELLE \$CONTACTBUSINESSRADIO\$
Adresse professionnelle	ADRESSE DE L'ENTREPRISE \$CONTACTBUSINESSADDRESS
Ville de l'entreprise	VILLE DE L'ENTREPRISE \$CONTACTBUSINESSCITY

État de l'entreprise	ÉTAT DE L'ENTREPRISE \$CONTACTBUSINESSSTATE\$
Code postal de l'entreprise	CODE POSTAL DE L'ENTREPRISE \$CONTACTBUSINESSZIPCODE\$
Pays de l'entreprise	PAYS DE L'ENTREPRISE \$CONTACTBUSINESSCOUNTRY
Adresse web de l'entreprise	ADRESSE WEB DE L'ENTREPRISE \$CONTACTBUSINESSWEBADDRESS
Autre	
Conjoint	\$CONTACTCONJOINT\$
Enfants	\$CONTACTENFANTS\$
Catégories	CATÉGORIES\$ DE CONTACT
Commentaire	COMMENTAIRE\$CONTACT

Voir :

Signatures client par défaut 138 Signatures par défaut 132 Gestionnaire de domaines | Signatures 210 Mon compte | Signature 807 Gestionnaire de domaines | Paramètres de Webmail 197 Paramètres du client MC | Signature 428

3.2.10 Paramètres



Nettoyage de compte & de courrier

Ces options sont utilisées pour déterminer si et quand les comptes inactifs ou les anciens messages seront supprimés par MDaemon. Tous les jours à minuit, MDaemon supprime tous les messages et comptes qui ont dépassé les limites de temps indiquées. Il existe des options similaires dans l'écranQuotas peuvent être utilisées pour remplacer ces paramètres pour des comptes individuels.

> Voir AccountPrune.txt dans le dossier"...MDaemon\App\" pour plus d'informations et les options de la ligne de commande.

Supprimer les comptes s'ils sont inactifs depuis plus plus de jours (0 = jamais)

Indiquez le nombre de jours pendant lesquels un compte appartenant à ce domaine doit être inactif avant d'être supprimé. Une valeur de "0" dans ce champ signifie que les comptes ne seront jamais supprimés pour cause d'inactivité.

Supprimer les messages plus anciens que ce nombre de jours (0 = jamais)

La valeur spécifiée dans ce champ correspond au nombre de jours pendant lesquels un message donné peut rester dans laboîte aux lettres d'un utilisateuravant d'être supprimé automatiquement par MDaemon. La valeur "0" signifie que les messages ne seront jamais supprimés en raison de leur ancienneté. **Remarque :** Le paramètre de cette option ne s'applique pas aux messages contenus dans les dossiers IMAP, sauf si vous activez également l'option " Nettoyer les anciens messages des dossiers IMAP également " ci-dessous.

PURGEZ les messages IMAP supprimés qui datent de plus de ce nombre de jours (0 = jamais)

Utilisez cette commande pour spécifier le nombre de jours pendant lesquels vous souhaitez que les messages IMAP marqués pour suppression restent dans les dossiers de vosutilisateurs. Les messages marqués pour suppression au-delà de ce nombre de jours seront supprimés de leurs boîtes aux lettres. La valeur "0" signifie que les messages marqués pour suppression ne seront jamais supprimés en raison de leur ancienneté.

Nettoyer également les anciens messages des dossiers IMAP

Cochez cette case si vous souhaitez que l'option"*Supprimer les messages effacés depuis plus d'un jour*" ci-dessus s'applique également aux messages des dossiers IMAP. Lorsque ce contrôle est désactivé, les messages ordinaires contenus dans les dossiers IMAP ne seront pas supprimés en raison de leur ancienneté.

Paramètres de domaine

Taille max. des messages provenant d'expéditeurs authentifiés [xx] Ko (0=pas limite) Utilisez cette option si vous souhaitez fixer une limite à la taille des messages qu'un expéditeur authentifié peut envoyer au domaine. La valeur est exprimée en kilooctets et est fixée à "0" par défaut, ce qui signifie qu'il n'y a pas de limite. Si vous souhaitez fixer une limite à la taille des messages pour les expéditeurs non authentifiés, utilisez l'option"...tous les autres expéditeurs" ci-dessous.

Taille max des messages provenant des autres expéditeurs [xx] Ko (0 = pas de limite) (0=pas de limite)

Utilisez cette option si vous souhaitez fixer une limite à la taille des messages qu'un expéditeur non authentifié peut envoyer au domaine. La valeur est exprimée en kilooctets et est fixée à "0" par défaut, ce qui signifie qu'il n'y a pas de limite. Si vous souhaitez fixer une limite de taille des messages pour les expéditeurs authentifiés, utilisez l'option précédente.

Espace disque max par compte [xx] par mois (0=pas de limite) (Cloud uniquement)

Utilisez cette option si vous souhaitez définir une limite sur l'espace disque que le domaine peut utiliser. Cette option est uniquement disponible dans MDaemon Private Cloud.

Nombre maximum de membres par liste de diffusion [xx] (0 = pas de limite) (Cloud uniquement)

Utilisez cette option si vous souhaitez définir un nombre maximum de membres autorisés pour chacune des listes de diffusion de ce domaine. Il existe une option globale correspondante sur l'écran Paramètres de la liste de diffusion du Gestionnaire de listes diffusion. Cette option est uniquement disponible dans MDaemon Private Cloud.

Max messages envoyés par heure [xx] (0=pas de limite) (Cloud uniquement)

Utilisez cette option si vous souhaitez désigner un nombre maximum de messages que le domaine peut envoyer par heure. Dans cette limite, les autres messages sont laissés dans la file d'attente jusqu'à ce que le compte soit réinitialisé. Le nombre de messages est réinitialisé toutes les heures et lorsque le serveur est redémarré. Cette option est uniquement disponible dans MDaemon Private Cloud.

Activer le service antivirus pour ce domaine

Cochez cette case si vous souhaitez que les paramètres de l'<u>AntiVirus</u> soient appliqués à ce domaine.

Activer le service anti-spam pour ce domaine

Cochez cette case si vous souhaitezque les paramètres actuels du Filtre anti-spam deMDaemonsoient appliqués à ce domaine.

Activer le service MDaemon Connector pour ce domaine (Cloud uniquement)

Cochez cette case si vous souhaitez activer le service<u>MDaemon Connector</u> pour ce domaine.

Voir :

Mon compte | Quotas 784

3.2.11 ActiveSync



Utilisez cette section du Gestionnaire de domaines pour administrer les paramètres ActiveSync du domaine. Vous pouvez gérer les paramètres ActiveSync et les paramètres par défaut de tous les domaines à partir de l'écran Domaines du Gestionnaire ActiveSync.

ActiveSync for MDaemon Management Plugin (Plugin de gestion d'ActiveSync pour MDaemon)

Activer le service ActiveSync pour ce domaine

Cette option contrôle si les utilisateurs du domaine pourront ou non utiliser par défaut un client ActiveSync pour accéder à leur courrier électronique et à leurs données PIM. Par défaut, l'état de ce paramètre est hérité de l'<u>état d'ActiveSync</u> <u>par défaut</u> [462], mais vous pouvez remplacer ce paramètre si vous le souhaitez en activant ou désactivant la case à cocher. Ce paramètre peut également être remplacé pour tous les <u>comptes</u> [479] ou <u>clients</u> [486] pour lesquels vous ne souhaitez pas utiliser le paramètre du domaine. **REMARQUE :** Si vous désactivez ActiveSync pour ce domaine, une boîte de confirmation s'ouvrira pour vous demander si vous souhaitez retirer aucun accès ActiveSync pour tous les utilisateurs du domaine. Choisissez **Non** si vous souhaitez permettre aux utilisateurs du domaine qui utilisent actuellement ActiveSync de continuer à l'utiliser. Si vous choisissez **Oui**, ActiveSync sera alors désactivé pour tous les utilisateurs de ce domaine.



Ce paramètre contrôle simplement si les comptes du domaine seront autorisés ou non à utiliser ActiveSync par défaut, lorsque le service ActiveSync est en cours d'exécution. L'option globale <u>Activer le protocole ActiveSync</u> [441] doit être activée pour que ActiveSync soit accessible aux domaines ou comptes activés.

Voir :

ActiveSync | Domaines 462 ActiveSync | Comptes 479 ActiveSync | Clients 488

3.2.11.1 Paramètres client

🛃 Domain Manager - Client Settings	
Domain Manager company.test Host Name & IP Smart Host Accounts MDIM	General FolderSync Options Content Handling Troubleshooting Log level Use inherited or default Archive transactions as XML WBXML Im Validate/correct PIM mrk file integrity
Calendar Webmail Dequeuing Signatures Client Signatures Client Signatures Settings ActiveSync <mark>Client Settings</mark> Policy Manager Assigned Policy Ascounts Clients	Client Options Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation New clients require administrative approval Max clients per user Use inherited or default Bandwidth reset Day Use inherited or default Security Exempt from Location Screen Dynamically allow remote address
example.com	Disallow Factory Reset Wipes Allow clients provisioned/managed by other servers Example of Settings Off On Inherit from parent Preview Effective Settings Settings are inherited in the order Global, Domain, Group, Account, Client Type, then Client. Any non- inherit setting in a subsequent level over-rides the previous level. Group based settings are applied in lowest to highest priority order. Not all options are available at all levels. If a setting is not available to Ok Cancel Apply Help

Cet écran vous permet de gérer les paramètres par défaut des comptes et des clients associés au domaine.

Non (par défaut), toutes les options de cet écran sont définies sur "Utiliser les paramètres hérités ou par défaut", ce qui signifie que chaque option prendra ses paramètres de l'option correspondante sur l' écran <u>Paramètres client globaux</u> [47]. De même, les paramètres des <u>comptes</u> [191] de ce domaine seront hérités de cet écran, puisqu'il s'agit de leur écran parent. Toute modification apportée aux options de cet

écran sera répercutée sur les écrans de ces comptes. En dessous, les <u>clients</u> [252] individuels ont également des écrans de paramètres qui héritent leurs paramètres des paramètres au niveau du compte. Cette configuration vous permet d'apporter des modifications à tous les comptes et clients du domaine en modifiant simplement cet écran, tout en vous permettant de remplacer ces paramètres pour n'importe quel compte ou client si nécessaire.

Général

Résolution des problèmes

Niveau de journalisation

ActiveSync for MDaemon prend en charge six niveaux de journalisation, du plus élevé au plus faible :

- Déboga Il s'agit du niveau de journalisation le plus complet. Il consigne
 ge toutes les entrées disponibles et n'est généralement utilisé que pour diagnostiquer un problème.
 - **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.
- AvertisLes avertissements, les erreurs, les erreurs critiques et lessementévénements de démarrage/arrêt sont consignés dans le journal.
 - **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Critiqu Les erreurs critiques et les événements de démarrage/arrêt sont e journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.
- **Hériter** Non (par défaut), le niveau journalisation est hérité de la hiérarchie des Paramètres clients. Ainsi, les clients héritent leurs paramètres des Types de clients, les Types de clients des Comptes, les Comptes des Groupes, etc. Le Paramètres globaux du client pour cette option est déterminé par le paramètre de niveau de journalisation dans le dialogue<u>Diagnostics</u>[457].

Archiver les transactions en [XML | WBXML]

Utilisez les options d'archivage*XML...* et *WBXML* si vous souhaitez enregistrer ces données, qui peuvent parfois être utiles à des fins de débogage. Les options globales sont désactivées par défaut.

Valider/corriger l'intégrité du fichier mrk PIM

Cette option exécute un processus de validation et de correction des données PIM du client afin de rechercher les problèmes connus susceptibles d'empêcher une synchronisation correcte, tels que des UID iCal en double ou des champs facultatifs vides. L'option globale est désactivée par défaut.

Options client

Appliquer les restrictions de protocole

Activez cette option si vous souhaitez refuser les connexions de tout client qui tente d'utiliser un protocole autre que les *Versions du protocole autorisées* spécifiées pour le client. Non (par défaut), cette option est désactivée, ce qui signifie que les restrictions de protocole n'empêchent pas un client d'utiliser un protocole différent ; elles indiquent simplement au client quels protocoles utiliser. Si un client tente malgré tout d'utiliser un protocole restreint, MDaemon autorisera quand même la connexion. Pour plus d'informations, voir <u>Restrictions de protocole</u> [459] pour plus d'informations.

Répondre à 'Get/UserInformation' en utilisant l'alias de l'identifiant comme 'adresse SMTP principale'

Dans ce cas, le service peut renvoyer un Alias/une adresse secondaire en tant qu'adresse primaire en réponse à une requête de type Configurer/Gérer/Informations sur l'utilisateur. Cela permet de contourner un problème causé par une mise à jour postérieure à iOS9.x qui faisait que les clients ne pouvaient pas envoyer de courrier à l'aide d'un alias. L'utilisation de cette option résulte en une réponse non conforme aux spécifications à Settings/Get/UserInformation.

Les nouveaux clients doivent recevoir l'autorisation de l'administrateuravant de synchroniser.

Activez cette option si vous souhaitez que les nouveaux clients soient autorisés par un administrateur avant de pouvoir commencer à se synchroniser avec un compte. La liste <u>Clients</u> indique tous les clients en attente d'autorisation, et l'administrateur peut les autoriser à partir du même écran. Ce paramètre est Non (par défaut).

Max. clients par utilisateur

Si vous souhaitez limiter le nombre de clients ActiveSync ou de terminaux qui peuvent être associés à un compte MDaemon, indiquez le nombre souhaité dans cette option. L'option globale est réglée sur "illimité" par défaut. Cette option est disponible sur les écrans Paramètres clients globaux, de domaine et de compte, et non sur les écrans Clients individuels.

Jour de réinitialisation de la bande passante

Utilisez cette option si vous souhaitez réinitialiser les statistiques d'utilisation de la bande passante pour les Terminaux ActiveSync un jour précis de chaque mois. L'événement de réinitialisation a lieu dans le cadre du processus de maintenance nocturne normal et est consigné dans le journal du système comme les autres routines de maintenance. L'option globale est réglée sur "0 (Jamais)" par défaut, ce qui signifie que les statistiques d'utilisation ne seront jamais réinitialisées. Paramétrez les options enfant sur un jour différent si, par exemple, vous souhaitez que le jour de réinitialisation coïncide avec la date de réinitialisation de la facturation de l'opérateur sans fil d'un utilisateur ou d'un client.

Sécurité

Exclure du Filtrage de pays

Activez cette option dans l'écran des paramètres d'un client ActiveSync si vous souhaitez que l'appareil puisse filtrer l' <u>écran de localisation</u> . Cela permet à un utilisateur valide de continuer à accéder à son compte via ActiveSync lorsque, par exemple, il se rend à un endroit où les tentatives d'authentification sont bloquées. Pour que l'appareil soit exempté, il doit s'être connecté et authentifié via ActiveSync dans le délai configuré dans le paramètre<u>Supprimer les clients inactifs après ce</u> <u>nombre de jours</u> 443 situé dans l'écran Régètres.

Autoriser dynamiquement l'adresse distante

Si vous excluez un pays du Filtrage de l'emplacement, activez cette option si vous souhaitez également autoriser l'adresse IP distante à partir de laquelle il se connecte. Cela peut s'avérer utile pour autoriser d'autres clients susceptibles de se connecter à partir de la même adresse IP.

Autoriser les clients gérés par d'autres serveurs

Par défaut, lorsque le serveur ActiveSync envoie des données de provisionnement/des spécificités de politiques à un client et que celui-ci signale qu'il est également géré par un autre serveur ActiveSync, le client sera toujours autorisé à se connecter à MDaemon. Dans ce cas, il n'y a aucun moyen de s'assurer que les spécificités de votre politique seront appliquées lorsqu'elles entrent en conflit avec la politique de l'autre serveur ActiveSync. En général, les clients utilisent par défaut l'option la plus restrictive en cas de conflit. Désactivez cette option si vous ne souhaitez pas autoriser ces clients à se connecter.

Interdire les réinitialisations aux paramètres d'usine

Si cette option est activée (On/Oui), il ne sera pas possible d'**effacer complètement** un client ActiveSync. Si vous souhaitez pouvoir effectuer un Effacer complètement à distance sur un client, vous devez d'abord désactiver cette option. L'option est désactivée par défaut. Pour plus d'informations, voir : <u>Effacer</u> <u>complètement un client ActiveSync</u> with sur la page Clients.

Options FolderSync

Options de dossier

Exclure

Dossier Expéditeurs bloqués autorisés/ bloqués

Par défaut, les dossiers Expéditeurs autorisés et Dossiers Expéditeurs bloqués de l'utilisateur ne sont pas synchronisés avec les périphériques. Ils ne sont généralement utilisés par MDaemon que dans le cadre de la prévention automatique du spam. C'est pourquoi ils n'ont pas besoin d'être affichés sur les appareils en tant que contacts.

Dossiers de courrier personnalisés (Non par défaut)

Par défaut, tous les Dossiers de courrier créés par l'utilisateur et par défaut peuvent être synchronisés avec le terminal. Activez cette option si vous souhaitez que seuls les dossiers courrier par défaut soient synchronisés, c'est-àdire la Boîte de réception, les Éléments envoyés, les Éléments supprimés, les Brouillons, etc. Aucun dossier créé par l'utilisateur ne sera inclus. Cette option est désactivée par défaut.

Dossiers PIM personnalisés non (par défaut)

Par défaut, tous les dossiers PIM de l'utilisateur (contacts, calendrier, notes, tâches, etc.) sont synchronisés avec l'appareil. Activez cette option si vous souhaitez que seuls les dossiers PIM par défaut soient synchronisés. Exemple : si cette option est activée et qu'un utilisateur possède plusieurs dossiers de calendrier, seul le calendrier par défaut sera synchronisé. Cette option est désactivée par défaut.

Inclure

Arborescence Dossiers publics

Cochez cette case si vous souhaitez que les <u>Dossiers publics</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers publics</u> auxquels il a accès. Cette option est autorisée par défaut.

Navigation dans les dossiers publics (affiche les noms de dossiers)

Non par défaut, pour qu'un client puisse synchroniser un sous-dossier public ou y accéder, le compte doit disposer de l'<u>autorisation de Recherche</u> and pour le sousdossier (c'est-à-dire le dossier enfant) et tous les <u>Dossiers publics</u> and parents situés au-dessus. Si le compte n'a pas l'autorisation de voir les dossiers parents, il ne peut pas non plus voir le dossier enfant, même s'il en a l'autorisation. Activez cette option si vous souhaitez autoriser le client à accéder à ces dossiers enfants. **Par nom : l** 'activation de cette option doit nécessairement révéler les noms des dossiers parents au client, ce qui pourrait être considéré comme un risque de sécurité. Cette option est désactivée par défaut.

Nombre max de Dossiers publics

Utilisez cette option si vous souhaitez limiter le nombre de Dossiers publics autorisés sur le périphérique. Lorsqu'une limite est définie, le serveur parcourt la liste des dossiers jusqu'à ce que la limite soit atteinte, puis plus aucun dossier n'est envoyé à l'appareil. Il n'existe aucun moyen de garantir l'ordre dans lequel les dossiers seront traités. Non (paramètres par défaut).

Dossiers IMAP partagés

Cochez cette case si vous souhaitez que les <u>dossiers partagés</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers partagés</u> auxquels il a accès. Cette option est autorisée par défaut.

Gestion du contenu

Options de gestion des e-mails

Créer des tâches/rappels pour les e-mails avec indicateurs

Cette option permet à MDaemon de rappeler à l'utilisateur les éléments marqués, en créant un élément de tâche pour chaque courrier électronique marqué. lorsque le client le demande. L'option globale de ce contrôle est activée par défaut.

Toujours envoyer les mises à jour de réunion lorsque l'événement est modifié

Certains clients n'envoient pas correctement les e-mails de mise à jour des réunions lorsqu'ils modifient une réunion. Cette option indique au service ActiveSync d'envoyer une mise à jour de la réunion lorsqu'un élément de la réunion est mis à jour par l'organisateur. Cette option ne doit être définie que pour les <u>clients</u> and et les <u>types de clients</u> ou n'envoient pas correctement les mises à jour de réunion, sous peine d'envoyer des mises à jour de réunion en double. Par conséquent, cette option n'est disponible que dans les pages de paramètres pour les Clients et les Types de clients.

Demander des confirmations de lecture pour tous les e-mails envoyés

Activez cette option si vous souhaitez que le serveur demande des confirmations de lecture pour tous les courriers envoyés par un client. Cette option est désactivée par défaut.

Envoyer des confirmations de lecture du serveur lorsque le courrier est marqué comme lu et lorsque l'expéditeur le demande.

Activez cette option si vous souhaitez que le serveur prenne en charge les demandes de confirmation de lecture et délivre un accusé de réception de lecture lorsqu'un message est marqué comme lu par un client. Cette option est désactivée par défaut.

Envoyer avec l'alias spécifié dans ReplyTo

Certains clients peuvent ne pas autoriser un expéditeur à envoyer du courrier à l'aide d'un alias. Cette fonctionnalité a été ajoutée au <u>protocole Exchange ActiveSync</u> (EAS) [459] 16.x, mais certains clients ne supportent pas la version 16.x. Par exemple, Outlook pour Windows n'utilise que EAS 14.0, et bien qu'il permette à un utilisateur de spécifier une autre adresse pour l'envoi, le message généré ne reflète pas correctement les choix de l'utilisateur. Cette faculté permet d'utiliser le champ ReplyTo pour envoyer l'e-mail, à condition que l'adresse ReplyTo soit un <u>alias</u> <u>valide</u> [84] pour cet utilisateur. L'option globale est activée par défaut.

Fusionner virtuellement les contacts publics et les contacts par défaut

Activez cette option si vous souhaitez fusionner les contacts publics avec les contacts par défaut de l'utilisateur sur le terminal. Il s'agit uniquement d'une fusion virtuelle, c'est-à-dire qu'ils ne sont pas réellement copiés dans le dossier des contacts de l'utilisateur. Cela peut être utile sur les clients qui ne prennent pas en charge les recherches dans la liste d'adresses globale (GAL). Non (par défaut).

Dossiers Expéditeurs bloqués lors du déplacement d'un courrier dans le dossier Courriers indésirables

Si cette option est activée, lorsqu'un client déplace un e-mail vers le dossier Courriers indésirables du compte, le service ajoute l'adresse SENDER\$ - adresse de l'expéditeur de cet e-mail au dossier Contacts des expéditeurs bloqués.

Forcer l'envoi des réponses aux réunions lorsqu'une demande de réunion est acceptée/déclinée, etc.

Dans cette option, lorsqu'un client accepte, refuse ou choisit une action en réponse à une demande de réunion, le service envoie une réponse à l'organisateur de la réunion. Cette fonction est destinée aux clients spécifiques qui n'envoient pas correctement ces mises à jour eux-mêmes.

Aperçu des paramètres effectifs

Ce bouton est disponible sur tous les écrans des Paramètres clients enfant (c.-à-d. <u>domaines</u> 402, <u>comptes</u> 479 et <u>clients</u> 480). Non (par défaut), les options de ces écrans sont définies pour hériter de leurs paramètres d'un écran parent. Utilisez cette fonction pour voir quels paramètres sont actuellement appliqués à l'écran affiché.

Voir :

ActiveSync | Paramètres du client 447 ActiveSync | Comptes 479 ActiveSync | Clients 488





Utilisez cet écran pour gérer les Politiques ActiveSync qui peuvent être attribuées aux terminaux des utilisateurs pour régir diverses options. Des politiques prédéfinies sont fournies, et vous pouvez créer, modifier et supprimer les vôtres. Les politiques par défaut et les politiques dérogatoires peuvent être attribuées au domaine et à chaque <u>compte</u> [479] et <u>client</u> [488] sur leurs écrans respectifs de Politique attribuée.

Tous les terminaux ActiveSync ne reconnaissent pas ou n'appliquent pas les politiques de manière cohérente. Certains peuvent ignorer les politiques ou certains éléments de politique, et d'autres peuvent nécessiter un redémarrage de l'appareil avant que les changements ne prennent effet. De plus, lorsque vous tentez d'attribuer une nouvelle politique à un terminal, elle ne sera pas appliquée à ce dernier avant sa prochaine connexion au serveur ActiveSync ; les politiques ne peuvent pas être "poussées" vers le terminal avant qu'il ne se connecte.

Politiques ActiveSync

Cliquez avec le bouton droit de la souris sur la liste pour ouvrir le menu contextuel avec les options suivantes :

Créer une stratégie

Cliquez sur cette option pour ouvrir l'<u>Éditeur de politiques ActiveSync</u> (234), utilisé pour créer et modifier vos politiques.

Supprimer

Pour supprimer une politique, sélectionnez une politique personnalisée dans la liste, puis cliquez sur **Supprimer**. Cliquez sur **Oui** pour confirmer l'action. Les règles prédéfinies ne peuvent pas être supprimées.

Modifier vos politiques

Pour modifier une politique, cliquez avec le bouton droit de la souris sur une politique personnalisée de la liste, puis cliquez sur **Modifier la politique**. Dans l'éditeur de politique, après avoir effectué les modifications souhaitées, cliquez sur **OK**. Les politiques prédéfinies ne peuvent pas être modifiées.

Afficher l'utilisation d'une politique

Cliquez avec le bouton droit de la souris sur une stratégie, puis choisissez cette option pour afficher une liste de tous les domaines, comptes et clients configurés pour utiliser cette stratégie.

Éditeur de politiques ActiveSync

L'Éditeur de politiques ActiveSync comporte quatre onglets : Général, Mots de passe, Sync et Paramètres avancés. L'onglet Paramètres avancés est caché à moins que vous n'activiez <u>Activer les options avancées de la politique</u> [441], situé sur l'écran Système ActiveSync System.

Général

Cet écran vous permet de donner un nom et une description à votre politique. Vous pouvez également prévisualiser le document XML de la politique.

Editing Policy: New Policy 2022-04-27T17:31:44.749Z {26a3ef60-bcee-415e-9225-d461	×
General Passwords Sync Advanced Settings	
Administrative Name New Policy 2022-04-27T17:31:44.7492 Description Preview Policy Document	
OK Cancel Help	

Nom administratif

Par nom

Indiquez ici un nom pour votre politique personnalisée.

Description

Utilisez cette zone pour décrire votre politique personnalisée. Cette description apparaît dans la boîte de dialogue Appliquer une politique lors de la sélection d'une politique à appliquer à un domaine, un compte ou un client.

Prévisualiser le document de politique

Cliquez sur ce bouton pour prévisualiser le document de politique XML pour cette politique.

■ Mots de passe

Les options mot passe et les mots requis pour la politique sont désignés dans cet onglet.

Editing Policy: New Policy 2022-04-27T17:31	:44.749Z {26a3ef60-bcee-415e-9225-d461 ×
General Passwords Sync Advanced Setti	ngs
Require password	
Allow client to save 'Recovery Password'	to server
Password Type	Password Strength
Simple PIN	Minimum length
Complex/Alpha-Numeric	Complexity level 1
Password Options	
	Days until password expires 0
Number of recent password	s remembered/disallowed by client 0
Minu	tes of inactivity before client locks
Wipe client or enter 'Timed Lockout Mode	after repeated failed password attempts
Failed password attempts before client wip	bes or enters 'Timed Lockout Mode' 0
ОК	Cancel Help

Exigences relatives aux mots passe

Cochez cette case si vous souhaitez exiger un mot de passe sur le périphérique. Elle est désactivée par défaut.

Activer le Mot de passe de récupération de l'appareil sur le serveur

Activez cette option si vous souhaitez autoriser les clients à utiliser l'option "Mot de passe de récupération" d'ActiveSync, qui permet à un appareil d'enregistrer un mot de passe de récupération temporaire sur le serveur pour déverrouiller l'appareil en cas d'oubli du mot de passe. L'administrateur peut trouver ce mot de passe de récupération dans les <u>détails du</u> (488) client . La plupart des appareils ne prennent pas en charge cette fonction.

Type de mot de passe

Code PIN simple

La mise en œuvre de cette option dépend largement du terminal, mais le fait de sélectionner *Code PIN simple* comme type de mot de passe signifie généralement qu'aucune restriction ou exigence de complexité n'est imposée au mot de passe du terminal, à l'exception de l' option*Longueur minimale du mot de passe* ci-dessous. Autoriser les mots de passe simples tels que : "111", "aaa", "1234", "ABCD", etc.

Complexe/Alpha-Numérique

Utilisez cette option de politique si vous souhaitez exiger des mots de passe de périphérique plus complexes et plus sûrs que l'option *Code PIN simple.* Utilisez l'option*Niveau du complexité* ci-dessous pour définir exactement le degré de

complexité du mot de passe. Il s'agit de la sélection par défaut lorsqu'un mot de passe est demandé par la politique.

Force du mot de passe

Longueur minimale

Utilisez cette option pour définir le nombre minimum de caractères que le mot de passe du périphérique doit contenir, de 1 à 16. Cette option est définie sur "1" par défaut.

Niveau de complexité

Cette option permet de définir le niveau de complexité requis pour les mots de passe de périphérique*complexes/alphanumériques*. Le niveau correspond au nombre de types de caractères différents que le mot de passe doit contenir : lettres majuscules, lettres minuscules, chiffres et caractères non alphanumériques (tels que la ponctuation ou les caractères spéciaux). Vous pouvez exiger de 1 à 4 types de caractères. Exemple : si cette option est définie sur "2", le mot de passe doit contenir au moins deux des quatre types de caractères : majuscules et chiffres, majuscules et minuscules, chiffres et symboles, etc. Cette option est fixée à "1" par défaut.

Options de mot de passe

Jours avant expiration du mot passe (0=jamais)

Il s'agit du nombre de jours autorisés avant que le mot de passe de l'appareil ne doive être modifié. Cette option est désactivée par défaut (définie sur "0").

Nombre de mots de passe récents retenus/refusés par le dispositif (0 = aucune)

Utilisez cette option si vous souhaitez empêcher le périphérique de réutiliser un nombre spécifié d'anciens mots de passe. Exemple : si cette option est réglée sur "2" et que vous modifiez le mot de passe de votre appareil, vous ne pourrez pas le remplacer par l'un des deux derniers mots de passe utilisés. Cette option est désactivée par défaut (paramètres par défaut).

Minutes d'inactivité avant le verrouillage de l'appareil (0 = jamais)

Il s'agit du nombre de minutes pendant lesquelles un appareil peut rester sans intervention de l'utilisateur avant de se verrouiller. Cette option de mot passe est désactivée par défaut (réglée sur "0").

Effacer le terminal ou passer en mode Verrouillage temporaire après des tentatives échouées consécutives.

Lorsque cette option est activée et que l'utilisateur échoue le nombre de tentatives échouées, le terminal se verrouille pendant un certain temps ou efface toutes les données, en fonction du terminal. Cette option est désactivée par défaut.

Tentatives échouées de mot de passe avant que l'appareil ne s'efface ou ne passe en mode "Verrouillage temporaire".

Lorsque l'option"*Effacer l'appareil…*" ci-dessus est activée et qu'un utilisateur échoue à ce nombre de tentatives de mot de passe, l'appareil

sera effacé ou le "mode de verrouillage temporisé" sera déclenché, en fonction de l'appareil.

Synchronisation

Cet écran contient divers paramètres régissant les e-mails au format HTML, autorisant les pièces jointes, limitant le nombre de caractères à transférer et les délais maximums de synchronisation du courrier et du calendrier.

Editing Policy: New Policy 2022-04-27T17:31:44.749Z {26a3ef60-bcee-415e-92	225-d461	\times
General Passwords Sync Advanced Settings		
Mail Settings		
Maximum attachment size in bytes (0=no limit)	0	
Maximum characters of text body to transfer (-1=no limt)	-1	
Maximum characters of HTML body to transfer (-1=no limt)	-1	
Maximum timeframe of mail to synchronize All	~	
Calendar Maximum historical timeframe of calendar to sync All	~	
OK Cancel	Help	

Paramètres du courrier

Autoriser les e-mails au format HTML

Non (par défaut), les e-mails au format HTML peuvent être synchronisés/envoyés aux clients ActiveSync. Décochez cette case si vous souhaitez envoyer uniquement du texte brut.

Autoriser pièces jointes

Autorise le téléchargement des pièces jointes sur terminal. Cette option est activée par défaut.

Taille maximale des pièces jointes en octets (0 = pas de limite) (0=pas de limite)

Il s'agit de la taille maximale de la pièce jointe qui peut être téléchargée automatiquement sur l'appareil. Aucune taille limite n'est fixée pour cette option par défaut (0=pas de limite).

Caractères max du corps du texte à transférer (-1 = pas de limite)

Ce nombre maximum de caractères dans le corps des messages électroniques au format texte brut qui seront envoyés au client. Si le corps du message contient plus de caractères que ce qui est autorisé, le corps sera tronqué jusqu'à la limite spécifiée. Non (par défaut) par défaut, aucune limite n'est fixée (option fixée à "-1"). Si la valeur de l'option est "0", seul l'en-tête du message est envoyé.

Caractères max du corps HTML à transférer (-1 = pas de limite)

Il s'agit du nombre maximum de caractères dans le corps des e-mails au format HTML qui seront envoyés au client. Si le corps du message contient plus de caractères que ce qui est autorisé, le corps sera tronqué jusqu'à la limite spécifiée. Non (par défaut), aucune limite n'est fixée (option fixée à "-1"). Si la valeur de l'option est "0", seul l'en-tête du message est envoyé.

Période max. de synchronisation des e-mails

Il s'agit de la quantité de courrier électronique passé, par plage de dates à partir d'aujourd'hui, qui peut être synchronisée par l'appareil. Non (par défaut), cette option est réglée sur "Tous", ce qui signifie que tous les courriels peuvent être synchronisés, quelle que soit leur ancienneté.

Calendrier

Période max. de synchronisation du calendrier à synchroniser

Il s'agit de l'intervalle de temps à partir d'aujourd'hui pendant lequel les entrées de calendrier passées peuvent être synchronisées par l'appareil. Non (par défaut) est réglé sur "Tous", ce qui signifie que toutes les entrées passées peuvent être synchronisées, quelle que soit leur ancienneté.

Paramètres avancés

L'onglet Paramètres avancés contient des options régissant les types de connexions autorisées, l'activation de certaines applications, le stockage et le cryptage, ainsi que l'itinérance.

Editing Policy: New Policy 2022-04-27T17:31:4	4.749Z {26a3ef60-bcee-415e-9225-d461 🗙
General Passwords Sync Advanced Setting	IS
Connections Allowed Bluetooth Yes ✓ WIFI Infrared (IrDA) Internet sharing (portable hotspot)	Storage Require client encryption Allow storage card Require storage card encryption Desktop sync
Applications Web browser enabled Camera enabled Consumer email enabled POP/IMAP email enabled	Remote Desktop enabled Unsigned applications allowed Unsigned installers allowed Text messaging enabled
Roaming Require manual sync while roaming OK	Cancel Help

Cet onglet est caché à moins que vous n'activiez <u>Activer l'édition des options</u> <u>de politique avancées</u> [41], situé sur l'écranServeur ActiveSync for MDaemon.

Connexions autorisées

Bluetooth

Cette option permet d'indiquer si les connexions Bluetooth sont autorisées ou non sur l'appareil. Vous pouvez choisir **Oui** pour autoriser les connexions Bluetooth, **Non** pour les empêcher, ou **Mains** libres pour restreindre le Bluetooth à la fonction Mains libres uniquement. Cette option est réglée sur **Oui (Paramètres** par défaut).

WIFI

Connexions autorisées. Non (par défaut).

Infrarouge (IrDA)

Connexions autorisées Infrarouge (IrDA). Activé par défaut.

Partage internet (point d'accès mobile)

Cette option permet à l'appareil d'utiliser le partage internet (point d'accès mobile). Elle est activée par défaut.

Stockage

Demander encodage du terminal

Cliquez sur cette option si vous souhaitez demander l'encodage du terminal. Tous les appareils n'appliquent pas le cryptage. Cette option est désactivée par défaut.

Autoriser les cartes de stockage

Autorise l'utilisation d'une carte de stockage dans l'appareil. Cette option est activée par défaut.

Exiger le chiffrement des cartes de stockage

Utilisez cette option si vous souhaitez exiger le chiffrement d'une carte de stockage. Cette option est désactivée par défaut.

Synchronisation du bureau

Autorise Desktop ActiveSync sur l'appareil. Non (par défaut).

Applications

Navigateur web activé

Autorise l'utilisation d'un navigateur sur l'appareil. Cette option n'est pas prise en charge sur certains appareils et peut ne pas s'appliquer aux navigateurs tiers. Elle est activée par défaut.

Appareil photo activé

Autorise l'utilisation d'un appareil photo sur l'appareil. Cette option est activée par défaut.

Messagerie perso activée

L'appareil permet à l'utilisateur de configurer un compte de courrier électronique personnel. Lorsqu'elle est désactivée, les types de comptes ou de services de messagerie interdits dépendent entièrement du client ActiveSync concerné. Cette option est activée par défaut.

Courrier POP/IMAP activé

Permet l'accès au courrier électronique POP ou IMAP. Cette option est activée par défaut.

Bureau distant activé

Permet au client d'utiliser le Bureau à distance. Non (par défaut).

Applications non signées autorisées

Cette option permet d'utiliser des applications non signées sur le périphérique. Cette option est activée par défaut.

Programmes d'installation non signés autorisés

Cette option autorise l'exécution de programmes d'installation non signés sur l'appareil. Cette option est activée par défaut.

Messagerie texte activée

Cette option autorise l'envoi de messages texte sur le terminal. Ce texte est activé par défaut.

Itinérance

Exiger une synchronisation manuelle en itinérance

Utilisez cette option de politique si vous souhaitez exiger que le terminal se synchronise manuellement en cas d'itinérance. Autoriser la synchronisation automatique en itinérance pourrait augmenter les coûts de données pour le terminal, en fonction de son opérateur et de son plan de données. Cette option est désactivée par défaut.

Voir :

 Gestionnaire de domaines | Politique attribuée

 Comptes ActiveSync

 Glients ActiveSync

3.2.11.3 Politique attribuée

🗐 Domain Manager - Assigned Policy			
Domain Manager company.test Host Name & IP Smart Host Accounts MDIM Calendar Webmail Dequeuing Signatures Client Signatures Settings Client Settings Policy Manager Accounts Clients Clients Clients example.com	Select Policy for Domain Current Effective Polic <no effective="" polic<="" td=""> Policy to Assign <no policy="" set=""></no></no>	company.test licy y>	
		Ok	Cancel Apply Help

Utilisez cet écran pour attribuer la <u>politique ActiveSync</u> and faut du domaine. Lorsqu'un client ActiveSync se connecte en utilisant l'un des comptes de ce domaine, c'est cette politique qui sera attribuée au client, à moins qu'une autre politique n'ait été définie spécifiquement pour ce compte.

Attribuer une Politique ActiveSync par défaut

Pour attribuer une politique ActiveSync par défaut pour le domaine, cliquez sur la liste déroulante **Politique à appliquer**, sélectionnez la politique souhaitée, puis cliquez sur **Ok**.

Voir :

<u>Gestionnaire de domaines | Gestionnaire de politiques</u> 233 <u>ActiveSync | Comptes</u> 479 <u>ActiveSync | Clients</u> 488

3.2.11.4 Comptes

	Select Domain con	nnanv.test	~ [Refresh	
Domain Manager	* Right-Click on or press the (Context-Menu on an a	account key to make	e modifications	
Host Name & IP Smart Host Accounts MDIM Calendar Webmail Dequeuing Signatures Client Signatures Settings ActiveSync Client Settings Policy Manager Assigned Policy Accounts Clients e. Assigned Policy Clients 	Account bill.farmer@company.test frank.thomas@company.test michael.mason@company.te michael.mason@company.te Eind user: Eind user: Summary 3 / Unlimited Active	Settings defined No No Sync licenses in use	Assigned Policy <no policy="" set=""> <no policy="" set=""> <no policy="" set=""> Add</no></no></no>	Revoke All Listed Accounts 3 in this domain	
				Ok Cancel Ap	pply Help

Utilisez cet écran pour désigner les comptes du domaine qui sont autorisés à utiliser ActiveSync. Vous pouvez modifier les paramètres client de chaque compte autorisé et lui attribuer une politique ActiveSync.

Autoriser les comptes

Cliquez sur **Ajouter** pour autoriser manuellement un ou plusieurs comptes du domaine à utiliser ActiveSync. La boîte de dialogue Sélection des utilisateurs s'ouvre et permet de rechercher et de sélectionner les comptes.

Select these object	Users	1			Object	Types
Select these object		·			Object	турсы
From these domains:	comp	any.test			Loca	tions
Common Queries Name contain:	s:				Find	d Now
Email contain	s:					
Description contain						
Description contains	s:					
Include Disabled Acco	ounts					
Include Disabled Acco	ounts		Help	ОК		Cancel
Include Disabled Acco	ounts Type	Email	Help	OK		Cancel
Include Disabled Acco	Type User	Email randy.peterma	Help	OK v.test		Cancel
Include Disabled Acco earch Results Name Randy Peterman	Type User User	Email randy.peterma sir.smith@com	Help an@company pany.test	OK v.test		Cancel
Include Disabled Acco	Type User User	Email randy.peterma sir.smith@com	Help an@company pany.test	OK v.test		Cancel
Include Disabled Acco	Type User User	Email randy.peterma sir.smith@com	Help an@company pany.test	OK v.test		Cancel
Include Disabled Acco	Type User User	Email randy.peterma sir.smith@com	Help an@company pany.test	OK v.test		Cancel

Requêtes communes

Utilisez les options de cette section pour limiter votre recherche en spécifiant tout ou partie du nom de l'utilisateur, son adresse électronique ou le contenu de la Description du compte. Laissez ces champs vides si vous souhaitez que les résultats de la recherche contiennent tous les utilisateurs correspondant aux Emplacements spécifiés ci-dessus.

Inclure les comptes désactivés

Cochez cette case si vous souhaitez inclure les <u>comptes désactivés</u> dans votre recherche.

Rechercher maintenant

Une fois que vous avez spécifié tous vos critères de recherche, cliquez sur **Rechercher maintenant** pour effectuer la recherche.

Chercher les résultats

Dans les résultats de la recherche, sélectionnez les utilisateurs souhaités et cliquez sur **OK** pour les ajouter à la liste des comptes autorisés.

Révocation de comptes

Pour retirer à un compte l'autorisation d'utiliser ActiveSync, sélectionnez-le dans la liste et cliquez sur **Retirer les comptes sélectionnés**. Si vous souhaitez retirer tous les comptes, cliquez sur le bouton**Retirer tous les comptes.**

Si vous avez activé l'option <u>Autoriser tous les comptes lors du</u> <u>premier accès via le protocole ActiveSync</u> [479], le fait de retirer l'accès à un compte le fera disparaître de la liste, mais la prochaine fois qu'un appareil se connectera pour le compte, il sera à nouveau autorisé.

Attribuer une Politique ActiveSync attribuée

Pour appliquer une <u>Politique attribuée</u> [470] au compte :

- 1. Sélectionnez un compte dans la liste.
- 2. Cliquez sur **Attribuer une politique**. La boîte de dialogue Appliquer une politique s'ouvre.
- 3. Cliquez sur la liste déroulante**Politique à appliquer** et choisissez la politique souhaitée.
- 4. Cliquez sur OK.

Cette politique sera attribuée à tout nouveau terminal qui se connectera pour ce compte.

Chercher dans la liste des comptes autorisés

Si vous disposez d'un grand nombre de comptes autorisés à utiliser ActiveSync, vous pouvez utiliser la boîte**Rechercher un utilisateur pour** rechercher un compte spécifique dans la liste. Il suffit de taper les premières lettres de l'adresse électronique du compte pour sélectionner l'utilisateur.

Paramètres

Sélectionnez un compte et cliquez sur **Paramètres** pour gérer les Paramètres clients du compte. Ces paramètres seront appliqués à tous les clients ActiveSync qui se connectent pour le compte.

Client Settings: frank.thomas@company.test	×
General FolderSync Options Content Handling	
Troubleshooting Log level Use inherited or default Archive transactions as XML WBXML Validate/correct PIM m	∽ Irk file integrity
Client Options Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in G New clients require administrative approval Max clients per user Use inherited or default Bandwidth reset Day Use inherited or default	et/UserInformation
Security Exempt from Location Screen Dynamically allow remote address Allow clients provisioned/managed by other servers Disallow Factory Reset Wipes	
Preview Runtime Settings OK	Cancel Help

Non (Paramètres par défaut), toutes les options de cet écran sont définies sur "Utiliser les paramètres hérités ou par défaut", ce qui signifie que chaque option prendra son paramètre de l'option correspondante sur l <u>'écran Paramètres clients du domaine</u>.

Général

Résolution des problèmes

Niveau de journalisation

ActiveSync for MDaemon prend en charge six niveaux de journalisation, du plus élevé au plus faible :

DébogaIl s'agit du niveau de journalisation le plus complet. Il consignegetoutes les entrées disponibles et n'est généralement utilisé que

pour diagnostiquer un problème.

- **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.
- **Avertis** Les avertissements, les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont consignés dans le journal.
- **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- **Critiqu** Les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.
- **Hériter** Non (par défaut), le niveau journalisation est hérité de la hiérarchie des Paramètres clients. Ainsi, les clients héritent leurs paramètres des Types de clients, les Types de clients des Comptes, les Comptes des Groupes, etc. Le Paramètres globaux du client pour cette option est déterminé par le paramètre de niveau de journalisation dans le dialogue<u>Diagnostics</u>[457].

Archiver les transactions en [XML | WBXML]

Utilisez les options d'archivage*XML...* et *WBXML* si vous souhaitez enregistrer ces données, qui peuvent parfois être utiles à des fins de débogage. Les options globales sont désactivées par défaut.

Valider/corriger l'intégrité du fichier mrk PIM

Cette option exécute un processus de validation et de correction des données PIM du client afin de rechercher les problèmes connus susceptibles d'empêcher une synchronisation correcte, tels que des UID iCal en double ou des champs facultatifs vides. L'option globale est désactivée par défaut.

Options client

Appliquer les restrictions de protocole

Activez cette option si vous souhaitez refuser les connexions de tout client qui tente d'utiliser un protocole autre que les *Versions du protocole autorisées* spécifiées pour le client. Non (par défaut), cette option est désactivée, ce qui signifie que les restrictions de protocole n'empêchent pas un client d'utiliser un protocole différent ; elles indiquent simplement au client quels protocoles utiliser. Si un client tente malgré tout d'utiliser un protocole restreint, MDaemon autorisera quand même la connexion. Pour plus d'informations, voir <u>Restrictions de protocole</u> [459] pour plus d'informations.

Répondre à 'Get/UserInformation' en utilisant l'alias de l'identifiant comme 'adresse SMTP principale'

Dans ce cas, le service peut renvoyer un Alias/une adresse secondaire en tant

qu'adresse primaire en réponse à une requête de type Configurer/Gérer/Informations sur l'utilisateur. Cela permet de contourner un problème causé par une mise à jour postérieure à iOS9.x qui faisait que les clients ne pouvaient pas envoyer de courrier à l'aide d'un alias. L'utilisation de cette option résulte en une réponse non conforme aux spécifications à Settings/Get/UserInformation.

Les nouveaux clients doivent recevoir l'autorisation de l'administrateuravant de synchroniser.

Activez cette option si vous souhaitez que les nouveaux clients soient autorisés par un administrateur avant de pouvoir commencer à se synchroniser avec un compte. La liste <u>Clients</u> indique tous les clients en attente d'autorisation, et l'administrateur peut les autoriser à partir du même écran. Ce paramètre est Non (par défaut).

Max. clients par utilisateur

Si vous souhaitez limiter le nombre de clients ActiveSync ou de terminaux qui peuvent être associés à un compte MDaemon, indiquez le nombre souhaité dans cette option. L'option globale est réglée sur "illimité" par défaut. Cette option est disponible sur les écrans Paramètres clients globaux, de domaine et de compte, et non sur les écrans Clients individuels.

Jour de réinitialisation de la bande passante

Utilisez cette option si vous souhaitez réinitialiser les statistiques d'utilisation de la bande passante pour les Terminaux ActiveSync un jour précis de chaque mois. L'événement de réinitialisation a lieu dans le cadre du processus de maintenance nocturne normal et est consigné dans le journal du système comme les autres routines de maintenance. L'option globale est réglée sur "0 (Jamais)" par défaut, ce qui signifie que les statistiques d'utilisation ne seront jamais réinitialisées. Paramétrez les options enfant sur un jour différent si, par exemple, vous souhaitez que le jour de réinitialisation coïncide avec la date de réinitialisation de la facturation de l'opérateur sans fil d'un utilisateur ou d'un client.

Sécurité

Exclure du Filtrage de pays

Activez cette option dans l'écran des paramètres d'un client ActiveSync si vous souhaitez que l'appareil puisse filtrer l' <u>écran de localisation</u> [609]. Cela permet à un utilisateur valide de continuer à accéder à son compte via ActiveSync lorsque, par exemple, il se rend à un endroit où les tentatives d'authentification sont bloquées. Pour que l'appareil soit exempté, il doit s'être connecté et authentifié via ActiveSync dans le délai configuré dans le paramètre<u>Supprimer les clients inactifs</u> <u>après ce nombre de jours</u> [443] situé dans l'écran Régètres.

Autoriser dynamiquement l'adresse distante

Si vous excluez un pays du Filtrage de l'emplacement, activez cette option si vous souhaitez également autoriser l'adresse IP distante à partir de laquelle il se connecte. Cela peut s'avérer utile pour autoriser d'autres clients susceptibles de se connecter à partir de la même adresse IP.

Autoriser les clients gérés par d'autres serveurs

Par défaut, lorsque le serveur ActiveSync envoie des données de

provisionnement/des spécificités de politiques à un client et que celui-ci signale qu'il est également géré par un autre serveur ActiveSync, le client sera toujours autorisé à se connecter à MDaemon. Dans ce cas, il n'y a aucun moyen de s'assurer que les spécificités de votre politique seront appliquées lorsqu'elles entrent en conflit avec la politique de l'autre serveur ActiveSync. En général, les clients utilisent par défaut l'option la plus restrictive en cas de conflit. Désactivez cette option si vous ne souhaitez pas autoriser ces clients à se connecter.

Interdire les réinitialisations aux paramètres d'usine

Si cette option est activée (On/Oui), il ne sera pas possible d'**effacer complètement** un client ActiveSync. Si vous souhaitez pouvoir effectuer un Effacer complètement à distance sur un client, vous devez d'abord désactiver cette option. L'option est désactivée par défaut. Pour plus d'informations, voir : <u>Effacer</u> <u>complètement un client ActiveSync</u> with sur la page Clients.

Options FolderSync

Options de dossier

Exclure

Dossier Expéditeurs bloqués autorisés/ bloqués

Par défaut, les dossiers Expéditeurs autorisés et Dossiers Expéditeurs bloqués de l'utilisateur ne sont pas synchronisés avec les périphériques. Ils ne sont généralement utilisés par MDaemon que dans le cadre de la prévention automatique du spam. C'est pourquoi ils n'ont pas besoin d'être affichés sur les appareils en tant que contacts.

Dossiers de courrier personnalisés (Non par défaut)

Par défaut, tous les Dossiers de courrier créés par l'utilisateur et par défaut peuvent être synchronisés avec le terminal. Activez cette option si vous souhaitez que seuls les dossiers courrier par défaut soient synchronisés, c'està-dire la Boîte de réception, les Éléments envoyés, les Éléments supprimés, les Brouillons, etc. Aucun dossier créé par l'utilisateur ne sera inclus. Cette option est désactivée par défaut.

Dossiers PIM personnalisés non (par défaut)

Par défaut, tous les dossiers PIM de l'utilisateur (contacts, calendrier, notes, tâches, etc.) sont synchronisés avec l'appareil. Activez cette option si vous souhaitez que seuls les dossiers PIM par défaut soient synchronisés. Exemple : si cette option est activée et qu'un utilisateur possède plusieurs dossiers de calendrier, seul le calendrier par défaut sera synchronisé. Cette option est désactivée par défaut.

Inclure

Arborescence Dossiers publics

Cochez cette case si vous souhaitez que les <u>Dossiers publics</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers publics</u> auxquels il a accès. Cette option est autorisée par défaut.

Navigation dans les dossiers publics (affiche les noms de dossiers)

Non par défaut, pour qu'un client puisse synchroniser un sous-dossier public ou y accéder, le compte doit disposer de l'<u>autorisation de Recherche</u> [327] pour le sous-dossier (c'est-à-dire le dossier enfant) et tous les <u>Dossiers publics</u> [325] parents situés au-dessus. Si le compte n'a pas l'autorisation de voir les dossiers parents, il ne peut pas non plus voir le dossier enfant, même s'il en a l'autorisation. Activez cette option si vous souhaitez autoriser le client à accéder à ces dossiers enfants. **Par nom : l** 'activation de cette option doit nécessairement révéler les noms des dossiers parents au client, ce qui pourrait être considéré comme un risque de sécurité. Cette option est désactivée par défaut.

Nombre max de Dossiers publics

Utilisez cette option si vous souhaitez limiter le nombre de Dossiers publics autorisés sur le périphérique. Lorsqu'une limite est définie, le serveur parcourt la liste des dossiers jusqu'à ce que la limite soit atteinte, puis plus aucun dossier n'est envoyé à l'appareil. Il n'existe aucun moyen de garantir l'ordre dans lequel les dossiers seront traités. Non (paramètres par défaut).

Dossiers IMAP partagés

Cochez cette case si vous souhaitez que les <u>dossiers partagés</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers partagés</u> auxquels il a accès. Cette option est autorisée par défaut.

Gestion du contenu

Options de gestion des e-mails

Créer des tâches/rappels pour les e-mails avec indicateurs

Cette option permet à MDaemon de rappeler à l'utilisateur les éléments marqués, en créant un élément de tâche pour chaque courrier électronique marqué. lorsque le client le demande. L'option globale de ce contrôle est activée par défaut.

Toujours envoyer les mises à jour de réunion lorsque l'événement est modifié

Certains clients n'envoient pas correctement les e-mails de mise à jour des réunions lorsqu'ils modifient une réunion. Cette option indique au service ActiveSync d'envoyer une mise à jour de la réunion lorsqu'un élément de la réunion est mis à jour par l'organisateur. Cette option ne doit être définie que pour les <u>clients</u> and et les <u>types de clients</u> out qui n'envoient pas correctement les mises à jour de réunion, sous peine d'envoyer des mises à jour de réunion en double. Par conséquent, cette option n'est disponible que dans les pages de paramètres pour les Clients et les Types de clients.

Demander des confirmations de lecture pour tous les e-mails envoyés

Activez cette option si vous souhaitez que le serveur demande des confirmations de lecture pour tous les courriers envoyés par un client. Cette option est désactivée par défaut.

Envoyer des confirmations de lecture du serveur lorsque le courrier est marqué comme lu et lorsque l'expéditeur le demande.

Activez cette option si vous souhaitez que le serveur prenne en charge les demandes de confirmation de lecture et délivre un accusé de réception de lecture lorsqu'un message est marqué comme lu par un client. Cette option est désactivée par défaut.

Envoyer avec l'alias spécifié dans ReplyTo

Certains clients peuvent ne pas autoriser un expéditeur à envoyer du courrier à l'aide d'un alias. Cette fonctionnalité a été ajoutée au <u>protocole Exchange</u> <u>ActiveSync (EAS)</u> [459] 16.x, mais certains clients ne supportent pas la version 16.x. Par exemple, Outlook pour Windows n'utilise que EAS 14.0, et bien qu'il permette à un utilisateur de spécifier une autre adresse pour l'envoi, le message généré ne reflète pas correctement les choix de l'utilisateur. Cette faculté permet d'utiliser le champ ReplyTo pour envoyer l'e-mail, à condition que l'adresse ReplyTo soit un <u>alias</u> <u>valide</u> [364] pour cet utilisateur. L'option globale est activée par défaut.

Fusionner virtuellement les contacts publics et les contacts par défaut

Activez cette option si vous souhaitez fusionner les contacts publics avec les contacts par défaut de l'utilisateur sur le terminal. Il s'agit uniquement d'une fusion virtuelle, c'est-à-dire qu'ils ne sont pas réellement copiés dans le dossier des contacts de l'utilisateur. Cela peut être utile sur les clients qui ne prennent pas en charge les recherches dans la liste d'adresses globale (GAL). Non (par défaut).

Dossiers Expéditeurs bloqués lors du déplacement d'un courrier dans le dossier Courriers indésirables

Si cette option est activée, lorsqu'un client déplace un e-mail vers le dossier Courriers indésirables du compte, le service ajoute l'adresse SENDER\$ - adresse de l'expéditeur de cet e-mail au dossier Contacts des expéditeurs bloqués.

Forcer l'envoi des réponses aux réunions lorsqu'une demande de réunion est acceptée/déclinée, etc.

Dans cette option, lorsqu'un client accepte, refuse ou choisit une action en réponse à une demande de réunion, le service envoie une réponse à l'organisateur de la réunion. Cette fonction est destinée aux clients spécifiques qui n'envoient pas correctement ces mises à jour eux-mêmes.

Aperçu des paramètres effectifs

Ce bouton est disponible sur tous les écrans des Paramètres clients enfant (c.-à-d. <u>domaines</u> [462], <u>comptes</u> [479] et <u>clients</u> [488]). Non (par défaut), les options de ces écrans sont définies pour hériter de leurs paramètres d'un écran parent. Utilisez cette fonction pour voir quels paramètres sont actuellement appliqués à l'écran affiché.

Voir :

ActiveSync | Paramètres client 447 ActiveSync | Domaines 462 ActiveSync " Clients 488

3.2.11.5 Clients

🛃 Domain Manager - Clients				×
Domain Manager	Right-Click on or press the Context-Menu on an account key to make modifications			
 Host Name & IP Smart Host Accounts MDIM Calendar Webmail Dequeuing Signatures Client Signatures Settings ActiveSync Client Settings Policy Manager Assigned Policy Accounts Clients example.com 	Email Address bill.farmer@company.test frank.thomas@company.test frank.thomas@company.test michael.mason@company.test michael.mason@company.test Filter Client Listing to	Client Type WindowsOutlook15 iPad SAMSUNGSGHI747 WindowsOutlook15 Collector_1.0 (Requires Approval) WindowsOutlook15	Client ID 48F708C28F654AC3A31AB6293 ApplDMRJJX05F182 SEC192C55F9C4C8A 90907568DAE942CFA4F56DFDC TIVANb7b552669e51cf8660b808 C44088A6A76341E192B25668D >	
		[Ok Cancel App	ly Help

Cet écran filtre par une entrée pour chaque périphérique ActiveSync associé au domaine.
ActiveSync Client		>
Email Address	frank.thomas@company.test	^
Domain	company.test	
Client Type	iPad	
Client ID	14A65AD03AA182FADF712A69	
User Agent	UA_iPad/9.6.9.8	
Client Model	iPad 4.22	
IMEI	528514162102	
Friendly Name	Frank's iPad	
Operating System	Fizzbin Mobile Systems 20.0	
Operating System Language	en-us	
Phone Number	8175559876	
Mobile Operator	Example Wireless Ltd.	
IP Address	192.168.0.100	
Last GMT Logon Time	2023-01-03T16:43:28.000Z (2023-01-03 10:43:28)	
Protocol Version	16.1	
Effective Policy	<no policy="" set=""></no>	
Device Wipe Requested	No	
Account Only Wipe Requested	No	
Authorization Time Stamp	2022-06-10T19:13:58.420Z (2022-06-10 14:13:58)	
Authorization made by	MDAirSync	
192.168.0.100	2023-01-03T16:00:00.000Z (2023-01-03 10:00:00)	~

Détails du client ActiveSync

Double-cliquez sur une entrée, ou cliquez avec le bouton droit de la souris sur l'entrée et cliquez sur **Voir les détails du client**, pour ouvrir la boîte de dialogue Détails du client. Cet écran filtre les informations relatives au client, telles que son Type de client, son ID client, l'heure de sa dernière connexion, etc.

Paramètres clients

Cliquez avec le bouton droit de la souris sur un client et cliquez sur **Personnaliser les paramètres du client** pour gérer ses Paramètres clients. Par défaut, ces paramètres sont hérités des paramètres du Type de client, mais ils peuvent être ajustés comme vous le souhaitez. Voir <u>Gérer les paramètres des clients d'un appareilGérer les</u>

Attribuer une Politique ActiveSync attribuée

Pour Attribuer une <u>Politique</u> 470 du terminal : Cliquez avec le bouton droit de la souris sur le terminal dans la liste:

- 1. Cliquez avec le bouton droit de la souris sur un périphérique dans la liste.
- 2. Cliquez sur **Appliquer politique**. La boîte de dialogue Appliquer une politique s'ouvre.
- 3. Cliquez sur la liste déroulante**Politique à appliquer** et choisissez la politique souhaitée.
- 4. Cliquez sur OK.

Statistiques de

Cliquez avec le bouton droit de la souris sur une entrée, puis cliquez sur **Afficher les statistiques** pour ouvrir la boîte de dialogue Statistiques du client, qui contient diverses statistiques d'utilisation pour le client.

Réinitialiser les statistiques

Si vous souhaitez réinitialiser les statistiques d'un client, cliquez avec le bouton droit de la souris sur le client, cliquez sur **Réinitialiser les statistiques**, puis sur **OK** pour confirmer l'action.

Suppression d'un client ActiveSync

Pour supprimer un client ActiveSync, cliquez avec le bouton droit de la souris sur le client et cliquez sur **Supprimer**, puis sur **Oui**. Cela supprimera le client de la liste et toutes les informations de synchronisation le concernant dans MDaemon. Dans ce cas, si à l'avenir le compte utilise ActiveSync pour synchroniser le même client, MDaemon traitera le client comme s'il n'avait jamais été utilisé sur le serveur ; toutes les données du client devront être resynchronisées avec MDaemon.

Effacer complètement un client ActiveSync

Lorsqu'une politique 470 a été appliquée à un client ActiveSync sélectionné, et que le client l'a appliquée et a répondu, il y aura une option d'Effacement complètement disponible pour ce client. Si c'est le cas, cliquez avec le bouton droit de la souris sur le client (ou sélectionnez-le si vous utilisez MDRA) et cliquez sur **Effacer complètement**. Lors de la prochaine connexion du client, MDaemon lui demandera d'effacer toutes les données ou de restaurer les paramètres par défaut. Selon le client, cela peut supprimer tout ce qu'il contient, y compris les applications téléchargées. En outre, tant que l'entrée ActiveSync du client existe, MDaemon continuera d'envoyer la demande d'effacement chaque fois que ce périphérique se connectera à l'avenir. Si, à un moment donné, vous souhaitez supprimer le client, assurez-vous de l'ajouter d'abord à la liste de blocage d'abord l'ajouter à la Liste de blocage 454, afin qu'il ne puisse plus se connecter à l'avenir. Enfin, si un terminal effacé est récupéré et que vous souhaitez l'autoriser à se connecter à nouveau, vous devez le sélectionner et cliquer sur **Annuler les actions "Effacer"**. Vous devez également le supprimer de la Liste de blocage.

Effacement du compte d'un client ActiveSync

Pour effacer les données de messagerie et de PIM du compte du client ou de l'appareil, cliquez avec le bouton droit de la souris et cliquez sur **Account Wipe Account Mail and PIM from client (Effacer le courrier et le PIM du client)**. L' option *Effacer le compte* est similaire à l' option*Effacer complètement* expliquée ci-dessus, mais au lieu d'effacer toutes les données, elle effacera uniquement les données du compte, telles que ses e-mails, entrées de calendrier, contacts et autres. Le reste, comme les applications, les photos ou la musique, est laissé en l'état.

Autoriser le client

Si l'option "Les nouveaux clients nécessitent une autorisation administrative" de l' écran <u>Paramètres du client ActiveSync</u> [447] est réglée sur l'autorisation, sélectionnez un client et cliquez sur Approuver le client pour la synchronisation, pour l'autoriser à se synchroniser avec le serveur.

Gérer les paramètres clients d'un terminal

L'écran Paramètres clients au niveau de l'appareil vous autorise à gérer les paramètres d'un appareil spécifique.

General	FolderSync Ontions	Content Handling
	r older office op doring	Content Honology
Trout	pleshooting	
	Log lev	Vei Use inherited or default V
	Archive transactions	as 🔳 XML 🔳 WBXML
		Validate/correct PIM mrk file integrity
Client	t Options	
🗖 En	force protocol restricti	ions
Re	spond with logon alias	as 'PrimarySmtpAddress' in Get/UserInformation
	Bandwidth reset Da	^{ay} Use inherited or default \vee
	Bandwidth reset Da	ay Use inherited or default V
Secur	Bandwidth reset Da	ay Use inherited or default \checkmark
- Secur	Bandwidth reset Da rity empt from Location Sc	ay Use inherited or default v
Secur Ex	Bandwidth reset Da rity cempt from Location Sc Dynamically allow remo	ay Use inherited or default v creen ote address
Secur Ex	Bandwidth reset Da rity empt from Location Sc Dynamically allow remo ow clients provisioned,	ay Use inherited or default v reen ote address /managed by other servers
Secur Ex All	Bandwidth reset Da rity empt from Location Sc Dynamically allow remo ow clients provisioned, sallow Factory Reset V	ay Use inherited or default v reen ote address /managed by other servers Vipes
Secur Ex All Dis	Bandwidth reset Da rity cempt from Location Sc Dynamically allow remo ow clients provisioned, sallow Factory Reset V	ay Use inherited or default v reen ote address /managed by other servers Vipes
Secur Ex All Dis	Bandwidth reset Da rity cempt from Location Sc Dynamically allow remo ow clients provisioned, sallow Factory Reset V	ay Use inherited or default v reen ote address /managed by other servers Vipes
Secur Ex All Dis	Bandwidth reset Da rity empt from Location Sc Dynamically allow remo ow clients provisioned, sallow Factory Reset V	ay Use inherited or default rreen ote address /managed by other servers Wipes

Non (par défaut), toutes les options de cet écran sont définies sur "Utiliser les paramètres hérités ou par défaut", ce qui signifie que chaque option est paramétrée à partir de l'option correspondante de l' écran<u>Paramètres clients de Types clients</u>. Toute modification apportée aux paramètres de cet écran sera répercutée sur cet écran. Inversement, toute modification apportée à cet écran remplacera le paramètre du type de clients pour ce terminal.

Général

Résolution des problèmes

Niveau de journalisation

ActiveSync for MDaemon prend en charge six niveaux de journalisation, du plus élevé au plus faible :

DébogaIl s'agit du niveau de journalisation le plus complet. Il consignegetoutes les entrées disponibles et n'est généralement utilisé que

pour diagnostiquer un problème.

- **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.
- **Avertis** Les avertissements, les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont consignés dans le journal.
- **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- **Critiqu** Les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.
- **Hériter** Non (par défaut), le niveau journalisation est hérité de la hiérarchie des Paramètres clients. Ainsi, les clients héritent leurs paramètres des Types de clients, les Types de clients des Comptes, les Comptes des Groupes, etc. Le Paramètres globaux du client pour cette option est déterminé par le paramètre de niveau de journalisation dans le dialogue<u>Diagnostics</u>[457].

Archiver les transactions en [XML | WBXML]

Utilisez les options d'archivage*XML...* et *WBXML* si vous souhaitez enregistrer ces données, qui peuvent parfois être utiles à des fins de débogage. Les options globales sont désactivées par défaut.

Valider/corriger l'intégrité du fichier mrk PIM

Cette option exécute un processus de validation et de correction des données PIM du client afin de rechercher les problèmes connus susceptibles d'empêcher une synchronisation correcte, tels que des UID iCal en double ou des champs facultatifs vides. L'option globale est désactivée par défaut.

Options client

Appliquer les restrictions de protocole

Activez cette option si vous souhaitez refuser les connexions de tout client qui tente d'utiliser un protocole autre que les *Versions du protocole autorisées* spécifiées pour le client. Non (par défaut), cette option est désactivée, ce qui signifie que les restrictions de protocole n'empêchent pas un client d'utiliser un protocole différent ; elles indiquent simplement au client quels protocoles utiliser. Si un client tente malgré tout d'utiliser un protocole restreint, MDaemon autorisera quand même la connexion. Pour plus d'informations, voir <u>Restrictions de protocole</u> [459] pour plus d'informations.

Répondre à 'Get/UserInformation' en utilisant l'alias de l'identifiant comme 'adresse SMTP principale'

Dans ce cas, le service peut renvoyer un Alias/une adresse secondaire en tant

qu'adresse primaire en réponse à une requête de type Configurer/Gérer/Informations sur l'utilisateur. Cela permet de contourner un problème causé par une mise à jour postérieure à iOS9.x qui faisait que les clients ne pouvaient pas envoyer de courrier à l'aide d'un alias. L'utilisation de cette option résulte en une réponse non conforme aux spécifications à Settings/Get/UserInformation.

Les nouveaux clients doivent recevoir l'autorisation de l'administrateuravant de synchroniser.

Activez cette option si vous souhaitez que les nouveaux clients soient autorisés par un administrateur avant de pouvoir commencer à se synchroniser avec un compte. La liste <u>Clients</u> indique tous les clients en attente d'autorisation, et l'administrateur peut les autoriser à partir du même écran. Ce paramètre est Non (par défaut).

Max. clients par utilisateur

Si vous souhaitez limiter le nombre de clients ActiveSync ou de terminaux qui peuvent être associés à un compte MDaemon, indiquez le nombre souhaité dans cette option. L'option globale est réglée sur "illimité" par défaut. Cette option est disponible sur les écrans Paramètres clients globaux, de domaine et de compte, et non sur les écrans Clients individuels.

Jour de réinitialisation de la bande passante

Utilisez cette option si vous souhaitez réinitialiser les statistiques d'utilisation de la bande passante pour les Terminaux ActiveSync un jour précis de chaque mois. L'événement de réinitialisation a lieu dans le cadre du processus de maintenance nocturne normal et est consigné dans le journal du système comme les autres routines de maintenance. L'option globale est réglée sur "0 (Jamais)" par défaut, ce qui signifie que les statistiques d'utilisation ne seront jamais réinitialisées. Paramétrez les options enfant sur un jour différent si, par exemple, vous souhaitez que le jour de réinitialisation coïncide avec la date de réinitialisation de la facturation de l'opérateur sans fil d'un utilisateur ou d'un client.

Sécurité

Exclure du Filtrage de pays

Activez cette option dans l'écran des paramètres d'un client ActiveSync si vous souhaitez que l'appareil puisse filtrer l' <u>écran de localisation</u> [609]. Cela permet à un utilisateur valide de continuer à accéder à son compte via ActiveSync lorsque, par exemple, il se rend à un endroit où les tentatives d'authentification sont bloquées. Pour que l'appareil soit exempté, il doit s'être connecté et authentifié via ActiveSync dans le délai configuré dans le paramètre<u>Supprimer les clients inactifs</u> <u>après ce nombre de jours</u> [443] situé dans l'écran Régètres.

Autoriser dynamiquement l'adresse distante

Si vous excluez un pays du Filtrage de l'emplacement, activez cette option si vous souhaitez également autoriser l'adresse IP distante à partir de laquelle il se connecte. Cela peut s'avérer utile pour autoriser d'autres clients susceptibles de se connecter à partir de la même adresse IP.

Autoriser les clients gérés par d'autres serveurs

Par défaut, lorsque le serveur ActiveSync envoie des données de

provisionnement/des spécificités de politiques à un client et que celui-ci signale qu'il est également géré par un autre serveur ActiveSync, le client sera toujours autorisé à se connecter à MDaemon. Dans ce cas, il n'y a aucun moyen de s'assurer que les spécificités de votre politique seront appliquées lorsqu'elles entrent en conflit avec la politique de l'autre serveur ActiveSync. En général, les clients utilisent par défaut l'option la plus restrictive en cas de conflit. Désactivez cette option si vous ne souhaitez pas autoriser ces clients à se connecter.

Interdire les réinitialisations aux paramètres d'usine

Si cette option est activée (On/Oui), il ne sera pas possible d'**effacer complètement** un client ActiveSync. Si vous souhaitez pouvoir effectuer un Effacer complètement à distance sur un client, vous devez d'abord désactiver cette option. L'option est désactivée par défaut. Pour plus d'informations, voir : <u>Effacer</u> <u>complètement un client ActiveSync</u> with sur la page Clients.

Options FolderSync

Options de dossier

Exclure

Dossier Expéditeurs bloqués autorisés/ bloqués

Par défaut, les dossiers Expéditeurs autorisés et Dossiers Expéditeurs bloqués de l'utilisateur ne sont pas synchronisés avec les périphériques. Ils ne sont généralement utilisés par MDaemon que dans le cadre de la prévention automatique du spam. C'est pourquoi ils n'ont pas besoin d'être affichés sur les appareils en tant que contacts.

Dossiers de courrier personnalisés (Non par défaut)

Par défaut, tous les Dossiers de courrier créés par l'utilisateur et par défaut peuvent être synchronisés avec le terminal. Activez cette option si vous souhaitez que seuls les dossiers courrier par défaut soient synchronisés, c'està-dire la Boîte de réception, les Éléments envoyés, les Éléments supprimés, les Brouillons, etc. Aucun dossier créé par l'utilisateur ne sera inclus. Cette option est désactivée par défaut.

Dossiers PIM personnalisés non (par défaut)

Par défaut, tous les dossiers PIM de l'utilisateur (contacts, calendrier, notes, tâches, etc.) sont synchronisés avec l'appareil. Activez cette option si vous souhaitez que seuls les dossiers PIM par défaut soient synchronisés. Exemple : si cette option est activée et qu'un utilisateur possède plusieurs dossiers de calendrier, seul le calendrier par défaut sera synchronisé. Cette option est désactivée par défaut.

Inclure

Arborescence Dossiers publics

Cochez cette case si vous souhaitez que les <u>Dossiers publics</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers publics</u> auxquels il a accès. Cette option est autorisée par défaut.

Navigation dans les dossiers publics (affiche les noms de dossiers)

Non par défaut, pour qu'un client puisse synchroniser un sous-dossier public ou y accéder, le compte doit disposer de l'<u>autorisation de Recherche</u> [327] pour le sous-dossier (c'est-à-dire le dossier enfant) et tous les <u>Dossiers publics</u> [325] parents situés au-dessus. Si le compte n'a pas l'autorisation de voir les dossiers parents, il ne peut pas non plus voir le dossier enfant, même s'il en a l'autorisation. Activez cette option si vous souhaitez autoriser le client à accéder à ces dossiers enfants. **Par nom : l** 'activation de cette option doit nécessairement révéler les noms des dossiers parents au client, ce qui pourrait être considéré comme un risque de sécurité. Cette option est désactivée par défaut.

Nombre max de Dossiers publics

Utilisez cette option si vous souhaitez limiter le nombre de Dossiers publics autorisés sur le périphérique. Lorsqu'une limite est définie, le serveur parcourt la liste des dossiers jusqu'à ce que la limite soit atteinte, puis plus aucun dossier n'est envoyé à l'appareil. Il n'existe aucun moyen de garantir l'ordre dans lequel les dossiers seront traités. Non (paramètres par défaut).

Dossiers IMAP partagés

Cochez cette case si vous souhaitez que les <u>dossiers partagés</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers partagés</u> auxquels il a accès. Cette option est autorisée par défaut.

Gestion du contenu

Options de gestion des e-mails

Créer des tâches/rappels pour les e-mails avec indicateurs

Cette option permet à MDaemon de rappeler à l'utilisateur les éléments marqués, en créant un élément de tâche pour chaque courrier électronique marqué. lorsque le client le demande. L'option globale de ce contrôle est activée par défaut.

Toujours envoyer les mises à jour de réunion lorsque l'événement est modifié

Certains clients n'envoient pas correctement les e-mails de mise à jour des réunions lorsqu'ils modifient une réunion. Cette option indique au service ActiveSync d'envoyer une mise à jour de la réunion lorsqu'un élément de la réunion est mis à jour par l'organisateur. Cette option ne doit être définie que pour les <u>clients</u> at les <u>types de clients</u> qui n'envoient pas correctement les mises à jour de réunion, sous peine d'envoyer des mises à jour de réunion en double. Par conséquent, cette option n'est disponible que dans les pages de paramètres pour les Clients et les Types de clients.

Demander des confirmations de lecture pour tous les e-mails envoyés

Activez cette option si vous souhaitez que le serveur demande des confirmations de lecture pour tous les courriers envoyés par un client. Cette option est désactivée par défaut.

Envoyer des confirmations de lecture du serveur lorsque le courrier est marqué comme lu et lorsque l'expéditeur le demande.

Activez cette option si vous souhaitez que le serveur prenne en charge les demandes de confirmation de lecture et délivre un accusé de réception de lecture lorsqu'un message est marqué comme lu par un client. Cette option est désactivée par défaut.

Envoyer avec l'alias spécifié dans ReplyTo

Certains clients peuvent ne pas autoriser un expéditeur à envoyer du courrier à l'aide d'un alias. Cette fonctionnalité a été ajoutée au <u>protocole Exchange</u> <u>ActiveSync (EAS)</u> 16.x, mais certains clients ne supportent pas la version 16.x. Par exemple, Outlook pour Windows n'utilise que EAS 14.0, et bien qu'il permette à un utilisateur de spécifier une autre adresse pour l'envoi, le message généré ne reflète pas correctement les choix de l'utilisateur. Cette faculté permet d'utiliser le champ ReplyTo pour envoyer l'e-mail, à condition que l'adresse ReplyTo soit un <u>alias</u> <u>valide</u> our cet utilisateur. L'option globale est activée par défaut.

Fusionner virtuellement les contacts publics et les contacts par défaut

Activez cette option si vous souhaitez fusionner les contacts publics avec les contacts par défaut de l'utilisateur sur le terminal. Il s'agit uniquement d'une fusion virtuelle, c'est-à-dire qu'ils ne sont pas réellement copiés dans le dossier des contacts de l'utilisateur. Cela peut être utile sur les clients qui ne prennent pas en charge les recherches dans la liste d'adresses globale (GAL). Non (par défaut).

Dossiers Expéditeurs bloqués lors du déplacement d'un courrier dans le dossier Courriers indésirables

Si cette option est activée, lorsqu'un client déplace un e-mail vers le dossier Courriers indésirables du compte, le service ajoute l'adresse SENDER\$ - adresse de l'expéditeur de cet e-mail au dossier Contacts des expéditeurs bloqués.

Forcer l'envoi des réponses aux réunions lorsqu'une demande de réunion est acceptée/déclinée, etc.

Dans cette option, lorsqu'un client accepte, refuse ou choisit une action en réponse à une demande de réunion, le service envoie une réponse à l'organisateur de la réunion. Cette fonction est destinée aux clients spécifiques qui n'envoient pas correctement ces mises à jour eux-mêmes.

Aperçu des paramètres effectifs

Ce bouton est disponible sur tous les écrans des Paramètres clients enfant (c.-à-d. <u>domaines</u> [462], <u>comptes</u> [479] et <u>clients</u> [488]). Non (par défaut), les options de ces écrans sont définies pour hériter de leurs paramètres d'un écran parent. Utilisez cette fonction pour voir quels paramètres sont actuellement appliqués à l'écran affiché. Voir :

ActiveSync | Comptes 479 ActiveSync | Sécurité 454

3.3 Gestionnaire de passerelles

Le Gestionnaire de passerelles est accessible à partir de la sélection de menuSetup | Gestionnaire de passerelles.... Cette fonction fournit un niveau de support secondaire limité mais utile pour l'hébergement de plusieurs domaines ou pour agir en tant que serveur de messagerie de secours pour quelqu'un.

Exemple :

Supposons que vous souhaitiez agir en tant que serveur de sauvegarde ou de dépôt de courrier pour un tiers, en recevant son courrier électronique entrant et en le stockant dans un courrier sur votre serveur, mais que vous ne souhaitiez pas héberger entièrement son domaine, en conservant ses comptes utilisateurs individuels. Votre nom est"exemple.com".

La première chose à faire est de créer la passerelle en cliquant sur **Nouvelle passerelle** dans le Gestionnaire de passerelles et en saisissant "exemple.com" comme nom. Dans ce cas, tout le courrier reçu par MDaemon pour ce domaine sera séparé du flux de courrier principal et placé dans le dossier désigné dans l 'écranDomaine de 2006 lla passerelle , quelles que soient les personnes à qui le message est adressé.

Ensuite, vous désignerez les méthodes de collecte ou de livraison que vous souhaitez autoriser ou utiliser pour acheminer le courrier électronique du domaine vers son serveur de messagerie actuel, où sont hébergés ses comptes utilisateurs. Il y a deux façons de procéder : utiliser l' option *Distribuer les messages enregistrés chaque fois que MDaemon traite le courrier distant* dans l'écran Domaine, 2008 ou utiliser les options de mise en file d'attente. 275 Vous pouvez également créer un compte MDaemon et modifier son Dossier courrier 768 pour qu'il corresponde au dossier de stockage 2008 utilisé par votre passerelle. Cela permettra à un client de messagerie de se connecter à MDaemon pour collecter le courrier électronique d'Exemple.com.

Enfin, vous devrez probablement modifier les Paramètres de DNS pourexample.com afin que votre serveur MDaemon soit un hôte MX désigné pour ce domaine.

Il existe de nombreuses autres fonctionnalités et options, mais l'Exemple ci-dessus représente la forme de base d'une passerelle typique. Si, toutefois, vous avez besoin d'une configuration atypique, vous devrez peut-être procéder différemment, par exemple si vous souhaitez utiliser un nom de domaine qui n'existe pas réellement sur Internet, comme "company.mail". Il est possible de recevoir des messages pour un nom de domaine qui n'est pas valide, mais qui doit être "caché" à l'intérieur d'une adresse de domaine par défaut. En utilisant cette méthode, il est possible de construire des adresses qui passeront par le domaine par défaut et se rendront jusqu'à la passerelle. Par exemple, si votre domaine par défaut est example.com et que vous avez une

passerelle pour company.mail, quelqu'un pourrait envoyer un message à"bob@company.mail" en utilisant l'adresse "bob{company.mail}@example.com". Puisque "example.com" est le domaine enregistré hébergé par MDaemon, ce message serait délivré correctement, mais lorsque MDaemon recevrait le message dans ce format et livrerait le message audossier spécifié pour cette passerelle. Par nom, la méthode la plus simple consiste à enregistrer un nom de domaine valide pour la passerelle, puis à faire pointer son enregistrement DNS ou MX vers exemple.com.

🗟 Gateway Manager		×
Gateway Manager Gateway Manager SecurityGateway Global Gateway Settings Automatic Gateway Creation example.test	Gateway Domain Management New gateway Delete gateway Rename gateway Copy gateway Select a gateway to delete or rename it. Double-click to edit. Court example.test	
	Ok Cancel Apply Hel	P

Liste des passerelles

Le volet de navigation situé à gauche de cette boîte de dialogue contient la liste de vos passerelles, avec des liens vers chaque écran utilisé pour configurer les différents paramètres spécifiques à la passerelle. Il permet également d'accéder aux écrans<u>Paramètres globaux des passerelles</u> [264] et <u>Création automatique de</u> <u>passerelles</u> [266]. La liste de droite est utilisée pour supprimer et renommer des domaines. Vous pouvez double-cliquer sur une passerelle dans cette liste pour passer à l'éditeur de passerelle afin de configurer ses paramètres.

Gestionnaire de domaines de passerelles

Nouvelle passerelle

Pour créer une nouvelle passerelle : cliquez sur **Nouvelle passerelle**, saisissez le nom de la passerelle (par exemple, exemple.mail) dans la boîte de dialogue Créer/Renommer un domaine de passerelle, puis cliquez sur **OK**.

Par nom, on entend généralement le nom de domaine Internet enregistré qu'un serveur DNS résout en adresse IP de la machine locale qui exécute le serveur, ou un alias qualifié de ce nom. Vous pouvez également choisir d'utiliser un nom de domaine interne ou non valide et non public (tel que "company.mail") pour le nom de votre passerelle. Dans ce cas, vous devrez utiliser la méthode du nom de domaine imbriqué décrite dans l'Exemple ci-dessus, ou utiliser un autre système de filtrage du contenu pour acheminer les messages là où ils doivent l'être.

Supprimer une passerelle

Pour supprimer une passerelle : sélectionnez-la dans la liste et cliquez sur **Supprimer la passerelle**, puis cliquez sur **Oui** pour confirmer votre décision.

Renommer une passerelle

Pour modifier le nom d'une passerelle : sélectionnez-la dans la liste, cliquez sur **Renommer la passerelle**, saisissez le nouveau nom dans la boîte de dialogue Créer/Renommer le domaine, puis cliquez sur **OK**.

Copier une passerelle

Si vous souhaitez créer une nouvelle passerelle dont les paramètres correspondent à ceux d'une autre passerelle, sélectionnez une passerelle dans la liste, cliquez sur ce bouton, puis indiquez le nom de la nouvelle passerelle.

Éditeur de passerelle

Les Paramètres des passerelles permettent de modifier les paramètres de chaque passerelle. Il comprend les écrans suivants :

Domaine 268

Cet écran permet d'activer/désactiver la passerelle, de désigner le dossier utilisé pour stocker les messages du domaine et de configurer d'autres options de distribution et de traitement des pièces jointes.

Vérification 270

Si le serveur du domaine distant est configuré pour maintenir un serveur LDAP ou Active Directory à jour avec toutes ses boîtes aux lettres, alias et listes de diffusion, ou s'il utilise un serveur Minger pour fournir une vérification d'adresse à distance, vous pouvez utiliser cette boîte de dialogue pour spécifier ce serveur et ainsi vérifier la validité des adresses des destinataires des messages entrants. Lorsque l'adresse d'un destinataire n'est pas valide, le message est rejeté. Cette méthode vous permet d'éviter de supposer que tous les destinataires des messages d'un domaine sont valides.

Transfert 274

Cet écran vous permet de déclarer un hôte ou une adresse à laquelle lecourrier dudomainesera transféré dès son arrivée. Il y a également des options pour indiquer si une copie de ces messages doit être conservée localement et pour désigner le port sur lequel les messages transférés doivent être envoyés.

Mise en file d'attente 275

Dans cet écran, vous pouvez configurer MDaemon pour qu'il réponde aux requêtes ETRN et ATRN effectuées au nom du domaine afin de mettre ses messages en file d'attente. Vous pouvez également configurer d'autres options liées à la mise en file d'attente.

Quotas 279

Cette boîte de dialogue permet d'attribuer une limite à l'espace disque que le domaine peut utiliser et au nombre maximum de messages qui peuvent être stockés.

Paramètres 280

Cet écran filtre un certain nombre d'autres options qui s'appliqueront à la passerelle de domaine sélectionnée. Par exemple, vous pouvez activer/désactiver l'Activer antispam pour cette passerelle, indiquer si l'authentification est requise ou non lors de la mise en file d'attente du courrier, désigner un mot de passe d'authentification, ainsi que plusieurs autres options.

Voir :

Paramètres globaux des passerelles2841Création automatique de passerelle2861Gestion de domaines1841

3.3.1 Paramètres globaux des passerelles

🧐 Gestionnaire de passerelles - Paramètres globaux des passerelles		
Paramètres globaux des passerelles Paramètres globaux des passerelles Création automatique de passerelles Création automatique de passerelles Elfectuer des vérifications sur les expéditeurs comme sur les destinataires Les vérifications Minger déclenchent également celles du Partage de domaine Ne pas envoyer le courrier transféré à l'hôte de relais après une erreur Exclure le courrier de passerelle des obligations de correspondance de fidentitiant (AUTH)		
OK Annuler Appliquer Aide		

Paramètres globaux des passerelles

Les options suivantes sont des options globales. Elles ne sont pas limitées à une passerelle particulière.

Mettre en cache les résultats des vérifications LDAP

Cochez cette case si vous souhaitez mettre en cache les résultats des requêtes de<u>vérification</u> 270 LDAP pour vos passerelles de domaine.

Effectuer des vérifications sur les expéditeurs comme sur les destinataires

Par défaut, lorsque les <u>options de vérification d'</u> adresse sont activées pour une passerelle, MDaemon tente de vérifier les destinataires et les destinataires des messages de la passerelle. Désactivez cette option si vous souhaitez vérifier uniquement les destinataires.

Les vérifications Minger déclenchent également les vérifications du Partage de domaine

Lorsque cette option est activée et que Minger est utilisé par l'une de vos passerelles pour la vérification des adresses, MDaemon interroge non seulement l'hôte Minger désigné dans l'<u>écran de vérification</u> [270], mais aussi les hôtes du <u>Partage</u> <u>partage de domaine</u> [113]. Cette option s'applique à toutes les passerelles configurées pour utiliser Minger pour la vérification des adresses.

Ne pas envoyer le courrier transféré aux hôtes de relais après une erreur

Cliquez sur cette option pour empêcher l'envoi des e-mails transférés vers l'hôte spécifié ci-dessus en cas d'erreurs de distribution. Cette option est désactivée par défaut.

Exclure le courrier de passerelle des obligations de correspondance de l'identifiant (AUTH)

Par défaut, le courrier de la passerelle est exempté des deux options suivantes situées dans l'écran<u>Authentification SMTP</u> [558]: "Les paramètres utilisés doivent correspondre à ceux de l'adresse du chemin de retour" et "Les paramètres utilisés doivent correspondre à ceux de l'adresse de l'en-tête 'From:'". Désactivez cette option si vous ne souhaitez pas exempter le courrier de la passerelle de ces exigences, mais cette désactivation pourrait entraîner des problèmes de stockage et de transfert du courrier de la passerelle.

Voir :

<u>Gestionnaire de passerelles</u> 261 <u>Editeur de passerelle | Vérification</u> 270 <u>Minger</u> ଉ2ଶି <u>Partage de domaine</u> 113

3.3.2 Création automatique de passerelles

Gestionnaire de passerelles - Création autor	matique de passerelles
Gestionnaire de passerelles SecurityGateway	Cet outil recherche les enregistrements MX dans les DNS. Lorsqu'un enregistrement MX est trouvé pour un domaine local, la passerelle correspondante est automatiquement créée.
 Paramètres globaux des passerelles Création automatique de passerelles example.test 	Créer automatiquement des passerelles Utiliser cette passerelle comme modèle
	 Ne pas créer de passerelle lorsque l'expéditeur du message est un utilisateur local Ne pas créer de passerelle lorsque les enregistrements MX renvoient vers une IP réservée Demander confirmation avant d'activer une passerelle Envoyer une demande de confirmation à La confirmation doit être reçue au bout de 1440 minutes La réponse au message de confirmation doit être renvoyée dans ce délai pour éviter la suppression de la passerelle. Distribuer le courrier de passerelle aux premiers hôtes MX à chaque traitement de la file d'attente
< III >	
	OK Annuler Appliquer Aide

Création automatique de passerelles

Cette fonctionnalité permet de créer automatiquement une passerelle [261] pour un domaine inconnu jusqu'alors, lorsqu'une autre source tente de transmettre les messages de ce domaineà MDaemon et qu'une requête DNS indique que l'emplacement deMDaemonest un enregistrement MX valide.

Exemple :

Lorsque la création automatique de passerelles est activée, si l'adresse IP du Domaine par défaut de MDaemon est 192.0.2.0 et qu'un message est délivré via SMTP pour un domaine inconnu exemple.com, MDaemon effectue des requêtes MX et A-record sur exemple .com pour voir si 192.0.2.0 est un hôte de relais de courrier connu pour lui. Si les résultats des requêtes DNS indiquent que l'adresse IP de MDaemonest un hôte MX valide pour exemple.com, MDaemon créera automatiquement une nouvelle passerelle de domaine pour celui-ci et acceptera son courrier électronique. Les messages destinés à exemple.com seront alors stockés dans un dossier spécial et, si vous le souhaitez, transmis aux hôtes MX de niveau supérieur à chaque intervalle de traitement du courrier distant. Cette fonctionnalité vous permet de devenir un serveur de secours pour un autre domaine en configurant simplement le système DNS pour qu'il utilise votre IP comme hôte MX alternatif.

266

Pour sécuriser cette fonctionnalité, MDaemon peut être configuré pour envoyer une demande de confirmation à une adresse électronique de votre choix. Pendant que MDaemon attend la réponse de confirmation, les messages pour le domaine seront acceptés et stockés mais pas délivrés. Vous devez répondre aux demandes de confirmation dans le délai que vous avez défini, faute de quoi la passerelle créée automatiquement sera supprimée et tous les messages stockés seront effacés. Si la confirmation est reçue avant l'expiration du délai, les messages stockés seront délivrés normalement.

Il est possible qu'une personne malveillante ou un "spammeur" tente d'exploiter cette fonctionnalité en configurant son serveur DNS de manière à ce que l'adresse IP de votre MDaemon soit listéecomme l'un de ses hôtes MX. La création automatique de passerelles doit donc être utilisée avec prudence. Dans la mesure du possible, il est recommandé d'utiliser la fonction*Envoyer un message de confirmation de création* à... pouréviter toute exploitation.

Créer automatiquement des domaines de passerelle

Cochez cette case si vous souhaitez que MDaemon crée automatiquement des passerelles de domaine en fonction des résultats des requêtes DNS.

Utiliser cette passerelle existante comme modèle

Sélectionnez une passerelle de domaine dans cette liste déroulante et MDaemon utilisera ses paramètres comme modèle pour toutes les futures passerelles créées automatiquement.

Ne pas créer de passerelles de domaine lorsque l'expéditeur du message est un utilisateur local

Activer cette passerelle si vous ne souhaitez pas que les messages provenant d'utilisateurs locaux déclenchent la création automatique de passerelles.

Nepas créer de passerelles de domaine lorsque le MX pointe vers des adresses IP réservées

Cochez cette case si vous souhaitez empêcher la création automatique d'une passerelle lorsque l'enregistrement MX pointe vers une adresse IP réservée telle que 127.*, 192.*, ou similaire.

Exiger une confirmation avant de rendre la passerelle active

Dans cette option, MDaemon envoie un message de confirmation à l'adresse email de votre choix afin de déterminer si la passerelle créée automatiquement est valide. MDaemon continuera d'accepter les messages pour le domaine en question mais ne les délivrera pas tant que la confirmation n'aura pas été reçue.

Envoyer le message de confirmation de création à

Utilisez cette zone de texte pour désigner l'adresse électronique à laquelle les messages de confirmation seront envoyés.

La confirmation doit être reçue dans un délai de [xx] minutes

Ce champ permet de définir le nombre de minutes pendant lesquelles MDaemon attendra une réponse à un message de confirmation donné. Si ce délai est dépassé, la passerelle de domaine en question sera supprimée.

Distribuer le courrier de la passerelle aux hôtes MX supérieurs à chaque file d'attente Si vous souhaitez que MDaemon tente de distribuerles messages decette passerelleaux hôtes MX de niveau supérieur à chaque fois que la file distante est traitée, activez cette option.

Voir :

Gestionnaire de passerelles 261

3.3.3 Éditeur de passerelle

3.3.3.1 Domaine

Gateway Manager - Domain	
Gateway Manager - Domain Gateway Manager Global Gateway Settings Automatic Gateway Creation	example.test Enable gateway service for this domain Messages arriving destined for all users of this gateway domain will be placed into a common mailbox folder. Store messages for this gateway domain here: c:\mdaemon\gateways\example.test\ Browse Deliver stored messages each time MDaemon processes remote mail use the Retry Queue (otherwise mail stays in gateway folder) Automatically extract embedded attachments Extracted attachments will be stored here: c:\mdaemon\gateways\example.test\FILES\
<u>[[]</u>]	Ok Cancel Apply Help

Domaine de la passerelle

Activer le service de passerelle pour ce domaine Cochez cette case pour activer cette passerelle de domaine.

Enregistrer les messages de ce domaine dans le répertoire :

Saisissez le répertoire dans lequel vous souhaitez stocker le courrier entrant pour le domaine. Tous ses messages seront stockés dans le même dossier, quels que soient les destinataires individuels auxquels chaque message est adressé.

Distribuer les messages enregistrés à chaque traitement du courrier distant

En général, lorsque MDaemon reçoit du courrier destiné à l'une de ses passerelles, il le stocke jusqu'à ce que le domaine concerné se connecte à MDaemon pour le récupérer. Dans certaines situations, vous pouvez souhaiter que MDaemon tente de distribuer le courrier directement via SMTP plutôt que d'attendre que le domaine le récupère. Lorsque cette option est activée, MDaemon tente de distribuer les messages dudomaine à chaque fois que le courrier distant esttraité.La boîte aux lettres de lapasserelleservira temporairement de file d'attente distante et la distribution sera tentée. Les messages qui ne peuvent pas être distribués resteront dans laboîte aux lettres de lapasserellejusqu'à ce qu'ils soient collectés par le domaine ou qu'ils soient distribués plus tard ; ils ne seront pas déplacés dans la file d'attente distante ou dans le système de relance. Cependant, si le DNS du domaine n'est pas correctement configuré ou si votre MDaemon est configuré pour transmettre tous les messages sortants à un autre hôte, ces messages risquent d'être pris dans une boucle de courrier et d'être considérés comme non distribuables.

Dans la File d'attente de relance (sinon le courrier reste dans le Dossier de la passerelle)

Activez cette option si vous souhaitez utiliser le mécanisme de<u>File de relance</u> pour la distribution du courrier. Cette option est désactivée par défaut, ce qui signifie que le courrier de la passerelle restera à jamais dans le Dossier de la passerelle, même s'il ne peut pas être distribué.

Extraire automatiquement les pièces jointes

Certains systèmes de messagerie exigent que les pièces jointes soient extraites avant la soumission des messages au flux de courrier. Pour cela, MDaemon peut extraire automatiquement les pièces jointes MIME entrantes et les placer dans le sous-dossier\Files\ sous le dossier message du domaine.Cochez cette case si vous souhaitez extraire automatiquement les pièces jointes.

3.3.3.2 Vérification

🧐 Gestionnaire de passerelles - Vérification		
 Gestionnaire de passerelles - Verification Gestionnaire de passerelles Gestionnaire de passerelles SecurityGateway Paramètres globaux des passerelles Création automatique de passerelles Création automatique de passerelles example.test Domaine Vérification Transfert Retrait de la file d'attente 	Vérification d'adresses Vérifier les adresses à l'aide de : Nom d'hôte ou IP 	Aucun Fichier LDAP Minger Port 389 Utiliser la version 3 du protocole Suivre les referrals Mot de passe
— Quotas — Paramètres	DN de base Filtre de recherche [(&(objectclass=user)([(mail=\$EMAIL\$ Si vous ne remplissez pas ce champ \$EMAIL\$ est remplacé par l'adresse par le nom de la boîte aux lettres. Étendue de la recherche DN de base uniquement Niveau inférieur au DN de base © DN de base et enfants	\$)(mail=SMTP:\$EMAIL\$)(proxyAddresses , MDaemon génère un filtre par défaut. complète et \$MAILBOX\$ est remplacé Les adresses e-mail peuvent également être vérifiées avec un fichier texte local. Fichier de vérification des adresses
< •		OK Annuler Appliquer Aide

Un problème courant avec les passerelles de domaine et les relais de courrier est qu'elles n'ont généralement pas de méthode pour déterminer si le destinataire d'un message entrant est valide ou non. Par exemple, si vous agissez en tant que passerelle pour exemple.com et qu'un message arrive pour user01@example.com, vous n'avez aucun moyen de savoir s'il existe ou non une boîte aux lettres, un alias ou une liste électronique correspondant à cette adresse sur le serveur e-mail de Serveurur.com. Vous n'avez donc pas d'autre choix que de supposer que l'adresse est valide et d'accepter le message. Dans la mesure où les spammeurs envoient souvent des messages à de nombreuses adresses non valides, ce problème peut entraîner l'acceptation d'un grand nombre de courriers électroniques indésirables par la passerelle.

MDaemon contient une méthode pour éviter ce problème en vérifiant les adresses des destinataires. Si le serveur du domaine distant est configuré pour maintenir un serveur LDAP ou Active Directory à jour avec toutes ses boîtes aux lettres, alias et listes de diffusion, ou s'il utilise un serveur Minger pour vérifier les adresses distantes, vous pouvez utiliser les options de cet écran pour spécifier le LDAP, l'Active Directory ou le Serveur distant où ces informations sont stockées. Ensuite, lorsqu'un message arrive à l'adresse Exemple.com, vous pouvez rechercher l'adresse du destinataire sur l'autre serveur et déterminer si elle est valide ou non.

Vérification des adresses

Vérifiez les adresses à l'aide de :

Rien

Choisissez cette option si vous ne souhaitez pas utiliser la Vérification des adresses e-mail pour cette passerelle de domaine. MDaemon traitera tous les messages entrants du domaine comme si le destinataire était une adresse valide, car il n'aura aucun moyen d'identifier les adresses qui existent réellement pour ce domaine.

Fichier

Choisissez cette option si vous souhaitez utiliser le fichier GatewayUsers.dat comme liste définitive d'adresses qui sera utilisée pour vérifier si le destinataire d'un message entrant pour ce domaine est valide ou non. Il s'agit d'une liste globale d'adresses, applicable à toutes vos passerelles de domaine, et même si vous avez choisi d'utiliser l'une des autres méthodes de vérification, cette liste sera toujours utilisée comme source supplémentaire d'adresses valides. En revanche, lorsque vous utilisez l' option *Fichier*, il s'agit de la seule méthode de vérification utilisée. Vous pouvez ouvrir et modifier la liste des adresses valides en cliquant sur le bouton*Fichier de vérification des adresses* ci-dessous.

LDAP

Choisissez cette option pour activer la vérification des adresses distantes via LDAP ou Active Directory. Chaque fois qu'un message arrive pour le domaine distant, son serveur LDAP ou Active Directory sera interrogé pour déterminer si le destinataire est valide ou non. Si ce n'est pas le cas, le message est rejeté. Si MDaemon ne parvient pas à se connecter au serveur LDAP/AD, il considère que l'adresse est valide.

Minger

Sélectionnez cette option si vous souhaitez interroger le serveur Minger du domaine pour vérifier les adresses des destinataires pour ce domaine. Si MDaemon ne parvient pas à se connecter au serveur, il considérera que l'adresse est valide. Il existe également une option globale située dans les <u>Paramètres des passerelles globales</u> al que vous pouvez utiliser pour que MDaemon interroge également les hôtes du<u>Partage de domaine.</u>

Nom d'hôte ou IP

Entrez le nom hôte ou l'adresse IP du serveur LDAP/Active Directory ou Minger du domaine. Il s'agit du serveur LDAP/AD ou Minger auquel MDaemon se connectera pour vérifier que le destinataire d'un message entrant est une adresse valide du domaine pour lequel ce MDaemon agit en tant que passerelle ou serveur de secours.

Port

Indiquez le port utilisé par le serveur LDAP/AD ou Port Minger du domaine. MDaemon utilisera ce port lors de la vérification des informations d'adresse via LDAP, Active Directory ou Port Minger.

Test

Cliquez sur ce bouton pour tester si les paramètres de vérification de l'adresse distante sont correctement configurés. MDaemon tentera simplement de se

connecter au serveur LDAP/AD désigné et vérifiera qu'il répond aux informations spécifiées.

Cache

Cliquez sur ce bouton pour ouvrir le Cache LDAP/Minger. Vous pouvez activer/désactiver le cache dans les <u>Paramètres globaux des passerelles</u> 284].

Utiliser la version 3 du protocole

Cochez cette case si vous souhaitez que la vérification de la passerelle utilise la version 3 du protocole LDAP avec votre serveur.

Suivre les referrals

Il arrive qu'un serveur LDAP ne dispose pas de l'objet demandé, mais qu'il ait une référence croisée à son emplacement, à laquelle il peut renvoyer le client. Si vous souhaitez que la vérification de la passerelle suive ces referrals, activez cette option. Cette option est désactivée par défaut.

Nom d'utilisateur ou DN de liaison

Saisissez le Nom utilisateur ou le DN du compte qui dispose d'un accès administratif au serveur LDAP/AD du domaine afin que MDaemon puisse vérifier les destinataires des messages entrants adressés au domaine pour lequel il fait office de passerelle ou de serveur de secours. Dans ce cas, il s'agit du DN utilisé pour l'authentification dans l'opération de liaison.

Mot de passe ou secret partagé Minger

Ce mot de passe sera transmis au serveur LDAP/AD du domaine avec la valeur du*DN de liaison* pour l'authentification. Si vous utilisez un serveur Minger, il s'agit du secret partagé ou du mot de passe utilisé.

Entrée base DN

Il s'agit du Distinguished Name (DN) ou du point de départ de l'arborescence (DIT) à partir duquel MDaemon interrogera votre serveur LDAP/AD pour vérifier l'adresse.

Filtre de recherche

Il s'agit du filtre de recherche LDAP/AD qui sera utilisé lors de l'interrogation de votre serveur pour vérifier les adresses. MDaemon définit un filtre de recherche par défaut qui devrait fonctionner dans la plupart des cas.

Portée de la recherche :

Il s'agit de la portée ou de l'étendue de vos recherches LDAP/AD.

DN de base uniquement

Cherchez cette option si vous souhaitez limiter votre recherche au seul DN de base spécifié ci-dessus. La recherche ne sera pas effectuée en dessous de ce point de l'arborescence (DIT).

1 niveau inférieur au DN de base

Utilisez cette option si vous souhaitez étendre votre recherche LDAP/AD à un niveau inférieur au DN fourni dans votre DIT.

DN de base et tous les enfants

Cette option permet d'étendre la portée de votre recherche du DN fourni à tous ses enfants, jusqu'à l'entrée enfant la plus basse de votre DIT.

Fichier de vérification des adresses

Cliquez sur ce bouton pour ouvrir la Liste des adresses e-mail valides de la passerelle (c'est-à-dire le fichier GatewayUsers.dat). Ce fichier contient une liste d'adresses que MDaemon considérera comme des destinataires valides pour les messages entrants adressés aux passerelles de votre domaine. Quelle que soit l'option de vérification choisie ci-dessus, MDaemon utilisera cette liste comme source supplémentaire d'adresses valides. Cependant, lorsque vous utilisez l' option*Fichier* ci-dessus, il s'agira de la seule et unique option de vérification utilisée.

Utilisation de plusieurs configurations pour les requêtes de vérification LDAP

Vous pouvez spécifier plusieurs configurations LDAP pour vos domaines de passerelle. Pour spécifier des jeux supplémentaires de paramètres LDAP, configurez votre premier jeu normalement, puis modifiez manuellement le fichierGATEWAYS.DAT à l'aide du Blocnotes.

Votre nouveau jeu de paramètres doit être créé en utilisant le format suivant :

```
LDAPHost1=<nom d'hôte>
LDAPPort1=<port>
LDAPBaseEntry1=<nom de l'entrée base>
LDAPRootDN1=<Nom de la racine>
LDAPObjectClass1=USER
LDAPRootPass1=<motdepasse>
LDAPMailAttribute1=mail
```

Pour chaque nouveau jeu de paramètres, augmentez le chiffre dunom dechaque paramètrede 1. Par exemple, dans le jeu d'échantillons ci-dessus, le nom de chaque paramètre se termine par "1". Pour créer un jeu supplémentaire, le nom de chaque paramètre se termine par "2". Dans un autre ensemble, chaque nom se terminerait par "3", et ainsi de suite.

Dans les requêtes LDAP, MDaemon effectue plusieurs requêtes LDAP en séquence pour trouver une correspondance. Si une erreur ou une correspondance est trouvée, aucune autre vérification n'est effectuée.

Voir :

Options LDAP/Carnet d'adresses 800

3.3.3.3 Transfert

Gateway Manager - Forwarding Gateway Manager Global Gateway Settings Automatic Gateway Creation Creample.test Domain Verification Forwarding Dequeuing Quotas Settings	Forwarding □ Forward mail to another mail system □ Domain name or IP Note: If you would like to forward mail to a specific host enclose the value above in brackets. For example, [c3po.altn.com]. AUTH Logon AUTH Password □ Forward mail to an email address Email address SMTP 'MAIL' value Port (default = 25) 25 Retain a local copy of all forwarded mail
	Ok Cancel Apply Help

Redirection

Transférer le courrier à un autre système de messagerie

Il est parfois avantageux de simplement Transférer une copie de tous les messages pour un domaine au fur et à mesure qu'ils arrivent. Si vous souhaitez configurer MDaemon dans ce sens, entrez le Nom ou l'Adresse IP du domaine vers lequel les copies du courrier entrant pour ce domaine doivent être envoyées. Si vous souhaitez transférer les messages à un hôte spécifique, placez la valeur entre parenthèses (par exemple, [host1.example.net]). Utilisez l'option Mot de passe AUTH pour inclure tous les identifiants de connexion nécessaires pour le serveur vers lequel vous transférez les messages.

Transférer le courrier à une adresse e-mail

Utilisez cette fonction si vous souhaitez transférer à une adresse électronique spécifique tous les messages électroniques destinés à ce domaine client.

Valeur SMTP 'MAIL'.

MDaemon utilisera cette adresse dans la transaction SMTP "Mail From" lors du transfert des messages.

Port (par défaut = 25)

MDaemon utilisera ce port pour transférer les messages.

Garder une copie locale du courrier transféré

Sélectionnez cette option si vous souhaitez que MDaemon conserve localement une copie d'archivage de chaque message une fois qu'il a été transféré.

3.3.3.4 Retrait de la file d'attente

- 6-1	This gateway honors ETRN requests		
Socurity Gateway	deliver stored mail to the IP of the bost making the request		
Global Gateway Settings			
Automatic Gateway Creation	deliver to domain, [host] or IP		
example.test	AUTH Logon		
Domain	ALITH Password		
Verification			
Forwarding	Port (default = 25) 25		
Dequeuing	If the domain listed above is local treat it as if it were foreign		
Quotas	ETRN requests require authenticated sessions		
Settings			
This gateway honors ATRN requests			
	Allow only one ATRN session at a time		
	ATPN encourage		
	Access		
	Honor dequeue requests from these IPs *****		
	O Ignore dequeue requests from these IPs		
	New ID - CIDD × 2 and the wildoards ok		
	Add Remove		

ETRN

Cette passerelle accepte les requêtes ETRN

Lorsque ce commutateur est activé, MDaemon répond aux requêtes ETRN effectuées par des hôtes qualifiés au nom du domaine pour lequel MDaemon joue le rôle de passerelle de messagerie. La commande ETRN est une extension SMTP qui signale à un serveur stockant du courrier pour un domaine particulier qu'il est temps de commencer à spouler le courrier. Lorsque MDaemon reçoit une requête ETRN pour un domaine, il commence immédiatement à spouler le courrier stocké pour le distribuer via des transactions SMTP ultérieures. Notez que la session SMTP qui émet une requête ETRN n'est pas celle qui reçoit le courrier stocké. MDaemon utilisera des transactions SMTP indépendantes pour envoyer le courrier stocké pour le domaine. Cette méthode préserve l'enveloppe du message et est plus sûre. Notez également que l'hôte vers lequel MDaemon enverra le courrier stocké ne commencera peut-être pas immédiatement à recevoir ces messages. L'ETRN garantit uniquement que le courrier stocké est *récupéré en* vue de sa distribution. Le *processus de* distribution est soumis à d'autres restrictions imposées par l'administrateur et peut devoir attendre dans la file d'attente du courrier sortant que le prochain traitement du courrier distant ait lieu. En raison de ces limitations, nous recommandons d'utiliser le <u>relais du courrier à la demande (ODMR</u> 2009)) et sa commande ATRN plutôt que l'ETRN. Cette méthode n'est cependant pas prise en charge par tous les clients et serveurs, et ne sera donc disponible que pour les domaines clients utilisant un serveur qui la prend en charge. MDaemon prend entièrement en charge l'ODMR, tant du côté client que du côté serveur.

Par défaut, MDaemon exige que l'hôte qui émet la requête ETRN s'authentifie d'abord via ESMTP AUTH en utilisant le <u>Nom</u> <u>du domaine</u> al et le <u>Mot de passe ATRN</u> de la passerelle comme identifiants de connexion. Si vous ne souhaitez pas exiger l'authentification, vous pouvez la désactiver dans les <u>paramètres</u> en désélectionnant l'option <u>Exiger l'authentification</u> pour le retrait courrier de la file d'attente ETRN.

...distribuer le courrier à l'IP de l'hôte ayant effectué la requête

Si vous sélectionnez cette option, MDaemon enverra le courrier stocké à l'adresse IP de la machine qui a fait la demande d'ETRN. La machine requérante doit disposer d'un serveur SMTP pour recevoir ces messages.

...Distribuer au domaine, à [l'hôte] ou à l'IP

Il s'agit du Nom hôte, du Domaine ou de l'adresse IP à laquelle le courrier stocké sera envoyé lorsqu'une requête ETRN est reçue et honorée. La machine réceptrice doit disposer d'un serveur SMTP pour recevoir ces messages. Par nom : lorsqu'un Nom de domaine est spécifié dans cette option, les enregistrements A et MX peuvent être utilisés, en fonction des résultats du DNS lors de la distribution. Si vous souhaitez envoyer les messages à un hôte particulier, placez le nom de l'hôte entre parenthèses (par exemple, [host1.example.net]) ou indiquez une adresse IP au lieu d'un nom de domaine. Saisissez les informations d'identification(*logo/mot de passe AUTH*) nécessaires à la distribution des messages à l'endroit indiqué.

Port (par défaut = 25)

Utilisez cette option pour spécifier le port sur lequel lecourrier dudomainesera envoyé.

Si le domaine ci-dessus est local, le traiter comme un domaine inconnu

Activez cette commande si le domaine est local mais que vous souhaitez que son courrier soit traité comme s'il était distant.

Les requêtes ETRN nécessitent des sessions authentifiées

Lors de la prise en compte des requêtes ESMTP ETRN, cette option sera utilisée par défaut pour exiger que l'hôte qui se connecte s'authentifie d'abord à l'aide de la

commande ESMTP AUTH. Dans cette option, vous devez désigner un mot de passe d'authentification dans l'option "Mot de passe ATRN" ci-dessous.

Décochez cette case si vous ne souhaitez pas requérir l'authentification des hôtes effectuant des requêtes ETRN.

ATRN

Cette passerelle accepte les requêtes ATRN

Activer cette option si vous souhaitez que MDaemon réponde aux commandes ATRN provenant du domaine de la passerelle. ATRN est une commande ESMTP utilisée dans le <u>relais de courrier à la demande (ODMR</u> 2009), qui est actuellement la meilleure méthode de relais disponible pour l'hébergement de courrier. Elle est supérieure à l'ETRN et à d'autres méthodes dans la mesure où elle requiert une authentification pour le retrait du courrier d'une file d'attente et où elle ne nécessite pas d'adresse IP statique. Une adresse IP statique n'est pas nécessaire car le flux de données entre MDaemon et le domaine client est immédiatement inversé et les messages sont déstockés sans qu'il soit nécessaire d'établir une nouvelle connexion, contrairement à l' ETRN, qui utilise une connexion distincte après l' envoi de la commandeETRN. Cela permet aux domaines clients ayant une adresse IP dynamique (non statique) de collecter leurs messages sans avoir à utiliser POP3 ou DomainPOP, car l'enveloppe SMTP d'origine est préservée.



ATRN nécessite une session à l'aide de la commande AUTH. Vous pouvez configurer les informations d'authentification dans l' écran<u>Paramètres</u> [280].

Autoriser une seule session ATRN à la fois

Cochez cette case si vous souhaitez limiter l'ATRN à une seule session à la fois.

Mot de passe ATRN

Lorsque vous utilisez ATRN pour mettre en file d'attente lecourrier de cette passerelle, ou lorsque vous demandez une authentification via l'option*Exigence d'authentification pour le retrait file d'attente ATRN* dans l'écran Paramètres, indiquez ici le mot de passe ATRN de la passerelle.

Le domaine pour lequel MDaemon joue le rôle de passerelle de messagerie doit utiliser son nom de domaine comme paramètre d'identification. Exemple : si la passerelle du domaine est "exemple.com" et qu'elle utilise Mot deTRN pour mettre son courrier en file d'attente, elle s'authentifiera en utilisant les identifiants de connexion "exemple.com" et le mot de passe spécifié ici.

Accès

Exécuter les demandes de retrait de file d'attente de ces IP

Sélectionnez ce commutateur pour que MDaemon honore les requêtes ETRN/ATRN effectuées à partir de n'importe quelle adresse IP figurant dans la liste d'adresses associée.

Ignorer les demandes de retrait de file d'attente de ces IP

Cochez cette case pour que MDaemon ignore les demandes d'ETRN/ATRN provenant de n'importe quelle adresse IP figurant dans la liste d'adresses associée.

Ajouter une nouvelle IP

Pour ajouter une Nouvelle IP à la liste actuelle, il suffit d'entrer l'IP dans ce texte et de cliquer sur le bouton*Ajouter*.

Supprimer

Cliquez sur ce bouton pour supprimer une entrée sélectionnée de la liste des adresses IP.

3.3.3.5 Quotas

🧐 Gestionnaire de passerelles - Quotas	
Gestionnaire de passerelles SecurityGateway Paramètres globaux des passerelles Création automatique de passerelles example.test Vérification Transfert Retrait de la file d'attente Quotas Paramètres	Quotas Appliquer les quotas de messages et d'espace disque à la passerelle Nombre maximal de messages stockés 0 Espace disque maximal autorisé 0 Mo Lorsque ces quotas sont atteints, les messages destinés à la passerelle sont refusés. Placer un message d'alerte dans la boîte aux lettres de la passerelle en cas de dépassement de quota Expéditeur des messages d'alerte
	OK Annuler Appliquer Aide

Quotas

Appliquer à la passerelle les quotas concernant le nombre de messages et l'espace disque

Activez cette option si vous souhaitez désigner un nombre maximal de messages autorisés à être stockés pour le domaine ou une quantité maximale d'espace disque (en kilo-octets) qu'il peut utiliser. Cela inclut toutes les pièces jointes décodées dans son répertoire Files. Lorsqu'un quota est atteint, tous les messages entrants adressés au domaine seront refusés.

Nombre maximal de messages stockés à la fois

Utilisez cette case pour indiquer le nombre maximum de messages que MDaemon stockera pour ce domaine de passerelle. Utilisez "0" dans cette option si vous ne souhaitez pas limiter le nombre de messages.

Espace disque maximal autorisé

Indiquez ici l'espace disque maximal autorisé. Lorsque les messages et les fichiers stockés pour le domaine atteignent cette limite, tous les messages entrants supplémentaires pour le domaine seront refusés. Utilisez "0" si vous ne souhaitez pas fixer de limite d'espace disque.

Afficher un message d'alerte dans le Dossier des messages d'une passerelle en cas de dépassement du quota

Si cette option est activée et qu'une tentative de distribution de courrier vers le domaine dépasse les limites maximales de messages ou d'espace disque, un message d'alerte approprié sera placé dans le Dossier courrier de lapasserelle dudomaine.Vous pouvez désignerci-dessous les en-têtes "From:" et "To:" dumessage d'avertissement.

Expéditeur des messages d'alerte

Dans cette option, vous pouvez spécifier l'adresse "From :" qui sera utilisée dans les messages d'alerte de dépassement de quota.

Destinataire des messages d'alerte

Dans cette option, vous pouvez spécifier l'adresse "À :" qui sera utilisée dans les messages d'alerte de dépassement de quota.

3.3.3.6 Paramètres

Global Gateway Settings Automatic Gateway Creation example.test Domain Verification Forwarding Dequeuing Quotas Settings	Enable AntiSpam scanning for this gateway Authenticated requests are valid regardless of connecting IP Authentication is required when sending mail as a user of this gateway
--	---

Paramètres

Activer l'analyse antivirus pour cette passerelle

Cliquez sur cette option si vous utilisez les fonctionsoptionnelles de<u>MDaemon</u> <u>AntiVirus</u> at que vous souhaitez queles messages de cette passerelle de domainesoient analysés. Si vous désactivez cette option, l'antivirus n'analysera pas les messages decette passerelle.

Activer l'analyse anti-spam pour cette passerelle

Cliquez sur cette option si vous voulez appliquer les paramètres du Filtre anti-spam aux messages de cettepasserelle de domaines.Sinon, ils seront exclus de l'analyse du Filtre anti-spam.

Les requêtes authentifiées sont valides quelle que soit l'IP qui se connecte

Activez cette case à cocher si vous souhaitez honorer les demandes authentifiées quelle que soit l'adresse IP d'où elles proviennent. Si ce contrôle n'est pas activé, seules les demandes provenant des adresses IP spécifiées dans la section Contrôle d'accès seront honorées.

L'authentification est requise pour l'envoi de courrier à partir de cette passerelle en tant qu'utilisateur.

Cochez cette case si vous souhaitez que tous les messages prétendant provenir de ce domaine requièrent une authentification requise. Si un message est censé provenir de ce domaine, il doit utiliser une connexion authentifiée (ou se connecter à partir d'une adresse IP autorisée), sinon il sera refusé. Cette option est activée par défaut.

Lorsque de nouvelles passerelles de domaine sont créées, cette option est activée par défaut. Si vous souhaitez modifier le paramètre par défaut afin que cette option soit désactivée pour les nouvelles passerelles, modifiez la clé suivante dans le fichierMDaemon.ini:

```
[Spécial]
GatewaySendersMustAuth=No ( Oui(par défaut) )
```

3.4 Gestionnaire de listes de diffusion

Les listes de diffusion, parfois appelées groupes de messagerie ou listes de distribution, permettent de s'adresser à des groupes d'utilisateurs comme s'ils partageaient tous une boîte aux lettres commune. Les copies des messages e-mail envoyés à la liste sont distribuées à chacun de ses membres.Les listes peuvent contenir des membres ayant des adresses de destination locales et/ou distantes, être publiques ou privées, modérées ou ouvertes, être envoyées au format<u>digest</u> au format de message normal, et bien d'autres choses encore.



Situé dans le menu Configuration | Gestionnaire de listes de diffusion..., le Gestionnaire de listes de diffusion est utilisé pour administrer vos listes.

Gestionnaire de listes de diffusion

Le volet de navigation situé à gauche de cette boîte de dialogue contient une entrée pour chacune de vos listes de diffusion, avec des liens vers chaque écran utilisé pour configurer les différents paramètres spécifiques à la liste. Il permet également d'accéder à l' écran <u>Paramètres liste de diffusion</u> [24], qui sert à configurer plusieurs options globales liées aux listes. Les options situées à droite de cette boîte de dialogue permettent de créer, de supprimer et de renommer vos listes. Vous pouvez double-cliquer sur une liste de diffusion pour passer à l'éditeur de liste de diffusion afin de configurer les paramètres de la liste.

Nouvelle liste

Pour créer une nouvelle liste de diffusion, cliquez sur **Nouvelle liste** pour ouvrir la boîte de dialogue Adresse e-mail de la liste de diffusion. Créez un Nom de la BAL et sélectionnez un domaine, tels que "MaListe" et "exemple.com" respectivement. Il s'agira de l'adresse électronique de la liste de diffusion (c'est-à-dire MyList@example.com). Les messages envoyés à cette adresse seront distribués aux membres de la liste, en fonction des paramètres particuliers de la liste. Cliquez sur **OK** pour créer la liste. Après avoir créé la liste, vous pouvez double-cliquer sur son entrée pour configurer ses paramètres et ajouter des membres. Par nom: Les noms de liste ne peuvent pas contenir " ! " ou " | ".

Mailing List Email Address			×
Mailing List Email Address			
Mailbox	MyList		
Domain	company.test	~	
		OK Cance	el -

Supprimer une liste

Pour supprimer une liste de diffusion : sélectionnez la liste, cliquez sur **Supprimer la liste** et cliquez sur **Oui** pour confirmer votre décision.

Renommer une liste

Pour renommer une liste de diffusion, sélectionnez la liste, puis cliquez sur **Renommer la liste** pour ouvrir la boîte de dialogue Adresse e-mail de la liste de diffusion. Apportez les modifications souhaitées et cliquez sur **OK**.

Copier une liste

Si vous souhaitez créer une liste de diffusion avec les mêmes paramètres et membres qu'une autre liste, sélectionnez la liste, cliquez sur ce bouton, puis indiquez un nom de boîte aux lettres et un domaine pour la nouvelle liste.

Modification d'une Liste de diffusion existante

Pour configurer une liste de diffusion, double-cliquez sur son entrée dans le Gestionnaire listes de diffusion. Dans le volet de navigation de gauche, cliquez sur l'écran que vous souhaitez modifier :

Membres 287 Paramètres 290 En-tête From: : TO : Dans l'en-tête FROM 294 Abonnement 297 Rappels 307 Modération 306 Synthèse 303 Routage 308 Notifications 304 Fichiers de support 317 Dossiers publics 314 Active Directory 315 ODBC 318

Paramètres des listes de diffusion

Cliquez sur **Paramètres de listes de diffusion** dans le volet de gauche pour ouvrir l' écran <u>Paramètres de listes de diffusion</u> [284], qui permet de configurer plusieurs paramètres globaux liés aux listes de diffusion.

Voir :

Liste de diffusion Paramètres de liste de diffusion 284

3.4.1 Paramètres de liste de diffusion

🧐 Gestionnaire de listes de diffusion - Paramètre	es de liste de diffusion 🛛 🔼
🗢 Castionnains de lister de diffusion	Paramètres de liste de diffusion
Paramètres de liste de diffusion	Créer des listes 'Everyone'
	Inclure les listes 'Everyone' et 'MasterEveryone' dans les exportations de fichiers
	Appliquer le filtre anti-spam et le filtre de contenu aux messages de liste avant d'envoyer des copies individuelles
	🔽 Répondre aux requêtes ' <liste>-subscribe' et '<liste>-unsubscribe'.</liste></liste>
	☑ Ajouter l'en-tête 'Sender: <list>' à tous les messages de liste</list>
	📃 Le nettoyeur de liste supprime les messages qu'il ne peut pas analyser
	🔽 Le nettoyeur de liste enregistre les messages qui entraînent la suppression d'un membre
	Rechercher le contenu inapproprié dans les messages destinés aux listes de diffusion
	Ne pas envoyer de copie du message de liste à l'expéditeur du message
	envoyé à plusieurs listes
	Ajouter l'en-tête personnalisé 'Header:value' à tous les messages de liste (exemple : 'Precedence:bulk')
	Precedence: bulk
	Objet des compilations de messages
	Compilation de \$LISTNAME\$ \$TIMESTAMP\$ \$ISSUE\$
	Nbre max. de membres par liste de diffusion 0 (0 = pas de limite) (Cloud uniquement)
	L'édition MDaemon Private Cloud (MDPC) inclut des fonctionnalités pour les fournisseurs de services cloud. Le service de messagerie hébergée peut être acheté directement auprès de MDaemon Technologies ou de son réseau de partenaires.
	Cliquez ici pour en savoir plus sur les options de messagerie dans le cloud de MDaemon.
	OK Annuler Appliquer Aide

Liste de diffusion Paramètres de liste de diffusion

Créer des listes de diffusion globales (Everyone)

Cochez cette case si vous souhaitez créer et maintenir des listes de diffusion "Everyone" pour tous vos domaines (Exemple : "everyone@example.com"). Une liste sera créée pour chaque domaine, ce qui vous permet d'envoyer un message à tous les utilisateurs d'un domaine en adressant simplement le message à "everyone@<domain>". Les<u>comptes privés</u> sont cachés des listes de diffusion "Tout le monde". Cette option est désactivée par défaut.

Créer une liste "MasterEveryone

Activer cette liste de diffusion si vous souhaitez qu'il y ait une liste de diffusion "MasterEveryone". Toutes les personnes figurant sur les listes "Tout le monde" spécifiques à votre domaine seront incluses dans cette liste. Cette option est désactivée par défaut.

Inclure les listes "Everyone" et "MasterEveryone" dans les exportations

Par défaut, les listes de diffusion 'Everyone' et 'MasterEveryone' sont incluses lorsque vous utilisez les options "Comptes | Exportation..." pour exporter des listes. Désactivez cette option si vous ne souhaitez pas inclure ces listes dans les exportations de listes de diffusion.

Appliquer les filtres de contenu et de spam aux listes avant de les dissocier en copies. Lorsque l' option *Distribuer le courrier de liste à chaque membre individuellement* est choisie dans l' écran<u>Routage</u> al de l'éditeur de listes de diffusion, l'activation de cette commande entraîne l'application des règles Filtre de contenu et Filtre anti-spam aux messages de la liste avant qu'ils ne soient copiés et distribués aux membres de la liste.

Répondre aux requêtes "<List>-subscribe" et "<List>-unsubscribe

Cochez cette case si vous souhaitez que MDaemon reconnaisse les adresses e-mail de ce format comme valides (tant que la liste existe) afin de faciliter l'inscription et la désinscription des utilisateurs de vos listes de diffusion. Exemple : supposons que vous ayez une liste appelée MyList@example.com. Les utilisateurs pourront s'inscrire ou se désinscrire de votre liste en envoyant un message électronique à MyList-Subscribe@example.com et MyList-

Unsubscribe@example.com. Le contenu de l'objet et du corps du message n'a aucune importance. De plus, lorsque cette fonctionnalité est activée, MDaemon insère l'en-tête suivant dans tous les messages de la liste :

List-Unsubscribe : <mailto:<List>-Unsubscribe@example.com>

Certains clients de messagerie peuvent s'en rendre compte et mettre automatiquement un bouton UNSUBSCRIBE à la disposition des utilisateurs.

Vous pouvez remplacer cette option pour des listes individuelles en spécifiant une valeur pour les en-têtes List-Subscribe et List-Unsubscribe dans les options **URL** de **listes de diffusion** situées dans l'écran de modération de l'éditeur de listes de diffusion.

Ajouter l'en-tête 'Sender : <List>' à tous les messages de liste

Activer cette option si vous souhaitez insérer l'en-têtesender dans les messages des listes de diffusion.

Le nettoyeur de liste supprime les messages qu'il ne peut pas analyser

Lorsque cette option est activée, MDaemon supprime les messages de la liste qui ne contiennent pas d'adresse analysable.

Le nettoyeur de liste enregistre les messages qui entraînent la suppression d'un membre Lorsque MDaemon analyse les messages de liste renvoyés pour tenter de supprimer les adresses des membres qui ne sont pas joignables, cette commande permet d'enregistrer les messages qui entraînent lasuppression d' un membre de la liste. Pour plus d'informations, consultez l' option *Supprimer les adresses électroniques non distribuables*... dans l' écran<u>Paramètres</u> [290].

Rechercher le contenu inapproprié dans les messages destinés aux listes de diffusion

Cochez cette case si vous souhaitez que MDaemon rejette les messages adressés à une liste de diffusion lorsqu'il détermine qu'ils auraient dû être adressés au Compte système. Exemple : un utilisateur peut rejoindre ou quitter une liste en plaçant la commande S'abonner ou Se désinscrire au début d'un message électronique et en envoyant ce message à l'adresse système (par exemple "mdaemon@example.com"). Souvent, les utilisateurs essaient par erreur d'envoyer ce type de message à la liste elle-même. Cette option empêchera l'envoi de ces messages à la liste.

Ne pas envoyer de copie du message de la liste à l'expéditeur du message

Lorsque cette option est activée et qu'un membre de la liste envoie un message à la liste, l'expéditeur ne reçoit pas de copie de ce message. Cette option est désactivée par défaut.

Supprimer les destinataires en double lorsqu'un même message est envoyé à plusieurs listes

Lorsque cette option est activée et qu'un message unique est adressé à plusieurs listes de diffusion, MDaemon ne remettra qu'une seule copie du message à tout destinataire <u>membre</u> [207] de plusieurs de ces listes. Exemple : si frank@example.net est membre de List-A@example.com et List-B@example.com et qu'un message entrant est adressé aux deux listes, Frank ne recevra qu'une seule copie du message au lieu de deux. Cette option ne s'applique qu'aux listes. Dans l'Exemple ci-dessus, si le message était adressé directement à Frank et aux deux listes, Frank recevrait deux copies du message au lieu de trois. Cette option est désactivée par défaut.

Son utilisation n'est généralement pas recommandée. Les listes de diffusion peuvent être utilisées et organisées de différentes manières par les utilisateurs, et il n'y a aucun moyen de savoir quelle liste recevra le message lorsque l'on limite les doublons de cette manière. Par conséquent, l'utilisation de cette option pourrait causer des difficultés inutiles à certains utilisateurs, en raison de leurs préférences en matière de filtrage des messages, de l'utilisation de <u>filtres IMAP</u> 7891 pour trier les messages dans des dossiers spécifiques, etc.

Ajouter l'en-tête personnalisé 'Header : value' à tous les messages de liste

Si vous souhaitez ajouter une combinaison en-tête/valeur statique (telle que "Precedence : bulk") à tous les messages de la liste, spécifiez ce texte ici.

Objet des compilations de messages :

Utilisez cette option si vous souhaitez personnaliser l'objet utilisé lorsque MDaemon envoie des messages<u>mailing list digest</u> [303]. Par défaut : "\$LISTNAME\$ message digest \$TIMESTAMP\$ \$ISSUE\$" Les macros s'étendent au nom de la liste de diffusion, à l'horodatage de la création du message digest et au numéro de l'édition.

Nombre maxistes de diffusion [xx] (0 = pas limite) (0=pas limite)

Utilisez cette option si vous souhaitez définir un nombre maximum de membres par liste de diffusion. Vous pouvez définir un maximum par domaine dans l'écran Paramètres du Gestionnaire de domaines. Cette option est uniquement disponible dans MDaemon Private Cloud.

Voir :

Gestionnaire liste de diffusion 281

3.4.2 Éditeur de liste de diffusion

3.4.2.1 Membres

Mailing List Manager	Email	Domain	Name
Maining List Wanger Mailing List Settings MyList@company.test MyList@company.test Settings Headers Subscription Reminders Digest Notifications Moderation Routing Support Files Public Folder Active Directory ODBC	Email S frank.thomas@comp I harry.mudd@exampl I michael.mason@co	Domain company.test example.com company.test	Name Frank Thomas Harcourt Fenton Mudd Michael Mason
	<		2
	Add Remove	Toggle digest Toggle re	ad only Toggle post on
	Member count: 3	L	Jp Down Import

Cet écran affiche les adresses e-mail et les noms de tous les membres actuellement inscrits à la liste. L'entrée de chaque membre indique également son "type" d'abonnement : normal, digest, lecture seule ou publication seule. Pour modifier les paramètres d'un membre, double-cliquez sur son nom.

Ajouter

Ce bouton permet de filtrer par l'écran Nouveau membre de la liste pour <u>ajouter de</u> <u>nouveaux membres</u> [289].

Supprimer

Pour supprimer un membre de la liste, sélectionnez son entrée, puis cliquez sur ce bouton.

Afficher le résumé

Sélectionnez un membre, puis cliquez sur ce bouton pour en faire un membre<u>Digest</u> 3031. Cliquez à nouveau sur ce bouton pour revenir au mode "normal".

Basculer en lecture seule

Sélectionnez l'entrée d'un membre, puis cliquez sur ce bouton pour la faire passer en mode "Lecture seule". Le membre recevra toujours des messages de la liste mais ne sera pas autorisé à en envoyer. Cliquez à nouveau sur le bouton pour revenir au mode "normal".

Basculer vers l'affichage uniquement

En cliquant sur ce bouton après avoir sélectionné un membre, celui-ci passe en mode "envoi/réception". Un membre "envoi/réception" peut envoyer des messages à la liste mais n'en reçoit pas. Cliquez à nouveau sur ce bouton pour revenir au mode "normal".

Haut/Bas

Sélectionnez un ou plusieurs membres, puis cliquez sur ces boutons pour les faire monter ou descendre dans la liste. Vous pouvez également trier la liste en cliquant sur l'en-tête de n'importe quelle colonne. **Remarque**: Si vous triez la liste en fonction de l'intitulé d'une colonne, cela annulera tout tri manuel effectué à l'aide des boutons Haut/Bas.

Importer

Cliquez sur ce bouton pour importer les membres de la liste à partir d'un fichier texte dont les champs sont séparés par des virgules (c'est-à-dire un fichier délimité par des virgules). Chaque entrée doit se trouver sur sa propre ligne et tous ses champs doivent être séparés par des virgules. En outre, la première ligne du fichier (la ligne de base) doit contenir les noms des champs et l'ordre dans lequel ils apparaissent dans les autres lignes. L'un des champs doit s'appeler "Adresse électronique" et contenir des adressese-mail. Il existe également deux champs facultatifs : "FullName" et "Type". Votre nom est le nom du membre de la liste.Le type peut avoir une valeur de : "read only", "post only", "digest", ou "normal". Tous les autres champs seront ignorés par l'importateur.

Exemple :

```
"Adresse e-mail", "Nom complet", "Type", "Adresse", "téléphone"
"user01@altn.com", "Michael Mason", "Digest", "123 Street St",
"519.555.0100".
```

Les membres importés ne reçoivent pas le dossier de bienvenue de la liste (s'il y en a un), et l'importateur ne vérifie pas s'il y a des doublons.
Nombre de membres :

Le nombre total de membres actuellement inscrits à la liste est affiché en bas de l'écran.

Ajout de nouveaux membres

No	uveau membr	e de liste	×
	Nouveau mem	bre de liste	
	E-mail		2
	Nom complet		
	Туре	Normal 🔹	
	Utilisez ''CON' champ ''E-mai soient ajoutés	TACTS:domain'' (sans les guillemets) da l''pour que les contacts publics de ce d comme membres de liste.	ns le Iomaine
	Utilisez "CONTACTS: <path>addrbook.mrk" (sans les guillemets) dans le champ "E-mail" pour que les contacts de "addrbook.mrk" soient inclus dans les membres de la liste.</path>		cts de liste.
		ОК	Annuler

Nouveaux membres de la liste

Courriel

Saisissez l'adresse électronique que vous souhaitez ajouter à la liste de diffusion, ou cliquez sur l'icône Compte si vous souhaitez parcourir les comptes MDaemon et groupes MDaemon à ajouter à la liste. Les adresses des membres de la liste ne peuvent pas contenir " ! "ou " | ".



Votre nom complet

Dans ce champ, entrezle nom dumembre. Ce nom apparaîtra dans l'en-tête "To :" des messages de la liste lorsque l'option" Remplacer l'en-tête 'TO:' 'Nom d'affichage' par le nom du membre" est sélectionnée dans l'écran En-têtes.

Type de message

Utilisez la liste déroulante pour choisir le type d'abonnement de l'utilisateur :

- **Normal : le**membre peut envoyer et recevoir des messages de liste normalement.
- **Digest** -Le membre peut envoyer et recevoir des messages de liste, mais les messages reçus seront au format digest.
- **Lecture seule Le**membre recevra des messages de la liste mais ne pourra pas y envoyer de messages.
- **Post only Le**membre de la liste peut envoyer des messages à la liste mais ne les reçoit pas.

3.4.2.2 Paramètres

Mailing List Manager - Settings	
Mailing List Manager Mailing List Settings MyList@company.test MyList@company.test Members Settings Headers Subscription Reminders Digest	Mailing List Settings
Motifications Moderation Routing Support Files Public Folder Active Directory ODBC	 Refuse messages from non list members Refuse messages from members who publish restrictive DMARC policy Hide this list from the global address book Enable EXPN and LIST commands for this list Remove undeliverable email addresses from list membership after this many consecutive permanent failures List refuses messages larger than KB (0 = no limit) Default list member access mode Normal
	Ok Cancel Apply Help

Liste de diffusion Paramètres de liste de diffusion

Activer cette liste de diffusion

Décochez cette case si vous souhaitez désactiver temporairement la liste de diffusion. Tant que la liste est désactivée, tout message arrivant via SMTP à destination ou en provenance de la liste générera une erreur temporaire 451 et sera refusé.

Description privée de la liste (non visible par les membres)

Vous pouvez entrer ici une description privée de la liste. Cette description est destinée à votre propre usage et ne sera pas affichée aux membres ou dans les entêtes.

Dernier accès

Affiche l'heure à laquelle quelqu'un a accédé à cette liste pour la dernière fois. Cela peut vous aider à identifier plus facilement les listes qui sont rarement ou plus utilisées.

Refuser les messages des utilisateurs non membres de la liste

Lorsque cette option est activée, la liste est considérée comme une liste "privée", ce qui signifie que seuls les membres de la liste peuvent y envoyer des messages. Les messages provenant de non-membres seront refusés.

Refuser les messages des domaines appliquant des politiques DMARC restrictives

Activez cette option si vous souhaitez refuser tout message entrant dans la liste envoyé par une personne provenant d'un domaine qui publie des politiques<u>DMARC</u> restrictives (c'est-à-dire p=quarantine ou p=reject). Il n'est généralement pas nécessaire d'activer cette option si vous utilisez l'option "*Remplacer l'adresse électronique 'From:' par l'adresse électronique de la liste si...*" située dans l' écran<u>En-tête</u>

> Si cette option et l'option "<u>Remplacer l'adresse e-mail 'De:' par</u> <u>l'adresse e-mail de la liste si...</u>^[294]" sont toutes deux désactivées, certains messages de la liste seront probablement rejetés par certains serveurs de réception et, dans certains cas, le destinataire <u>sera automatiquement exclu de la liste</u>^[292]. Vous devez donc veiller à ce qu'au moins l'une de ces options soit activée.

Masquer cette liste dans le carnet d'adresses global

Cliquez sur cette option pour masquer la liste de diffusion dans les carnets d'adresses publics du Webmail et de LDAP.

Activer les commandes EXPN et LIST pour cette liste

Dans le but de préserver la confidentialité des membres de la liste, MDaemon n'accepte pas par défaut les commandes EXPN et LIST pour les listes. Si vous activez cette option, l'appartenance à la liste sera signalée en réponse à une commande EXPN ou LISTS lors d'une session de messagerie.

Supprimer automatiquement les adresses e-mail non valides de la liste

Lorsque cette fonctionnalité est activée, MDaemon supprime automatiquement une adresse de la liste des membres lorsqu'il rencontre une erreur fatale permanente lors d'une tentative de distribution. Une adresse est également supprimée lorsque le message est déplacé vers le système de<u>relance</u> active active de ce système.

... après ce nombre de défaillances permanentes consécutives : [xx] Ce paramètre permet de spécifier le nombre d'échecs de distribution permanents consécutifs qui doivent se produire avant que le membre de la liste ne soit supprimé. Non (par défaut), la valeur par défaut est de 3, afin d'éviter que des membres ne soient supprimés après un seul échec.

L'option*Supprimer les adresses électroniques non distribuables…* n'est conçue que pour aider dans les situations où le serveur de courrier distant refuse d'accepter les messages. Elle ne fonctionne que si l'option "*Distribuer le courrier individuellement à chaque membre*" a été sélectionnée dans l'<u>écran de diffusion</u> (306). Si vous acheminez plutôt les messages de liste vers un Hôte relais, reportez-vous à la section <u>Élagage de liste amélioré</u> [202] ci-dessous pour plus d'informations.

Refuser les messages supérieurs à [xx] plus :. Refuser les messages de la liste supérieurs à plus de

Cette commande fixe une limite supérieure à la taille des messages acceptés pour cette Liste de diffusion. Les messages supérieurs à cette limite sont refusés. Refuser les messages supérieurs à :.

Non (par défaut liste) mode d'accès des membres.

Utilisez la liste déroulante pour définir le mode d'accès par défaut à utiliser pour les nouveaux membres. Vous pouvez modifier les paramètres du mode d'accès de n'importe quel membre existant à partir de l'écran<u>Membres.</u> Il existe quatre modes d'adhésion :

- **Normal : le**membre peut envoyer et recevoir des messages de liste normalement.
- **Digest** Le membre peut envoyer et recevoir des messages de liste, mais les messages reçus seront au format digest.
- Lecture seule : lemembre reçoit des messages de la liste mais ne peut pas lui en envoyer.
- **Post only Le**membre de la liste peut envoyer des messages à la liste mais ne les reçoit pas.

Élagage de liste amélioré

Lorsque l'option *Supprimer les adresses e-mail non diffusables des membres de la liste* est activée et que vous avez spécifié une boîte aux lettres locale comme chemin de

retour des messages de la liste (voir l' option *Adresse SMTP de diffusion de la liste* dans <u>Notifications</u> (304)), MDaemon tente chaque jour à minuit d'analyser les adresses email non diffusables des messages renvoyés et de supprimer les membres de la liste qui n'ont pas pu être joints. Cela permet d'élaguer plus efficacement les adresses n'est pas valide des listes de diffusion, en particulier lorsque vous acheminez les messages de la liste vers un Hôte de relais plutôt que de les diffuser directement.

Dans les <u>Options listes diffusion</u> [24], deux options sont associées à cette fonctionnalité. L'option*SUPPRIMERLEESSAGEMESSAGE!supprimeles messages qu'il ne peut pas analyser* entraîne la suppression de tous les messages renvoyés qui ne contiennent pas d'adresse analysable, et l' option*SUPPRIMER LEESSAGE MESSAGE ! supprime les messages qui entraînent* la diffusion d'un membre de la liste.



Configurer <u>l'adresse SMTP 'Bounce' de la liste</u> au sur l'adresse d'un utilisateur local peut entraîner la suppression de l'adresse électronique de cet utilisateur en raison des paramètres d'élagage de la liste indiqués dans les <u>Paramètres de la liste de</u> <u>diffusion</u> 2041.

Dans le cas où l'envoi à une adresse aboutit à une erreur 5xx, l'adresse sera enregistrée dans le fichierBadAddress.txt situé dans le dossier de journalisation. Cela peut vous aider, par exemple, à identifier les mauvaises adresses dans vos listes de diffusion plus rapidement qu'en cherchant dans les journaux SMTP sortants. Ce fichier est automatiquement supprimé à minuit chaque nuit pour éviter qu'il ne devienne trop volumineux.

3.4.2.3 En-têtes

휞 Mailing List Manager - Headers	
Mailing List Manager Mailing List Settings MyList@company.test Mulist@company.test Mulist@company.test Settings Settings Subscription Reminders Digest Notifications Moderation Routing Support Files Public Folder Active Directory ODBC	Header Changes Replace 'To:' header 'Display Name' with Nothing (make no changes) List's name (ex: To: ''Mylist List Member'') Member's name (if known, ex: To: ''Frank Thomas'') Replace 'Reply-To' header email address with Nothing (make no changes) List's email address This email address This email address Replace 'From' with List's name and email address Replace 'From' email address with list's email address if message is sent from a domain that publishes restrictive DMARC policy. When restrictive DMARC is found a 'Display Name' is constructed by appending 'via List' to the 'Display Name' data. Prepend 'Subject.' header text with name of list. Append 'Subject.' header text with thread number.
	Ok Cancel Apply Help

Modification des en-têtes From

Remplacer le nom d'affichage de l'en-tête 'To' par :

Cette option permet de définir le texte à afficher dans l'en-tête TO : lorsque MDaemon reçoit un message destiné à la liste.

Rien (ne pas effectuer de changement) - Lorsque cette option est sélectionnée, MDaemon n'effectue aucun changement. Le Nom d'affichage et l'adresse contenus dans l'en-tête TO : apparaîtront exactement tels que l'expéditeur du message les a saisis.

Nom de la liste- Cette option permet de remplacer le nom affiché par le nom de la liste plus " Membre de la liste ". Exemple : pour une liste de diffusion nommée "Ma famille", le nom affiché dans l'en-tête En-tête From sera "Membre de la liste".

Nom du membre (si connu) - Si cette option est sélectionnée, l'en-tête TO : contiendra le nom (si disponible) et l'adresse du membre de la liste à qui le message est destiné.



L'option*Nom de la* liste ne peut être choisie que lorsque l'option "Distribuer le courrier individuellement à chaque membre" a été sélectionnée dans l'écran de diffusion. Lorsque l'option "*Distribuer le courrier en utilisant les commandes RCPT pour chaque membre*" est sélectionnée, MDaemon choisit par défaut l' *option "Nom de laliste"*.

Remplacer la valeur de l'en-tête 'Reply-To' par :

Cette option permet de désigner l'adresse électronique qui apparaîtra dans l'en-tête Reply-To : de chaque message de la liste.

Rien (ne pas effectuer de changement)

Choisissez cette option si vous souhaitez laisser l'en-tête Reply-To : inchangé par rapport au message original qui sera distribué à la liste. C'est généralement l'option à choisir lorsque vous souhaitez que les réponses soient renvoyées à la personne qui a envoyé le message à la liste, plutôt qu'à tous les membres de la liste.

Adresse e-mail de la liste [Cette adresse e-mail est généralement choisie lorsque vous souhaitez que les réponses soient adressées à la personne qui a posté le message sur la liste plutôt qu'à tous les membres de la liste.

Choisissez cette option si vous souhaitez que les réponses soient adressées à la liste plutôt qu'à une personne ou une adresse spécifique. C'est l'option à choisir si vous souhaitez utiliser la liste comme outil de discussion de groupe, où les réponses sont envoyées à tous les membres.

Cette adresse électronique [...

Si vous souhaitez que les réponses soient envoyées à une adresse électronique spécifique, saisissez-la ici, ou cliquez sur l'icône Compte si vous souhaitez rechercher un compte MDaemon spécifique à utiliser. Vous pouvez utiliser cette option, par exemple, pour une lettre d'information électronique avec une adresse électronique spécifique pour les réponses.

Remplacer 'From:' par le nom et l'adresse e-mail de la liste

Cochez cette case si vous souhaitez remplacer le contenu de l'en-tête "From :" par le nom et l'adresse électronique de la liste de diffusion.

Remplacer l'adresse e-mail 'From:' par celle de la liste si le message est envoyé par un domaine appliquant une politique DMARC restrictive

Par défaut, lorsqu'un message entrant dans la liste est envoyé par un utilisateur d'un domaine qui applique une politique <u>DMARC</u> restrictive (p=quarantine ou p=reject), MDaemon remplace l'adresse électronique de l'utilisateur dans l'en-tête From : par l'adresse de la liste, avant d'envoyer le message à la liste. [Cette mesure est nécessaire pour éviter que le message dela liste ne soit envoyé àun autreutilisateur . Cette opération est nécessaire pour éviter que le message de la liste ne soit rejeté par les serveurs qui appliquent des politiques DMARC restrictives. Outre la modification de l'adresse électronique de l'en-tête From :, le nom affiché sera également modifié pour ajouter "via List Name", afin de montrer qu'il s'agit d'un

message envoyé par cette liste de diffusion au nom de la personne nommée. En outre, chaque fois que l'en-tête From : est modifié par cette fonction, les données de l'en-tête From : d'origine sont déplacées dans l'en-tête Reply-To :, mais uniquement si le message n'a pas d'en-tête Reply-To : au départ et si la liste n'est pas configurée pour afficher un en-tête Reply-To : personnalisé.



Cette action ne sera entreprise que si l' option <u>DMARC</u> <u>Verification</u> cet activée et que le message entrant a fait l'objet d'une vérification.

Vous ne devez pas désactiver cette option si vous n'en comprenez pas toutes les ramifications et si vous n'êtes pas certain de devoir le faire. La désactivation de cette option entraînerait probablement le rejet de certains messages de liste par certains serveurs de réception et, dans certains cas, la <u>radiation automatique du</u> 22 destinataire <u>de la liste</u> 221. Vous pouvez également activer l' option<u>Refuser les messages des</u> <u>domaines des politiques DMARC restrictives</u> 2001, qui permet de refuser les messages entrants dans la liste lorsqu'ils proviennent d'un domaine dont la politique DMARC est restrictive.

Le texte de l'en-tête 'Subject:' est précédé du nom de la liste

Ce paramètre permet à MDaemon de mettre le nom de la liste entre parenthèses (par exemple [Nom de la liste]) et de l'ajouter au début de l'Objet : de tous les messages envoyés à la liste. Cette option est activée par défaut.

Le texte de l'en-tête 'Subject' est suivi d'un numéro de fil de discussion

Ce commutateur vous permet d'activer ou non l'affichage des numéros de fil dans l' en-têtesubject : des messages envoyés à la liste. Ils sont ajoutés à la fin de la ligne de l'objet entre accolades et utilisés comme pseudo-numéro de fil. En triant votre boîte de réception par sujet, les messages de la liste seront classés par ordre chronologique. Cette option est désactivée par défaut.

3.4.2.4 Inscription

😒 Mailing List Manager - Subscription	X
Mailing List Manager Mailing List Settings MyList@company.test Members Settings Headers Subscription Reminders Digest Notifications Moderation Routing Support Files Public Folder Active Directory ODBC	Subscribe / Unsubscription requests Confirm subscription requests Confirm autoresponder generated subscription requests Allow subscription requests from list's domain only Allow subscription requests from local domains only Allow unsubscription requests Confirm unsubscription requests Confirm autoresponder generated unsubscription requests Confirmations must be received within 7200 minutes Notify subscribers/unsubscribers on the status of their requests Membership Limit Limit this list's membership to members (0 = no limit)
	Ok Cancel Apply Help

S'inscrire ou se désinscrire

Autoriser les inscriptions par e-mail

Cette option détermine si la liste autorise ou non les inscriptions par e-mail spécialement formaté ou par autorépondeur. Pour plus d'informations, voir : <u>S'abonner à des listes de diffusion</u> [299].

Confirmer les inscriptions par e-mail

Lorsque cette case est cochée, MDaemon tente de confirmer les demandes d'inscription en générant un code unique et en l'envoyant dans un message à l'adresse de la personne qui demande à s'inscrire à la liste. Si la personne répond à ce message de confirmation, MDaemon l'ajoutera automatiquement à la liste. Les messages de confirmation sont sensibles au temps, ce qui signifie que l'utilisateur doit répondre au message dans le nombre de minutes indiqué cidessous. **Remarque : Le** contenu du message de confirmation se trouve dans le fichierSubConf.dat, situé dans le dossier "MDaemon\app".

Confirmer les demandes de désinscription par e-mail générées par l'autorépondeur

Lorsque cette case est cochée, MDaemon tente de confirmer les requêtes d'inscription générées automatiquement par l'option<u>autorépondeur</u> (777) "Ajouter l'expéditeur à cette liste de diffusion". Comme pour l'option précédente, MDaemon envoie un code unique dans un message à l'adresse qui attend d'être ajoutée à la liste de*diffusion*. Si la personne répond ensuite à ce message de confirmation, MDaemon ajoutera automatiquement le membre à la liste. Ces messages de confirmation sont également sensibles au temps et doivent donc être traités dans le nombre de minutes indiqué ci-dessous.

Autoriser les demandes d'inscription au domaine de la liste uniquement

Choisissez cette option si vous souhaitez autoriser les inscriptions par les demandes d'inscription au domaine de la liste uniquement. Exemple : pour la liste "MyList@example.com", seuls les utilisateurs "@example.com" seraient autorisés à s'abonner à la liste.

Autoriser les demandes d'inscription aux domaines locaux uniquement

Sélectionnez cette option si vous souhaitez autoriser les inscriptions par e-mail uniquement des utilisateurs appartenant à l'un des domaines locaux du serveur MDaemon.

Désabonnement

Autoriser les désinscriptions par e-mail

Cette option permet d'autoriser ou non les demandes de désinscription, soit par le biais de messages électroniques spécialement formatés, soit par le biais d'autorépondeurs. Pour plus d'informations, voir : <u>S'abonner à des listes de</u> <u>diffusion</u> 2001.

Confirmer les demandes de désinscription par e-mail

Lorsque cette case est cochée, MDaemon tente de confirmer les demandes de désinscription d'un membre de la liste, en générant un code unique et en l'envoyant dans un message à l'adresse de la personne demandant à se désinscrire de la liste. Si la personne répond à ce message de confirmation, MDaemon supprimera automatiquement le membre de la liste. Les messages de confirmation sont sensibles au temps, ce qui signifie que l'utilisateur doit répondre au message dans le nombre de minutes indiqué ci-dessous. **Remarque : Le** contenu du message de confirmation se trouve dans le fichierUnSubConf.dat, situé dans le dossier "MDaemon\app".

Confirmer les demandes de désinscription par e-mail générées par l'autorépondeur Lorsque cette case est cochée, MDaemon tente de confirmer les requêtes de

désinscription générées automatiquement via l'option du<u>répondeur</u> <u>automatique</u> "" Supprimer l'expéditeur de cette liste de diffusion". Comme pour l'option*Confirmer les requêtes de désinscription* par e-mail ci-dessus, MDaemon exécute un code unique dans un message envoyé à l'adresse qui attend d'être supprimée de la diffusion. Si la personne répond ensuite à ce message de confirmation, MDaemon supprimera automatiquement le membre. Ces messages de confirmation sont également sensibles au temps et doivent donc recevoir une réponse dans le nombre de minutes indiqué ci-dessous.

Délai d'expiration des confirmations [xx] minutes

Il s'agit du nombre de minutes dont dispose le destinataire d'un message de confirmation d'abonnement ou de désabonnement avant que le message n'expire. Si ce délai est dépassé avant que MDaemon ne reçoive une réponse au message, l'adresse ne sera ni ajoutée ni supprimée de la liste. L'adresse devra alors soumettre une nouvelle demande pour rejoindre ou quitter la liste. Le paramètre par défaut de cette option est de 7200 minutes (soit cinq jours).

Il s'agit d'unevaleurglobale quis'applique à toutes vos listes de diffusion et non à la liste spécifique que vous modifiez.

Notifier les inscrits/non-inscrits du statut de leur requête

Lorsque cette case est activée, MDaemon envoie un message de notification d'achèvement à l'utilisateur qui a été abonné/désabonné à cette Liste de diffusion.0



Le contenu d'un fichier appelé UnSubUser.dat (s'il existe) sera ajouté à l'e-mail envoyé aux utilisateurs lorsqu'ils se désabonnent des listes.

Nombre maximal de membres

Limiter le nombre d'inscrits sur cette liste à [xx] membres (0=pas de limite). Cette fonction vous permet de fixer une limite supérieure au nombre de personnes autorisées à s'inscrire à la Liste d'autorisation. Entrez un zéro dans ce champ À : si vous ne souhaitez pas limiter les abonnements à la liste.

> Cette limite ne s'applique qu'aux adresses électroniques souscrites par le biais des méthodes décrites dans la section <u>S'abonner à des listes de diffusion</u> s'applique pas aux abonnements saisis manuellement dans l' écran <u>Membres</u> mot de passe de la liste set inclus.

Voir :

<u>S'abonner à des listes de diffusion</u> व्यमे <u>Répondeur automatique</u> गारी

3.4.2.4.1 Inscription aux listes de diffusion

S'inscrire ou se désinscrire par commande de courrier électronique

Pour s'abonner ou se désabonner d'une liste de diffusion, envoyez un message électronique adressé à MDaemon (ou à l'un de ses alias) dans le domaine hébergeant la liste de diffusion, et placez la commande S'abonner ou Se désinscrire sur la première ligne du corps du message. Exemple : une liste de diffusion appelée MD-Support est hébergée sur le domaine mdaemon.com. Vous pouvez vous abonner à la liste en composant un message adressé à"mdaemon@mdaemon.com" et en plaçant la valeur :SUBSCRIBE MD-Support@mdaemon.com comme première ligne du corps du message. L'objet du message n'a pas d'importance et peut être laissé en blanc.

Pour plus de détails sur la manière de former ce message et d'autres messages de contrôle, voir : <u>Contrôle de serveurs distants par courrier électronique</u>

Il arrive que des utilisateurs tentent de s'inscrire ou de se désinscrire de listes par e-mail en envoyant les commandes à la liste elle-même plutôt qu'au Compte système de MDaemon. Dans ce cas, la commande est envoyée à la liste et l'utilisateur n'est pas inscrit ou désinscrit. Pour éviter que ce type de message ne soit envoyé aux listes de diffusion, il existe une option située dans <u>Configuration | Préférences | Système</u>, [525] appelée "*Filtrer les messages entrants aux listes de diffusion pour le contenu inapproprié à la liste*". Cette option est activée par défaut.

S'inscrire ou se désinscrire par le biais d'adresses électroniques

L'option "Honor '<List>-subscribe' et '<List>-unsubscribe' addresses", située dans <u>Setup</u> <u>J Gestionnaire de listes de diffusion | Paramètres de liste de diffusion</u>²²⁴, permet aux utilisateurs de s'inscrire ou de se désinscrire des listes de diffusion en envoyant un message à une adresse électronique spéciale au lieu d'utiliser les commandes de courrier électronique décrites plus haut dans Listes*inscrites ou désinscrites*. Pour utiliser cette méthode, il suffit d'envoyer un message à l'adresse de la liste, mais en ajoutant "-subscribe" ou "-unsubscribe" à la partie "boîte aux lettres" de l'adresse. Par exemple, si le nom de la liste est"franks-list@example.com", un utilisateur peut s'abonner à la liste en envoyant un message à"franks-list-subscribe@example.com". Pour se désabonner de la liste, le message doit être envoyé à "franks-listunsubscribe@example.com". Dansles deux cas, le contenu de l'objet et du corps du message n'a pas d'importance. De plus, lorsque cette fonctionnalité est activée, MDaemon insère l'en-tête suivant dans tous les messages de la liste :

List-Unsubscribe : <mailto:<List>-Unsubscribe@example.com>

Certains clients de messagerie peuvent s'en rendre compte et mettre automatiquement un bouton UNSUBSCRIBE à la disposition des utilisateurs.

S'inscrire ou se désinscrire par l'intermédiaire d'un autorépondeur

Vous pouvez également utiliser des répondeurs mil automatiques pour ajouter ou supprimer automatiquement des membres de la liste. Pour ce faire, vous devez créer un ou plusieurs comptes MDaemon dont le seul but est d'ajouter ou de supprimer automatiquement les adresses qui envoient des messages à ces comptes, via les répondeurs automatiques configurés pour chaque compte. Exemple : si vous avez une liste de diffusion appelée"franks-list@example.com", vous pouvez créer un compte MDaemon avec l'adresse :"join-franks-list@example.com". Vous pouvez alors

configurer un autorépondeur pour ce compte afin d'ajouter à "franks-list@example.com" toutes les adresses qui lui envoient des messages.. then, to join that list, all someone would have to send an email to "join-franks-list@example.com". Cette solution est simple pour les utilisateurs, car elle ne leur demande pas de se souvenir des commandes de courrier électronique spéciales requises par la méthode "*Se souvenir de moi ou se désinscrire par courrier électronique*" décrite ci-dessus.

Voir :

Abonnement 207 Contrôle d'un serveur distant par courrier électronique 968 Répondeur automatique 9777 Préférences - Système 625 Préférences - Divers 635

3.4.2.5 Rappels

🧐 Gestionnaire de listes de diffusion - Rappels	s
Gestionnaire de listes de diffusion	Rappels d'inscription
- Paramètres de liste de diffusion	Envoyer des rappels d'inscription mensuels à tous les membres de la liste
MyList@company.test MyList@company.test MyList@company.test Paramètres En-têtes Inscription Compilation Notifications Modération Routage Fichiers de support Dossier public Active Directory ODBC	Les rappels sont envoyés en texte/HTML, vous pouvez donc utiliser du code HTML. Certaines variables sont également disponibles (voir Aide) : Ce message vous est envoyé une fois par mois pour vous rappeler votre inscription à la liste de diffusion >\$LISTADDRESS\$ /p> Pour vous désinscrire de cette liste, envoyez un e-mail à l'adresse \$UNSUBADDRESS (p) Ceci est un message automatique. Veuillez ne pas répondre.
	OK Annuler Appliquer Aide

Rappels d'inscription

Envoyer des rappels d'inscription mensuels à tous les membres de la liste

Activez cette option si vous souhaitez envoyer le contenu de la zone de texte fournie comme message de rappel d'abonnement à chaque membre de la liste le premier jour de chaque mois. Ce texte est envoyé au format text/html, ce qui vous permet de rédiger en HTML le texte du rappel si vous le souhaitez. Les macros suivantes sont disponibles pour être utilisées dans le message de rappel :

- \$LISTADDRESS\$ se développe en adresse électronique de la liste de diffusion (par exemple, MyList@example.com).
- \$LISTNAME\$ se développe en partie locale de l'adresse e-mail de la liste de diffusion (par exemple, MyList).
- \$UNSUBADDRESS\$ développe l'adresse de désabonnement de la liste (l'adresse du système MDaemon, par exemple mdaemon@example.com).
- \$MEMBERADDRESS\$ développe l'adresse électronique du membre de la liste qui reçoit le rappel (par exemple frank.thomas@example.com).

Si vous souhaitez envoyer des rappels un autre jour du mois, vous pouvez le faire en définissant la clé suivante dans le fichier MDaemon.ini :

```
[Spécial]
ListReminderDay=X
```

Attribuez à "X" une valeur comprise entre 1 et 28, représentant le jour du mois où vous souhaitez envoyer les rappels.

3.4.2.6 Compilation

🧐 Gestionnaire de listes de diffusion - Compil	lation 💌
Gestionnaire de listes de diffusion Paramètres de liste de diffusion MyList@company.test MyList@company.test Paramètres Paramètres En-têtes Inscription Rappels Compilation Notifications Modération Routage Fichiers de support Dossier public Active Directory ODBC	Compilation Activer la compilation des messages pour la liste de diffusion Forcer tous les membres de la liste à utiliser le mode compilation Envoi de compilations de messages Envoyer une compilation de messages à 9 12 3 6 AM PM Envoyer une compilation au bout de messages accumulés (0=N/A)
	OK Annuler Appliquer Aide

Compilation

Activer la compilation des messages pour cette liste de diffusion

Cochez cette case si vous souhaitez autoriser la prise en charge de la numérisation pour cette liste de diffusion. Lorsque la prise en charge du mode digest est activée, une copie de chaque message envoyé à la liste de diffusion est archivée, de sorte que les membres de la liste dont le <u>type d'adhésion</u> at défini sur *Digest* reçoivent périodiquement des lots de ces messages archivés dans un format compact et indexé, au lieu de les recevoir un par un.

Forcer tous les utilisateurs de la liste à utiliser le mode compilation

Non (par défaut), les membres de la liste peuvent décider s'ils souhaitent recevoir le trafic de la liste au format "digest" ou au format normal. Cochez cette case si vous souhaitez obliger tous les membres à utiliser le mode condensé, quel que soit le mode qu'ils ont eux-mêmes choisi.

Quand envoyer des résumés ?

Les options suivantes déterminent la fréquence et les circonstances de l'envoi des compilations aux membres de la liste qui sont configurés pour recevoir le courrier au format compilations. Toutes les options sont indépendantes les unes des autres, ce

qui signifie que n'importe laquelle d'entre elles ou toutes peuvent entraîner l'envoi d'un condensé.

Envoyer une compilation de messages à 9 AM, 12 AM, 3 AM, 6 PM

Cette option permet de programmer la fréquence d'envoi des résumés de cette liste. Si vous cochez toutes les cases de cette option, des analyses seront envoyées toutes les trois heures, en plus de celles qui peuvent être déclenchées par les options ci-dessous.

Envoyer la compilation au bout de [xx] messages accumulés (0 = N/A)

Si vous souhaitez envoyer automatiquement des résumés dès qu'un certain nombre de messages accumulés se sont accumulés, indiquez ce nombre ici. Utilisez "0" si vous ne souhaitez pas utiliser cette option. "0" est le paramètre par défaut.

Voir :

<u>Membres</u> 287 <u>Serveur distant via email</u> 958ी

3.4.2.7 Notifications

🧐 Gestionnaire de listes de diffusion - Notific	ations	×
Gestionnaire de listes de diffusion Paramètres de liste de diffusion MyList@company.test Paramètres Paramètres En-têtes Inscription Rappels Compilation Notifications Modération Routage Fichiers de support Dossier public Active Directory ODBC	Notifications Notifier Image: Sinscrit à la liste de diffusion Image:	
	OK Annuler Appliquer Aid	e

Notifications

Notification

Utilisez cette option pour indiquer une adresse qui sera notifiée lorsque les événements sélectionnés auront lieu.

...lorsqu'un utilisateur s'inscrit à la liste de diffusion

Cochez cette case si vous souhaitez envoyer une note à l'adresse désignée chaque fois qu'une personne s'abonne à la liste de diffusion.

...lorsqu'un utilisateur se désinscrit de cette liste de diffusion

Cochez cette case si vous souhaitez envoyer une note à l'adresse désignée chaque fois qu'un utilisateur se désabonne de la liste de diffusion.

...lorsqu'un message entrant dépasse la taille autorisée

Cochez cette case si vous souhaitez envoyer une note à l'adresse désignée chaque fois que quelqu'un envoie à la liste de diffusion un message dont la taille est supérieure à la limite *Refuse les messages supérieurs à [xx] KB* désignée dans les <u>Paramètres</u>²⁰⁰.

Notifier les non inscrits du rejet de leurs messages

Lorsque cette option est activée et que des non-membres d'une liste privée envoient un message à la liste, MDaemon les informe que la liste est privée. Ils recevront également des instructions sur la manière de s'abonner à la liste. Les listes sont désignées comme privées en utilisant l' option *Seuls les membres de la liste peuvent envoyer des messages à cette liste* située dans <u>Paramètres</u> 2001.

Courrier retourné

Adresse SMTP 'Bounce' de la liste

Cette option permet de spécifier l'adresse à laquelle doivent être envoyés les messages de notification d'état générés par le trafic de la liste. Un message envoyé à une Liste de diffusion de 100 destinataires peut avoir, par Exemple, dix adresses non distribuables en raison de changements d'adresse, de serveurs en panne, etc. Le système SMTP génère et renvoie à l'expéditeur du message un message de notification concernant ces conditions de non distribution. Cette option vous permet de désigner l'adresse qui doit recevoir ces messages pour vos listes de diffusion. Vous pouvez également choisir que personne ne les reçoive, auquel cas MDaemon placera le courrier de la liste dans le flux de courrier de telle sorte qu'il ne sera pas possible de le renvoyer. Cette adresse ne doit PAS être l'adresse de la liste de diffusion.

> Configurer *l'adresse SMTP 'Bounce' de la liste à l* 'adresse d'un utilisateur local pourrait entraîner la suppression de l'adresse email de cet utilisateur en raison des paramètres d'élagage de la liste indiqués dans les <u>Paramètres de la</u> ²²⁴ liste <u>de diffusion</u>. ²²⁴ . Soyez prudent avant de configurer cette option sur l'adresse d'un utilisateur local. Pour plus d'informations, voir <u>Élagage de</u> <u>liste amélioré</u> ²²².

3.4.2.8 Modération

🧐 Gestionnaire de listes de diffusion - Modéra	ation	×
 Gestionnaire de listes de diffusion Paramètres de liste de diffusion MyList@company.test Membres Paramètres En-têtes Inscription Rappels Compilation Notifications Modération 	Modération Cette liste est modérée par Tous les messages envoyés à la liste seront transférés à ce modérateur. Mot de passe Quiconque connaît le mot de passe peut poster un message URL de la liste de diffusion (voir RFC 2369)	
Routage Fichiers de support Dossier public Active Directory ODBC	Aide Inscriptions Désinscriptions Inscriptions Propriétaire Inscription Archivage Inscription Description Inscription Pour connaître la syntaxe correcte de ces URL, consultez la RFC 2369. Le texte saisi dans "Description" (facultatif) sera ajouté à l'en-tête List-ID.	
	OK Annuler Appliquer A	ide

Modération

Cette liste est modérée par

Cochez cette case et indiquez un compte si vous souhaitez que la liste soit modérée par l'utilisateur désigné. souhaitez que cette liste soit modérée par l'utilisateur désigné. Cette liste est modérée par le modérateur. Seul le modérateur peut soumettre ou transférer des messages à la liste.

Mot passe de liste

Si vous souhaitez attribuer un mot de passe à cette liste, saisissez-le ici. Les mots de passe de liste peuvent être utilisés avec l'option *Tout le monde peut poster qui connaît le mot de passe de la liste* ci-dessous, et pour remplacer l'option *Nombre maximal de membres* sur la liste d'inscription 2007. Ils donnent également accès à un certain nombre de fonctions décrites dans la section *Contrôle du serveur distant par courrier électronique*.

Quiconque connaît le mot de passe peut poster un message

Si un mot de passe est attribué à la liste et que cette option est activée, toute personne qui indique le mot de passe de la liste au début de l'objet d'un message peut envoyer un message à la liste, même si la liste est modérée mais que l'expéditeur n'est pas le modérateur.

URL de liste de diffusion (Voir RFC 2369)

MDaemon peut ajouter aux messages de listes de diffusion l'un des six champs d'entête décrits dans la RFC 2369 : *The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message En-tête FieldsRFC*. Les six entêtes sont les suivants : List-Help, List-Subscribe, List-Unsubscribe, List-Post, List-Owner et List-Archive. Si vous souhaitez utiliser l'un de ces en-têtes pour les messages de la liste, saisissez la valeur d'en-tête souhaitée dans l'un des champs À :. Les valeurs d'en-tête doivent être formatées conformément à la spécification RFC 2369 (par exemple, <mailto:list@example.com?subject=help>). En-tête From : Les valeurs d'en-tête doivent être formatées conformément à la spécification RFC 2369 (par exemple, <>). Voir le document lié pour plusieurs exemples de chaque entête. MDaemon ne modifie pas ces données, donc si elles sont mal formées, il n'obtiendra aucun résultat.

Description (utilisée dans l'en-tête List-ID : FROM)

Entrez ici une courte description de votre liste de diffusion si vous souhaitez l'ajouter à l'en-tête List-ID : inclus dans les messages envoyés à la liste. La description et l'identifiant de la liste seront inclus dans l'en-tête (Exemple : List-ID : "Frank's personal mailing list" <MyList.example.com>). Dans ce cas, l'identifiant de la liste est l'adresse de la liste de diffusion avec "." à la place de "@" afin de respecter la <u>spécification List-IDLink</u>. Si vous laissez l'option *Description* vide, l'en-tête List-ID : ne contiendra que l'identifiant de la liste (par exemple List-ID : <MyList.example.com>). Si un message entrant adressé à la liste comporte un entête List-ID : préexistant, MDaemon remplacera l'ancien en-tête par celui correspondant à la liste.

> Les en-têtes List-Subscribe et List-Unsubscribe sont inclus par défaut dans tous les messages de liste de diffusion lorsque l'option"Honor '<List>-subscribe' et '<List>-unsubscribe' addresses"*est activée dans l'écran Préférences* | *Divers ".* Si vous souhaitez passer outre cette option pour cette liste, en utilisant des valeurs d'en-tête différentes de celles ajoutées automatiquement par cette option, saisissez les valeurs souhaitées ici. Si cette option est désactivée, aucune Valeur d'En-tête S'inscrire ou vous désinscrire ne sera ajoutée aux messages de la liste, à moins que vous n'en indiquiez la valeur ici.

3.4.2.9 Routage

휞 Mailing List Manager - Routing	
Mailing List Manager Mailing List Settings MyList@company.test MyList@company.test Members Settings Headers Subscription Reminders Digest Notifications Moderation Routing Support Files Public Folder Active Directory ODBC	Routing Deliver list mail to each member individually Replace Message-ID with unique value for each member Replace macros found within message body but only when the sender provides the list's password Macro legend: \$LISTNAME\$ - name of mailing list \$SENDER\$ - sender's email address \$FULLNAME\$, \$FIRSTNAME\$, \$LASTNAME\$ - list member's name \$EMAIL\$ - list member's email address O Deliver list mail using individual RCPT commands for each member Deliver to this host AUTH Logon AUTH Password Limit RCPTs to per message (0 = no limit) Ignore RCPT errors when sending to host
	Ok Cancel Apply Help

Routage

Distribuer le courrier individuellement à chaque membre

Si cette option est sélectionnée, lorsque des messages sont reçus pour être distribués à la liste, une copie distincte de chaque message sera créée et envoyée à chaque membre de la liste. Dans ce cas, de nombreux messages individuels sont créés, ce qui peut affecter les performances du serveur, en fonction de la taille de la liste et de la charge du serveur. Cette option est sélectionnée par défaut.

Générer une valeur Message-ID unique pour chaque membre

Si MDaemon est configuré pour générer une copie séparée de chaque message pour chaque membre, cochez cette case si vous souhaitez que chacun de ces messages ait un Message-ID unique. Cette option est désactivée par défaut et n'est pas recommandée, sauf si des circonstances particulières l'exigent.

Remplacer les macros identifiées dans le corps du message

Activer cette option si vous souhaitez autoriser l'utilisation de macros spéciales dans les messages de cette liste diffusion. Lorsqu'une macro est trouvée, MDaemon la remplacera par la valeur correspondante que la macro représente, pour chaque message distinct avant de l'envoyer à chaque membre de la liste.

...mais uniquement si l'expéditeur fournit le mot de passe de la liste

Si vous autorisez les macros dans le corps du message, cliquez sur cette option si vous souhaitez demander <u>le mot de passe de la liste</u> pour que quelqu'un puisse utiliser des macros dans son message. Lorsque cette option est désactivée, toute personne pouvant envoyer un message à la liste pourra utiliser des macros.

Macros:

NOM DE LA LISTE	Le nom de la liste ou la partie "boîte aux lettres" de l'adresse de la liste (par exemple, "Ma liste" de MyList@example.com).
\$LISTD OMAIN \$	Le domaine de la liste (par exemple, "Exemple.com" de MyList@example.com).
\$SEND ER\$ (EXPÉ DITEU R)	L'adresse e-mail de l'expéditeur du message.
\$FULL NAME\$ \$FIRST NAME\$ (NOM DE FAMILL E) NOM DE FAMILL E	Le Nom complet du membre de la liste, son Prénom et son Nom, respectivement (si disponible).
\$EMAI L\$	L'adresse e-mail du membre de la liste.

Distribuer le courrier en utilisant une commande RCPT pour chaque membre

Si cette option est sélectionnée, MDaemon routera une seule copie de chaque message de liste vers l'hôte intelligent spécifié, plutôt que d'envoyer des messages individuels à chaque membre. Cette méthode utilise plusieurs commandesRCPT To au cours de la session SMTP avec l'hôte spécifié.

Distribuer à cet hôte

Désignez l'hôte intelligent auquel vous souhaitez transmettre tous les messages de la liste, en utilisant des instructions RCPT To pour chaque membre.

Mot de passe AUTH

Tout identifiant de connexion requis par l'hôte.

Limiter les commandes RCPT à [xx] par message (0=pas de limite)

Certains hôtes limitent le nombre d' instructions RCPT To qu'ils acceptent lorsque vous tentez d'acheminer une seule copie d'un message par leur intermédiaire. Si vous indiquez une limite dans cette commande, MDaemon la contournera en créant des copies supplémentaires du message et en divisant la liste en groupes plus petits. Il distribuera alors le message à ces groupes, évitant ainsi de dépasser la limite. Cette méthode est similaire à l' option*Distribuer le courrier individuellement à chaque membre* ci-dessus, mais elle génère moins de copies, envoyant chaque copie à des groupes d'adresses plutôt que de générer une copie distincte pour chaque membre.

Ignorer les erreurs RCPT lors de l'envoi à cet hôte

Étant donné que certains serveurs intelligents refusent de mettre en file d'attente ou de spooler le courrier pour certains domaines, l'approche routée de la diffusion de listes pourrait causer de nombreux problèmes. Un code d'erreur renvoyé par l'hôte intelligent à la suite de ce refus entraînerait normalement l'abandon de la tentative de distribution par MDaemon. Cochez cette option si vous souhaitez que MDaemon ignore les codes d'erreur renvoyés par l'hôte intelligent lors de la distribution du courrier de la liste routée, afin que les membres acceptés aient une chance de recevoir le message.

3.4.2.10 Fichiers de support

🧐 Gestionnaire de listes de diffusion - Fichiers d	e support	×
 □- Gestionnaire de listes de diffusion □- Paramètres de liste de diffusion □- MyList@company.test □- Membres □- Paramètres □- En-têtes □- Inscription 	Fichiers de Support Message de bienvenue Ce fichier est envoyé à chaque nouveau membre inscrit manuellement ou par e-mail. Liste noire	
Rappels Compilation Notifications Modération Routage <mark>Fichiers de support</mark> Dossier public Active Directory ODBC	Parcourir Ce fichier contient les adresses des utilisateurs n'étant pas autorisés à poster dans cette liste. En-tête Parcourir Créer Pied de page Parcourir Créer	

Fichiers de support

Fichier de bienvenue

Si vous le spécifiez, le fichier indiqué ici sera traité et son contenu sera envoyé par e-mail à tous les nouveaux membres juste après leur inscription. Vous pouvez utiliser les macros suivantes dans un fichier de bienvenue destiné aux nouveaux membres :

\$PRIMARYDOMAI N\$	Cette macro prend la forme du Domaine par défaut de MDaemon, qui est indiqué dans le <u>Gestionnaire de domaines</u> [184].
<pre>\$PRIMARYIP\$ CETTE MACRO RENVOIE LE NOM DU DOMAINE PAR DÉFAUT DE MDAEMON, QUI EST DÉSIGNÉ DANS LE</pre>	Cette macro renvoie l'adresse IPv4 associée au Domaine par défaut - Domaine Domaine.

GESTIONNAIRE DE DOMAINE.	
\$PRIMARYIP6\$ CETTE MACRO RETOURNE L'ADRESSE IPV6 ASSOCIÉE AU DOMAINE PAR DÉFAUT DE MDAEMON.	Cette macro renvoie l'adresse IPv6 associée au Domaine par défaut de MDaemon.
\$DOMAINIP\$ CETTE MACRO RENVOIE L'ADRESSE IPV4 ASSOCIÉE AU DOMAINE PAR DÉFAUT DE MDAEMON.	Cette macro renvoie l'adresse IPv4 associée au domaine.
DOMAINEIP6\$ CETTE MACRO RENVOIE L'ADRESSE IPV6 ASSOCIÉE AU DOMAINE PAR DÉFAUT DE MDAEMON.	Cette macro renvoie l'adresse IPv6 associée au domaine.
\$MACHINENAME\$ (NOM DE LA MACHINE)	Cette macro renvoie le contenu de l'option FQDN désignée dans l'écran Domaine.
\$LISTEMAIL\$ CETTE MACRO RENVOIE LE CONTENU DE L'OPTION FQDN DÉSIGNÉE DANS L'ÉCRAN DOMAINE.	Affiche l'adresse e-mail de la liste. Exemple : MyList@example.com
\$LISTNAME\$\$ AFFICHE LE NOM DE LA LISTE DE DIFFUSION.	Affiche le nom de la liste de diffusion. Exemple : ${\tt MyList}$

\$LISTDOMAIN\$\$	Cette macro renvoie le domaine de la liste de diffusion.
(DOMAINE DE	Exemple : example.com
LA LISTE DE	
DIFFUSION)	
%SETSUBJECT%%	Cette macro permet de désigner un autre Sujet du message
(OBJET)	bienvenue. Ce texte peut inclure d'autres macros de liste telles
	que \$LISTEMAIL\$. Exemple : %SetSubject%=Bienvenue à la
	liste \$LISTNAME\$.

Liste Fichier de blocage

Si cette option est spécifiée, le fichier indiqué ici sera utilisé pour supprimer les messages envoyés par les utilisateurs spécifiés.

Fichier d'en-tête From: : Fichier du pied de page

Le contenu des fichiers spécifiés ici sera utilisé comme Fichier d'en-tête et/ou de pied de page pour les messages de la liste.

Créer un fichier

Pour créer un nouveau fichier, cliquez sur le bouton *Créer* correspondant au fichier que vous souhaitez créer, indiquez un nom, puis cliquez sur *Ouvrir*. Dans ce cas, le fichier nouvellement créé s'ouvre dans le Bloc-notes pour que vous puissiez le modifier.

3.4.2.11 Dossier public

🧐 Gestionnaire de listes de diffusion - Dossier p	ublic 💌
Gestionnaire de listes de diffusion Paramètres de liste de diffusion MyList@company.test Membres Paramètres En-têtes Inscription Rappels Compilation Notifications Modération Routage Fichiers de support Obscier public Active Directory ODBC	Copier les messages de liste dans un dossier public
	OK Annuler Appliquer Aide

MDaemon permet d'utiliser les <u>Dossiers publics IMAP</u> [116] avec les listes de diffusion. Contrairement aux dossiers IMAP personnels, qui ne sont généralement accessibles que par un seul utilisateur, les Dossiers publics sont des dossiers supplémentaires accessibles à plusieurs utilisateurs IMAP. Les options de cet écran permettent de faire en sorte que tous les messages destinés à la Liste de diffusion soient automatiquement copiés dans un de vos Dossiers publics.

Copier les messages de liste dans un dossier public

Activez cette commande si vous souhaitez que les messages decette listesoient copiés dans l'un de vos Dossiers publics en plus d'être livrés à la liste.

Sélectionnez un dossier public

Cliquez sur le Dossier public que vous souhaitez associer aux messages decette liste.

3.4.2.12 Active Directory

8 Mailing List Manager - Active Directory	
Mailing List Manager Mailing List Settings	Active Directory Authentication & Search User name or Bind DN
MyList@company.test Members Settings Headers	Password Use secure authentication
Subscription Reminders Digest Notifications	Base entry DN Search filter
Moderation Routing Support Files Public Folder Active Directory ODBC	(&(objectClass=user)(objectCategory=person)) Contact search filter
	Search scope: displayName, mail AD attributes Base DN only mail 1 level below base DN Verbose AD logging
	Ok Cancel Apply Help

Utilisez les options de cet écran si vous souhaitez extraire certaines adresses de membres de la liste à partir d'Active Directory.

Authentification & Recherche Active Directory

Nom d'utilisateur ou DN de liaison

Il s'agit de l'identifiant de connexion du compte Windows ou du DN que MDaemon utilisera pour se lier à Active Directory à l'aide de LDAP. Active Directory autorise l'utilisation d'un compte Windows ou d'un UPN lors de la liaison.



Dans le cas où vous utilisez un DN dans cette option plutôt qu'un logon Windows, vous devez désactiver/effacer l'option*"Utiliser l'authentification sécurisée*" ci-dessous.

Mot de passe

Il s'agit du mot de passe correspondant au DN ou à l'identifiant Windows utilisé dans l' option*DN de liaison* ci-dessus.

Utiliser l'authentification sécurisée

Cochez cette case si vous souhaitez utiliser une authentification sécurisée lors de vos recherches dans Active Directory. Vous ne pouvez pas utiliser cette option si vous utilisez un DN plutôt qu'une connexion Windows dans l' option*DN de liaison* cidessus.

Utiliser l'authentification SSL

Cochez cette case si vous souhaitez utiliser l'authentification SSL lors de vos recherches dans Active Directory.

L'utilisation de cette option nécessite un serveur SSL et une infrastructure sur votre réseau Windows et Active Directory. Contactez votre service informatique si vous n'êtes pas certain que votre réseau est configuré de cette manière, et pour savoir si vous devez activer cette option.

Entrée base DN

Indiquez le Nom Distingué (DN) ou le point de départ dans l'Arbre d'Informations du Répertoire (DIT) à partir duquel MDaemon cherchera des adresses dans Active Directory. Vous pouvez utiliser "LDAP://rootDSE" dans cette option pour commencer à chercher au DSE racine, qui est l'entrée la plus haute dans votre hiérarchie Active Directory. En désignant un point de départ plus précis et plus proche de l'emplacement de vos comptes utilisateurs ou du groupe d'adresses souhaité dans votre arborescence Active Directory, vous pouvez réduire le temps nécessaire pour chercher dans le DIT. Laissez ce champ À : si vous ne souhaitez pas extraire d'adresses de liste d'Active Directory.

Filtre de recherche

Il s'agit du filtre de recherche LDAP qui sera utilisé pour chercher dans Active Directory. Ce filtre permet à MDaemon de localiser plus précisément les comptes utilisateurs ou les adresses que vous souhaitez traiter comme membres de la liste.

Test

Utilisez ce bouton pour tester les paramètres de votre filtre de recherche.

displayName, mail AD attributes

Vous devez utiliser ce champ pour spécifier l'attribut qui contiendra les adresses électroniques utilisées par cette liste. Par exemple, si vous avez utilisé "À" dans ce champ, chaque compte Active Directory que vous souhaitez traiter comme membre de la liste doit avoir l'attribut "À", et cet attribut doit contenir une adresseélectronique. Vous pouvez également saisir un attribut Active Directory pour le champ du nom complet des membres de la liste avant l'attribut de l'adresse électronique, en le séparant par une virgule. Exemple : vous pouvez saisir : "displayName, mail" au lieu de "mail" dans cette option. Le premier est l'attribut Active Directory où réside le nom complet, et le second est l'attribut de l'adresse électronique.

Étendue de la recherche :

Il s'agit de la portée ou de l'étendue de vos recherches dans Active Directory.

DN de base uniquement

Cherchez cette option si vous souhaitez limiter votre recherche au seul DN de base spécifié ci-dessus. La recherche ne sera pas effectuée en dessous de ce point de l'arborescence (DIT).

1 niveau inférieur au DN de base

Utilisez cette option si vous souhaitez étendre votre recherche Active Directory à un niveau inférieur au DN fourni dans votre DIT.

DN de base et tous les enfants

Cette option permet d'étendre la portée de votre recherche du DN fourni à tous ses enfants, jusqu'à l'entrée enfant la plus basse de votre DIT.

Pas de journalisation AD verbeuse

Non (par défaut) MDaemon utilise la Pas de journalisation par défaut pour Active Directory. Décochez cette case si vous souhaitez utiliser une Pas de journalisation Active Directory moins poussée.

3.4.2.13 ODBC

🧐 Gestionnaire de listes de diffusion - ODBC		
Gestionnaire de listes de diffusion Paramètres de liste de diffusion MyList@company.test - Membres - Paramètres - Paramètres - En-têtes - Inscription - Rappels - Compilation - Notifications - Modération - Routage - Fichiers de support - Dossier public - Active Directory	ODBC Connecter à une nouvelle source ODBC	Déconnecter de la source ODBC
	ОК	Annuler Appliquer Aide

Dans cette fonctionnalité, vous pouvez maintenir la liste des membres de la liste dans une base de données compatible ODBC. L'écran ODBC de l'éditeur de listes de diffusion permet de sélectionner une source de données, une table et des champs pour que MDaemon les relie à la liste. Lorsque des messages arrivent sur votre liste, une ou plusieurs requêtes SQL sont effectuées automatiquement et les adresses électroniques résultantes sont traitées comme faisant partie des membres de laliste.

Vous pouvez ajouter, supprimer et modifier les membres de votre liste dans la base de données en utilisant l'application de base de données ODBC de votre choix.

ODBC

Cette section affiche les propriétés ODBC actuelles que vous avez définies pour la liste de diffusion. Elle affiche les correspondances entre les champs de labase de donnéeset les requêtes SQL que vous avez configurées pour désigner lestatut d'appartenance dechaque membre(c.-à-d. Normal, Publier seulement, Lecture seulement et/ou mode Digest).

Connexion à une nouvelle source ODBC

Cliquez sur ce bouton pour ouvrir l'assistant de sélection ODBC afin de choisir la source de données système que vous souhaitez utiliser pour la liste de diffusion.

Déconnecter de la source ODBC

Cliquez sur ce bouton pour déconnecter la liste de la source de données ODBC indiquée dans l'espace ci-dessus.

Voir :

Configuration d'une source de données système ODBC pour une liste de diffusion <u>Création d'une nouvelle source de données système</u>

3.4.2.13.1 Configuration d'une source de données ODBC

Pour utiliser une base de données accessible par ODBC avec une liste de diffusion :

1. Sur l'<u>écran ODBC</u> at l'éditeur de Liste de diffusion, cliquez sur **Connecter à une nouvelle source ODBC** pour ouvrir l'assistant de sélection ODBC.

🚳 ODBC Selector Wiz	zard	×
	First, select a data source. MS Access Database Excel Files dBASE Files My Data Source Some data sources require a logon and password.	
<i>71</i> 111 - E	Password New DSN]
	< Back Next > Cancel	

- Sélectionnez la source de données que vous souhaitez utiliser pour la liste. Si aucune source de données compatible n'est répertoriée, cliquez sur Nouveau DSN, puis suivez les instructions indiquées sous <u>Création d'une nouvelle source de</u> <u>données ODBC</u> [32[†]].
- 3. Si nécessaire, entrez le Logon et le Mot de passe de la source de données.
- 4. Cliquez sur Next (Suivant).
- 5. La source de données doit contenir au moins une table avec des champs pour les adresses électroniques et les noms. Si la source de données contient une ou plusieurs tables admissibles, choisissez la table souhaitée et cliquez sur Suivant. Sinon, cliquez sur Annuler pour quitter l'assistant de sélection ODBC, puis utilisez

votre application de base de données pour ajouter une table à la base de données concernée avant de continuer.

ODBC Selector Wiz	ard	×
	Second, select a table from the data source. Data source name: My Data Source This data source contains the following tables: contacts domains userlist	
	< Back Next > Cano	;el

 Utilisez les listes déroulantes pour désigner les champs de la table qui correspondront à l'adresse électronique, au Prénom et au Nom. Cliquez sur Suivant.

ODBC Selector Wiz	ard 🛛 🔀
	Next, map table columns to email and name fields Table name: contacts This table column contains the member's email address Final Address This table column contains the member's first name First Name This table column contains the member's last name Last Name T
	< Back Next > Cancel

7. L'assistant de sélection ODBC va construire une requête SQL basée sur les sélections effectuées à l'étape 6. MDaemon l'utilisera pour récupérer les données des membres de la liste normale dans votre base de données. Vous pouvez modifier cette instruction à votre guise et inclure d'autres instructions de requête dans les autres commandes pour que les membres reçoivent les messages en mode Modifier vos, et pour désigner les membres comme étant en lecture seule ou en affichage seul. Un bouton **Test** est disponible à côté de chaque contrôle afin que vous puissiez tester vos requêtes pour vous assurer qu'elles récupèrent les bonnes données. Lorsque vous avez terminé de configurer vos requêtes, cliquez sur **Suivant**.

ODBC Selector Wiz	zard 🛛 🔀
	Last step. The wizard has constructed the following SQL query statements to fetch member data from the data source. Feel free to tweak these statements as needed. Click the finish button when done. Normal list member query IName + '' + Last Name) as FullName from contacts Test Digest only list member query Test Read only list member query Test Post only list member query Test
	< Back Next > Cancel

8. Cliquez sur **Terminer**.

Voir :

 Mes listes Listes diffusion | ODBC

 Gréation d'une nouvelle source de données ODBC

 321

3.4.2.13.2 Création d'une source de données

Pour créer une nouvelle source de données système ODBC à utiliser par une Liste de diffusion :

- 1. Dans l'<u>écran ODBC</u> at de l'éditeur de Liste de diffusion, cliquez sur **Connecter à une nouvelle source ODBC** pour ouvrir l'assistant de sélection ODBC.
- 2. Cliquez sur **New DSN** pour ouvrir la boîte de dialogue Select Data Source.

ODBC Selector Wit	zard	×
	First, select a data source. MS Access Database Excel Files	-
	dBASE Files My Data Source	•
	Some data sources require a logon and password.	
	Password	
	< Back. Next > Cancel	

3. Passez à l'onglet **Machine Data Source**, et cliquez sur **New...** pour ouvrir la boîte de dialogue Create New Data Source (Créer une nouvelle source de données).

Select	Data Source			? 🔀
File D Da dB Ex MS W	ata Source Machine Data ata Source Name ASE Files cel Files 5 Access Database ebAdmin	Source Type User User User System	Description WebAdmin Database	
				New
A Machine Data Source is specific to this machine, and cannot be shared. "User" data sources are specific to a user on this machine. "System" data sources can be used by all users on this machine, or by a system-wide service.				
			OK Cancel	Help

4. Sélectionnez System Data Source (Source de données système) et cliquez sur Next (Suivant).



5. Sélectionnez le **pilote debase de données** pour lequel vous souhaitez configurer la source de données, puis cliquez sur **Next (Suivant)**.

Create New Data Source		X
	Select a driver for which you want to set up a data Name Driver da Microsoft para arquivos texto (*.txt; *.csv Driver do Microsoft Access (*.ndb) Driver do Microsoft dBase (*.dbf) Driver do Microsoft Paradox (*.db) Driver para o Microsoft Visual FoxPro Microsoft Access Driver (*.ndb) Microsoft Access Driver (*.ndb) Microsoft dBase Driver (*.ndb) Microsoft dBase Driver (*.dbf)	source.
	< Dack Next>	Jancer

 Cliquez sur Finish pour afficher la boîte de dialogue de configuration spécifique au pilote. L'apparence de cette boîte de dialogue varie en fonction du pilote que vous avez sélectionné (la boîte de dialogue de configuration de Microsoft Access est illustrée ci-dessous).

ODBC Microsoft Access Setup	? 🛛
Data Source Name: MD_Mailing_Lists	ОК
Description: My MDaemon Mailing Lists	Cancel
Database	
Database: C:\MDaemon\App\MDlists.mdb	Help
Select Create Repair Compact	Advanced
System Database	
None	
C Database:	
System Database	Options>>

- 7. Désignez un nom de source de données pour votre nouvelle source de données et fournissez toute autre information requise par la boîte de dialogue spécifique au pilote (comme la création ou la spécification d'une base de données, le choix d'un répertoire ou d'un serveur, etc.)
- 8. Cliquez sur **OK** pour fermer la boîte de dialogue spécifique au pilote.
- 9. Cliquez sur **OK** pour fermer la boîte de dialogue Select Data Source.

Voir :

<u>ODBC - Listes de diffusion</u> आଣे <u>Configuration d'une source de données ODBC pour une Liste de diffusion</u> ଆଶି
Dossiers publics Company.test Markan Balance	Gestion des dossiers publics Nouveau dossier Supprimer dossier Renommer dossier
Contacts	Activer les dossiers publics
	Nom et type Nom de dossier Dossiers publics Modifier les droits d'accès
Calendrier Contacts Documents Journal	Paramètres
Notes Tâches Mail Archive	Adresse d'envoi
	Garder des indicateurs d'état distincts Activez cette option pour que chaque utilisateur ayant accès au dossier public garde son propre indicateur d'état (lu, non lu, etc.) pour chaque message. Désactivez l'option pour que tous les utilisateurs aient le même indicateur d'état.
	Attribuer un numéro de ticket (ou suivi) unique aux messages Activez cette option pour insérer un identifiant unique dans le sujet des
	messages. Lette option est valable uniquement avec les dossiers de type "courrier" pour lesquels une adresse d'envoi est configurée.
	OK Annuler Appliquer Aide

3.5 Gestionnaire de dossiers publics

Utilisez cet écran pour gérer vos <u>Dossiers publics</u> 116. Pour accéder à la Gestion des dossiers publics, cliquez sur "Configuration | Gestion des Dossiers publics...".

Gestion des dossiers publics

Nouveau dossier

Pour créer un nouveau dossier public, sélectionnez dans la liste le dossier que vous souhaitez voir devenir son dossier parent, puis cliquez sur *Nouveau dossier*. Saisissez un Nom de dossier, choisissez le Type de dossier et cliquez sur *OK*.

Éditeur de dossier public	×
Propriétés du dossier public	
Nom du dossier public	
Type de dossier public	
Courrier	•
ſ	
l	UK Annuler

Supprimer un dossier

Pour supprimer un dossier public de la liste, sélectionnez le dossier souhaité, puis cliquez sur le bouton*Supprimer le dossier*.

Renommer un dossier

Pour renommer un dossier public, sélectionnez un dossier et cliquez sur *Renommer le dossier*. Tapez un nouveau nom et cliquez sur *Ok*.

Activer les dossiers publics

Cochez cette case si vous souhaitez permettre aux utilisateurs d'accéder aux Dossiers publics. Les utilisateurs qui peuvent y accéder et le niveau d'accès accordé sont contrôlés en sélectionnant un dossier et en cliquant sur le bouton*Modifier l'accès.*

Nom et type

Nom du dossier

Ce champ affiche le nom du dossier que vous avez sélectionné dans la liste. Les autres options de cet écran s'appliquent au dossier sélectionné.

Type de dossier

Utilisez la liste déroulante pour désigner le Type de dossier : Courrier, Contacts, Calendrier, etc.

Modifier les listes de contrôle d'accès

Choisissez un dossier, puis cliquez sur ce bouton pour ouvrir la boîte de dialogue<u>Liste de contrôle d'accès</u> ar pour ce dossier. Utilisez la Liste de contrôle d'accès pour désigner les utilisateurs ou les groupes qui pourront accéder au dossier et les autorisations pour chaque utilisateur ou groupe.

Paramètres

Adresse d'envoi

Saisissez une adresse électronique locale ou choisissez un compte MDaemon spécifique à associer au dossier partagé, afin que les messages destinés à cette *Adresse d'envoi* soient automatiquement routés vers le dossier partagé. Cependant, seuls les utilisateurs ayant reçu l'autorisation de " poster " dans le dossier pourront envoyer des messages à cette adresse.

Maintenir des indicateurs d'état distincts pour les messages

Cochez cette case si vous souhaitez queles indicateurs de message du dossier(lu, non lu, répondu, transféré, etc.) soient définis par utilisateur et non globalement. Aucun utilisateur ne verra l'état des messages dans le dossier partagé affiché en fonction de son interaction personnelle avec eux. Un utilisateur qui n'a pas lu un message le verra marqué comme "non lu", tandis qu'un utilisateur qui l'a lu verra le statut "lu". Si cette option est désactivée, tous les utilisateurs verront le même statut. Ainsi, lorsqu'un utilisateur a lu un message, tous les utilisateurs le voient marqué comme "lu".

Attribuer un numéro de ticket (ou suivi) unique aux messages

Utilisez cette option si vous souhaitez configurer le Dossier public comme dossier public de ticketing des messages. MDaemon ajoutera le *Nom du dossier* et un identifiant unique à l'objet des messages envoyés à l'Adresse d'envoi du dossier public. Pour tous les messages sortants dont l'objet est spécialement formaté, l'adresse De sera remplacée par l'adresse de soumission du dossier public et une copie du message sera placée dans un dossier public enfant nommé " Répondu à ". Dans ce cas, une copie du message sortant sera placée dans un dossier public enfant intitulé "Répliqué à". Dans le même temps, tous les messages entrants dont l'objet a été spécialement formaté seront automatiquement redirigés vers le dossier public, quelle que soit l'adresse à laquelle le message a été envoyé.

Voir :

Contrôle d'accès 327 Dossiers publics - Vue d'ensemble 116 Dossiers publics & partagés 118 Éditeur de compte | Dossiers partagés 786 Liste des dossiers | Dossiers publics ". 314

3.5.1 Liste de contrôle d'accès

La Liste de contrôle d'accès (ACL) est utilisée pour définir les droits d'accès des utilisateurs ou des groupes pour vos <u>Dossiers publics et partagés</u> [116]. On y accède à partir du bouton *Modifier les listesde contrôle d'accès* dans le <u>Gestionnaire des</u> <u>dossiers publics</u> [325] ou du bouton *Modifier la liste de contrôle d'accès* dans l'écran Dossiers publics et partagés de l'Éditeur de comptes.

curité Général		
om de robjet: Contacts oms de groupes ou d'utili	sateurs:	
Nom	Туре	E-mail
🥝 anyone	Intégrés	
😹 Bill Farmer	Utilisateur	Bill.Farmer@company.test
📚 company .test Membr	es Groupe	anyone@company.test
🚨 Frank Thomas	Utilisateur	Frank.Thomas@company.test
🚨 Michael Mason	Utilisateur	michael.mason@company.test
😹 Randy Peterman	Utilisateur	Randy.Peterman@company.test
our modifier les droits d'a	iccès, cliquez su	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès	ccès, cliquez su ner Autorisa	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration	accès, cliquez su ner Autorisa	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création	ccès, cliquez su ner Autorisa Non Non	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer	ccès, cliquez su ier Autorisa Non Non Non	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu"	accès, cliquez su ner Autorisa Non Non Non Non	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion	eccès, cliquez su ner Autorisa Non Non Non Non Non	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion V Consultation	ccès, cliquez su ier Autorisa Non Non Non Non Non Oui	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion Consultation Envoi	ccès, cliquez su ner Autorisa Non Non Non Non Non Oui Non	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion Consultation Envoi Lecture	ccès, cliquez su ner Autorisa Non Non Non Non Oui Non Oui	ur Modifier Modifi <u>e</u> r

Chemin du dossier:	C:\MDaemon\Public Folders \company.test.IMAP\Contacts.IMAP
Nom de dossier:	Contacts
Type de dossier:	IPF.Contact
Nombre d'éléments:	2
Taille du dossier:	719
Nombre de sous-dossiers IMAP:	0
Éléments dans les sous-dossiers:	0
Taille des sous-dossiers IMAP:	0
ID ActiveSync:	
ID partagé ActiveSync:	
ID utilisateur ActiveSync:	
Quvrir	Ouvrir le dossier dans l'Explorateur Windows
Commentaires sur le dossier:	
	A

Sécurité

Cet onglet affiche la liste des groupes ou des utilisateurs associés au dossier et les autorisations d'accès spécifiques accordées à chacun. Dans la liste, sélectionnez un groupe ou un utilisateur afin d'afficher ses <u>autorisations</u> dans la fenêtre Permissions ci-dessous. Pour modifier les autorisations, cliquez sur <u>Modifier</u> 2001.

Général

Cet onglet affiche les propriétés du dossier, telles que son chemin d'accès, son Nom, son type, sa taille, etc.

Éditeur ACL

Cliquez sur **Modifier** dans l'onglet Sécurité de la liste de contrôle d'accès pour ouvrir l'éditeur de liste de contrôle d'accès afin de modifier les autorisations d'accès.

Nom		
	Туре	E-mail
🥝 anyone	Intégrés	
Bill Farmer	Utilisateur	Bill.Farmer@company.test
📚 company.test Memb	ores Groupe	anyone@company.test
😣 Frank Thomas	Utilisateur	Frank.Thomas@company.test
😣 Michael Mason	Utilisateur	michael.mason@company.test
🚨 Randy Peterman	Utilisateur	Randy.Peterman@company.test
roits d'accès de Bill F	armer	Ajouter Supprimer
yroits d'accès de Bill F Droit d'accès	armer Autorisa	Ajouter Supprimer
roits d'accès de Bill F Droit d'accès Administration	Farmer Autorisa Non	Ajouter Supprimer
roits d'accès de Bill F Droit d'accès Administration Création	Farmer Autorisa Non Non	Ajouter Supprimer
roits d'accès de Bill F Droit d'accès Administration Création Supprimer	Autorisa Non Non Non Non	Ajouter Supprimer
roits d'accès de Bill F Droit d'accès Administration Création Supprimer Marqueur "lu"	Farmer Autorisa Non Non Non Non	Ajouter Supprimer
roits d'accès de Bill F Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion	Farmer Autorisa Non Non Non Non Non	Ajouter Supprimer
roits d'accès de Bill F Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion Consultation	Autorisa Non Non Non Non Non Non Oui	Ajouter Supprimer
proits d'accès de Bill F Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion Consultation Envoi	Autorisa Non Non Non Non Non Oui Oui	Ajouter Supprimer

Par nom

Votre nom est celui de l'objet ou du dossier auquel les autorisations de la liste de contrôle d'accès s'appliqueront.

Nom du groupe ou de l'utilisateur

Il s'agit des groupes ou des utilisateurs auxquels un certain niveau d'accès a été accordé. Sélectionnez un groupe ou un utilisateur pour afficher ses autorisations dans la fenêtre*Autorisations pour <groupe ou utilisateur* > ci-dessous. Cochez la case en regard de toute autorisation d'accès que vous souhaitez accorder au groupe ou à l'utilisateur.

Ajouter

Pour accorder des autorisations d'accès à un groupe ou à un utilisateur qui ne figure pas dans la liste ci-dessus, cliquez sur **<u>Ajouter</u>** and.

Supprimer

Pour supprimer un groupe ou un utilisateur, sélectionnez son entrée dans la liste cidessus et cliquez sur **Supprimer**.

Autorisations pour <groupe ou utilisateur>

Cochez la case en regard de toute autorisation d'accès que vous souhaitez accorder au groupe ou à l'utilisateur sélectionné ci-dessus.

Vous pouvez accorder les autorisations de contrôle d'accès suivantes :

Administrer - l'utilisateur peut gérer les droits d'accès d'un dossier.

Créer - l'utilisateur peut créer des sous-dossiers dans ce dossier.

- Supprimer l'utilisateur peut supprimer des éléments de ce dossier.
- **Marqueur lu** l'utilisateur peut modifier l'état lu/non lu des messages de ce dossier.
- Insérer l'utilisateur peut ajouter et copier des éléments dans ce dossier.
- **Liste des dossiers** l'utilisateur peut voir ce dossier dans sa liste personnelle de dossiers IMAP.
- **Dossiersiers -** l'utilisateur peut envoyer du courrier directement à ce dossier (si le dossier le permet).
- Lire l'utilisateur peut ouvrir ce dossier et en consulter le contenu.
- **Écrire l'** utilisateur peut modifier les drapeaux sur les messages de ce dossier.

Appliquer à tous les dossiers enfants

Cochez cette case si vous souhaitez appliquer les autorisations de contrôle d'accès de ce dossier à tous les sous-dossiers qu'il contient actuellement. Cela ajoutera les autorisations d'utilisateur et de groupe du dossier aux dossiers enfants, en les remplaçant en cas de conflit. Toutefois, cela ne supprimera pas les autres autorisations d'utilisateur ou de groupe qui ont actuellement accès à ces dossiers.

Exemple,

Le dossier parent accorde certaines autorisations à User_A et User_B. Le dossier enfant accorde des autorisations à User_B et User_C. Cette option ajoutera les autorisations de User_A au dossier enfant, remplacera les autorisations de User_B du dossier enfant par celles du dossier parent et ne modifiera pas les autorisations de User_C. Le dossier enfant disposera donc des autorisationsUser A, User B et User C.

Écraser les dossiers enfants

Cochez cette case si vous souhaitez que toutes les autorisations d'accès des dossiers enfants soient remplacées par les autorisations actuelles du dossier parent. Les autorisations du dossier enfant seront alors identiques à celles du dossier parent.

Ajout d'un groupe ou d'un utilisateur

Cliquez sur **Ajouter** dans l'éditeur ACL si vous souhaitez ajouter un autre groupe ou utilisateur à la liste de contrôle d'accès. L'écran Ajouter un groupe ou un utilisateur s'ouvre et vous permet de le rechercher, puis de l'ajouter.

💷 Sélec	tion d	'utilisateurs	, de groupes ou d'objets intégrés	— ×-
Séle	ctionne d'objet	er les types is suivants:	Intégré, Groupes, Utilisateurs	Types d' <u>o</u> bjets
D	e ces d	omaines :	Tous les domaines	Emplacements
Requi	êtes coi	mmunes		Trouver maintenant
	Le <u>n</u> o	om contient		
	L'e- <u>n</u>	nail contient		
Lag	descript	ion contient		
Inc	lure les	; comptes dé	sactivés	
<u>R</u> ésulta	its de la	recherche	<u>A</u> ide OK	Annuler
Nom	Туре	E-mail		

Sélectionnez ces types d'objets

Cliquez sur **Types d'objets...** pour sélectionner les types d'objets dans lesquels vous souhaitez rechercher les groupes ou les utilisateurs que vous souhaitez ajouter. Vous pouvez sélectionner : Intégré, Groupes et Utilisateurs.

À partir de ces emplacements

Cliquez sur **Lieux...** pour sélectionner les domaines que vous souhaitez rechercher. Vous pouvez sélectionner Tous les domaines MDaemon ou des domaines spécifiques.

Requêtes courantes

Utilisez les options de cette section pour limiter votre recherche en spécifiant tout ou partie du nom de l'utilisateur, son adresse électronique ou le contenu de la Description du compte. Laissez ces champs vides si vous souhaitez que les résultats de la recherche contiennent tous les groupes et utilisateurs correspondant aux types d'objets et aux emplacements spécifiés ci-dessus.

Inclure les comptes désactivés

Cochez cette case si vous souhaitez inclure les <u>comptes désactivés</u> dans votre recherche.

Rechercher maintenant

Une fois que vous avez spécifié tous vos critères de recherche, cliquez sur **Rechercher maintenant** pour effectuer la recherche.

Chercher les résultats

Dans les résultats de la recherche, sélectionnez les groupes ou utilisateurs souhaités et cliquez sur **OK** pour les ajouter à la liste de contrôle d'accès.

Les droits d'accès sont contrôlés grâce à laprise en charge parMDaemondes listes de contrôle d'accès (ACL). L'ACL est une extension du protocole IMAP4 (Internet Message Access Protocol) qui vous permet de créer une liste d'accès pour chacun de vos Dossiers de courrier IMAP, accordant ainsi des droits d'accès aux dossiers à d'autres utilisateurs qui ont également des comptes sur votre serveur de messagerie. Si votre client de messagerie ne prend pas en charge l'ACL, vous pouvez toujours définir les autorisations à l'aide des commandes de cette boîte de dialogue.

L'ACL est traité en détail dans la RFC 2086, qui peut être consultée à l'adresse <u>suivante</u> : http://www.rfc-editor.org/rfc/rfc2086.txt.

Voir :

Gestionnaire des dossiers publics325Dossiers publics - Vue d'ensemble116Dossiers publics & partagés118Éditeur de compte | Dossiers partagés796Liste des dossiers | Dossiers publics314

3.6 Services web & MI

3.6.1 Webmail

3.6.1.1 Vue d'ensemble

MDaemon Webmail est une solution de messagerie en ligne incluse dans MDaemon et conçue pour offrir aux utilisateurs les fonctionnalités d'un client de messagerie à partir de leur navigateur Web favori. Webmail peut facilement rivaliser avec les clients de messagerie traditionnels tout en offrant l'avantage supplémentaire de permettre aux utilisateurs d'accéder à leur messagerie de n'importe où et à n'importe quel moment tant qu'ils disposent d'une connexion Internet ou d'un réseau. De plus, comme tous les dossiers de courrier électronique, les contacts, les calendriers, etc. résident sur le serveur et non sur l'ordinateur local, les utilisateurs peuvent accéder à tout comme s'ils étaient à leur bureau.

MDaemon Webmail offre de nombreux avantages aux administrateurs de messagerie. Comme le Webmail ne dépend pas d'un poste de travail, vous pouvez tout configurer à partir du serveur, contrairement à de nombreuses applications clientes. Cela vous évite d'avoir à configurer et à maintenir chaque client de messagerie individuel. Vous pouvez également personnaliser les images graphiques et les pages HTML rédigées en HTML pour répondre aux besoins de votre entreprise ou de votre client. En outre, vous pouvez donner à vos utilisateurs la possibilité de gérer les paramètres de leur propre compte, ce qui vous permet de gagner du temps - vous pouvez donner autant ou aussi peu de contrôle à vos utilisateurs que vous le souhaitez.

Enfin, outre la commodité d'un client basé sur le web, il existe de nombreuses fonctionnalités supplémentaires qui profiteront à vos utilisateurs, telles que : une fonctionnalité de courrier électronique étendue, une interface côté client disponible dans près de 30 langues, des carnets d'adresses personnels et globaux, des dossiers de courrier et des filtres gérables, l'envoi/la réception de pièces jointes, plusieurs "thèmes" visuels pour l'interface, des thèmes pour les appareils mobiles, des fonctions de calendrier, des fonctions de messagerie instantanée, des dossiers Pièces jointes, et bien plus encore.

Calendrier et système de planification

MDaemon est équipé d'un système de collaboration complet. Depuis le Webmail, vous pouvez facilement créer des rendez-vous, planifier des réunions et travailler avec des carnets d'adresses. Les rendez-vous récurrents sont entièrement pris en charge et les rendez-vous disposent de nombreux champs pour les décrire. En outre, les contacts, les calendriers et les données relatives aux tâches sont stockés sous forme de dossiers IMAP dans le dossier racine la messagerie dechaque utilisateur.Grâce au Webmail, vos utilisateurs peuvent accéder à ces dossiers personnels et contrôler quels autres utilisateurs y ont accès. Tous les thèmes de Webmail ont des modèles qui présentent les dossiers de contacts, de calendriers, de notes et de tâches d'une manière logique et attrayante.

Le système d'agenda étant intégré à MDaemon, il est possible de recevoir des notifications par courrier électronique pour les rendez-vous, qu'ils soient programmés par vous ou par un tiers. Lorsque quelqu'un d'autre que vous planifie un rendez-vous pour vous, vous recevrez un message électronique résumant le rendez-vous. Chaque personne désignée pour participer à un rendez-vous recevra un message électronique précisant ladate, l'heure, le lieu, l'objet durendez-vouset la liste des participants. En outre, tous les participants dont les entrées de calendrier entrent en conflit avec lecréneau horaire durendez-vousrecevront un message les informant du rendez-vous et de son conflit avec leur emploi du temps. La personne qui a programmé la réunion recevra un message résumé reprenant tous lesdétails de laréunionet les participants invités qui ont ou n'ont pas de conflit d'horaire.

Le système d'agenda est également compatible avec le calendrier Internet (iCal) utilisé par Microsoft Outlook et d'autres programmes de messagerie électronique compatibles avec iCalendar. Le système de gestion des calendriers peut détecter et traiter les informations iCalendar envoyées à vos utilisateurs et mettre à jour leurs calendriers en conséquence. Dans le Webmail, lorsqu'un utilisateur ouvre une pièce jointe iCalendar, l'information contenue dans la pièce jointe sera reflétée dans lecalendrier Webmail de l'utilisateur. De plus, lorsque les utilisateurs créent de nouvelles réunions ou de nouveaux rendez-vous, ils peuvent indiquer une ou plusieurs adresses e-mail auxquelles ils souhaitent qu'un e-mail iCalendar soit envoyé. Cette fonction peut être paramétrée par les utilisateurs individuels dans leurs options Webmail.

MDaemon Instant Messenger

MDaemon Instant Messenger (MDIM) est leclient de messagerie instantanée sécurisée deMDaemonet l'applet de la barre d'état système qui offreun accès rapide auxfonctions de messagerie duWebmail.MDIM peut être téléchargé par chaque utilisateur de Webmail, puis installé surson ordinateur local. Il est préconfiguré pour l'utilisateur spécifique lorsqu'il est téléchargé, ce qui limite la nécessité de le configurer manuellement.

MDIM fonctionne en arrière-plan et vérifie si votre compte contient de nouveaux messages en interrogeant directement le serveur de Webmail. Il n'est donc pas nécessaire d'ouvrir un navigateur ou d'en garder un ouvert pour consulter votre courrier électronique. MDIM vérifie l'arrivée de nouveaux messages et vous en informe par une alerte sonore ou visuelle. MDIM affiche également une Liste des dossiers de courrier ainsi que le nombre et le type de messages que chacun contient (nouveaux, non lus et lus). De plus, il peut être utilisé pour lancer votre navigateur et le déplacer immédiatement dans un Dossier courrier spécifique.

MDIM est également équipé d'un client de messagerie instantanée complet. Vous pouvez consulter votre liste de contacts MDIM et lestatut en ligne dechacun d'entre eux(en ligne, absent, hors ligne), démarrer une conversation avec un ou plusieurs d'entre eux, définir votre propre statut en ligne et consulter les conversations passées dans un dossier historique.

Pour obtenir des instructions spécifiques sur l'utilisation de la Messagerie instantanée de MDaemon, consultez son système d'aide en ligne.

Le système de messagerie instantanée de MDaemon Instant Messenger

Le MDIM est équipé d'un client de messagerie instantanée qui utilise le serveur XMPP de MDaemon. Grâce à cette fonctionnalité, vous pouvez ajouter d'autres utilisateurs qui partagent votre domaine (et éventuellement d'autres domaines hébergés sur votre serveur MDaemon) à votre liste de contacts MDIM, puis communiquer avec eux instantanément. Vous pouvez définir votre statut en ligne, voir le statut de vos contacts, utiliser des émoticônes, définir la couleur du texte, envoyer des fichiers, définir des sons de notification et contrôler d'autres préférences. Vous pouvez également démarrer une conversation de groupe avec plusieurs contacts à la fois. Les fonctions de messagerie instantanée sont disponibles via le menu contextuel de l'icône de la barre des tâches et depuis la fenêtre MDIM.

Le système de messagerie instantanée de MDaemon Messagerie instantanée est également scriptable, ce qui permet à des programmes personnalisés de s'interfacer avec lui. En créant des fichiers sémaphores (SEM) dans le dossier MDaemon World Client, une application externe peut envoyer des messages instantanés à vos utilisateurs MDIM. Voici le format du fichier SEM :

À : userl@example.com	Adresse électronique de l'utilisateur du MDIM.
De : user2@example.com	Adresse électronique de l'expéditeurdu message instantané.
<ligne blanche=""></ligne>	
Texte du message instantané.	Ce texte est envoyé sous forme de message instantané.

Le Nom du fichierSEM doit commencer par les caractères "IM-" et être suivi d'une valeur numérique unique. Exemple : "IM-0001.SEM". Les applications doivent également créer un fichier correspondant appelé "IM-0001.LCK" pour verrouiller le fichier SEM. Une fois le fichier SEM terminé , le fichier LCK est supprimé et le fichierSEM est traité. À propos de MDaemon, cette méthode de script permet d'envoyer des rappels par messages instantanés concernant les rendez-vous et les réunions à venir.

Le système Filtre de contenu est équipé d'une action qui utilise cette méthode de script pour envoyer des messages instantanés. De plus, les règles utilisant cette action peuvent utiliser les macros du Filtre de contenu dans la messagerie instantanée. Exemple : vous pouvez créer une règle pour envoyer un message instantané contenant des lignes comme celle-ci :

```
Vous avez reçu un E-mail de $SENDER$.
Objet : $SUBJECT$
```

Cette règle constituerait un moyen efficace d'envoyer des alertes de nouveau courrier par l'intermédiaire du MDIM.

Dans la mesure où certains administrateurs hésitent à utiliser un système de messagerie instantanée dans leur entreprise en raison du manque inhérent de responsabilité centralisée et de l'incapacité à surveiller le trafic de messagerie instantanée qui se trouve dans des clients de messagerie traditionnels et bien connus, nous avons conçu lesystème de messagerie instantanée de MDIMde manière à minimiser ces défauts. Tout d'abord, notre système n'est pas de type "peer-to-peer" - les clients connectés de MDIM ne se connectent pas directement les uns aux autres pour la messagerie instantanée. Dans la mesure où chaque message instantané passe par le serveur, chaque message est pas journalisé dans un endroit central accessible à l'administrateur de MDaemon. Ainsi, un enregistrement de toutes les conversations peut être conservé pour la sécurité de votre entreprise et de vos employés ou utilisateurs. L'activité de la messagerie instantanée est enregistrée dans un fichier appelé XMPPServer-<date>.log situé dans le répertoire deMDaemon\LOGS\.

La messagerie instantanée est fournie par domaine. La commande globale permettant d'activer la messagerie instantanée est filtrée <u>par l'écran MDIM</u> [346] de la boîte de dialogue Webmail (Configuration | Services web & IM | Webmail | MDIM). Un écran similaire dans le <u>Gestionnaire de domaines</u> [193] permet d'activer ou de désactiver la messagerie instantanée pour des domaines spécifiques.

Habillages de la MDaemon Instant Messenger

L'interface de MDIM est compatible avec les skins *msstyles*, qui sont facilement disponibles sur Internet. Plusieurs styles sont inclus, mais pour installer un nouveau style, téléchargez le fichier *.msstyles et placez-le dans le dossier Nouveau dossier de MDIM , dans un sous-dossier portant le même nom que le fichier. Exemple, si le fichier s'appelle Red.msstyles, le Chemin du fichier sera alors :"\Styles\Red\Red.msstyles"

Intégration avec Dropbox

Un nouvel écran a été ajouté à Ctrl+W|Webmail|Dropbox. Ce texte contient des contrôles permettant d'entrer votre Clé d'application Dropbox, votre Code secret d'application Dropbox et le texte de votre politique de confidentialité. Tous ces éléments sont nécessaires pour activer le service intégré et sont obtenus lorsque vous enregistrez votre MDaemon Webmail en tant qu''application'' Dropbox en visitant le site Web de Dropbox. Nous ne pouvons pas le faire à votre place, mais cela ne doit être fait qu'une seule fois. Pour des instructions complètes sur la manière d'enregistrer votre Webmail en tant qu'app auprès de Dropbox, veuillez consulter l'article de la Base de connaissances : <u>Comment activer et configurer l'intégration avec Dropbox et utiliser les fonctionnalités de Dropbox dans le Webmail ?</u>

Une fois la "clé d'application" et le "secret d'application" configurés, le Webmail pourra connecter ses comptes à un compte Dropbox. La première fois qu'un utilisateur se connecte au thème WorldClient ou LookOut, une liste déroulante s'affiche en haut de la page. L'utilisateur a trois options : afficher la liste déroulante lors de la prochaine connexion, ne plus jamais l'afficher ou accéder à la nouvelle vue Options | Cloud Apps. Dans la vue Options | Cloud Apps, l'utilisateur peut cliquer sur le bouton Configurer Dropbox. Une fenêtre contextuelle OAuth 2.0 s'ouvre alors. Cette fenêtre détaille ce à auoi l'utilisateur se connecte et les autorisations demandées par Webmail. Elle contient également un lien vers la politique de confidentialité et le bouton "Se connecter à Dropbox". Lorsque l'utilisateur clique sur le bouton "Connecter à Dropbox", la page navique vers Dropbox. Si l'utilisateur n'est pas journalisé, Dropbox lui propose de se connecter ou de créer un compte. Si l'utilisateur n'est pas connecté à Dropbox, un site lui permettra de se connecter ou de créer un compte. Si cette étape est terminée, l'utilisateur se verra proposer une autre page Dropbox qui lui demandera s'il souhaite autoriser Webmail à avoir un accès total à son compte. En cliquant sur "Autoriser", l'utilisateur retourne sur la page Webmail et indique si l'autorisation a été accordée ou non. Cette autorisation est valable pour une semaine, après quoi le même écran est à nouveau présenté et un autre jeton d'accès est obtenu et utilisé pour la semaine suivante. Une fois l'autorisation terminée, l'utilisateur voit apparaître une icône Dropbox à côté de chaque pièce jointe. En cliquant sur cette icône, la pièce jointe est enregistrée dans le compte Dropbox de l'utilisateur, dans le dossier /WorldClient_Attachments.

Dans la vue Composer des thèmes WorldClient et LookOut, les utilisateurs pourront choisir des fichiers dans leur compte Dropbox en cliquant sur l'icône Dropbox dans la barre d'outils de l'éditeur HTML (en haut à gauche). Cette fonctionnalité ne nécessite pas que les utilisateurs configurent l'accès à leurs comptes via la vue Options | Mon Comptes et OAuth 2.0. Elle ne nécessite que la "clé de l'application" et le "secret de l'application".

La prise en charge de Dropbox est désactivée par défaut, mais peut être activée sur l' écran<u>Dropbox</u> and MDaemon. Si vous souhaitez activer ou désactiver Dropbox pour chaque utilisateur, vous pouvez le faire en ajoutant "DropboxAccessEnabled=Yes" au fichier User.ini.

Utilisation de Webmail

De...

Il existe trois façons de démarrer/arrêter le serveur Webmail :

- 1. Dans le volet Stats situé à gauche de l'interface graphique de MDaemon, cliquez avec le bouton droit de la souris sur l'entrée Webmail et choisissez la sélection *Basculer actif/inactif* dans le menu contextuel.
- 2. Cliquez sur "File | Enable Webmail" server dans l'interface principale.
- 3. Cliquez sur "Setup | Web & IM Services" dans l'interface principale, puis cliquez sur *Webmail runs using built-in web server* dans l'écran Serveur Web.

Pasalisation de la journalisation sur Webmail

- 1. Pointez votre navigateur web sur http://example.com:WebmailPortNumber. Ce port est désigné sur l'écran <u>Serveur Web de</u> [339] la section Webmail. Si vous configurez Webmail pour qu'il écoute le port web par défaut (port 80), alors vous n'avez pas besoin d'indiquer le numéro de port dans l'URL de connexion (par exemple www.example.com au lieu de www.example.com: 3000).
- 2. Tapez le Nom d'utilisateur et le mot de passe de votre compte MDaemon.
- 3. Cliquez sur Connexion.

Modifier les paramètres du port du Webmail

- 1. Cliquez sur "Setup | Web & IM Services" dans la barre de menu.
- 2. Utilisez le numéro de port souhaité dans le champ intitulé Run Webmail Server using this port TCP.
- 3. Cliquez sur OK.

Aide côté client

Webmail est équipé d'une aide complète côté client pour vos utilisateurs. Consultez le système d'aide en ligne de Webmail pour obtenir des informations sur les caractéristiques et les fonctions du client.

Pour plus d'options du carnet d'adresses, voir :

<u>Webmail | MDIM</u> 346ो <u>LDAP</u> छि0

3.6.1.2 Serveur Web

🧐 Web & IM Services - Web Server	
Webmail Web Server SSL & HTTPS MDIM Calendar RelayFax Dropbox Settings Remote Administration Terms of Use Attachment Linking CaIDAV & CardDAV XMPP	MD aemon Webmail Webmail is disabled Webmail runs using built-in web server Webmail runs using external webserver (IIS, Apache, etc) Run Webmail server using this TCP port 3000 Maximum number of concurrent sessions 200 Sessions not composing a message expire after 20 Image: Sessions composing a message expire after 120 Image: Session composing a message expire after 120 Image: Session composing a message expire after Image: Session Image: Session compresexpir
	Ok Cancel Apply Help

Cet écran filtre divers paramètres globaux, au niveau du serveur, qui régissent laconfiguration et le comportement de Webmail, quels que soient les utilisateurs ou les domaines auxquels ils appartiennent.

MDaemon Webmail

Webmail est désactivé

Choisissez cette option pour désactiver le Webmail. Vous pouvez également activer/désactiver le Webmail dans le menu Fichier ou dans la section Serveurs du cadre Stats de l'interface graphique principale de MDaemon.



Le Webmail doit être actif lorsque vous utilisez la fonctionnalité<u>Liens les pièces jointes</u> (300).

Serveur Web utilise le serveur web intégré

Choisissez cette option pour exécuter le Serveur Webmail en utilisant le serveur Web intégré deMDaemon.Vous pouvez également activer/désactiver le Webmail à partir du menu Fichier ou de la section Serveurs du cadre Stats de l'interface graphique principale de MDaemon.

Webmail fonctionne avec un serveur Web externe (IIS, Apache, etc.)

Choisissez cette option si vous souhaitez exécuter le Webmail sous Internet Information Server (IIS) ou un autre serveur web au lieu du serveur intégré deMDaemon.Cela permet d'éviter l'accès à certains éléments de l'interface graphique qui pourraient causer des conflits avec votre autre serveur.

Pour plus d'informations, consultez l'article de la base de connaissances de MDaemon Technologies : <u>Comment configurer les services Webmail, MDaemon Remote Admin,</u> <u>ActiveSync, CalDav, CardDav, AutoDiscover, MDDP, Webmail API et XML API dans</u> <u>IISS Mise en place de</u>

Exécuter le serveur Webmail en utilisant ce port TCP

Il s'agit du port sur lequel le Webmail écoutera les connexions des navigateurs web devos utilisateurs.

Nombre maximal de sessions simultanées

Il s'agit du nombre maximum de sessions qui peuvent être connectées au Webmail en même temps.

Les sessions ne composant pas de message expirent après [xx] minutes inactives.

Dans le cas où un utilisateur est connecté à Webmail mais ne compose pas de message, il s'agit de la durée pendant laquelle sa session restera inactive avant que Webmail ne la ferme.

Les sessions en cours de composition d'un message expirent après [xx] minutes inactives.

Cette minuterie détermine la durée pendant laquellela session d'un utilisateurreste ouverte lorsqu'il compose un message et que la session reste inactive. Il est conseillé de fixer ce délai à un niveau plus élevé que le délai" *Sessions ne composant pas de message...*", car le temps d'inactivité est généralement plus long lorsque l'utilisateur compose un message. En effet, la composition d'un message ne nécessite aucune communication avec le serveur jusqu'à ce que le message soit envoyé.

Les sessions IP locales ne composant pas de message expirent après [xx] minutes inactives.

Dans le cas où un utilisateur sur une IP locale est connecté à Webmail mais ne compose pas de message, il s'agit de la durée pendant laquelle sa session restera inactive avant que Webmail ne la ferme. **Note :** Cette option n'est disponible que dans MDRA.

Programmer l'expiration des sessions IP locales en cours de rédaction d'un message au bout de [xx] minutes inactives.

Cette minuterie détermine la durée pendant laquelle lasession d'un utilisateur sur une IP locale reste ouverte lorsqu'il compose un message et que la session reste inactive. Il est conseillé de définir cette minuterie plus haut que la minuterie *Sessions ne composant pas de message...,* étant donné que le temps d'inactivité est généralement plus important lorsqu'un utilisateur compose un message. En effet, la composition d'un message ne nécessite aucune communication avec le serveur jusqu'à ce que le message soit envoyé. **Note :** Cette option n'est disponible que dans MDRA.

Mettre en cache les modèles HTML pour augmenter les performances du serveur web

Cochez cette case pour que le webmail mette les modèles en cache dans la mémoire plutôt que de les lire à chaque fois qu'ils doivent être accédés. Cela peut augmenter considérablement les performances du serveur, mais Webmail devra être redémarré si vous apportez une modification à l'un des fichiers de modèles.

Utiliser des cookies pour mémoriser l'Identifiant, le thème et d'autres propriétés

Cliquez sur cette option si vous souhaitez que Webmail stockele Nom d'Identifiant, le thème et certaines autres propriétés dechaque utilisateurdans un cookie sur son ordinateur local. L'utilisation de cette fonction permet à vos utilisateurs de bénéficier d'une expérience de connexion plus "personnalisée", mais nécessite que la prise en charge des cookies soit activée dans leur navigateur.

Exiger la persistance de l'IP pendant la session du webmail

À titre de mesure de sécurité supplémentaire, vous pouvez cocher cette case pour que Webmail limite chaque session utilisateur à l'adresse IP à partir de laquelle l'utilisateur s'est connecté au début de la session. Ainsi, personne ne peut "voler" lasession de l'utilisateurpuisque la persistance de l'IP est requise. Cette configuration est plus sûre mais peut poser des problèmes aux utilisateurs qui utilisent un serveur proxy ou une connexion Internet qui attribue et change dynamiquement les adresses IP.

Utiliser l'en-tête X-Forwarded-For

Cochez cette case pour activer l'utilisation de l' en-têtex-Forwarded-For, qui est parfois ajouté par les serveurs proxy. Cette option est désactivée par défaut. Ne l'activez que si votre serveur proxy insère cet en-tête.

Utiliser la compression HTTP

Cochez cette case si vous souhaitez utiliser la compression HTTP dans vos sessions de webmail.

Envoyer des données d'utilisation anonymes

Non par défaut, Webmail envoie des données d'utilisation anonymes et bénignes telles que : le système d'exploitation utilisé, la version du navigateur utilisée, la langue, etc. Ces données sont utilisées par MDaemon Technologies pour nous aider à améliorer le Webmail. Désactivez cette option si vous ne souhaitez pas envoyer de données d'utilisation anonymes.

Lierle serveur web deWebmailà ces IP/ports uniquement

Si vous souhaitez restreindre le serveur Webmail à certaines adresses IP ou à certains ports, indiquez ici ces adresses IP et ces ports en les séparant par des virgules. Utilisez le format : "Adresse_IP:Port" pour désigner un port (par exemple, 192.0.2.0:80). Si vous n'indiquez pas de port, le port TCP par défaut spécifié cidessus et le port HTTPS par défaut spécifié sur l'écran<u>SSL & HTTPS</u> [342] seront utilisés. Utilisez "*" si vous souhaitez que le Webmail écoute sur tous les ports. Exemple : "*, *:80" signifie que Webmail écoutera sur toutes les Adresses IP, sur les ports par défaut spécifiés (3000 et 443), et qu'il écoutera également sur toutes les Adresses IP sur le port 80. Si vous laissez ce champ vide, Webmail surveillera toutes les adresses IP désignées pour vos <u>Domaines</u> [184].

Redémarrer Webmail (nécessaire lorsque le port ou la valeur IIS change)

Cliquez sur ce bouton si vous souhaitez redémarrer le serveur Webmail. Dans le cas d'une modification desparamètres du port deWebmail, vous devez redémarrer Webmail pour que le nouveau paramètre soit pris en compte.

En-têtes de réponse HTTP

Cette option permet de définir des En-têtes de réponse HTTP personnalisés pour le serveur Webmail intégré à MDaemon. Vous devez redémarrer le serveur Webmail pour que les modifications en-têtes soient pris en compte. **Remarque :** cette option est uniquement disponible dans MDaemon Remote Admin.

3.6.1.3 SSL & HTTPS

🧐 Services web, & MI - SSL & HTTPS				×
Webmail Serveur Web SI & HTTPS MDIM Calendrier BelavFax	Accepter ces types de cor HTTP uniquement HTTPS uniquement Vérifier les certificats à utilise	nexions HTTP et HTTPS HTTP redirigé en HTTPS r avec HTTPS. Sélectionnez l'éto	Port HTTPS 4	43 aut.
Dropbox Paramètres MDaemon Remote Admin Conditions d'utilisation Liens vers les pièces jointes CalDAV & CardDAV MPP	Sujet Sujet Sujet Créer un certificat	Autres noms d'hôtes	Date d'expiration 4/25/2021	Fournisse mail.com
		OK Annu	uler Appliquer	Aide

Le serveur Web intégré à MDaemon prend en charge le protocole Secure Sockets Layer (SSL). SSL est la méthode standard pour sécuriser les communications serveur/client sur le web. Il permet l'authentification du serveur, le cryptage des données et, en option, l'authentification du client pour les connexions TCP/IP. En outre, la prise en charge du protocole HTTPS (c'est-à-dire HTTP sur SSL) étant intégrée dans tous les principaux navigateurs, il suffit d'installer un certificat numérique valide sur votre serveur pour activer les capacités SSL du client qui se connecte.

Les options permettant d'activer et de configurer le Webmail pour qu'il utilise HTTPS se trouvent sur l'écran SSL & HTTPS sous Activer | Services web & IM | Webmail". Cependant, pour votre commodité, ces options sont également reflétées sous "Sécurité" "Gestionnaire de sécurité" "SSL & TLS" "Webmail". | SSL & TLS | Webmail".

Pour plus d'informations sur le protocole SSL et les certificats, voir : <u>SSL &</u> <u>Certificats</u>

> Cet écran ne s'applique au Webmail que lorsque vous utilisez leserveur Web intégré de MDaemon. Si vous configurez Webmail pour utiliser un autre serveur Web tel que IIS, ces options ne seront pas utilisées - le support SSL & HTTPS devra être configuré en utilisant les outils de l'autre serveur Web.

Accepter ces types de connexions

HTTP uniquement

Choisissez cette option si vous ne souhaitez pas autoriser les connexions HTTPS au Webmail. Seules les connexions HTTP seront acceptées.

HTTP et HTTPS

Choisissez cette option si vous souhaitez activer le support SSL dans Webmail, mais ne souhaitez pas forcer vos utilisateurs Webmail à utiliser HTTPS. Webmail écoutera les connexions sur le port HTTPS désigné ci-dessous, mais répondra toujours aux connexions http normales sur le port TCP de Webmail désigné sur l' écran<u>Serveur</u> Web

HTTPS uniquement

Choisissez cette option si vous souhaitez exiger le protocole HTTPS lors de la connexion à la messagerie Web. Webmail ne répondra qu'aux connexions HTTPS lorsque cette option est activée - il ne répondra pas aux requêtes HTTP.

HTTP redirigé vers HTTPS

Choisissez cette option si vous souhaitez rediriger toutes les connexions HTTP vers HTTPS sur le port HTTPS.

Port HTTPS

Il s'agit du port TCP que le Webmail écoutera pour les connexions SSL. Le port SSL par défaut est 443. Si le port SSL par défaut est utilisé, vous ne devrez pas inclure le numéro de port dans l'URL deWebmaillorsque vous vous connectez via HTTPS (c'est-à-dire que "https://example.com" est équivalent à "https://example.com:443").



Ce n'est pas la même chose que le port du Webmail qui est désigné sur l' écran<u>Serveur Web</u> (338) du Webmail. Si vous autorisez toujours les connexions HTTP au Webmail, ces connexions doivent utiliser cet autre port pour réussir à se connecter. Les connexions HTTPS doivent utiliser le port HTTPS.

Sélectionnez le certificat à utiliser avec HTTPS/SSL

Cette boîte affiche vos certificats SSL. Cochez la case en regard des certificats que vous souhaitez activer. Cliquez sur l'étoile en regard de celui que vous souhaitez définir comme certificat par défaut. MDaemon prend en charge l'extension Server Name Indication (SNI) du protocole TLS, ce qui permet d'utiliser un certificat différent pour chaque nom d'hôte de votre serveur. MDaemon examine les certificats actifs et choisit celui qui contient le nom d'hôte demandé dans le champ Subject Alternative Names (vous pouvez spécifier les noms alternatifs lors de la création du certificat). Si le client ne demande pas de Nom d'hôte, ou si aucun certificat correspondant n'est trouvé, le certificat par défaut est utilisé. Double-cliquez sur un certificat pour l'ouvrir dans la boîte de dialogue Certificat de Windows afin de l'examiner (disponible uniquement dans l'interface d'application, pas dans l'administration à distance basée sur le navigateur).

Supprimer

Sélectionnez un certificat dans la liste, puis cliquez sur ce bouton pour le supprimer. Une boîte de confirmation s'ouvre et vous demande si vous êtes sûr de vouloir supprimer le certificat.

Créer un certificat

Cliquez sur ce bouton pour ouvrir la boîte de dialogue Créer un certificat SSL.

Créer un certificat SSL	
Détails du certificat	
Nom d'hôte (ex. : wc.altn.com)	mail.company.test
Nom de l'organisation/entreprise	Example Corp
Autres noms d'hôtes (séparez plusi	ieurs entrées par des virgules)
Longueur de la clé de cryptage	2048 💌
Algorithme de hachage	SHA2
Pays/région	United States US 🔹
	OK Annuler

Détails du certificat

Nom d'hôte

Lors de la création d'un certificat, entrez le nom d'hôte auquel vos utilisateurs se connecteront (par exemple, "wc.example.com").

Nom de l'organisation/entreprise

Entrez ici le nom de l'organisation ou de la société qui "possède" le certificat.

Autres noms d'hôtes (séparez plusieurs entrées par des virgules)

Si les utilisateurs se connectent à d'autres noms d'hôte et que vous souhaitez que ce certificat s'applique également à ces noms, entrez ici ces noms de domaine en les séparant par des virgules. Les caractères joker sont autorisés, ainsi "*.example.com" s'applique à tous les sous-domaines de example.com (par exemple, "wc.example.com", "mail.example.com", etc.)

MDaemon prend en charge l'extension SNI (Server Name Indication) du protocole TLS, ce qui permet d'utiliser un certificat différent pour chaque nom d'hôte de votre serveur. MDaemon examine les certificats actifs et choisit celui qui contient le nom d'hôte demandé dans son champ À :. Si le client ne demande pas de Nom d'hôte, ou si aucun certificat correspondant n'est trouvé, le certificat par défaut est utilisé.

Longueur de clé de cryptage

Choisissez la longueur de clé de cryptage souhaitée pour ce certificat. Plus la clé de cryptage est longue, plus les données transférées sont sécurisées. Notez toutefois que toutes les applications ne prennent pas en charge des longueurs de clé supérieures à 512.

Pays/région

Choisissez le pays ou la région dans lequel votre serveur réside.

Algorithme de hachage

Choisissez l'algorithme de hachage que vous souhaitez utiliser : SHA1 ou SHA2. Le paramètre par défaut est SHA2.

Redémarrer les serveurs Web

Cliquez sur ce bouton pour redémarrer le serveur Web. Le serveur Web doit être redémarré avant qu'un nouveau certificat ne soit utilisé.

Utiliser Let's Encrypt pour gérer votre certificat

Let's Encrypt est une autorité de certification (AC) qui fournit des certificats gratuits via un processus automatisé conçu pour éliminer le processus actuellement complexe de création, de validation, de signature, d'installation et de renouvellement manuels des certificats pour les sites web sécurisés.

Dans le cadre de l'utilisation du processus automatisé de Let's Encrypt pour gérer un certificat, l' écran Let's Encrypt [632] est fourni pour vous aider à configurer et à exécuter facilement le script PowerShell inclus dans le dossier "MDaemon\LetsEncrypt". L'exécution du script permet de tout configurer pour Let's Encrypt, y compris de placer les fichiers nécessaires dans le dossier HTTP du Webmail pour relever le défi http-01. Il utilise le nom d'hôte SMTP [187] du domaine par défaut [184] comme domaine pour le certificat, inclut tout *autre nom d'hôte que* vous avez spécifié, récupère le certificat, l'importe dans Windows et configure MDaemon pour qu'il utilise le certificat pour MDaemon, Webmail et Remote Admin. Dans le dossier "MDaemon\Logs\",

le script crée un fichier journal appelé LetsEncrypt.log. Ce fichier journal est supprimé et recréé à chaque fois que le script est exécuté, et il inclut la date et l'heure début du script. De plus, des e-mails de notification seront envoyés lorsque des erreurs se produisent si vous spécifiez un *E-mail de l'administrateur pour les notifications*. Voir la rubrique Let's Encrypt

Voir :

SSL et certificats 613

Créer et utiliser des certificats SSL 974

3.6.1.4 MDIM

Services web, & MI - MDIM Webmail Serveur Web SSL & HTTPS Calendrier RelayFax Dropbox Paramètres MDaemon Remote Admin Conditions d'utilisation Liens vers les pièces jointes CalDAV & CardDAV XMPP	MDaemon Instant Messenger (MDIM) par défa MDIM fournit un accès rapide aux e-mails, di d'autres services via Webmail et XMPP. Activer MDIM (active Webmail) Activer la messagerie instantanée Les utilisateurs de la messagerie instantan domaines MDaemon dans leurs listes de Autoriser les transferts de fichiers dans M Les rappels de la messagerie instantanée sont envoyés par (From) :	aut ossiers, messages instantanés et à née visualisent tous les contacts Daemon Instant Messenger MDaemon	
	ОК	Annuler Appliquer Ai	de

Cet écran contrôle les paramètres par défaut de <u>MDaemon Instant Messenger</u> (<u>MDIM</u> [335]) pour les nouveaux domaines. Les paramètres de domaines spécifiques peuvent être modifiés via l'écran MDIM du Gestionnaire de domaines. Les services de MDaemon Instant Messenger peuvent être activés ou désactivés pour des comptes ou des groupes spécifiques via les écrans<u>Services Web</u> [771] et <u>Propriétés du groupe</u> [838] respectivement.

MDaemon Instant Messenger (MDIM)

Activer MDIM (active le Webmail)

Activez cette option si vous souhaitez que MDaemon Instant Messenger puisse être téléchargé par défaut à partir de Webmail. Les utilisateurs peuvent le télécharger à

partir de la page *Options* | *MDaemon Messagerie instantanée.* Le fichier d'installation téléchargé sera automatiquement personnalisé pour lecompte de chaque utilisateurafin de faciliter l'installation et la configuration. Cette option permet également à MDIM d'utiliser les fonctionnalités de Dossiers de courrier, ce qui permet aux utilisateurs de vérifier la présence de nouveaux courriers électroniques et d'ouvrir le Webmail directement à partir du menu contextuel de MDIM. MDIM est activé par défaut.

Activer la messagerie instantanée

Par défaut, les comptes peuvent utiliser MDIM et des clients XMPP witiers pour envoyer des messages instantanés aux autres membres de leur domaine. Décochez cette case si vous ne souhaitez pas autoriser la messagerie instantanée par défaut.

Les utilisateurs de la messagerie instantanée visualisent tous les domaines MDaemon et leurs listes de contacts.

Cochez cette option si vous souhaitez que vos utilisateurs puissent ajouter par défaut des contacts à leur liste d'amis à partir de tous vos domaines MDaemon. Lorsque cette option est désactivée, les contacts doivent se trouver sur le même domaine. Exemple : si MDaemon héberge le courrier de example.com et de example.org, l'activation de cette option permet aux utilisateurs d'ajouter des contacts de messagerie instantanée à partir des deux domaines. Désactivés, les utilisateurs de exemple.com ne peuvent ajouter que d'autres utilisateurs de exemple.com, et exemple.org ne peut ajouter que exemple.org. Cette option est désactivée par défaut. Une option équivalente dans le <u>Gestionnaire de domaines</u> permet d'activer ou de désactiver cette fonctionnalité pour des domaines spécifiques.

Autoriser les transferts de fichiers dans MDaemon Instant Messenger

Non (par défaut), les utilisateurs de MDIM peuvent transférer des fichiers à leurs contacts MDIM. Décochez cette case si vous ne souhaitez pas que MDIM soit utilisé pour transférer des fichiers.

Activer la synchronisation de la liste d'amis

Utilisez cette option pour remplir automatiquement les listes d'amis des utilisateurs pour le domaine. Ce paramètre est également disponible <u>par domaine</u> [193].

Les rappels de messagerie instantanée sont envoyés par ('From')

Lorsqu'un rendez-vous est programmé dans le calendrier du MDaemon Webmail d'un utilisateur, l'événement peut être configuré pour envoyer un rappel à l'utilisateur à une heure spécifiée. Si le système de messagerie instantanée est actif pour le domaine de l'utilisateur, le rappel sera envoyé dans un message instantané à l'utilisateur. Utilisez ce texte pour spécifier le nom du destinatairedumessage. Il s'agit du paramètre par défaut pour les nouveaux domaines. Vous pouvez le modifier pour des domaines spécifiques via l' <u>écran</u> (1931) MDaemon Instant Messenger du Gestionnaire de domaines.

Voir :

<u>Gestionnaire de domaines | Gérer la MDaemon Instant Messenger</u>

3.6.1.5 Calendrier

🧐 Services web, & MI - Calendrier	
	Paramètres par défaut du calendrier Paramètres par défaut du calendrier C Envoyer des rappels pour le calendrier et les tâches Y compris aux utilisateurs de MDaemon Connector Premier jour de la semaine Dimanche Service de disponibilité Activer le service de disponibilité (active Webmail) Pour utiliser la planification avec Outlook, ce dernier doit être configuré pour envoyer une requête à l'URL : http:///Serveur Webmail><:Port>/Worldclient.dll? view=fbinfo&user= %NAME%@%SERVER% Remplacez <serveur webmail=""> par l'IP ou le nom de votre serveur Webmail. Mot de passe Le mot de passe doit être ajouté à l'URL (ex. : &password=secret) Autoriser les utilisateurs à consulter les disponibilités des 3 prochains mois</serveur>
	OK Annuler Appliquer Aide

Cet écran contrôle les paramètres par défaut des fonctions de calendrier de MDaemon. Les paramètres de certains domaines peuvent être filtrés par l'écran Calendrier du Gestionnaire de domaines.

Paramètres par défaut du calendrier

Envoyer des rappels pour le calendrier et les tâches

Cochez cette case si vous souhaitez queles rappels du calendrier et des tâches duWebmailsoient envoyés à vos utilisateurs par courrier électronique et par la messagerie instantanée de MDaemon. Messagerie instantanée de MDaemon.

... même aux utilisateurs MDaemon Connector

Si vous avez activé l'option "*Envoyer des rappels pour le calendrier et les tâches*" cidessus, cliquez sur cette option si vous souhaitez également activer les rappels pour les utilisateurs<u>MDaemon Connector</u> 409.

Premier jour de la semaine

Choisissez un jour dans la liste déroulante. Le jour sélectionné apparaîtra dans les calendriers comme le premier jour de la semaine.

Non (par défaut) Planification par défaut

MDaemon comprend un serveur Free/Busy, qui permet à un organisateur de réunion de voir la disponibilité des participants potentiels à une réunion. Pour accéder à cette fonctionnalité, cliquez sur Planification dans le Webmail lorsque vous créez un nouveau rendez-vous. Une fenêtre de planification s'ouvre alors, contenant la liste des participants et une grille de calendrier codée par couleur avec une ligne pour chacun d'entre eux.La ligne de chaque participantest codée par couleur pour indiquer les heures auxquelles il pourrait être disponible pour une réunion. Les couleurs correspondent à Occupé, Provisoire, Absent du bureau et Pas d'information. Il existe également un boutonAuto-Pick Next qui vous permet d'interroger le serveur pour connaître le prochain créneau horaire auquel tous les participants peuvent être disponibles. Lorsque vous avez terminé de créer le rendez-vous, une invitation est envoyée à tous les participants, qui peuvent alors l'accepter ou la refuser.

Le serveur Free/Busy deWebmailest également compatible avec Microsoft Outlook. Pour l'utiliser, configurez Outlook de manière à ce qu'il interroge l'URL mentionnée cidessous pour obtenir les données Free/Busy. Dans Outlook 2002, par exemple, les options Free/Busy se trouvent sous "Outils | Options | Options de calendrier... | Options Free/Busy..."

URL du serveur Free/Busy pour Outlook :

```
http://<Webmail><:Port>/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

Remplacez"<Webmail>" par l'adresse IP ou le nom de domaine de votre serveur Webmail, et"<:Port>" par le numéro de port (si vous n'utilisez pas le port Web par défaut).Exemple :

http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%0%
SERVER%.

Pour en savoir plus sur la manière d'utiliser lesfonctions Free/Busy deWebmailpour planifier vos rendez-vous, consultez le système d'aide en ligne de Webmail.

Activer les services de planification

Cliquez sur cette option si vous souhaitez donner accès aux fonctionnalités du serveur Free/Busy aux utilisateurs.

Mot de passe Free/Busy

Si vous souhaitez demander un mot de passe lorsque les utilisateurs tentent d'accéder aux fonctions du serveur Free/Busy via Outlook, indiquez le mot de passe ici. Ce mot de passe doit être ajouté à l'URL mentionnée ci-dessus (sous la forme :"&password=FBServerPass") lorsque les utilisateurs configurent leurs paramètres Free/Busy dans Outlook. Exemple : http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%0% SERVER%&password=MyFBServerPassword

Permettre aux utilisateurs d'interroger X mois de données libres/occupés Utilisez cette option pour indiquer le nombre de mois de données Free/Busy que vos utilisateurs peuvent consulter.

Voir :

Gestionnaire de domaines | Calendrier

3.6.1.6 RelayFax

Avis de fin de vie

MDaemon Technologies a annoncé la fin de vie des ventes de son logiciel<u>RelayFax</u> à compter du 30 juin 2021. Les achats de nouvelles licences, de renouvellements ou de licences expirées ne sont plus disponibles. Les propriétaires de licences RelayFax existantes peuvent continuer à utiliser RelayFax, mais les mises à jour logicielles et l'assistance technique ne sont plus disponibles.

🧐 Services web, & MI - RelayFax	
Webmail Serveur Web SSL & HTTPS MDIM Calendrier RelayFax Dropbox Paramètres MDaemon Remote Admin Conditions d'utilisation Liens vers les pièces jointes CalDAV & CardDAV XMPP	RelayFax est une passerelle fax<->e-mail avec laquelle vous pouvez envoyer et recevoir des fax à partir de Webmail ou d'un client de messagerie traditionnel. Pour plus d'informations, consultez la page d'accueil RelayFax Autoriser les utilisateurs de Webmail à envoyer des fax via RelayFax Utiliser SMTP pour distribuer les télécopies à RelayFax Adresse e-mail du serveur RelayFax: © Distribuer directement les fax dans la file d'attente de RelayFax Chemin de la file d'attente (ne pas remplir si RelayFax est installé en local) : Parcourir
	OK Annuler Appliquer Aide

Le serveur RelayFax deMDaemon Technologies est une passerelle email-fax et fax-email qui peut être intégrée de manière transparente à Webmail afin de fournir ses services à vos utilisateurs. Lorsque cette fonctionnalité est activée, les utilisateurs de Webmail auront accès à diverses fonctions qui leur permettront de composer et d'envoyer des fax via les pages du client Webmail.



Cet écran de configuration de RelayFax n'est pas filtré par MDRA ou par l'application Session de configuration MDaemon, sauf si RelayFax est installé ou si le Webmail utilise RelayFax.

Options d'intégration de RelayFax

Permettre aux utilisateurs de Webmail de composer et d'envoyer des fax via RelayFax Cliquez sur cette option pour intégrer RelayFax au Webmail. Lorsqu'elle est activée, une commande "Composer un fax" et d'autres fonctions liées au fax apparaissent sur les pages du Webmail.

Utiliser SMTP pour distribuer les télécopies à RelayFax

RelayFax surveille une boîte aux lettres spécifique pour les messages entrants qui doivent être faxés. Cliquez sur cette option et MDaemon utilisera le processus normal de distribution SMTP pour envoyer ces messages à l'adresseélectronique de cette boîte aux lettres.Cette option est utile lorsque RelayFax surveille une boîte aux lettres située ailleurs que sur votre réseau local. Si RelayFax réside sur votre réseau, vous pouvez choisir de demander à MDaemon de livrer les messages directement dans lafile d'attente de RelayFaxet d'éviter ainsi le processus de livraison SMTP. Pour plus d'informations sur cette méthode, voir *Distribuer directement les fax dans la file d'attente deRelayFaxci-dessous*.

Adresse e-mail du serveur RelayFax

Indiquez l'adresse électronique à laquelle vous souhaitez que les messages destinés à la télécopie soient livrés. Cette valeur doit correspondre à l'adresse que vous avez configurée pour que RelayFax surveille ces messages.

Distribuer directement les fax dans la file d'attente de RelayFax

Si RelayFax réside sur votre réseau local, vous pouvez choisir cette méthode plutôt que le protocole SMTP pour distribuer les messages destinés à la télécopie. Lorsque MDaemon reçoit un message destiné à RelayFax, il est placé directement dans lafile d'attente des messages entrantsde RelayFaxau lieu d'être distribué par SMTP.

Chemin de la file d'attente du fax

Si RelayFax réside sur la même machine que MDaemon, vous pouvez laisser ce chemin d'accès vide. Sinon, vous devez spécifier le chemin réseau vers ledossier \app\ deRelayFax.

3.6.1.7 Dropbox

🧐 Services web, & MI - Dropbox		×
 Webmail Serveur Web SSL & HTTPS MDIM Calendrier RelayFax Dropbox Paramètres MDaemon Remote Admin Conditions d'utilisation Liens vers les pièces jointes CalDAV & CardDAV XMPP 	Intégration avec Dropbox Activer l'intégration avec Dropbox Les utilisateurs de Webmail peuvent enregistrer leurs pièces jointes directement dans leur compte Dropbox. Une clé d'application (App key) et un code secret d'application (App secret) sont pour cela nécessaires. Ces informations sont obtenues directement auprès de Dropbox, lors de l'enregistrement de MDaemon. Voir l'article 1166 de la base de connaissances pour plus d'informations. Clé d'application Dropbox Code secret d'application Dropbox En vous fournissant la clé d'application et le code secret, Dropbox vous demande une "URI de redirection". Utilisez cette valeur : https://mail.company.test/WorldClient.dll?View=DAuth&AuthRequest=Dropbox Dropbox exige qu'un lien vers une politique de confidentialité approuvée soit régulièrement fourni aux utilisateurs Modifier le texte de la politique de confidentialité	
	OK Annuler Appliquer Aid	te

Webmail est équipé d'un support direct pour Dropbox, qui permet à vos utilisateurs d'enregistrer des pièces jointes à leurs comptes Dropbox, et d'insérer des liens directs vers des fichiers Dropbox dans les messages sortants. Pour offrir cette fonctionnalité aux utilisateurs de votre Webmail, vous devez configurer votre Webmail en tant qu'application Dropbox sur la <u>plateforme Dropboxdevelopers</u>. Il s'agit d'une procédure simple, qui vous demande seulement de vous connecter à un compte Dropbox, de créer un Nom complet pour une application avec un accès total à Dropbox, de spécifier l'URI de redirection vers le Webmail, et de modifier un paramètre par défaut. Dans un second temps, vous copierez et collerez la Clé d'application d'Dropbox et le Secret d'application Dropbox dans les options de cet écran dans MDaemon. Après cela, vos utilisateurs pourront lier leurs comptes Dropbox à Webmail lors de leur prochaine connexion à Webmail. Pour des instructions pas à pas sur la façon de créer votre application Dropbox et de la lier à Webmail, voir : <u>Création et liaison de votre application</u> <u>DropboxCréation</u> d'

Lorsque vous créez votre application Dropbox, elle a initialement le statut "Développement". Cela permet à un maximum de 500 utilisateurs de votre webmail de lier leurs comptes Dropbox à l'application. Selon Dropbox, "une fois que votre application aura relié 50 utilisateurs Dropbox, vous disposerez de deux semaines pour demander et recevoir l'approbation du statut "Production" avant que la capacité de votre application à relier d'autres utilisateurs Dropbox ne soit figée, quel que soit le nombre d'utilisateurs entre 0 et 500 que votre application aura reliés". Cela signifie que l'intégration avec Dropbox continue de fonctionner, mais qu'aucun utilisateur supplémentaire ne pourra être relié à ses comptes. L'obtention de l'autorisation de production est un processus simple qui permet de s'assurer que votre application est conforme aux directives et aux conditions d'utilisation de Dropbox. Pour plus d'informations, consultez la section Approbation de la production du <u>guide du développeur de la plateforme Dropbox</u>.

Dans votre application Webmail créée et configurée correctement, chaque utilisateur de Webmail aura la possibilité de connecter son compte à son compte Dropbox lorsqu'il se connectera à Webmail. Dans ce cas, l'utilisateur doit se connecter à Dropbox et autoriser l'application à accéder à son compte Dropbox. Ensuite, l'utilisateur sera redirigé vers Webmail en utilisant un URI qui a été transmis à Dropbox au cours de la procédure d'authentification. Pour des raisons de sécurité, cet URI doit correspondre à l'un des URI de redirection (voir ci-dessous) que vous avez spécifiés <u>surinformation de</u> <u>votre application</u> à Dropbox.com. Enfin, Webmail et Dropbox échangeront un code d'accès et une clé d'accès, qui permettront à Webmail de se connecter au compte Dropbox de l'utilisateur afin que ce dernier puisse y enregistrer des pièces jointes. Le jeton d'accès échangé expire tous les sept jours, ce qui signifie que périodiquement l'utilisateur doit réautoriser son compte pour utiliser Dropbox. Les utilisateurs peuvent également déconnecter manuellement leur compte de Dropbox, ou le réautoriser si nécessaire, à partir de l'écran des options Cloud Apps dans Webmail.

Intégration avec Dropbox

Activer l'intégration avec Dropbox

Une fois que vous avez créé votre application Dropbox et que vous l'avez liée à Webmail, cochez cette case pour permettre aux utilisateurs de votre Webmail d'établir un lien avec leurs comptes Dropbox. Si vous souhaitez activer ou désactiver Dropbox pour chaque utilisateur, vous pouvez le faire en ajoutant "DropboxAccessEnabled=Yes (OU No)" au fichier User.ini.

Clé d'application secret d'application Dropbox

La Clé d'application secret d'application Dropbox se trouve sur la <u>information de</u> <u>votre application</u> à Dropbox.com. Saisissez-les ici pour lier le Webmail à votre application Dropbox.

URI de redirection

Vous devez spécifier un URI de redirection sur la <u>information application</u> sur Dropbox.com. MDaemon affiche automatiquement un URI que vous pouvez utiliser. Vous pouvez cependant ajouter plusieurs URI de redirection. Dans ce cas, vous pouvez ajouter un URI pour chacun de vos domaines et même un URI pour localhost, qui peut être utilisé pour se connecter au Webmail à partir de la machine sur laquelle tourne le serveur.

Exemple :

```
https://mail.company.test/WorldClient.dll?
View=OAuth&AuthRequest=Dropbox
https://example.com/WorldClient.dll?
View=OAuth&AuthRequest=Dropbox
```

https://localhost/WorldClient.dll?View=OAuth&AuthRequest=Dropbox

Dropbox exige que les URI de redirection soient sécurisés, c'est pourquoi <u>HTTPS</u> [342] doit être activé pour le Webmail.

Modifier la politique de confidentialité

Cliquez sur ce bouton pour modifier le fichier texte contenant la politique de confidentialité de votre application Webmail. Dropbox exige qu'une politique privée approuvée soit régulièrement fournie aux utilisateurs. Un lien "Politique privée" vers le contenu de ce fichier est donc fourni sur la page**Connexion à Dropbox** affichée aux utilisateurs. Ce lien ouvre une petite fenêtre contenant le texte et un bouton Télécharger sur lequel les utilisateurs peuvent cliquer pour télécharger le fichier. Rédigez en HTML dans le fichier si vous souhaitez mettre en forme le texte ou si vous voulez qu'il contienne des liens.

Créer et lier votre application Dropbox

Instructions étape par étape pour créer votre application Dropbox et la lier au Webmail.

- 1. Dans votre navigateur, accédez à Dropbox PlatformDropbox.
- 2. Connexion à votre compte Dropbox
- 3. Choisissez Dropbox API
- 4. Choisissez Full Dropbox
- 5. Donnez un nom unique à votre application.
- 6. Cliquez sur Créer une application.
- 7. Cliquez sur Activer les utilisateurs supplémentaires, puis sur OK.
- 8. Remplacez Allow implicit grant par Disallow
- Saisissez un ou plusieurs URI de redirection, en cliquant sur Ajouter après chacun d'eux. Il doit s'agir d'URL sécurisées vers votre Webmail (HTTPS doit être activé dans le Webmail).

Exemple :

https://mail.company.test/WorldClient.dll?View=OAuth&AuthRequest=Dropbox

https://localhost/WorldClient.dll?View=OAuth&AuthRequest=Dropbox

- 10. En laissant votre navigateur ouvert sur la page d'information de votre application, ouvrez l'interface graphique de MDaemon.
- 11. Cliquez sur **Configuration**
- 12. Cliquez sur Services Web & IM
- 13. Cliquez sur Dropbox sous Webmail
- 14. Copiez/collez la Clé d'application d'application et le Code secret d'applicationDropbox depuis votre navigateur vers l' écranDropbox de MDaemon.
- 15. Cliquez sur Appliquer
- 16. Cliquez sur OK

Pour obtenir des instructions sur la liaison d'un compte d'utilisateur Webmail au compte Dropbox de l'utilisateur, consultez le système d'aide en ligne dans Webmail, ou consultez l'article de la Base connaissances de MDaemon : <u>Comment activer et</u> <u>configurer l'intégration avec Dropbox et utiliser les fonctionnalités de Dropbox dans</u> <u>Webmail ?</u>

3.6.1.8 Google Drive

Cette page est uniquement disponible dans l'interface web de<u>MDaemon Remote Admin</u> [376] (MDRA).

Intégration de Google Drive

Le MDaemon Webmail peut présenter aux utilisateurs des options leur permettant d'enregistrer les pièces jointes des messages directement sur leur compte Google Drive, ainsi que de modifier et de travailler avec les documents qui y sont stockés. Pour ce faire, une clé API, un ID client et un Code secret client sont nécessaires. Vous pouvez les obtenir directement auprès de Google en créant une application à l'aide de la console API de Google et en enregistrant votre MDaemon auprès de leur service. Un composant d'authentification OAuth 2.0 fait partie de cette application, qui permet à vos utilisateurs de Webmail de se connecter à Webmail, puis d'autoriser l'accès à leur compte Google Drive via MDaemon. Une fois autorisés, les utilisateurs peuvent consulter leurs dossiers et fichiers qui se trouvent dans Google Drive. En outre, ils peuvent charger, télécharger, déplacer, copier, renommer et supprimer des fichiers, ainsi que copier/déplacer des fichiers vers et depuis les dossiers de documents locaux. Si l'utilisateur souhaite modifier un document, il lui suffit de cliquer sur l'option d'affichage du fichier dans Google Drive pour pouvoir y apporter des modifications conformément aux autorisations définies dans Google Drive. Le processus de configuration de Google Drive est similaire aux fonctionnalités d'Intégration avec Dropbox 352 et d' Intégration OAuth pour MultiPOP 144 de MDaemon .

Activer l'intégration de Google Drive

Cochez cette case pour activer l'intégration de Google Drive. Voir : <u>Création et</u> <u>liaison de votre application Google Drive</u> ci-dessous.

Clé d'API Google Drive :

Il s'agit de votre clé API unique qui sera générée pour vous dans la console API Google Drive pendant que vous créez votre app. Copiez et collez la clé ici.

ID client de Google Drive

Il s'agit de l'ID client unique attribué à votre application Google Drive lorsque vous la créez dans la console API de Google. Après avoir créé votre app, copiez son ID client et collez-le ici.

Code secret client Google Drive

Il s'agit du Code secret client unique attribué à votre application Google Drive lorsque vous la créez dans la Google API Console. Après avoir créé votre application, copiez son Code secret client et collez-le ici.

URI de redirection

Vous devez spécifier un ou plusieurs URI de redirection lors de la création de votre application Google Drive. L'exemple d'URI de redirection est construit à partir du <u>nom</u> <u>d'hôte SMTP</u> 187 de votre Domaine par défaut 184 - 187 *** 187, qui devrait fonctionner pour les utilisateurs de ce domaine lorsqu'ils se connectent au Webmail. Vous devez ajouter d'autres Connexions à MDaemon Webmail à votre application pour tous les autres domaines MDaemon auxquels vos utilisateurs accèdent lorsqu'ils se connectent à Webmail. Exemple :"https://mail.example.com/WorldClient.dll? View=OAuth&AuthRequest=GoogleDrive" fonctionnera pour tous les utilisateurs qui se connectent à mail.example.com lorsqu'ils se connectent à Webmail. Voir : **Création et liaison de votre application Google Drive** ci-dessous pour plus d'informations.

Modifier la politique de confidentialité

L'intégration de Google Drive exige que vous présentiez régulièrement aux utilisateurs un lien vers une politique de confidentialité approuvée. Cliquez sur ce bouton pour modifier vos règles de confidentialité.

Création et liaison de votre application Google Drive

Instructions étape par étape pour créer votre application Google Drive.

- Suivez les étapes ci-dessous pour créer une application Google afin de permettre aux utilisateurs d'accéder à leur Google Drive au sein de Webmail sur la page**Documents.**
- 1. Connectez-vous à <u>MDaemon Remote Admin</u> and et allez sur la page Google Drive (située sous Main | Paramètres Webmail), et activez l'option**Activer l'intégration de Google Drive**.
- 2. Dans un autre onglet du navigateur, connectez-vous à votre Mon compte Google et accédez à la <u>console Google Google</u>.
- 3. Si vous êtes sur la liste des projets, cliquez sur **NOUVEAU PROJET**, ou si vous êtes sur la <u>page Gérer les Gérer les</u>, cliquez sur **(+) CRÉER UN PROJET**.
- 4. Saisissez un nom de projet, par exemple "Google Drive pour MDaemon", puis cliquez sur Modifier si vous souhaitez modifier l'ID du projet, ou laissez la valeur par défaut. Remarque : l 'ID du projet ne peut pas être modifié après la création du projet.
- 5. Si vous disposez d'une <u>OrganisationOrganisation</u>, choisissez-la dans **Emplacement**. Sinon, laissez la valeur "Pas d'organisation".
- 6. Une fois le projet chargé, cliquez sur + ACTIVER LES APIS ET LES SERVICES.
- 7. Dans le champ de recherche, tapez "Google Drive", sélectionnez l'**API Google Drive**, puis cliquez sur **Activer**.
- 8. Dans le volet de gauche, sous **API et services**, cliquez sur **Informations d'identification**.
- Dans le haut de la page, cliquez sur + Créer des informations d'identification, puis sélectionnez Clé API dans le menu déroulant.

- Copiez votre clé API (une icône Copier dans le presse-papiers se trouve à côté).
- 11. Basculez dans l'onglet MDaemon de votre navigateur et collez-la dans le champ**Clé d'API Google Drive** de la page Google Drive dans MDaemon (ou enregistrez-la ailleurs si vous souhaitez le faire plus tard).
- 12. Dans le volet de gauche, sous **API et services,** cliquez sur **Écran de consentement OAuth**.
- 13. Sous Type d'utilisateur, sélectionnez Externe, puis cliquez sur Créer. Remarque : si vous disposez d'une <u>OrganisationOrganisation</u>, ou en fonction du statut de publication de votre application, choisir Interne peut s'avérer un meilleur choix. Voir la note sur le<u>statut de publication</u> selection d'informations.
- 14. Saisissez le nom de l'application (par exemple, Google Drive pour Webmail), une adresse électronique d'assistance à laquelle les utilisateurs peuvent s'adresser et une adresse électronique de développeur à laquelle Google peut s'adresser en cas de modification de votre projet. C'est tout ce qui est requis sur cette page pour la configuration, mais en fonction de votre organisation particulière ou des exigences de vérification, vous pouvez également saisir le logo de votre entreprise et les liens vers vos conditions d'utilisation at votre politique de confidentialité (voir ci-dessus). Les champs " Domaine" seront remplis automatiquement lorsque vous ajouterez les URI de redirection dans une étape ultérieure. Remarque : ces informations sont utilisées pour l'écran de consentement qui sera présenté aux utilisateurs pour autoriser Webmail à accéder à leur Google Drive.
- 15. Cliquez sur **Enregistrer et continuer**.
- 16. Cliquez sur Ajouter ou supprimer des champs d'application et copiez/collez les URI ci-dessous (vous pouvez les copier/coller tous en même temps) dans la case située sous "Ajouter manuellement des champs d'application", puis cliquez sur Ajouter au tableau.

```
https://www.googleapis.com/auth/userinfo.email
https://www.googleapis.com/auth/drive.file
https://www.googleapis.com/auth/drive
https://www.googleapis.com/auth/drive.readonly
https://www.googleapis.com/auth/drive.metadata
https://www.googleapis.com/auth/drive.photos.readonly
https://www.googleapis.com/auth/drive.activity.readonly
https://www.googleapis.com/auth/drive.activity.readonly
https://www.googleapis.com/auth/drive.activity.readonly
```

- 17. Cliquez sur **Save and Continue**.
- 18. Sous Test Users (Utilisateurs de test), cliquez sur **ADD USERS** (**Ajouter des utilisateurs**), saisissez chaque compte Google auquel Google Drive MDaemon accèdera par le biais de cette application, puis cliquez sur **ADD** (voir la note cidessous concernant le <u>statut de publication</u> de votre application).
- 19. Cliquez sur Enregistrer et continuer.
- 20. Dans le Résumé, cliquez sur **RETOUR AU TABLEAU DE BORD** en bas de la page.

- 21. Dans le volet de gauche, cliquez sur **Credentials**, cliquez sur **(+) Create Credentials** et sélectionnez **OAuth client ID**.
- 22. Dans la liste déroulante "Type d'application", sélectionnez Application Web, et sous "URI de redirection autorisés", cliquez sur + AJOUTER DES URI. Saisissez l'URI de redirection. L'URI de redirection affiché sur la page Google Drive dans MDaemon est un exemple construit à partir du nom d'hôte SMTP 187 de votre Domaine par défaut 184 187 *** 187, qui devrait fonctionner pour les utilisateurs de ce domaine lorsqu'ils se connectent à Webmail. Vous devez ajouter des Connexions à MDaemon Webmail pour tous les autres domaines de MDaemon auxquels vos utilisateurs se connectent. Exemple :"https://mail.example.com/WorldClient.dll? View=OAuth&AuthRequest=GoogleDrive" fonctionnera pour tous les utilisateurs qui se connectent à mail.example.com lorsqu'ils se connectent à Webmail. Si vous hébergez également un domaine appelé "mail.company.test", vous devrez également saisir un URI de redirection pour ce domaine, c'est-à-dire "https://mail.company.test/WorldClient.dll? View=OAuth&AuthRequest=GoogleDrive".
- 23. Cliquez sur **CREATE**.
- 24. Copiez les valeurs de **Votre ID client** et de **Votre Code secret client** dans les champs*ID client Google Drive* et *Code secret client Google Drive* de la page Google Drive dans MDaemon. Vous pouvez également saisir votre Clé d'API Google Drive si vous ne l'avez pas fait précédemment.

État de la publication - Ces instructions concernent la création d'une application Google dont l'<u>état de la publicationPlus</u> <u>d'informations</u> est défini sur "**Test**". Pour ce faire, vous devez ajouter chaque compte Google spécifique qui utilisera l'application pour accéder à son Google Drive, et ce nombre est limité à 100 utilisateurs. De plus, dans le MDaemon Webmail, lorsqu'il est demandé aux utilisateurs d'autoriser MDaemon à accéder à Google, un message d'alerte s'affiche "pour confirmer que l'utilisateur a un accès de test à votre projet, mais qu'il doit tenir compte des risques associés à l'autorisation d'accès à ses données à une application non vérifiée". Cette autorisation expire au bout de sept jours, ce qui signifie que chaque utilisateur doit réautoriser l'accès à Google toutes les semaines.

Si vous souhaitez supprimer ces exigences et limitations, vous devez alors changer votre statut en "**En production**", ce qui peut nécessiter ou non de changer votre type d'utilisateur d'externe à interne, de passer par un processus de vérification de l'app, ou les deux. Pour plus d'informations sur la vérification des applications et le statut de publication, consultez les articles suivants de Google : Filtrerpar l'écran de consentement Google et FAQ sur la vérification de l'API Google.

Autorisation de Google Drive dans le webmail

Dans le cas où vous avez créé votre application Google Drive et configuré la page Google Drive de MDaemon selon les instructions ci-dessus, chaque utilisateur qui souhaite accéder à son Google Drive dans le MDaemon Webmail doit d'abord en autoriser l'accès. Pour ce faire, chaque utilisateur doit

- 1. Se connecter à Webmail.
- 2. Cliquez sur l'icône Options dans le coin supérieur droit, puis cliquez sur Apps cloud.
- 3. Cliquez sur **Configurer Google Drive** (une page**OAuth 2.0 s** 'ouvre alors).
- 4. Cliquez sur **Connexion à Google Drive**.
- 5. Si l'utilisateur n'est pas connecté, Google Drive lui demandera des informations de connexion ou de choisir un compte.
- Il se peut qu'un message d'avertissement s'affiche, indiquant que "Google n'a pas vérifié cette application". Vous avez accès à une application en cours de test. Ne continuez que si vous connaissez le développeur qui vous a invité". Cliquez sur **Continuer**.
- 7. Sélectionnez les fonctionnalités de Google Drive auxquelles le webmail pourra accéder, puis cliquez sur **Continuer**.
- 8. Une page finale s'affiche, indiquant que MDaemon est désormais connecté à Google Drive. Ils peuvent alors fermer cette fenêtre.
- 9. Ils peuvent alors accéder à Google Drive à partir de leur page**Documents** dans Webmail.

Voir :

OAuth pour MultiPOP 144 Intégration avec Dropbox 352

3.6.1.9 OneDrive

Cette page est uniquement disponible dans l' interface web de<u>MDaemon Remote Admin</u> [376] (MDRA).

Intégration OneDrive

La fonctionnalité Intégration avec OneDrive est similaire aux fonctionnalités <u>Google</u> <u>Drive</u> **Dropbox Dropbox Dropbox** composant d'authentification OAuth 2.0 fait partie de cette appli, qui permet aux utilisateurs de votre Webmail de se connecter à OneDrive, puis d'autoriser l'accès à leur compte OneDrive Work ou School par le biais de MDaemon. Une fois autorisés, les utilisateurs peuvent consulter leurs dossiers et fichiers qui se trouvent dans OneDrive. En outre, ils peuvent charger, télécharger, déplacer, copier, renommer et supprimer des fichiers, ainsi que copier/déplacer des fichiers vers et depuis les dossiers de documents locaux. Si l'utilisateur souhaite modifier un document, un clic sur l'option d'affichage du fichier dans OneDrive lui permettra d'y apporter des modifications conformément aux autorisations définies dans OneDrive. Le processus de configuration de OneDrive est similaire à la fonctionnalité d'intégration OAuth pour MultiPOP

Activer l'intégration OneDrive

Cochez cette case pour activer l'intégration OneDrive. Voir : **Créer et lier votre application OneDrive OAuth** ci-dessous.

Identifiant Client OneDrive

Il s'agit de l'ID client unique attribué à votre appli OneDrive lorsque vous la créez dans Microsoft Azure. Après avoir créé votre app, copiez son ID client et collez-le ici.

Code Client OneDrive

Il s'agit du Code secret client unique attribué à votre application OneDrive lorsque vous la créez dans Azure. Après avoir créé votre application, copiez son Code secret client et collez-le ici.

URI de redirection

Vous devez spécifier un ou plusieurs URI de redirection lors de la création de votre application OneDrive. L'exemple d'URI de redirection est construit à partir du <u>nom</u> <u>d'hôte SMTP</u> <u>application</u> <u>application</u>

View=OAuth&AuthRequest=OneDrive" fonctionnera pour tous les utilisateurs qui se connectent à mail.example.com lorsqu'ils se connectent à Webmail.

Modifier la politique de confidentialité

L'intégration de OneDrive exige que vous présentiez périodiquement aux utilisateurs un lien vers une politique de confidentialité approuvée. Cliquez sur ce bouton pour modifier votre politique de confidentialité.

Créer et lier votre application OneDrive OAuth

Instructions étape par étape pour créer votre application OneDrive OAuth 2.0.

Microsoft OneDrive

Suivez les étapes ci-dessous pour créer une application Microsoft Azure afin de permettre à Webmail de s'authentifier à l'aide d'OAuth 2.0 lors de la connexion de vos utilisateurs à OneDrive.
- Accédez à la page <u>Microsoft AzureMicrosoft</u> du portail Azure et cliquez sur **App Registrations** dans le volet de gauche (vous devez vous inscrire à un compte Azure gratuit ou payant si vous n'en avez pas déjà un).
- 2. Cliquez sur + New Registration.
- Dans le champÀ : Par nom, entrez un nom d'application (par exemple, "OneDrive OAuth for Webmail").
- Pour "Types de comptes pris en charge", sélectionnez Comptes dans n'importe quel répertoire d'organisation (Tout répertoire Azure AD -Multitenant).
- 5. Pour "URI de redirection", sélectionnez web, puis saisissez votre URI de redirection OneDrive . L'URI de redirection affiché sur l'écran OneDrive est un exemple construit à partir du nom d'hôte SMTP [187] *** [187] de votre Domaine défaut Domaine Domaine [184], qui devrait fonctionner pour les utilisateurs de ce domaine lors de la signature par Webmail. Vous devez ajouter d'autres Connexions à MDaemon Webmail à votre application pour tous les autres domaines de MDaemon auxquels vos utilisateurs accèdent lorsqu'ils se connectent à Webmail. Exemple :"https://mail.example.com/WorldClient.dll? View=OAuth&AuthRequest=OneDrive" fonctionnera pour tous les utilisateurs qui se connectent à mail.example.com lorsqu'ils se connectent à Webmail.
- 6. Cliquez sur **Enregistrer**.
- Notez l'ID de l'application (client) (un bouton "copier dans le presse-papiers" se trouve à côté). Vous pourrez retrouver cet identifiant plus tard en cliquant sur Vue d'ensemble dans le volet de gauche.
- Si vous devez ajouter des URI de redirection supplémentaires, cliquez sur le lien web Redirect URIs : 1 à droite. Cliquez sur Ajouter un URI et saisissez l'URI, en répétant l'opération si nécessaire, puis cliquez sur Enregistrer.
- 9. Cliquez sur **API Permissions** dans le volet de gauche.
- 10. Cliquez sur + Ajouter une autorisation.
- 11. Cliquez sur Microsoft Graph.
- 12. Cliquez sur Delegated Permissions (Autorisations déléguées).
- 13. Sous Autorisations OpenId, sélectionnez offline_access.
- 14. Faites défiler vers le bas jusqu'à **Fichiers** et sélectionnez toutes les autorisations répertoriées.
- 15. Faites défiler vers le bas jusqu'à **Utilisateur** et sélectionnez **Utilisateur.Lire**.
- 16. Cliquez sur **Ajouter des autorisations**.
- 17. Veillez à cliquer sur Accorder le consentement de l'administrateur pour % DOMAIN%.
- 18. Dans le volet de gauche, cliquez sur **Certificats & Secrets**.
- 19. Cliquez sur + Nouveau Code secret client.
- 20. Saisissez une description (par exemple, "Secret client pour l'application OneDrive OAuth").

- 21. Sélectionnez le délai d'expiration du secret client.
- 22. Cliquez sur Ajouter.
- 23. Notez le secret client généré dans le champ Valeur (il y a un bouton copier dans le presse-papiers à côté). REMARQUE : le secret client ne sera plus visible sur cette page il y aura une icôneSupprimer à côté de l'entrée pour que vous puissiez la supprimer et créer un nouveau secret client si nécessaire.
- 24. Saisissez les valeurs de l'Identifiant (client) de l'application et du Code secret client dans les champs**Identifiant client** et **Secret client de** la page OneDrive sous Paramètres en Webmail.

Utiliser OneDrive dans le webmail

Dans le cas où vous avez créé votre application OneDrive et configuré la page OneDrive de MDRA selon les instructions ci-dessus, chaque utilisateur qui souhaite accéder à son compte Microsoft OneDrive travail/école dans le Webmail doit d'abord autoriser l'accès à le faire. **Remarque :** Microsoft n'autorise pas les comptes personnels à se connecter à OneDrive par le biais de cette configuration. Seuls les comptes travail/école peuvent être utilisés ici.

Pour autoriser MDaemon à accéder à votre compte OneDrive de travail ou d'école :

- 1. Connectez-vous au thème Pro du Webmail.
- 2. Dans le coin supérieur droit, cliquez sur l'icône**Paramètres**.
- 3. Cliquez sur **Cloud Apps**.
- 4. Cliquez sur **Configurer OneDrive**.
- 5. Une boîte de dialogue OAuth 2.0 s'ouvre.
- 6. Cliquez sur **Connecter à OneDrive**.
- 7. Si vous n'êtes pas connecté, Microsoft OneDrive vous demandera vos informations de connexion.
- 8. Si vous êtes connecté, Microsoft OneDrive vous demandera si vous souhaitez accorder à MDaemon l'accès à votre compte Microsoft OneDrive.
- Lorsque vous fermez la boîte de dialogue OAuth 2.0, cette page se recharge peu après.

La connexion de votre compte MDaemon à votre compte Microsoft OneDrive vous permet de :

- Enregistrer les pièces jointes des messages sur Microsoft OneDrive.
- Télécharger des fichiers sur Microsoft OneDrive.
- Afficher une liste des dossiers Microsoft OneDrive dans la liste des dossiers.
- Supprimer et télécharger des fichiers situés dans les dossiers Microsoft OneDrive.

- Copier des fichiers depuis des dossiers MDaemon Document vers des dossiers Microsoft OneDrive.
- Copier et déplacer des fichiers des dossiers Microsoft OneDrive vers les dossiers MDaemon Document.

Limitations de OneDrive :

- Le glisser-déposer n'est pas disponible pour les dossiers OneDrive.
- Vous ne pouvez pas copier/déplacer de OneDrive vers Google Drive ou Dropbox, ou vice versa.
- Vous ne pouvez pas créer/supprimer des dossiers OneDrive.

Voir :

OAuth pour MultiPOP 144 Intégration avec Dropbox 352

3.6.1.10 Catégories



Les options de catégories se trouvent dans l'interface d'Administration Remote Admin de MDaemon, à l'endroit suivant : **Main | Paramètres de MDaemon Webmail | Catégories**.

Le MDaemon Webmail supporte les catégories pour les messages électroniques, les événements, les notes et les tâches dans les thèmes LookOut et WorldClient. Les utilisateurs peuvent ajouter la colonne Catégories à la liste des messages en allant dans "**Options | Colonnes**" et en cochant "**Catégories**" dans la section Liste des messages.

Dans la liste des messages, pour définir des catégories pour un ou plusieurs messages, sélectionnez les messages et cliquez avec le bouton droit de la souris sur l'un d'entre eux. Utilisez le menu contextuel pour définir la catégorie. Vous pouvez également ouvrir un message et définir une catégorie à l'aide de l'option de la barre d'outils.

Catégories

Dans la page Catégories de l'interface d'administration à distance de MDaemon, vous pouvez définir les Catégories du domaine, c'est-à-dire une liste fixe de catégories que les utilisateurs verront dans le Webmail mais qu'ils ne pourront ni modifier ni supprimer. Vous pouvez également créer la liste par défaut des Catégories personnelles qui seront affichées aux nouveaux utilisateurs.

Catégories de domaine

Les Catégories de domaine sont des catégories fixes qui ne peuvent pas être réorganisées, modifiées ou supprimées par vos utilisateurs. Dans l'option*Activer les catégories de domaine*, la liste apparaîtra en haut de la liste des catégories de votre

utilisateur dans le MDaemon Webmail. Vous pouvez réorganiser, modifier, supprimer ou créer de nouveaux Catégories de domaine à l'aide des options proposées.

Catégories personnelles

Il s'agit de la liste de catégories par défaut qui sera copiée dans les nouveaux comptes des utilisateurs du MDaemon Webmail. Les utilisateurs ont un contrôle total sur leur liste de catégories personnelles. Ils peuvent les réorganiser, les modifier, les supprimer et en créer de nouvelles. Si, toutefois, vous utilisez également des Catégories de domaine, ces catégories seront listées en haut pour chaque utilisateur et ne pourront pas être modifiées ou dupliquées par eux. Toute catégorie personnelle dont le nom correspond à une catégorie de domaine sera masquée. Si vous ne souhaitez pas autoriser les catégories personnelles, décochez la case **Les utilisateurs peuvent modifier les catégories personnelles**. Dans ce cas, seules les catégories de domaine seront affichées. Si l'option Catégories de domaine est également désactivée, aucune option de catégorie ne sera disponible pour les utilisateurs.



Dans les fichiers MDaemon dans lesquels les catégories et les traductions de catégories sont gérées, vous trouverez des informations plus détaillées :

MDaemon\WorldClient\CustomCategories.txt.

3.6.1.11 Paramètres

	Web & IM Services - Settings Webmail De WebServer L SSL & HTTPS T Oropbox De Settings Calendar Oropbox Settings CalDAV & CardDAV CalDAV & CardDAV XMPP M	fault Webmail Si anguage heme ate format Display time u Empty trash or Use advancer Save message Save message Block HTML ed Enable Passw Enable Remer Push client sig Allow user-cre Enable Al mes tessage listing si lessage listing re ogin failure 'Help	ettings en (English) WorldClient Tem/Zd/ZY sing AM/PM n exit d compose es to 'Sent' folder mages fitor when composing new mess ord recovery mber Me gnature sated signatures ssage features hows this many messages per p sfresh frequency (in minutes) o' text (can contain HTML code	Macros Send read confirmations? always never prompt sages 50 10 10
--	--	--	--	--

Cet écran désigne les paramètres par défaut de l'écran Paramètres Webmail du Gestionnaire par défaut - Domaine. Lorsqu'un utilisateur se connecte au Webmail, ces options régissent le fonctionnement initial des différentes fonctionnalités du Webmail pour cet utilisateur. La plupart de ces paramètres peuvent ensuite être personnalisés par l'utilisateur via les pages Options en page Webmail.

Non (par défaut) Paramètres de MDaemon Webmail

Langue

Utilisez la liste déroulante pour choisir la langue par défaut dans laquelle l'interface du Webmail s'affichera lorsque vos utilisateurs se connecteront pour la première fois au domaine sélectionné. Dans la page de Connexion au Webmail, les utilisateurs peuvent modifier leurs paramètres linguistiques personnels, ainsi que par le biais d'une option dans Options | Personnaliser dans le Webmail.

Utiliser par défaut la langue du navigateur

Lorsque cette case est cochée, la langue des utilisateurs du Webmail sera celle de leur navigateur au lieu de la *langue*par défaut ci-dessus. **Note :** Cette option n'est disponible que dans <u>MDRA</u> [376].

Thème

Dans cette liste déroulante, vous pouvez désigner le thème par défaut du Webmail qui sera utilisé par les utilisateurs lorsqu'ils se connectent pour la première fois. Les utilisateurs peuvent personnaliser le thème à partir de Paramètres | Personnaliser dans le Webmail.

Format de la date

Ce texte permet de définir le format des dates dans le Webmail. Dans le bouton*Macros*, vous pouvez afficher une liste de codes de macros qui peuvent être utilisés dans ce texte. Vous pouvez utiliser les macros suivantes dans cette commande :

- **%A** Nom complet du jour de la semaine
- %B Nom complet du mois
- %d Jour du mois (affiche "01-31")
- %m Mois (affiche "01-12")
- %y Année à 2 chiffres
- %Y Année à 4 chiffres

Exemple : "%m/%d/%Y" peut être affiché dans le Webmail comme "12/25/2011".

Macros

Cliquez sur ce bouton pour afficher la liste des codes macro pouvant être utilisés dans le *format Date*.

Envoyer des confirmations de lecture ?

Cette option régit la manière dont le Webmail répondra aux messages entrants qui contiennent une demande de confirmation de lecture.

toujours

Si cette option est sélectionnée, MDaemon enverra une notification à l'expéditeur indiquant que le message a été lu. L'utilisateur du Webmail qui a reçu le message ne verra aucune indication que la confirmation de lecture a été demandée ou a fait l'objet d'une réponse.

jamais

Choisissez cette option si vous souhaitez que le Webmail ignore les demandes de confirmation de lecture.

prompt

Choisissez cette option si vous souhaitez demander aux utilisateurs du Webmail s'ils doivent ou non envoyer une confirmation de lecture à chaque fois qu'un message qui en fait la demande est ouvert.

Afficher les horaires au format AM/PM

Cochez cette option si vous souhaitez que les horaires au format 12 AM/PM soient affichés dans le Webmail. Décochez la case si vous souhaitez utiliser une horloge de 24 heures. Les utilisateurs individuels peuvent modifier ce paramètre via l'option "*Afficher mes heures au format AM/PM*" située sur la page Options | Calendrier dans le Webmail.

Vider la corbeille en quittant

Cette option permet devider la corbeille de l'utilisateurlorsqu'il se déconnecte de Webmail. Les utilisateurs individuels peuvent modifier ce paramètre à partir de la page Paramètres | MDaemon Webmail.

Utiliser la rédaction avancée

Cochez cette case si vous souhaitez que les utilisateurs voient l'écran de composition avancée dans Webmail plutôt que l'écran de composition normal par défaut. Les utilisateurs individuels peuvent modifier ce paramètre à partir de la page Paramètres | Composer dans le Webmail.

Enregistrer les messages dans le dossier "Envoyés

Cliquez sur cette option si vous souhaitez qu'une copie de chaque message envoyé soit enregistrée dans le dossier Envoyés de votreboîte aux lettres. Les utilisateurs individuels peuvent modifier ce paramètre à partir de la pageParamètres de MDaemon Webmail" Composer ".

Options de blocage des images

Les options de blocage d'images peuvent être utilisées pour contribuer à la sécurité et à la prévention du spam, car de nombreux messages de spam contiennent des images avec des URL spéciales qui peuvent aider l'expéditeur à identifier des éléments sur le destinataire, tels que la validité de son adresse e-mail, sa localisation, l'heure à laquelle le message a été consulté, la plate-forme utilisée, etc. **Note :** Ces options (à l'exception de "Bloquer les images HTML") ne sont*disponibles* que*dans MDRA.*

Bloquer les images HTML distantes dans les courriers indésirables et les messages qui échouent à l'authentification DMARC, DNSBL ou SPF.

Activez cette case à cocher si vous souhaitez empêcher l'affichage automatique des images distantes dans les messages électroniques HTML du Webmail lorsque le message a échoué à l'authentification DMARC, DNSBL ou SPF. Dans ce cas, l'utilisateur doit cliquer sur la barre qui apparaît au-dessus du message dans la fenêtre du navigateur pour voir les messages des files.

Bloquer les images HTML

Activez cette case à cocher si vous souhaitez empêcher l'affichage automatique des images distantes lors de la consultation des messages HTML dans le Webmail. Dans le but de voir les messages des files, l'utilisateur doit cliquer sur la barre qui apparaît au-dessus du message dans la fenêtre du navigateur. Cette option est activée par défaut.

Toujours bloquer les images HTML distantes

Cette option est similaire à l'option"*Bloquer les images distantes HTML dans tous les messages*" ci-dessus, sauf que l'utilisateur n'a pas la possibilité d'afficher les messages. Dans le cas d'une réponse ou d'un transfert de message, elle empêche également l'affichage des images du message d'origine dans la vue de composition.

Conditions de Blocage des images

Note : Ces options ne sont disponibles que dans MDRA 376.

... sauf lorsque l'en-tête From correspond à un contact figurant dans les listes d'Expéditeurs autorisés du domaine ou de l'utilisateur.

Cochez cette case si vous ne voulez pas que les options de blocage des images s'appliquent lorsque l'en-tête From du message correspond à un contact de la liste Expéditeurs autorisés du domaine ou de l'utilisateur. Toutefois, si l'option "*Toujours Bloquer les images HTML distantes*" est activée, les messages provenant d'adresses figurant dans la liste des Expéditeurs autorisés de l'utilisateur verront leurs images distantes bloquées ; cette exception ne s'appliquera qu'aux messages provenant d'une personne figurant dans la liste des Acteurs **Actifs. Remarque :** Cette option n'est disponible que dans <u>MDRA</u> [376].

Bloquer également les images HTML intégrées

Utilisez cette option si vous souhaitez également appliquer les options de blocage d'images aux images en ligne/incorporées.

Désactivez les hyperliens dans les spams et les messages qui échouent à l'authentification DMARC, DNSBL ou SPF.

Non (par défaut), lorsqu'un message est signalé comme spam ou échoue à la vérification <u>DMARC</u> [560], <u>DNS-BL</u> [751] ou <u>SPF</u> [560], tous les hyperliens contenus dans le message sont désactivés. Décochez cette case si vous ne souhaitez pas désactiver les liens dans ces messages. **Remarque :** Cette option n'est disponible que dans <u>MDRA</u> [376].

...sauf lorsque l'en-tête From correspond à un contact figurant dans les listes d'Expéditeurs autorisés du domaine ou de l'utilisateur.

Cochez cette case si vous souhaitez exempter les messages marqués de la désactivation des hyperliens lorsque l'en-tête du message correspond à un contact figurant dans les listes d'Expéditeurs autorisés du domaine ou de l'utilisateur. **Note :** Cette option n'est disponible que dans MDRA

Utiliser l'éditeur HTML pour la rédaction des messages

Cochez cette case si vous voulez que les utilisateurs voient l'éditeur de composition HTML par défaut dans le Webmail. Ils peuvent contrôler eux-mêmes ce paramètre à partir de Paramètres | Composer dans Webmail.

Activer la récupération de mot passe

Si cette option est activée, les utilisateurs autorisés à modifier leur mot de passe [771] pourront saisir une autre adresse e-mail dans Webmail, à laquelle ils pourront envoyer un lien pour réinitialiser leur mot de passe s'ils l'oublient. Pour configurer cette adresse, les utilisateurs doivent saisir l'adresse e-mail de récupération du mot de passe et leur mot de passe actuel dans Webmail sur la page Options | Sécurité. Dans ce cas, le lien "Mot de passe oublié ?" sur la page de connexion au Webmail les conduira à une page de confirmation de l'adresse e-mail de secours. Si l'adresse est correcte, un e-mail sera envoyé avec un lien vers une page de modification du mot de passe. Cette fonction est Non (par défaut).

Vous pouvez activer ou désactiver cette option pour chaque utilisateur en ajoutant la clé suivante au fichier user.inid'un utilisateur de Webmail (par exemple, \Users\example.com\frank\WC\user.ini):

```
[Utilisateur]
```

EnablePasswordRecovery=Yes (ou "=No" pour désactiver l'option pour l'utilisateur).

Autoriser l'option Se souvenir de moi pour l'authentification en deux étapes

Dans le cas où un utilisateur utilise l'authentification à deux facteurs (2FA) pour se connecter au Webmail ou à Remote Admin, une option "Se souvenir de moi" est généralement disponible sur la page d'authentification 2FA. Cette option empêche le serveur de redemander l'authentification à deux facteurs à cet utilisateur pendant un certain nombre de jours (voir l'option "Enable Se souvenir de moi" ci-dessous). Effacez cette case à cocher si vous ne souhaitez pas afficher l'option 2FA Se souvenir de moi, ce qui signifie que tous les utilisateurs dont l'authentification 2FA est activée devront saisir un code 2FA à chaque fois qu'ils se connectent. **Note :** Cette option n'est disponible que dans l' interface web de<u>MDaemon Remote Admin</u> (MDRA) [376].

Activer Se souvenir de moi

Cochez cette case si vous souhaitez que la page de connexion au MDaemon Webmail comporte une case *Se souvenir de moi* lorsque les utilisateurs se connectent via le port<u>https</u> 342. Si les utilisateurs cochent cette case au moment de la Connexion, leurs informations d'identification seront mémorisées pour ce périphérique. Dans ce cas, chaque fois qu'ils utiliseront ce dispositif pour se connecter au Webmail, ils seront automatiquement connectés, jusqu'à ce qu'ils se déconnectent manuellement de leur compte ou que leur jeton Se souvenir de moi expire.

Par défaut, les informations d'identification de l'utilisateur sont mémorisées pendant un maximum de 30 jours avant que l'utilisateur ne soit obligé de se connecter à nouveau. Si vous souhaitez augmenter le délai d'expiration, vous pouvez modifier la valeur de l'option *Expirer les jetons Se souvenir de moi après ce nombre de jours* dans l'interface Web de <u>MDaemon Remote Admin (MDRA)</u> [376]. Vous pouvez également modifier la clé RememberUserExpiration=30 dans la section [Default:Settings] du fichier Domains.ini, situé dans le dossier \Daemon\WorldClient\. La valeur d'expiration peut être fixée à un maximum de 365 jours. **Remarque :** L'authentification à deux facteurs [771] (2FA) possède sa propre clé d'expiration Se souvenir de moi (TwoFactorAuthRememberUserExpiration=30), située dans la section [Default:Settings] du fichier Domains.ini, dans le dossier\Daemon\WorldClient\N. Dans ce cas, l'option 2FA sera à nouveau requise à l'ouverture de session lorsque le jeton 2FA Se souvenir de moi expirera, même si le jeton normal est toujours valide.

L'option *Se souvenir de moi* est désactivée par défaut et s'applique à tous vos domaines. Si vous souhaitez remplacer ce paramètre pour des domaines spécifiques, utilisez le paramètre *Se souvenir de moi* situé sur l'écran Webmail du Gestionnaire de domaines.

Se souvenir de moi" permet aux utilisateurs de bénéficier d'une connexion persistante sur plusieurs appareils. Il est conseillé de ne pas utiliser Se souvenir de moi sur les réseaux publics. De plus, si vous soupçonnez une faille de sécurité dans un compte, MDRA dispose d'un bouton "Réinitialiser Se souvenir *de moi*" que vous pouvez utiliser pour réinitialiser les jetons Se souvenir de moi pour tous les utilisateurs. Tous les utilisateurs devront alors se connecter à nouveau.

Activer le dossier Documents

Le dossier Documents est disponible par défaut pour les utilisateurs du Webmail. Cette option contrôle l'état par défaut de l'option spécifique au domaine du même nom située sur la page Webmail du Gestionnaire de domaines. Si vous modifiez ce paramètre pour un domaine spécifique, il remplacera ce paramètre global pour ce domaine. **Remarque :** Cette option et les options Liens de Documents ci-dessous ne sont disponibles que dans l' interface web de<u>MDaemon Remote Admin (MDRA)</u>

Permettre aux utilisateurs de créer des liens temporaires vers des documents personnels

Cet utilisateur pourra créer des liens vers des documents personnels qui pourront être partagés avec n'importe qui. Les utilisateurs pourront créer des liens vers des documents personnels qui peuvent être partagés avec n'importe qui. Les liens de plus de 30 jours sont automatiquement purgés.

Voir les Liens de Documents

Cliquez sur ce bouton pour afficher la pageLiens de Documents, qui contient une liste de tous les liens de documents actifs. À partir de cette page, vous pouvez révoquer les Liens de votre choix. Les liens datant de plus de 30 jours seront automatiquement révoqués.

Transmettre la signature client

Cochez cette case si vous souhaitez transmettre la <u>Signature client par défaut</u> aux utilisateurs de Webmail. Dans le Webmail, cela créera une signature appelée "Système" sous les options de signature à : **Options | Composer**. Les utilisateurs peuvent alors choisir d'insérer automatiquement cette signature dans l'Affichage du message lors de la rédaction d'un nouveau message. Si vous souhaitez personnaliser ou activer/désactiver la signature client pour des domaines spécifiques, utilisez les options Signatures client et Webmail du Gestionnaire de domaines.

Autoriser les signatures créées par l'utilisateur

Cochez cette case si vous souhaitez autoriser les utilisateurs à créer leurs propres signatures créées par l'utilisateur dans le Webmail. Les utilisateurs peuvent alors choisir la signature qu'ils souhaitent insérer automatiquement dans la Voir les messages des files lors de la rédaction des messages. Lorsque vous n'autorisez pas les signatures créées par l'utilisateur, mais que l' option *Transmettre la signature client* ci-dessus est activée, seule la <u>Signature client</u> (c'est-à-dire la signature "Système" dans le Webmail) peut être insérée automatiquement. Dans le Webmail, les options de signature se trouvent à l'adresse suivante : **Options | Composer**.

Autoriser les utilisateurs à modifier le nom d'affichage de leurs alias

Cochez cette case si vous souhaitez autoriser les utilisateurs à modifier le nom d'affichage de leurs alias associés à leur compte. Ils peuvent le faire en utilisant l' option *Modifier les noms d'affichage des alias*, située dans le thème Pro du Webmail, sous Paramètres | Composer. Cette option est désactivée par défaut. **Note :** Cette option n'est disponible que dans l' interface web de<u>MDaemon Remote Admin</u> (MDRA) [376].

Activer l'assistant IA pour les e-mails

Cochez cette case si vous souhaitez activer l'assistant pour les IA les e-mails de MDaemon dans le MDaemon Webmail pour tous vos domaines. Vous pouvez modifier ce paramètre pour des domaines spécifiques en utilisant l'option du même nom située dans l'écran Paramètres du Webmail du Gestionnaire de domaines. **Remarque :** Activer assistant IA pour les e-mails pour un domaine ne permet pas à tous les utilisateurs de ce domaine d'accéder à ces fonctions. Vous devez activer l' option *Activer les options IA pour les e-mails sur* l'écran <u>Services Web</u> 771 de l'éditeur de compte pour tout utilisateur que vous souhaitez autoriser à les utiliser. Vous pouvez également utiliser les fonctions<u>Modèles de comptes</u> 477 et <u>Groupes</u> 500 pour affecter des utilisateurs à un groupe qui a accès aux fonctions de messages AI. Voir : "<u>Fonctionnalités des messages AI du webmail</u> 374" ci-dessous pour des informations importantes et des mises en garde concernant l'utilisation de ces fonctionnalités.

Nombre de messages affichés par page

Il s'agit du nombre de messages qui seront affichés sur chaque page de la Liste des dossiers pour chacun de vos dossiers courrier. Si un dossier contient plus que ce nombre de messages, des contrôles situés au-dessus et au-dessous de la liste vous permettront de passer aux autres pages. Les utilisateurs individuels peuvent modifier ce paramètre à partir de Options | Personnaliser dans WorldClient.

Fréquence d'actualisation de la liste de messages (en minutes)

Il s'agit du nombre de minutes pendant lesquelles le Webmail attendra avant d'actualiser automatiquement la liste des messages. Les utilisateurs individuels peuvent modifier ce paramètre à partir de Paramètres | Personnaliser dans le Webmail.

Texte d'aide pour l'échec de la connexion (peut contenir du code HTML)

Vous pouvez utiliser cette option pour spécifier une phrase de texte (texte brut ou HTML) à afficher sur la page de connexion du Webmail lorsqu'un utilisateur rencontre un problème pour se connecter. Ce texte s'affiche en dessous du texte par défaut suivant : "Ouverture de session incorrecte, veuillezréessayer. Si vous avez besoin d'aide, veuillez contacter votre administrateur de messagerie" Ce texte peut être utilisé pour diriger les utilisateurs vers une page ou des informations de contact pour obtenir de l'aide concernant la connexion au Webmail.

Paramètres de sécurité (Note : Les options de cette section ne sont disponibles que dans l' interface web de<u>MDaemon Remote Admin (MDRA</u> (376)).

Autoriser WebAuthn lors de la connexion

Cochez cette case si vous souhaitez autoriser les utilisateurs de MDaemon Webmail à se connecter en utilisant l'API d'authentification Web (également connue sous le nom de WebAuthn), qui leur offre une expérience de connexion sans mot passe sécurisée, en leur permettant d'utiliser la biométrie, les clés de sécurité USB, Bluetooth, etc. pour l'authentification. Non (par défaut).

Inviter les utilisateurs à enregistrer leur appareil à la première connexion

Cochez cette case si vous souhaitez inviter les utilisateurs à enregistrer leur appareil actuel (téléphone, données biométriques, etc.) pour la connexion sans passe lorsqu'ils se connectent pour la première fois à leur compte.

Permettre la connexion WebAuthn de contourner la page d'authentification à deux facteurs

WebAuthn étant déjà une forme d'authentification à plusieurs facteurs, l'utilisation d'une autre forme d'authentification à deux facteurs (2FA) après que quelqu'un a déjà utilisé WebAuthn pour se connecter pourrait être considérée comme redondante ou excessive par certains utilisateurs ou administrateurs. Vous pouvez donc cocher cette case si vous souhaitez ignorer l'authentification à deux facteurs lorsque quelqu'un utilise l'authentification par WebAuthn à l'ouverture de session. **Connexion :** Indépendamment de ce paramètre, lorsqu'un compte est spécifiquement configuré pour <u>requérir une authentification à deux</u> <u>facteurs</u> [771], ce compte ne pourra pas contourner l'authentification à<u>deux</u> <u>facteurs</u> [771], même s'il utilise WebAuthn pour se connecter.



Visitez : **webauthn.guide**, pour plus d'informations sur WebAuthn et son fonctionnement.

Activer la récupération de mot passe

Si cette option est activée, les utilisateurs autorisés à modifier leur mot de passe mil pourront saisir une autre adresse électronique dans le Webmail, à laquelle un lien peut être envoyé pour réinitialiser leur mot de passe s'ils l'oublient. Pour configurer cette adresse, les utilisateurs doivent saisir l'adresse e-mail de Récupération du mot de passe et leur mot de passe actuel dans Webmail sur la page Options | Sécurité. Si l'utilisateur tente de se connecter dans le Webmail avec un mot de passe incorrect, un lien "Mot de passe oublié" apparaîtra. Ce lien l'amène à une page qui lui demande de confirmer son adresse e-mail de récupération du mot de passe. Si l'adresse est saisie correctement, un e-mail sera envoyé avec un lien vers une page de modification du mot de passe. Cette fonction est désactivée par défaut.

Vous pouvez activer ou désactiver cette option pour chaque utilisateur en ajoutant la clé suivante au fichier user.inid'un utilisateur de Webmail (par exemple : \Users\example.com\frank\WC\user.ini) :

```
[Utilisateur]
EnablePasswordRecovery=Yes (ou "=No" pour désactiver l'option pour
l'utilisateur)
```

Autoriser les utilisateurs Active Directory à modifier leurs mots de passe via MDaemon Webmail

Lorsque cette case est cochée/activée, les utilisateurs dont les comptes sont configurés pour utiliser l'authentification Active Directory peuvent utiliser l'option "Modifier mot passe" de Webmail. Lorsque cette option est désactivée, seuls les utilisateurs dont les mots de passe sont définis dans MDaemon au lieu d'Active Directory peuvent modifier leur mot de passe à partir de Webmail. Le Gestionnaire de domaines dispose d'une <u>option du même nom que</u> [197] vous pouvez utiliser pour remplacer ce paramètre pour des domaines spécifiques.

Autoriser les utilisateurs à afficher les mots de passe saisis

Dans cette option, le champ du mot de passe sur la page de connexion à Webmail comporte une icône sur laquelle l'utilisateur peut cliquer pour rendre visible le mot de passe tapé. Décochez cette case si vous ne souhaitez pas autoriser la visibilité du mot de passe.

Autoriser les utilisateurs à recevoir par e-mail les codes de vérification de l'authentification en deux étapes

Par défaut, les utilisateurs sont autorisés à saisir une autre adresse e-mail dans le Webmail lors de la configuration de l'authentification à deux facteurs, afin qu'ils puissent recevoir les codes de vérification par e-mail plutôt que de devoir utiliser l'application Google authentification. Désactivez cette option si vous ne souhaitez pas autoriser les codes de vérification par e-mail. Vous pouvez remplacer cette option séparément pour chacun de vos domaines en utilisant l'option du même nom sur la page Paramètres Webmail du Gestionnaire de domaines.

Le code de vérification de l'authentification en deux étapes envoyé par e-mail expire au bout de : [xx] minutes.

Lors de la réception de codes d'Authentification à deux facteurs par email, il s'agit de la durée pendant laquelle l'utilisateur devra saisir le code avant qu'il n'expire. Non (par défaut), cette durée est fixée à **10** minutes.

Autoriser WebAuthn pour l'authentification à deux facteurs

Cochez cette case si vous souhaitez autoriser les utilisateurs du MDaemon Webmail à utiliser l'API WebAuthn pour l'authentification à deux facteurs. WebAuthn permet aux utilisateurs d'utiliser la biométrie, les clés de sécurité USB, Bluetooth, etc. pour l'authentification. Non (par défaut) pour l'authentification à deux facteurs, WebAuthn est autorisé.

> Dans un souci de sécurité, vous ne pouvez pas utiliser la même méthode d'authentification pour la Connexion sans mot passe et l'authentification à deux facteurs. Par conséquent, si vous souhaitez utiliser à la fois l'authentification sans mot de passe et l'authentification à deux facteurs, choisissez une méthode d'authentification différente pour chacune d'entre elles.

Visitez : **webauthn.guide**, pour plus d'informations sur WebAuthn et son fonctionnement.

Autoriser l'option Se souvenir de moi pour l'authentification en deux étapes

Lorsque quelqu'un utilise l'authentification à deux facteurs (2FA) pour se connecter au Webmail ou à Remote Admin, l'utilisateur dispose généralement d'une option Se souvenir de moi sur la page d'authentification 2FA, qui empêchera le serveur de demander à nouveau l'authentification 2FA à cet utilisateur pendant un certain nombre de jours (voir l'option "Expirer les facteurs Paramètres à deux paramètres" cidessous). Effacez cette case à cocher si vous ne souhaitez pas afficher l'option 2FA Se souvenir de moi, ce qui signifie que tous les utilisateurs dont l'authentification 2FA est activée devront saisir un code 2FA à chaque fois qu'ils se connectent.

Fonctionnalités des messages IA du Webmail

Dans la version 23.5.0 de MDaemon, le thème Pro du client Webmail de MDaemon inclut diverses fonctionnalités d'intelligence artificielle (IA) pour aider vos utilisateurs à gérer leur courrier électronique et à augmenter leur productivité. Ces fonctionnalités sont facultatives et désactivées par défaut, mais peuvent être activées pour tout utilisateur de votre choix.

Grâce à ces fonctionnalités, dans le MDaemon Webmail, vous pouvez utiliser l IA pour :

- Vous donner un résumé du contenu d'un message électronique.
- Suggérer une réponse au message, selon plusieurs directives que vous pouvez demander à l'IA d'utiliser. Vous pouvez définir le *ton de* la réponse (professionnel, respectueux ou décontracté). La position à adopter dans la réponse peut être intéressée ou non, d'accord ou non, ou sceptique. L'attitude à adopter dans la réponse peut être confiante, enthousiaste, calme ou apologétique. Les derniers peuvent indiquer la *longueur de* la réponse, qui peut être très brève ou détaillée.
- Vous aider à composer un nouveau message électronique, sur la base d'un texte que vous avez déjà inclus. Comme pour l'option *Suggérer* ci-dessus, vous pouvez également définir le ton, la position, l'attitude et la longueur que l'IA utilisera pour rédiger le message.

L' option Activer les fonctions IA pour les messages de la boîte de dialogue principale Paramètres du Webmail (365) permet de déterminer si la prise en charge des fonctions IA est activée par défaut pour vos domaines. Une option du même nom située dans la boîte de dialogue du (197) Gestionnaire de domaines peut être utilisée pour remplacer ce paramètre principal pour des domaines spécifiques. **Remarque :** Activer assistant IA pour les e-mails pour un domaine ne permet pas à tous les utilisateurs de ce domaine d'accéder à ces fonctions. Vous devez activer l' option Activer les options IA pour les *e-mails dans* l'écran Services Web (771) de l'éditeur de compte pour tout utilisateur que vous souhaitez autoriser à les utiliser. Vous pouvez également utiliser les fonctionsModèles de comptes (847) et Groupes (836) pour affecter des utilisateurs à un groupe ayant accès aux fonctions de messages AI.

> Activer les assistants IA pour les e-mails de MDaemon permet aux comptes d'envoyer et de recevoir des informations en provenance et à destination de services d'IA générative tiers, en particulier ChatGPT d'OpenAI. Les administrateurs et les utilisateurs doivent donc être conscients que cela introduit plusieurs problèmes potentiels de confidentialité en raison de la capacité de la fonctionnalité à traiter des données personnelles et à générer des informations potentiellement sensibles. Pour répondre à ces préoccupations, il est essentiel que les organisations forment leurs employés à une utilisation responsable de l'IA. **Remarque :** Les données soumises à/depuis I OpenAI ne sont pas stockées sur le serveur local ou sur notre réseau.

Vous trouverez la politique d'utilisation de l'IA de MDaemon Technologies sur notre <u>page d'information sur l'intelligence</u> <u>artificielle (IA)-la MDaemon</u>. Sur cette même page, il y a également un lien vers les Conditions d'utilisation d'OpenAI.

Personnalisation des dossiers Expéditeurs autorisés et Expéditeurs bloqués

Vous pouvez personnaliser certaines fonctions standard du Webmail en modifiant certains fichiers du dossierMDaemon Webmail:

Vous pouvez masquer les Dossiers Expéditeurs autorisés et Expéditeurs bloqués pour les utilisateurs du Webmail par défaut. Pour ce faire, ouvrez le fichier MDaemon\WorldClient\Domains.ini, et sous [Default:UserDefaults] changez la valeur de "HideWhiteListFolder=" ou "HideBlackListFolder=" de "No" à "Yes". Vous pouvez masquer ou afficher ces dossiers pour des utilisateurs spécifiques en modifiant ces mêmes clés dans le fichier User.ini, dans la section[User].

Voir :

Gestionnaire de domaines | Paramètres de MDaemon Webmail

3.6.1.12 Personnalisation du logo

Si vous souhaitez personnaliser les images de la bannière du Webmail qui apparaissent sur la page de connexion et dans la barre latérale de navigation, vous pouvez le faire à partir de la page Personnalisation dans MDaemon Webmail Admin.

Pour utiliser des images personnalisées :

- 1. Cliquez sur **Utiliser des images personnalisées** dans la section Personnalisation.
- Dans la section Image de la page de connexion, utilisez l' option Choisir un fichier ou Parcourir (selon votre navigateur) pour sélectionner le fichier que vous souhaitez télécharger. Cette section indique également la taille par défaut de chaque image. pour chaque image.
- 3. Cliquez sur Ajouter image personnalisée.
- 4. Répétez les étapes 2 et 3 pour l'image d'arrière-plan de la page d'inscription, l'image de la page de navigation et l'image de la page d'accueil. Image d'arrièreplan de la page Connexion, Image barre de navigation, et l'Image barre latérale de navigation inversée.

Les images uploadées apparaîtront dans les cases correspondantes et seront désormais utilisées à la place des images par défaut du Webmail.

3.6.2 MDaemon Remote Admin

L'interface web de MDaemon Remote Admin (MDRA) est conçue pour vous permettre d'administrer MDaemon à distance à l'aide d'un navigateur web. Dans ce cas, il s'agit d'une application serveur conçue pour fonctionner en arrière-plan sur le même ordinateur que MDaemon. Pour accéder à MDaemon Remote Admin, ouvrez votre navigateur sur l'URL et le numéro de port sur lesquels le serveur d'administration à distance réside (Exemple : www.example.com:1000). Après avoir fourni vos identifiants de connexion, vous aurez accès à divers contrôles et paramètres au sein de MDaemon. Le type et le nombre de paramètres auxquels vous aurez accès dépendent du niveau d'accès accordé. Il existe trois niveaux d'accès pour les utilisateurs de l'administration à distance : Global, Domaine et Utilisateur.

- Administrateurs globaux Les administrateurs globaux sont des utilisateurs dont l'autorisation d'accès global est activée dans les paramètres de leur compte au sein de MDaemon. L'accès global signifie que l'utilisateur peut voir et configurer tous les paramètres et contrôles accessibles via MDaemon Remote Admin. Les Administrateurs globaux peuvent ajouter, modifier et supprimer des utilisateurs, des domaines et des listes de diffusion. Ils peuvent modifier les fichiers INI des produits, désigner d'autres utilisateurs en tant qu'Administrateurs de domaines, gérer les mots de passe et bien d'autres choses encore ; ils disposent d'un contrôle administratif complet.
- Administrateurs de domaine Comme les administrateurs globaux, les administrateurs de domaine ont également le contrôle des utilisateurs et des paramètres accessibles via MDaemon Remote Admin. Leur contrôle administratif est toutefois limité au(x) domaine(s) auquel(s) ils ont été autorisés à accéder et aux autorisations désignées dans l' écran des <u>Services web.</u> (771) Les administrateurs de domaine et les domaines sur lesquels ils ont le contrôle sont désignés à partir de MDaemon Remote Admin par un administrateur globaux ou par un autre administrateur de domaine ayant accès à ces domaines.
- **Utilisateurs** Le niveau le plus bas d'accès à MDaemon Remote Admin est l'accès utilisateur. Les utilisateurs de MDaemon peuvent se connecter à l'interface d'administration à distance et, par exemple, afficher les paramètres de leur compte individuel et modifier leurs entrées MultiPOP, leurs filtres de messagerie, leurs filtres automatiques, etc. Le type et le nombre de paramètres qui peuvent être modifiés dépendent des autorisations données dans les paramètres du compte dechaque utilisateur.

Toute personne autorisée à accéder à la fois à Webmail et à MDaemon Remote Admin peut accéder à MDaemon Remote Admin à partir de Webmail, au lieu de devoir se connecter aux deux comptes séparément. MDaemon Remote Admin s'ouvre dans une fenêtre de navigation séparée à partir de Webmail en cliquant sur le lien "Paramètres avancés" sous "Options".

Voir :

MDaemon Remote Admin | Serveur Web 377 MDaemon Remote Admin | HTTPS 384 Gestionnaire de modèles | Services Web 385 Mon compte Editor | Services Web 777 Article KB : Comment configurer les services Webmail, MDaemon Remote Admin, ActiveSync, CalDav, CardDav, AutoDiscover, MDDP, Webmail API et XML API dans IIS ?

3.6.2.1 Serveur web

	MDaemon Remote Administration
Remote Administration	Remote Administration is disabled
···· Web Server	Remote Administration runs using built-in web server
SSL & HTTPS	Remote Administration runs using external webserver (IIS, Apache, etc)
Terms of Use Attachment Linking CalDAV & CardDAV YMPP	Remote Administration server uses TCP port 1000 Sessions expire after 15
	Use cookies to remember logon name and other properties
	☐ Require IP persistence throughout remote administration session
	Stop Remote Administration when MDaemon stops
	Use HTTP compression
	Use X-Forwarded-For Header
	Enable Bemember Me
	Remote Administration URL (leave blank for default)
	Bind Remote Administration's web server to these IPs only. Separate multiple values with commas. Leave blank to bind to all IP addresses.
	Restart Remote Administration Edit Mailing List Admins
	Ok Cancel Anniu Hein

MDaemon Remote Admin

Désactiver MDaemon Remote Admin

Choisissez cette option pour désactiver l'administration à distance. Vous pouvez également activer/désactiver l'administration à distance à partir du menu Fichier ou de la section Serveurs du cadre Stats dans l'interface graphique principale de MDaemon.

Exécuter MDaemon Remote Admin avec le serveur web intégré

Choisissez cette option pour exécuter l'Administration à distance à l'aide du serveur web intégré de MDaemon. Vous pouvez également activer/désactiver l'Administration à distance à partir du menu Fichier ou de la section Serveurs du cadre Statistiques de l'interface graphique principale de MDaemon.

Exécuter MDaemon Remote Admin à l'aide d'un serveur web externe (IIS, Apache, etc.)

Choisissez cette option si vous souhaitez exécuter l'Administration Remote sous Internet Information Server (IIS) ou un autre serveur web au lieu du serveur intégré deMDaemon.Cela permet d'éviter l'accès à certains éléments de l'interface graphique qui pourraient causer des conflits avec votre autre serveur.

Pour plus d'informations, voir l'article de la Base de connaissances : <u>Comment</u> <u>configurer les services Webmail, MDaemon Remote Admin, ActiveSync, CalDav,</u> <u>CardDav, AutoDiscover, MDDP, Webmail API, et XML API dans IIS</u>.

Le serveur d'administration à distance utilise le port TCP

Il s'agit du port sur lequel MDaemon Remote Admin écoutera les connexions de votre navigateur Web. Le port par défaut est 1000.

Les sessions expirent au bout de [xx] minutes inactives.

Dans le cas où vous êtes connecté au MDaemon MDaemon Remote Admin, il s'agit du temps pendant lequel votre session est autorisée à rester inactive avant que l'Administration à distance ne la ferme. La valeur par défaut est de 15 minutes.

Paramètres de sécurité

Remarque : Les options de cette section sont disponibles dans l'interface web de <u>MDaemon Remote Admin (MDRA 376</u>).

Utiliser des jetons de falsification croisée des requêtes (Cross-Site-Request-Forgery)

Non (par défaut), les jetons Cross-Site-Request-Forgery (CSRF) sont utilisés pour les transactions plus sécurisées, afin de prévenir les attaques CSRF.

Autoriser les utilisateurs à afficher les mots de passe saisis

Non par défaut, les utilisateurs peuvent cliquer sur une icône pour afficher les caractères du mot de passe qu'ils sont en train de taper lorsqu'ils se connectent à l'interface web d'administration à distance. Décochez cette case si vous ne souhaitez pas autoriser cela.

Autoriser WebAuthn lors de la connexion

Cochez cette case si vous souhaitez autoriser les utilisateurs de MDRA à se connecter en utilisant l'API d'authentification Web (également connue sous le nom de WebAuthn), qui leur offre une expérience de connexion sécurisée et sans mot de passe, en leur permettant d'utiliser la biométrie, les clés de sécurité USB, Bluetooth, etc. pour l'authentification. Non (par défaut).

Permettre la connexion WebAuthn de contourner la page d'authentification à deux facteurs

WebAuthn étant déjà une forme d'authentification à plusieurs facteurs, l'utilisation d'une autre forme d'Authentification à deux facteurs (2FA) lors de la Connexion pourrait être considérée comme redondante ou excessive par certains utilisateurs ou administrateurs. Si c'est le cas, vous pouvez cocher cette case si vous souhaitez ignorer l'authentification à deux facteurs lorsque quelqu'un utilise l'authentification WebAuthn à l'ouverture de session. **REMARQUE :** Indépendamment de ce paramètre, lorsqu'un compte est spécifiquement configuré pour <u>requérir une authentification à deux facteurs</u> [771], ce compte ne pourra pas contourner l'authentification à deux facteurs, même s'il utilise WebAuthn.

Autoriser WebAuthn pour l'authentification à deux facteurs

Cochez cette case si vous souhaitez autoriser les utilisateurs de MDRA à utiliser l'API d'Authentification Web (également connue sous le nom de WebAuthn) pour l'authentification à deux facteurs. WebAuthn permet aux utilisateurs d'utiliser la biométrie, les clés de sécurité USB, Bluetooth, etc. pour l'authentification. Non (par défaut) pour l'authentification à deux facteurs, WebAuthn est autorisé.

> Dans un souci de sécurité, vous ne pouvez pas utiliser la même méthode d'authentification pour la Connexion sans mot passe et l'authentification à deux facteurs. Par conséquent, si vous souhaitez utiliser à la fois l'authentification sans mot de passe et l'authentification à deux facteurs, choisissez une méthode d'authentification différente pour chacune d'entre elles.

Visitez : **webauthn.guide**, pour plus d'informations sur WebAuthn et son fonctionnement.

Activer Se souvenir de moi

Cochez cette case si vous souhaitez que la page d'ouverture de session de MDaemon Remote Admin (MDRA) comporte une case *Se souvenir de moi* lorsque les utilisateurs se connectent via le port <u>https</u> [34]. Si les utilisateurs cochent cette case lors de la connexion, leurs informations d'identification seront mémorisées pour ce périphérique. Dans ce cas, chaque fois qu'ils utiliseront ce dispositif pour se connecter à MDRA, ils seront automatiquement connectés, jusqu'à ce qu'ils se déconnectent manuellement de leur compte ou que leur jeton Se souvenir de moi expire. L'option*Se souvenir moi* est désactivée par défaut.

Les jetons "Se souvenir de moi" expirent au bout de (en jours)

Utilisez cette option pour indiquer le nombre de jours pendant lesquels les informations d'identification de vos utilisateurs seront mémorisées. Par défaut, les informations d'identification sont conservées pendant 30 jours au maximum avant que l'utilisateur ne soit contraint de se connecter à nouveau. Cette option peut être réglée sur un maximum de 365 jours. **Remarque :** L'authentification à deux facteurs mil (2FA) possède sa propre clé d'expiration Se souvenir de moi (TwoFactorAuthRememberUserExpiration=30), située dans la section [Default:Settings] du fichier Domains.ini, situé dans le dossier\MDaemon\WorldClient\. Dans ce cas, l'authentification 2FA sera à nouveau requise à l'ouverture de session lorsque le jeton 2FA Se souvenir de moi expirera, même si le jeton normal est toujours valide.

Réinitialiser Se souvenir de moi

Cliquez sur ce bouton si vous pensez qu'une faille de sécurité a été commise sur un compte. Dans ce cas, les jetons Se souvenir de moi sont réinitialisés pour tous les utilisateurs, ce qui les oblige à se connecter à nouveau.



Se souvenir de moi" permet aux utilisateurs de bénéficier d'une connexion persistante sur plusieurs appareils. Il est conseillé de ne pas utiliser de moi" sur des réseaux publics.

Paramètres divers

Utiliser des cookies pour mémoriser l'identifiant et d'autres propriétés

Par défaut, l'interface MDaemon Remote Admin utilise des cookies pour que le navigateur de l'utilisateur puisse se souvenir de son Nom d'utilisateur et d'autres propriétés. Désactivez cette case à cocher si vous ne souhaitez pas utiliser de cookies. L'utilisation de cette fonction permet aux utilisateurs de bénéficier d'une expérience de connexion plus personnalisée, mais nécessite que la prise en charge des cookies soit activée dans leur navigateur.

Exiger la persistance de l'IP pendant la session d'administration à distance

À titre de mesure de sécurité supplémentaire, vous pouvez cocher cette case pour que MDaemon Remote Admin limite chaque session à l'adresse IP à partir de laquelle vous vous êtes connecté au début de la session. Ainsi, personne ne peut "voler" la session puisque la persistance de l'IP est requise. Cette configuration est plus sûre mais peut poser des problèmes si vous utilisez un serveur proxy ou une connexion Internet qui attribue et change dynamiquement les adresses IP.

Arrêter MDaemon Remote Admin en même temps que MDaemon

Cliquez sur cette option si vous souhaitez que l'Administration à distance soit arrêtée lors de l'arrêt de MDaemon. Dans le cas contraire, MDaemon Remote Admin continuera à fonctionner en arrière-plan.

Utiliser la compression HTTP

Cochez cette case si vous souhaitez utiliser la compression HTTP dans vos sessions de MDaemon Remote Admin.

Informer de nouvelles versions à l'ouverture session

Non par défaut, vous serez averti sur la page Connexion lorsqu'une nouvelle version de MDaemon est disponible. Décochez cette case si vous ne souhaitez pas être notifié à cet endroit. **Note :** Cette option est disponible dans l'interface web de<u>MDaemon Remote Admin (MDRA).</u>

Envoyer des données d'utilisation anonymes

Par défaut, le client web de MDaemon Remote Admin Admin envoie des données d'utilisation anonymes et bénignes telles que : le système d'exploitation utilisé, la version du navigateur utilisée, la langue, etc. Ces données sont utilisées par MDaemon Technologies pour nous aider à améliorer MDaemon Remote Admin. Désactivez cette option si vous ne souhaitez pas envoyer de données d'utilisation anonymes.

X-Forwarded-For header

Cochez cette case pour activer l'utilisation de l'en-têtex-Forwarded-For, qui est parfois ajouté par les serveurs proxy. Cette option est désactivée par défaut. Ne l'activez que si votre serveur proxy insère cet en-tête.

Activer Se souvenir de moi

Cochez cette case si vous souhaitez qu'une case *Se souvenir de moi*apparaisse sur la page d'ouverture de session de MDaemon Admin lorsque les utilisateurs se connectent via le port<u>https.</u> 384 Si les utilisateurs cochent cette case lors de la connexion, leurs informations d'identification seront mémorisées pour ce périphérique. Dans ce cas, chaque fois qu'ils utiliseront cet appareil pour se connecter à l'avenir, ils seront automatiquement connectés, jusqu'à ce qu'ils se déconnectent manuellement de leur compte ou que leur jeton Se souvenir de moi expire.

Non (par défaut), les informations d'identification de l'utilisateur sont mémorisées pendant un maximum de 30 jours avant que l'utilisateur ne soit contraint de se connecter à nouveau. Si vous souhaitez augmenter le délai d'expiration, vous pouvez modifier la valeur de l'option *Expirer les jetons Se souvenir de moi après ce nombre de jours* dans l'interface Web de MDaemon Remote Admin (MDRA). Vous pouvez également modifier la clé RememberUserExpiration=30 dans la section [Default:Settings] du fichier Domains.ini, situé dans le dossier \Daemon\WorldClient\. La valeur d'expiration peut être fixée à un maximum de 365 jours. **Remarque :** L'authentification à deux facteurs [771] (2FA) possède sa propre clé d'expiration Se souvenir de moi (TwoFactorAuthRememberUserExpiration=30), située dans la section [Default:Settings] du fichier Domains.ini, dans le dossier\Daemon\WorldClient\N. Dans ce cas, l'option 2FA sera à nouveau requise à l'ouverture de session lorsque le jeton 2FA Se souvenir de moi expirera, même si le jeton normal est toujours valide.

L'optionSe souvenir de moi est désactivée par défaut.

Se souvenir de moi" permet aux utilisateurs de bénéficier d'une connexion persistante sur plusieurs appareils. Il est conseillé de décourager les utilisateurs d'utiliser l'option *Se souvenir de moi* sur les réseaux publics. De plus, si vous soupçonnez une faille de sécurité dans un compte, MDRA dispose d'un bouton "*Réinitialiser Se souvenir de moi*" que vous pouvez utiliser pour réinitialiser les jetons Se souvenir de moi pour tous les utilisateurs. Tous les utilisateurs devront alors se connecter à nouveau.

URL de MDaemon Remote Admin

Il s'agit de l'URL que Webmail utilisera en interne lorsque les utilisateurs cliqueront sur le lien Paramètres avancés pour modifier les paramètres de leur compte via MDaemon Remote Admin. Dans le cas où vous utilisez le MDaemon Remote Admin avec le Serveur Web distant, laissez ce champ vide. Si vous utilisez un autre serveur Web, tel que IIS, et que vous avez configuré le MDaemon Admin Remote pour qu'il s'exécute à une autre URL ou adresse IP, indiquez cette URL ici.

Lier le serveur Web de MDaemon Remote Admin à ces IP uniquement

Si vous souhaitez restreindre le serveur d'administration à distance à certaines adresses IP seulement, indiquez ces adresses ici en les séparant par des virgules. Si vous laissez ce champ vide, le système d'administration à distance surveillera toutes les adresses IP que vous avez désignées pour vos <u>domaines</u> [184].

Redémarrer MDaemon Remote Admin (nécessaire en cas de modification du port ou de la valeur IIS)

Cliquez sur ce bouton si vous souhaitez redémarrer le serveur d'administration à distance. Dans : lorsque vous modifiez le paramètre du port, vous devez redémarrer MDaemon Remote Admin pour que le nouveau paramètre soit reconnu.

Modifier admin. de liste de diffusion

Cliquez sur ce bouton si vous souhaitez ouvrir le fichier des administrateurs de listes de diffusion pour l'afficher ou le modifier.



All of the options below are only available in the MDaemon Remote Administration (MDRA) web-interface.

En-têtes de réponse HTTP

Cette option permet de définir des En-têtes de réponse HTTP personnalisés pour le serveur Remote Admin intégré à MDaemon. Vous devez redémarrer le serveur En-tête From Admin pour que les modifications en-têtes soient prises en compte.

Paramètres de mise en page

Nombre de lignes affichées par page : [xx] (par défaut = 50)

Il s'agit du nombre de lignes affichées par page par l'interface MDaemon Remote Admin. Lorsqu'il y a plus de lignes de données disponibles, les options de mise en page au bas de la page seront utilisées pour les données supplémentaires. Exemple : par défaut, la page Comptes affiche jusqu'à 50 comptes. Si le nombre de comptes est supérieur à 50, ils seront affichés sur autant de pages supplémentaires que nécessaire, à raison de 50 comptes par page.

Number of log lines displayed per page: [xx] (default = 500)

This is the number of lines that the Remote Administration interface will display per page when you are viewing a log file. By default each page will display 500 lines of logging data. If a log file contains more than 500 lines then rest of the log will be displayed on additional pages at 500 lines per page.

Mailing List Subscription Manager Options

Enable mailing list subscriptions manager

If enabled, users may access "My Mailing Lists" to manage their subscriptions. Global administrators always have access to "My Mailing Lists".

Only authenticated users can access the mailing list subscriptions manager

Disable this option to allow users without an MDaemon Remote Administration account to manage their mailing list subscriptions.

Limit displayed mailing lists to the user's own domain

Disable this option to display all mailing lists that allow subscriptions. This option only applies to authenticated users. A user can always view any list for which they have administrative access.

Edit Mailing List Admins

Click this button if you wish to open the mailing list administrators file to view or edit it.

Report Settings

Use this option to specify any of your MDaemon email addresses that you wish to exclude from Reports.

Voir :

MDaemon Remote Admin 376

MDaemon Admin | HTTPS 384

Gestionnaire de modèles | Services Web

Mon compte Editor | Services Web

Article KB : <u>Comment configurer les services Webmail, MDaemon Remote Admin,</u> <u>ActiveSync, CalDav, CardDav, AutoDiscover, MDDP, Webmail API et XML API dans IIS ?</u>

3.6.2.2 SSL & HTTPS

🧐 Services web, & MI - SSL & HTTPS				×
- Webweit	Accepter ces types de cor	nexions		
⊕- MDaemon Remote Admin	HTTP uniquement	HTTP et HTTPS	Port HTTPS 4	44
Serveur Web <mark>SSL & HTTPS</mark>	HTTPS uniquement	🔿 HTTP redirigé en HTTPS		
Conditions d'utilisation Liens vers les pièces jointes	Vérifier les certificats à utilise	r avec HTTPS. Sélectionnez l'éto	ile du certificat par défa	aut.
	Sujet	Autres noms d'hôtes	Date d'expiration	Fournisse
···· XMPP	🛛 ★ mail.company.test		4/25/2021	mail.com
	<	m		Þ
	Créer un certificat	Redémarrer le serveur Web		Supprimer
		OK Annu	ler Appliquer	Aide

Le serveur Web intégré à MDaemon prend en charge le protocole SSL (Secure Sockets Layer). SSL est la méthode standard pour sécuriser les communications serveur/client sur le Web. Il permet l'authentification du serveur, le cryptage des données et, en option, l'authentification du client pour les connexions TCP/IP. En outre, la prise en charge du protocole HTTPS (c'est-à-dire HTTP sur SSL) étant intégrée dans tous les principaux navigateurs, il suffit d'installer un certificat numérique valide sur votre serveur pour activer les capacités SSL du client qui se connecte.

Les options permettant d'activer et de configurer le MDaemon Remote Admin pour utiliser HTTPS se trouvent dans l'écran SSL & HTTPS sous | Setup | Web & IM Services | MDaemon Remote Admin". Pour plus de commodité, ces options sont également reprises sous "Sécurité | Paramètres de sécurité | SSL & TLS | Administration à distance".

Pour plus d'informations sur le protocole SSL et les certificats, voir : <u>SSL &</u> <u>Certificats</u> 613



Cet écran ne s'applique à l'Administration à distance que lorsque vous utilisez leserveur web intégré de MDaemon. Si vous configurez l'Administration à distance pour utiliser un autre serveur web tel que IIS, ces options ne seront pas

384

utilisées - le support SSL/HTTPS devra être configuré en utilisant les outils de l'autre serveur web.

Accepter ces types de connexions

HTTP uniquement

Choisissez cette option si vous ne souhaitez pas autoriser de connexions HTTPS vers MDaemon Remote Admin. Seules les connexions HTTP seront acceptées.

HTTP et HTTPS

Choisissez cette option si vous souhaitez activer la prise en charge de SSL dans MDaemon Remote Admin, mais ne souhaitez pas obliger les utilisateurs de MDaemon Remote Admin à utiliser HTTPS. MDaemonRemote Admin écoutera les connexions sur le port HTTPS désigné ci-dessous, mais répondra toujours aux connexions http normales sur le port TCP de MDaemon Remote Admin désigné sur l' écran <u>Serveur</u> <u>Web</u> [377].

HTTPS uniquement

Choisissez cette option si vous souhaitez exiger le protocole HTTPS lors de la connexion au MDaemon Remote Admin. MDaemon Remote Admin ne répondra qu'aux connexions HTTPS lorsque cette option est activée - il ne répondra pas aux demandes HTTP.

HTTP redirigé vers HTTPS

Choisissez cette option si vous souhaitez rediriger toutes les connexions HTTP vers HTTPS sur le port HTTPS.

Port HTTPS

Il s'agit du port TCP que MDaemon Remote Admin écoutera pour les connexions SSL. Le port SSL par défaut est 444. Si le port SSL par défaut est utilisé, il n'est pas nécessaire d'inclure le numéro de port dans l'URL de l'administration à distancelors de la connexion via HTTPS (c'est-à-dire que "https://example.com" équivaut à "https://example.com:444").

> Il ne s'agit pas du même port que celui désigné pour le MDaemon Admin dans l' écran <u>Serveur Web</u> 3771. Si vous autorisez toujours les connexions HTTP au MDaemon Remote Admin, ces connexions doivent utiliser cet autre port pour réussir à se connecter. Les connexions HTTPS doivent utiliser le port HTTPS.

Sélectionnez le certificat à utiliser avec HTTPS/SSL

Cette boîte affiche vos certificats SSL. Cochez la case en regard des certificats que vous souhaitez activer. Cliquez sur l'étoile en regard de celui que vous souhaitez définir comme certificat par défaut. MDaemon prend en charge l'extension Server Name Indication (SNI) du protocole TLS, ce qui permet d'utiliser un certificat différent pour chaque nom d'hôte de votre serveur. MDaemon examine les certificats actifs et choisit

celui qui contient le nom d'hôte demandé dans le champ Subject Alternative Names (vous pouvez spécifier les noms alternatifs lors de la création du certificat). Si le client ne demande pas de Nom d'hôte, ou si aucun certificat correspondant n'est trouvé, le certificat par défaut est utilisé. Double-cliquez sur un certificat pour l'ouvrir dans la boîte de dialogue Certificat de Windows afin de l'examiner (disponible uniquement dans l'interface d'application, pas dans l'administration à distance basée sur le navigateur).

Supprimer

Sélectionnez un certificat dans la liste, puis cliquez sur ce bouton pour le supprimer. Une boîte de confirmation s'ouvre et vous demande si vous êtes sûr de vouloir supprimer le certificat.

Créer un certificat

Cliquez sur ce bouton pour ouvrir la boîte de dialogue Créer un certificat SSL.

С	réer un certificat SSL	
	Détails du certificat	
	Nom d'hôte (ex. : wc.altn.com)	mail.company.test
	Nom de l'organisation/entreprise	Example Corp
	Autres noms d'hôtes (séparez plusi	eurs entrées par des virgules)
	Longueur de la clé de cryptage	2048 🔹
	Algorithme de hachage	SHA2 -
	Pays/région	United States US 🔹
		OK Annuler

Détails du certificat

Nom d'hôte

Lors de la création d'un certificat, entrez le nom d'hôte auquel vos utilisateurs se connecteront (par exemple, "wc.example.com").

Nom de l'organisation/entreprise

Entrez ici le nom de l'organisation ou de la société qui "possède" le certificat.

Autres noms d'hôtes (séparez plusieurs entrées par des virgules)

Si les utilisateurs se connectent à d'autres noms d'hôte et que vous souhaitez que ce certificat s'applique également à ces noms, entrez ici ces noms de domaine en les séparant par des virgules. Les caractères joker sont autorisés, ainsi "*.example.com" s'applique à tous les sous-domaines de example.com (par exemple, "wc.example.com", "mail.example.com", etc.)

MDaemon prend en charge l'extension SNI (Server Name Indication) du protocole TLS, ce qui permet d'utiliser un certificat différent pour chaque nom d'hôte de votre serveur. MDaemon examine les certificats actifs et choisit celui qui contient le nom d'hôte demandé dans son champ À :. Si le client ne demande pas de Nom d'hôte, ou si aucun certificat correspondant n'est trouvé, le certificat par défaut est utilisé.

Longueur de clé de cryptage

Choisissez la longueur de clé de cryptage souhaitée pour ce certificat. Plus la clé de cryptage est longue, plus les données transférées sont sécurisées. Notez toutefois que toutes les applications ne prennent pas en charge des longueurs de clé supérieures à 512.

Pays/région

Choisissez le pays ou la région dans lequel votre serveur réside.

Algorithme de hachage

Choisissez l'algorithme de hachage que vous souhaitez utiliser : SHA1 ou SHA2. Le paramètre par défaut est SHA2.

Redémarrer les serveurs Web

Cliquez sur ce bouton pour redémarrer le serveur Web. Le serveur Web doit être redémarré avant qu'un nouveau certificat ne soit utilisé.

Utiliser Let's Encrypt pour gérer votre certificat

Let's Encrypt est une autorité de certification (AC) qui fournit des certificats gratuits via un processus automatisé conçu pour éliminer le processus actuellement complexe de création, de validation, de signature, d'installation et de renouvellement manuels des certificats pour les sites web sécurisés.

Dans le cadre de l'utilisation du processus automatisé de Let's Encrypt pour gérer un certificat, l' écran Let's Encrypt 🖼 est fourni pour vous aider à configurer et à exécuter facilement le script PowerShell inclus dans le dossier

"MDaemon\LetsEncrypt". L'exécution du script permet de tout configurer pour Let's Encrypt, y compris de placer les fichiers nécessaires dans le dossier HTTP du Webmail pour relever le défi http-01. Il utilise le <u>nom d'hôte SMTP</u> [187] du <u>domaine par défaut</u> [184] comme domaine pour le certificat, inclut tout *autre nom d'hôte que* vous avez spécifié, récupère le certificat, l'importe dans Windows et configure MDaemon pour qu'il utilise le certificat pour MDaemon, Webmail et Remote Admin. Dans le dossier "MDaemon\Logs\", le script crée un fichier journal appelé LetsEncrypt.log. Ce fichier journal est supprimé et recréé à chaque fois que le script est exécuté, et il inclut la date et l'heure début du script. De plus, des e-mails de notification seront envoyés lorsque des erreurs se produisent si vous spécifiez un *E-mail de l'administrateur pour les notifications*. Voir la rubrique Let's Encrypt Pour plus d'informations sur SSL et les certificats, voir :

SSL et certificats 613 Créer et utiliser des certificats SSL 974

Pour plus d'informations sur le MDaemon Remote Admin, voir :

Configuration à distance MDaemon MDaemon Remote Admin | Serveur Web Mon (par défaut) accès Web Mon compte | Web Mon compte | Web Article KB : Comment configurer les services Webmail, MDaemon Remote Admin, ActiveSync, CalDav, CardDav, AutoDiscover, MDDP, Webmail API et XML API dans IIS ?

3.6.3 Conditions d'utilisation

🧐 Services web, & MI - Conditions d'utilisation	
Webmail MDaemon Remote Admin Conditions d'utilisation Liens vers les pièces jointes	Conditions d'utilisation Les utilisateurs de MDaemon Webmail et MDaemon Remote Admin doivent accepter les conditions d'utilisation ci-dessous. Entrez vos conditions d'utilisation :
	OK Annuler Appliquer Aide

Les utilisateurs de Webmail et MDaemon Remote Admin doivent accepter les Conditions d'utilisation définies ci-dessous.

Cochez cette case et entrez vos Conditions d'utilisation dans l'espace prévu si vous souhaitez exiger des utilisateurs du Webmail et du MDaemon Remote Admin qu'ils acceptent les Conditions d'utilisation à chaque fois qu'ils se connectent.

3.6.4 Liens vers les pièces jointes

🧐 Web & IM Services - Attachment Linking	
Web & IM Services - Attachment Linking Webmail Web Server SSL & HTTPS MDIM Calendar Dropbox Settings Remote Administration Terms of Use Attachment Linking CalDAV & CardDAV MPP	Attachment linking works by removing attachments from email messages and replacing them with URL links. When users read the email they will see that it contains a URL link to the file rather than the file itself. Accounts must be configured to use Attachment Linking for this to work. Enable attachment linking Let Webmail automatically manage Attachment Linking Manually configure Attachment Linking Attachment path: Attachment path: Webmail URL: Webmail URL: Webmail must be able to access the Attachment Path. Account macros can be used in the Attachment Path value. Ignore attachments smaller than this many KB (0 = none)
	Delete attachments from disk when messages are deleted Extract quoted-printable "text/plain" attachments Exempt list Header text: MDaemon replaced the following files with these links: HTML filename: attachmentlinks.html
	Ok Cancel Apply Help

Liens vers les pièces jointes (Configuration | Services Web et de messagerie instantanée | Liens vers les pièces jointes) est une fonctionnalité qui permet à MDaemon de supprimer toutes les pièces jointes des messages entrants, de les stocker dans un emplacement désigné, puis de placer des liens URL vers les fichiers dans chaque message d'où ils sont extraits. Les destinataires peuvent alors cliquer sur ces liens pour télécharger les fichiers. Cette méthode peut accélérer considérablement le traitement du courrier lorsque vos utilisateurs récupèrent leurs messages ou synchronisent leurs dossiers courrier, puisque les messages seront dépourvus de pièces jointes volumineuses. Cela peut également renforcer la sécurité et le niveau de protection de vos utilisateurs, car les pièces jointes peuvent être stockées dans un emplacement central pour être contrôlées par l'administrateur et ne seront pas téléchargées automatiquement vers des clients de messagerie où elles pourraient être exécutées automatiquement. De plus, si vous choisissez l'option "Laisser le Webmail gérer automatiquement Liens vers les pièces jointes", la gestion des emplacements des fichiers et de l'URL du Webmail est prise en charge automatiquement. Si vous choisissez de gérer Liens vers les pièces jointes manuellement, vous pouvez spécifier l'emplacement où les fichiers seront stockés, et vous pouvez utiliser des macros spéciales pour rendre l'emplacement dynamique. Pour que le Liens vers les pièces jointes fonctionne, il doit être activé globalement à l'aide de l'option de cet écran, et chaque compte vers lequel vous souhaitez l'utiliser doit être configuré spécifiquement à cet effet dans l'écran Pièces jointes 787 de l'Éditeur de compte. Sur ce même écran, il existe également une option permettant d'appliquer le Liens vers les pièces jointes aux

messages sortants ; les pièces jointes des messages sortants du compte seront extraites et remplacées par un lien vers les fichiers stockés. Enfin, les liens vers les pièces jointes que MDaemon place dans les messages ne contiennent pas de chemin de fichier direct. Ils contiennent un identifiant unique (GUID) que le serveur utilise pour faire correspondre le fichier au chemin d'accès réel. Ce GUID est stocké dans le fichierAttachmentLinking.dat.

> Liens vers les pièces jointes essaie d'utiliser le nom de fichier fourni dans les En-têtes MIME (s'il y en a). Si le nom du fichier comporte plus de 50 caractères, seuls les 50 derniers seront utilisés. Si le Nom du fichier est manquant, l'extension".att" sera ajoutée.

Activer les liens vers les pièces jointes

Cochez cette case pour activer le Liens vers les pièces jointes pour tous les comptes qui sont spécifiquement configurés pour l'utiliser dans l'écran <u>Pièces</u> jointes vous demande si vous souhaitez également activer l'option spécifique au compte pour tous les comptes MDaemon. Si vous choisissez "Oui", l'option Liens vers les pièces jointes sera activée pour tous les comptes et l'option correspondante du modèle<u>Nouveaux comptes</u> arai sera également activée. Si vous choisissez "Non", la fonctionnalité Liens vers les pièces jointes sera activer manuellement pour chaque compte que vous souhaitez utiliser. Lorsque Liens vers les pièces jointes est activé, le serveur Webmail doit être activé.

Laisser Webmail gérer automatiquement Liens vers les pièces jointes

Il s'agit de l'option par défaut lorsque Liens vers les pièces jointes est activé. Utilisez cette option si vous souhaitez que le Webmail gère automatiquement le Liens vers les pièces jointes. Les pièces jointesseront stockées dans : "... \MDaemon\Attachments\\$DOMAIN\$\\$MAILBOX\$\".

Configurer manuellement les liens vers les pièces jointes

Choisissez cette option si vous souhaitez désigner le dossier dans lequel les pièces jointes extraites seront stockées. Vous devez indiquer le Chemin des pièces jointes et l'URL du Webmail lorsque vous choisissez cette option.

Chemin des pièces jointes

Dans cette zone de texte, indiquez le dossier dans lequel les pièces jointes extraites seront stockées. Vous pouvez définir un chemin d'accès statique ou utiliser des macros de<u>modèles</u> and et de <u>scripts</u> with pour rendre le chemin d'accès dynamique. Par exemple, "\$ROOTDIR\$\Attachments\\$DOMAIN\$\" regroupera toutes les pièces jointes dans un sous-dossier nommé en fonction du domaine auquel appartient l'utilisateur, qui se trouve sous un autre sousdossier appelé "Pièces jointes" contenu dans le dossier racine de MDaemon (généralement C:\MDaemon\). Ainsi, pour"user1@example.com", l'exemple cidessus placerait les pièces jointes extraites dans le sous-dossier "C: \MDaemon\Attachments\example.com\". Vous pourriez subdiviser davantage le stockage des pièces jointes en ajoutant la macro de modèle"\$MAILBOX\$" à l'exemple ci-dessus. Ainsi, les fichiers de l'utilisateur 1 seraient stockés dans un sous-dossier sous "\example.com\" appelé "user1" Dans ce cas, le nouveau chemin de fichier serait : "C:

\MDaemon\Attachments\example.com\user1\".

URL de Webmail

Saisissez ici l'URL de la messagerie Web (par exemple, "http://mail.example.com:3000/WorldClient.dll"). MDaemon utilisera cette URL pour insérer les liens vers les pièces jointes jointes extraites dans les messages.

Ignorer les pièces jointes inférieures à (en Ko, 0 = pas de limite)

Il s'agit de la taille minimale requise pour qu'une pièce jointe soit extraite d'un message. Utilisez cette option si vous ne souhaitez pas extraire les pièces jointes plus petites. Si cette valeur est fixée à "0", Liens vers les pièces jointes extrait toutes les pièces jointes, quelle que soit leur taille.

Supprimer les pièces jointes de plus de (en jours, 0 = jamais)

Utilisez cette option si vous souhaitez fixer une limite au nombre de jours pendant lesquels les pièces jointes seront stockées. Lors du nettoyage quotidien, MDaemon supprime les pièces jointes stockées depuis plus longtemps que la limite fixée, si elles se trouvent dans le dossier par défaut ou dans l'un de ses sous-dossiers. Le dossier par défaut est :"<MDaemonRoot>\Attachments\...". Les pièces jointes ne seront pas supprimées si vous personnalisez le dossier des pièces jointes pour qu'il pointe ailleurs. Cette option est désactivée par défaut (valeur "0").

Supprimer les pièces jointes du disque une fois les messages effacés

Cliquez sur cette option si vous souhaitez supprimer les pièces jointes extraites du serveur lorsque les messages auxquels elles sont liées sont supprimés.

Lorsque cette option est activée et qu'un utilisateur collecte son courrier électronique via un client POP3 qui n'est pas configuré pour laisser des messages sur le serveur, toutes les pièces jointes extraites seront irrémédiablement perdues. Si cette option n'est pas activée, aucune pièce jointe ne sera perdue, mais une grande partie de l'espace de votre disque dur pourrait être occupée par des fichiers périmés et inutiles dont le destinataire initial ne veut plus ou n'a plus besoin. Pratiquement tous les clients POP ont la possibilité de laisser des messages sur le serveur.

Extraire les pièces jointes "text/plain" imprimables et cotées

Non (par défaut), les pièces jointes jointes imprimables "texte/plain" ne seront pas extraites. Cochez cette case si vous souhaitez les inclure dans l'extraction automatique.

Liste des Exceptions

Cliquez sur ce bouton pour ouvrir la liste des Exceptions Liens vers les pièces jointes jointes. Ajoutez-y les noms des fichiers que vous ne souhaitez pas extraire des messages. Non (par défaut), Winmail.dat est inclus dans cette liste.

Texte d'en-tête From : TO : dans l'en-tête FROM

Utilisez cette option pour modifier le texte explicatif que MDaemon placera dans les messages lorsqu'il remplacera une pièce jointe par un lien. Non par défaut, il utilise le texte suivant : "MDaemon a Remplacé les fichiers suivants par ces liens :"

Nom de fichier HTML

Cette option permet de modifier le Nom du fichier HTML qui sera utilisé pour accéder aux pièces jointes liées. Non (par défaut), MDaemon utilise : "attachmentlinks.html"

Voir :

<u>Nouveau Modèles de comptes</u> ଖେବି <u>Mon compte | Pièces jointes</u> 78ମି <u>Macros de modèle</u> ଛେଗି <u>Macros de script</u> ଉତ୍ତି

3.6.5 CalDAV & CardDAV

🧐 Services web, & MI - CalDAV & CardDAV	
Webmail MDaemon Remote Admin Conditions d'utilisation Liens vers les pièces jointes CalDAV & CardDAV XMPP	CalDAV est un standard Internet ouvert conçu pour le partage de données de calendrier et de lanification. Le serveur CalDAV de MDaemon permet à un client CalDAV authentifié d'accéder ux données de calendrier et de planification stockées dans MDaemon. Plusieurs clients peuvent iccéder aux mêmes informations, ce qui donne la possibilité d'effectuer des planifications sommunes et de partager des données. CardDAV est un standard Internet ouvert conçu pour l'accès aux informations de carnet l'adresses. Le serveur CardDAV de MDaemon permet à un client CardDAV authentifié d'accéder ux informations de carnet d'adresses stockées dans MDaemon. Vebmail est requis et doit être activé pour utiliser CalDAV ou CardDAV. Image: Activer les services CalDAV & CardDAV Sélectionnez le domaine Image: Activer les services CalDAV & CardDAV pour ce domaine Niveau de journalisation (2) Normal Image: MDWebDAV! expertes et des réponses HTTP Activer la journalisation des requêtes et des réponses HTTP Activez cette option uniquement si le service technique vous le demande. En l'activant, le dossier "MDWebDAV!" est créé dans le répertoire "Logs" de MDaemon, et contient la copie des données envoyées et reçues par les serveus CalDAV & CardDAV. Cliquez ici pour obtenir de l'aide sur la configuration du client CalDAV
	OK Annuler Appliquer Aide

CalDAV est un standard Internet pour la gestion et le partage des calendriers et des informations de planification. La prise en charge de CalDAV par MDaemon permet à vos comptes d'utiliser n'importe quel client prenant en charge CalDAV pour accéder à leurs calendriers et tâches personnels et les gérer. Ils peuvent également accéder à tous les calendriers ou tâches <u>publics</u> [325] ou <u>partagés</u> [796] en fonction de <u>leurs droits d'accès</u> [327]. CardDAV est une norme permettant d'accéder aux contacts et aux carnets d'adresses. Le serveur CardDAV de MDaemon permet à un client CardDAV authentifié d'accéder aux informations de contact stockées dans MDaemon.

Activer les serveurs CalDAV & CardDAV

La prise en charge de CalDAV & CardDAV est activée par défaut. Cependant, le Webmail est nécessaire et <u>doit</u> donc <u>être activé</u> pour pouvoir être utilisé. Désactivez cette option si vous ne souhaitez pas prendre en charge CalDAV & CardDAV. Pour l'activer/désactiver pour des domaines individuels, utilisez les options ci-dessous.

Modifier les paramètres < Domain CalDAV & CardDAV par défaut - Domaines

Dans un premier temps, tous les domaines de MDaemon auront CalDAV/CardDAV activé ou désactivé en fonction de la sélection *Défaut* dans la liste déroulante*Sélectionner le domaine.* Pour modifier les paramètres par défaut :

1. Dans la liste déroulante *Sélectionnez domaine*, choisissez **Défaut**.

- Cochez la case en regard de Activer le service CalDAV & CardDAV pour ce domaine si vous voulez que CalDAV/CardDAV soit activé par défaut pour tous les domaines, ou décochez la case si vous voulez qu'il soit désactivé par défaut.
- 3. Cliquez sur Ok.

Activer/Désactiver CalDAV & CardDAV pour des domaines spécifiques

Pour remplacer les paramètres du Domaine CalDAV & CardDAV*par défaut* pour des domaines individuels :

- 1. Dans la liste déroulante*Sélectionnez le domaine*, choisissez un domaine spécifique.
- Cochez la case en regard de Activer le service CalDAV & CardDAV pour ce domaine si vous souhaitez que le service CalDAV/CardDAV soit activé pour le domaine, ou décochez la case si vous souhaitez qu'il soit désactivé.
- 3. Cliquez sur **OK**.

Pas de journalisation

Pas de journalisation

Utilisez cette liste déroulante pour désigner le degré de journalisation des activités de CalDAV & CardDAV. Il existe six niveaux de journalisation possibles : 1-Journalisation de débogage, 2-Journalisation normale (par défaut), 3-Avertissements et erreurs uniquement, 4-Erreurs uniquement, 5-Erreurs critiques uniquement, et 6-Pas de journalisation. Il s'agit d'un paramètre global qui ne peut pas être appliqué à des domaines spécifiques.

Activer la journalisation des requêtes et des réponses HTTP

Si cette option est activée, un dossierMDWebDAVest créé dans le dossier de journalisation de MDaemon. Toutes les données envoyées et reçues par le Serveur CalDAV & CardDAV seront journalisées dans ce dossier. En règle générale, cette option n'est utilisée qu'à des fins de diagnostic et ne doit pas être activée, sauf si le support technique vous le demande.

Configuration des clients CalDAV

Pour configurer les clients qui prennent en charge la <u>RFC 6764 (Locating Services for</u> <u>Calendaring Extensions to WebDAV (CalDAV)</u>, seuls le serveur, le nom d'utilisateur et le mot de passe devraient être requis. Vous pouvez configurer vos enregistrements DNS de manière à ce que le client soit dirigé vers l'URL correcte. Dans le cas où un enregistrement DNS n'a pas été configuré, l'utilisateur peut saisir une "URL bien connue" spéciale dans le client : "hostname/.well-known/caldav". Exemple : http://example.com:3000/.well-known/caldav . Le serveur Web intégré du Webmail prend en charge l'URL bien connue.

Les clients qui ne prennent pas en charge la localisation automatique du service CalDAV, comme Mozilla Thunderbird via le plugin Lightning, auront besoin d'une URL complète pour chaque liste de calendriers et de tâches. Les URL CalDAV de MDaemon sont construites comme suit :

Calendriers et Tâches

Calendrier ou liste de tâches par défaut de l'utilisateur :

http://[hôte]/webdav/calendrier
(Exemple : http://example.com:3000/webdav/calendar)

http://[host]/webdav/tasklist
(ex. http://example. com/webdav/tasklist)

Calendrier ou liste de tâches personnalisés de l'utilisateur :

http://[hôte]/webdav/calendar/[nom du calendrier]
(par exemple http://example.com/webdav/calendar/personal)

http://[hôte]/webdav/tasklist/[nom de la liste de tâches]
(par exemple : http://example.com/webdav/tasklist/todo)

Calendrier personnalisé de l'utilisateur ou liste de tâches dans un sous-dossier :

http://[host]/webdav/calendar/[folder]/[calendar-name]
(p.ex. http://example. com/webdav/calendar/my-stuff/personal)

http://[host]/webdav/tasklist/[folder]/[tasklist-name]
(ex. http://example. com/webdav/tasklist/my-stuff/todo)

Calendriers et tâches partagés

Calendrier ou liste de tâches par défaut d'un autre utilisateur :

http://[hôte]/webdav/calendars/[domaine]/[utilisateur]
(p.ex. http://example. com/webdav/calendars/example.net/frank)

http://[hôte]/webdav/tasks/[domaine]/[utilisateur]
(ex. http://example. com/webdav/tasks/example.net/frank)

Calendrier personnalisé ou liste de tâches d'un autre utilisateur :

http://[host]/webdav/calendars/[domain]/[user]/[calendar-name]
(e.g. http://example.com/webdav/calendars/example.net/frank/personal)

http://[host]/webdav/tasks/[domain]/[user]/[tasklist-name]
(e.g. http://example.com/webdav/tasks/example.net/frank/todo)

Calendriers et tâches publics

Le calendrier ou la liste de tâches par défaut du Domaine par défaut - Domaine :

http://[host]/webdav/public-calendars/[domain]
(ex. http://example.com/webdav/public-calendars/example.com)

http://[host]/webdav/public-tasks/[domain]
(e.g. http://example.com/webdav/public-tasks/example.com)

Calendrier ou liste des dossiers dans la racine de la hiérarchie des Dossiers publics :

http://[hôte]/webdav/public-calendars/[nom-du-calendrier]
(par ex. http://example. com/webdav/public-calendars/holidays)

http://[hôte]/webdav/public-tasks/[nom de la liste des tâches]
(par exemple http://example.com/webdav/public-tasks/projects)

Il convient d'être particulièrement vigilant si l'on teste le client OutlookDAV. Si plusieurs profils MAPI existent, nous avons vu le client envoyer des commandes de suppression au serveur pour tous les éléments du calendrier renvoyés par le serveur. OutlookDAV ne prend en charge que le profil MAPI par défaut.



Pour plus d'informations sur la configuration des clients CalDAV, cherchez " CalDav " dans la <u>Base de connaissances de CalDAV</u>.

Configuration des clients CardDAV

Pour configurer les clients qui prennent en charge la <u>RFC 6764 (Locating Services for</u> <u>Calendaring Extensions to WebDAV (CalDAV) and vCard Extensions to WebDAV</u> (<u>CardDAV</u>), seuls l'adresse du serveur, le nom d'utilisateur et le mot passe sont requis. Le carnet d'adresses d'Apple et iOS prennent en charge cette norme. Des enregistrements DNS peuvent être configurés pour diriger le client vers l'URL correcte. Dans le cas où aucun enregistrement DNS n'a été configuré, les clients interrogent une "URL bien connue" qui, dans le cas de CardDAV, est /.bien connue/carddav. Le serveur web intégré du Serveur Web prend en charge cette URL bien connue. Les clients qui ne prennent pas en charge la localisation automatique du service CardDAV exigeront une URL complète.

Les principaux clients CardDAV sont Apple Contacts (inclus dans Mac OS X), Apple iOS (iPhone) et Mozilla Thunderbird via le <u>plugin SOGO</u>.

Depuis OS X 10.11 (EL Capitan), l'application Apple Contacts ne prend en charge qu'une seule collection/un seul dossier. Lorsque le serveur CardDAV détecte l'application Apple Contacts, il ne renvoie que le dossier de contacts par défaut de l'utilisateur authentifié. Dans OS X 10.11 (EL Capitan), un problème connu empêche l'ajout d'un compte CardDAV à l'aide de la vue "Avancé" de la boîte de dialogue.

Accès aux carnets d'adresses

Le chemin "addressbook" est un raccourci vers votre propre carnet d'adresses par défaut.

```
http://[host]/webdav/addressbook - votre dossier de contacts par défaut.
```

```
http://[host]/webdav/addressbook/friends - votre dossier de contacts
    "amis".
```
Accès aux Dossierssierssierssiers partagés d'un autre utilisateur auxquels vous avez accès

Le chemin "contacts" est un raccourci vers les dossiers de contacts partagés.

- http://[host]/webdav/contacts/example.com/user2/myfolder le dossier de contacts "myfolder" de user2@example.com

Accéder aux Dossiers publics auxquels vous avez accès

Le chemin "public-contacts" est un raccourci vers les Dossiers publics de contacts.

http://[host]/webdav/public-contacts/foldername - dossier de contacts
 "foldername" à la racine de la hiérarchie des dossiers publics.



Il convient d'être particulièrement vigilant si l'on teste le client OutlookDAV. OutlookDAV ne prend en charge que le profil MAPI par défaut. Si plusieurs profils MAPI existent, le client peut envoyer au serveur des commandes de suppression pour tous les éléments renvoyés par le serveur.



Pour plus d'informations sur la configuration des clients CardDAV, cherchez " CardDav " dans la <u>Base de connaissances</u> <u>CardDAV</u>.

3.6.6 XMPP

🧐 Web & IM Services - XMPP	
Webmail Remote Administration Terms of Use Attachment Linking CalDAV & CardDAV	XMPP Server MD aemon's XMPP server allows you to send and receive instant messages using your favorite Jabber capable client. Enable XMPP Server Enable SSL Port 5222 SSL Port 5223 Log message conversation Enable BOSH Server (for Webmail IM) HTTP Port 7070 HTTPS Port 7443 Hostname Configure Persistent Chat Room
	Ok Cancel Apply Help

MDaemon est équipé d'un serveur XMPP (Extensible Messaging and Presence Protocol), parfois appelé serveur Jabber. Cela permet à vos utilisateurs d'envoyer et de recevoir des messages instantanés à l'aide de la <u>Messagerie instantanée de MDaemon</u> at de <u>clients XMPP</u> tiers, tels que <u>Pidgin</u>, <u>Gajim</u>, <u>Swift</u> et bien d'autres. Des clients sont disponibles pour la plupart des systèmes d'exploitation et des plateformes de périphériques mobiles.

Le serveur XMPP est installé en tant que service Windows, et les ports par défaut du serveur sont 5222 (SSL via STARTTLS) et 5223 (SSL dédié). Le serveur XMPP Activera la configuration SSL de MDaemon si elle est activée dans MDaemon. Par ailleurs, certains clients XMPP utilisent les enregistrements DNS SRV pour la découverte automatique des noms d'hôte. Pour plus d'informations, consultez le site http://wiki.xmpp.org/web/SRV_Records.

Les utilisateurs se connectent via le client XMPP de leur choix en utilisant leur adresse électronique et leur mot de passe. Dans certains clients, cependant, l'adresse électronique doit être divisée en plusieurs éléments pour la connexion. Exemple : au lieu de "frank@example.com", certains clients exigent que vous utilisiez "frank" comme nom de connexion/nom d'utilisateur et "example.com" comme domaine.

Pour le service de discussion multi-utilisateurs/groupe, les clients l'affichent généralement sous forme de "salles" ou de "conférences". Lorsque vous souhaitez démarrer une session de discussion de groupe, créez une salle/conférence (en lui donnant un nom) et invitez ensuite les autres utilisateurs à cette salle. Pour la plupart des clients, il n'est pas nécessaire d'indiquer l'emplacement du serveur pour la conférence; il suffit de lui donner un nom. Toutefois, si vous devez le faire, utilisez "conference.<votre domaine>" comme emplacement (par exemple, conference.exemple.com). Dans certains clients, vous devez saisir le nom et l'emplacement ensemble sous la forme : "room@conference.<votre domaine>" (par exemple, Room01@conference.example.com).

Certains clients (tels que <u>Pidgin</u>) prennent en charge le service de recherche d'utilisateurs, ce qui vous permet de chercher des utilisateurs sur le serveur par leur nom ou leur adresse électronique, ce qui facilite grandement l'ajout de contacts. En général, vous n'aurez pas à indiquer un lieu de recherche, mais si on vous le demande, utilisez "search.<votre domaine>" (par exemple, search.example.com). Lors de la recherche, le symbole % peut être utilisé comme joker. Ainsi, vous pouvez utiliser "% @example.com" dans le champ de l'adresse électronique pour afficher une liste de tous les utilisateurs dont l'adresse électronique se termine par "@example.com".

Serveur XMPP

Activer le serveur XMPP

Cliquez sur cette option pour Activer le serveur XMPP. Pour autoriser la messagerie instantanée, vous devez également vous assurer que l'option **Activer la messagerie instantanée** est activée sur l'écran<u>MDIM.</u>

Activer SSL

Cliquez sur cette option si vous souhaitez prendre en charge SSL pour le Serveur XMPP, en utilisant le *Port SSL* spécifié ci-dessous. **Remarque :** ceci s'applique également à l' option*Port HTTPS du* serveur BOSH ci-dessous.

Port

Le port par défaut pour XMPP est 5222, qui prend en charge SSL via STARTTLS.

Port SSL

Le port SSL dédié à XMPP est 5223.

Redémarrer le serveur XMPP

Cliquez sur ce bouton pour Redémarrer le serveur XMPP.

Enregistrer les discussions dans le journal

Par défaut, toutes les conversations de messages instantanés sont enregistrées dans un fichier appelé XMPPServer-<date>.log, situé dans le dossierMDaemon\Logs\. Décochez cette case si vous ne souhaitez pas journaliser les conversations.

Activer le serveur BOSH (pour la messagerie instantanée)

Cliquez sur cette option pour activer le serveur BOSH, permettant la messagerie instantanée au sein de MDaemon Webmail.

Port HTTP

Non les paramètres par défaut le serveur BOSH utilise le port HTTP 7070.

Port HTTPS

Le serveur BOSH utilise ce port HTTPS lorsque l' option*Activer SSL* ci-dessus est activée. Le port par défaut est 7443.

Nom d'hôte

Utilisez cette option pour spécifier un nom d'hôte si nécessaire.

Configurer des salles de discussion permanentes

Cliquez sur ce bouton pour ouvrir la boîte de dialogue Salles de discussion de groupe. Normalement, lorsqu'un utilisateur crée une salle de discussion, celle-ci disparaît lorsque la dernière personne quitte la salle, mais vous pouvez utiliser ces options pour créer des salles de discussion permanentes qui resteront en place même si elles sont vides. Vous pouvez également supprimer des salons et convertir des salons temporaires existants en salons permanents.

0	Group Chat Rooms				×
	Select chat service	conference.company.test			~
	Chat room		Description		Persistent
	DeptA@conference.	company.test	Department A's Chat Room		Yes
	<				>
	<u>N</u> ew <u>D</u> elete	<u>M</u> ake Persistent			
				ОК	Cancel

Sélectionnez un service de chat

Sélectionnez le service de discussion pour afficher les salles de discussion de ce domaine.

Nouveau

Cliquez sur ce bouton pour ajouter un salon de discussion permanent.

New Chat Room		×
Chat service:	conference.company.test	~
Room name:	DeptA	
Room description:	Department A's Chat Room	
Password (optional):		
		OK Cancel

Sélectionnez un service de chat

Sélectionnez le service de chat pour la salle.

Votre nom de salle

Nom et type de la salle de discussion, sans espace.

Description de la salle

Incluez ici une description de la salle. Les utilisateurs verront cette description lorsqu'ils sélectionneront une salle à rejoindre.

Mot de passe (facultatif)

Si vous souhaitez demander un mot de passe pour participer à la discussion, entrez le mot de passe ici.

Supprimer

Si vous souhaitez supprimer un salon, sélectionnez-le et cliquez sur ce bouton pour le supprimer.

Rendre permanent

Si un salon de discussion temporaire figure dans la liste, sélectionnez-le et cliquez sur ce bouton si vous souhaitez le rendre permanent.

Voir :

Webmail | MDIM 346

3.7 Programmation d'événement

3.7.1 Programmation antivirus

3.7.1.1 Mises à jour antivirus

🧐 Programmation d'événement - Mises à jour AntiVirus		
 Programmation d'événement - Mises à jour Programmation antivirus Mises à jour AntiVirus Programmation Programmation Programmation de courrier 	AntiVirus Mises à jour AntiVirus Attendre 240 minutes après la dernière mise à jour antivirus avant d'en lancer une autre	
	OK Annuler Appliquer Aid	e

Mises à jour AntiVirus

Attendre [xx] minutes après la dernière mise à jour de l'AntiVirus avant de procéder à une nouvelle mise à jour.

Cochez cette case et indiquez le nombre de minutes que vous voulez qu'AntiVirus attende avant de vérifier les nouvelles mises à jour des signatures de virus. Notez qu'il s'agit en fait du nombre de minutes qu'AntiVirus *tentera d'* attendre après la dernière vérification d'une mise à jour, que la mise à jour ait été déclenchée par le programmateur ou manuellement. Le programmateur et les mises à jour déclenchées manuellement ont la priorité sur ce paramètre et réinitialiseront donc ce compteur si un événement de mise à jour AntiVirus est déclenché par l'une de ces autres méthodes. Ainsi, par exemple, si vous avez défini cette option pour vérifier les mises à jour toutes les 240 minutes et que vous vérifiez manuellement la présence d'une mise à jour au bout de 100 minutes, ce compteur sera réinitialisé à 240.

Voir :

Mises à jour AntiVirus AntiVirus Mises à jour AntiVirus 723

3.7.1.2 Programmation

🧐 Programmation d'événement - Programmation				
Programmation antivirus Mises à jour AntiVirus Programmation Programmation Programmation de courrier	Programmer [[Tous les jours] from [00:20] to [23:59], recurring every [60] minutes			
	Jour(s) Supprimer la programmation Supprimer Effacer tout Tous les jours De A Toutes les minutes Ajouter Indiquez des heures au format 24 heures comme : 7:15 ou 22:10 Laissez les champs 'A' et 'Toutes les' vides pour créer un événement unique. OK Annuler Appliquer Aide			

Le calendrier des mises à jour de l'AntiVirus permet de définir des heures précises pour la vérification des mises à jour de l'AntiVirus. Le programme se trouve à l'adresse suivante Configuration | Programmation d'événements | AntiVirus Planification | Planification.

Planifier

Supprimer

Pour supprimer un événement de la liste, sélectionnez l'entrée, puis cliquez sur ce bouton.

Effacer tout

Ce bouton permet de supprimer toutes les entrées de la planification.

Création d'événements de la programmation

Jour(s)

Lors de la création d'un nouvel événement pour la programmation, commencez par sélectionner le ou les jours au cours desquels cet événement de contrôle des mises à jour programmées se produira. Vous pouvez sélectionner : Tous les jours, les jours de la semaine (du lundi au vendredi), les week-ends (samedi et dimanche) ou certains jours de la semaine.

De...

Saisissez l'heure à laquelle vous souhaitez que le contrôle de mise à jour commence. L'heure doit être au format 24 heures, de 00:00 à 23:59. Si vous souhaitez qu'il s'agisse d'un événement unique plutôt que d'un événement récurrent, c'est la seule valeur temporelle que vous devez saisir (laissez les options À... et *Toutes les...* vides).

À...

Saisissez l'heure à laquelle vous souhaitez que l'événement de vérification de la mise à jour se termine. L'heure doit être au format 24 heures, de 00:01 à 23:59, et elle doit être supérieure à la valeur *De...*. Exemple : si la valeur*De...* était "10:00", cette valeur pourrait être comprise entre "10:01" et "23:59". Laissez cette option vide si vous souhaitez qu'il s'agisse d'un événement unique plutôt que d'un événement récurrent.

Toutes les [xx] minutes.

Il s'agit de l'intervalle de temps pendant lequel AntiVirus vérifiera les mises à jour entre les heures*De début à...* et À...désignées . Laissez cette option vide si vous souhaitez qu'il s'agisse d'un événement unique plutôt que d'un événement récurrent.

Ajouter

Une fois que vous avez indiqué le (s) jour(s) et l' heure de début à..., ainsi que l'heure de fin à... et la valeur derécurrence Toutes les..., cliquez sur ce bouton pour ajouter l'événement à la programmation.

Voir :

 Mises à jour AntiVirus
 402

 AntiVirus
 718

 Mises à jour AntiVirus
 723

3.7.2 Programmation de courrier

3.7.2.1 Envoi & collecte de courrier

🧐 Programmation d'événement - Envoi & collect	te de courrier 🛛 💌
Programmation antivirus Programmation de courrier Collecte MultiPOP Default' -Programmation	Paramètres Généraux Paramètres Généraux Distribuer les messages dès qu'ils entrent dans la file d'attente y compris pour les passerelles Envoyer uniquement les messages mis en file d'attente au cours des Intervalles Nom Default Nom Vouveau Supprimer Envoyer le courrier à un intervalle de: 5 minutes 1 60 Attendre 10 minutes après le dernier envoi avant de lancer le suivant Envoyer le courrier s'il y a 5 messages ou plus dans la file d'attente Envoyer si un message est en attente depuis Associer cette programmation à la file C:\MD aemon\Queues\Remote\ Files d'attente
	OK Annuler Appliquer Aide

Cliquez sur Configuration | Programmation d'événements pour ouvrir leprogrammateur d'événements de MDaemon. Cet écran vous permet de programmer lesévénements de traitement du courrier distant de MDaemonde la manière la plus complète ou la plus simple possible. Vous pouvez utiliser un compteur pour traiter le courrier à intervalles réguliers ou programmer des heures précises pour la distribution et la collecte du courrier à l'aide des écrans <u>Mail Schedule</u>.

3.7.2.2 Collecte MultiPOP

406

Event Scheduling - MultiPOP Collection	X
AntiVirus Scheduling Mail Scheduling Mail Sending & Collecting MultiPOP Collection "Default' Schedule	MultiPOP Collection Collect MultiPOP mail every time remote mail is processed Collect MultiPOP mail once every But no more often than Wait at least Output Dutter the set of times per hour Wait at least Output Dutter the set of times between each collection
	Ok Cancel Apply Help

Collecte MultiPOP

Collecter le courrier MultiPOP lors du traitement du courrier distant

Choisissez cette option si vous voulez que MDaemon collecte tout le courrier <u>MultiPOP</u> [792] lors du traitement du courrier distant.

Collecter le courrier MultiPOP au bout de [xx] fois que le courrier distant est traité

Choisissez cette option et indiquez un chiffre dans la case si vous souhaitez que la Collecte du courrier MultiPOP soit inférieure à la fréquence de traitement du courrier distant. Le chiffre indique combien de fois le courrier distant sera traité avant que le courrier MultiPOP ne soit collecté.

Collecter le courrier MultiPOP dynamiquement

Choisissez cette option si vous souhaitez collecter les messages MultiPOP de manière dynamique. En règle générale, la Collecte du courrier MultiPOP est effectuée pour tous les utilisateurs en même temps, à chaque intervalle de traitement du courrier distant ou tous les *x* intervalles. Lorsqu'ils sont collectés dynamiquement, les messages MultiPOP sont collectés pour chaque utilisateur lorsque celui-ci consulte son courrier local via POP, IMAP ou Webmail, et non pour tous les utilisateurs en même temps. Toutefois, comme la Collecte MultiPOP est déclenchée par un utilisateur qui consulte son courrier électronique, les nouveaux messages MultiPOP collectés ne seront pas visibles pour l'utilisateur tant qu'il n'aura pas consulté à *nouveau* son courrier . Il devra donc consulter son courrier à deux reprises pour voir

les nouveaux messages MultiPOP. La première fois pour déclencher la Collecte MultiPOP et la deuxième fois pour voir le courrier qui a été collecté.

Mais pas plus de [xx] fois par heure.

Dans le but de réduire la charge que l'utilisation intensive de MultiPOP peut potentiellement imposer à votre MDaemon, vous pouvez utiliser ce contrôle pour spécifier un nombre maximum de fois par heure que MultiPOP peut être collecté pour chaque utilisateur.

Attendre au moins [xx] minutes entre chaque collecte

Cette option permet de réduire la charge du serveur de messagerie en limitant la fréquence à laquelle les messages Collecte MultiPOP peuvent être collectés par chaque utilisateur. Elle limitera la Collecte courrier MultiPOP au bout à une fois toutes les tant de minutes par utilisateur. User specified the number of minutes that you wish to require the user to wait before being allowed to check MultiPOP again.

Voir :

MultiPOP 144 Mon compte | MultiPOP 792

3.7.2.3 Programmation de courrier

🧐 Programmation d'événement - 'Default' -Prog	grammation
Programmation antivirus Programmation antivirus Programmation de courrier Collecte MultiPOP Default' -Programmation	Programmer
	Jour(s) Supprimer la programmation Supprimer Effacer tout Tous les jours ▼ De À Toutes les Indiquez des heures au format 24 heures comme : 7:15 ou 22:10 Laissez les champs 'À' et 'Toutes les' vides pour créer un événement unique.
	OK Annuler Appliquer Aide

Chaque calendrier de courrier correspond au calendrier du même nom figurant dans la liste déroulante *Nom de* l'<u>écran Envoi et collecte du courrier</u>. (405) Utilisez chaque calendrier de courrier pour désigner les heures spécifiques auxquelles le traitement(s) du courrier distant aura lieu pour ce calendrier. Les calendriers d'envoi se trouvent à l'adresse suivante Configuration | Programmation d'événements | Programmation d'envois | Programme 'ScheduleName'.

Programme

Supprimer programmation

Ce bouton permet de supprimer la programmation personnalisée. La programmation sera supprimée et son entrée sera supprimée de la liste déroulante *Nom de*<u>l'écran</u> <u>Mes listes de diffusion.</u> ADE Après avoir cliqué sur ce bouton, une boîte de confirmation s'ouvre pour vous demander si vous êtes sûr de vouloir supprimer la programmation. Cette option n'est disponible que pour les programmations personnalisées - la programmation par défaut ne peut pas être supprimée.

Supprimer

Pour supprimer une entrée de la liste, sélectionnez-la, puis cliquez sur ce bouton.

Effacer tout

Ce bouton permet de supprimer toutes les entrées de la programmation.

Création d'événements de programmation

Jour(s)

Lorsque vous créez un nouvel événement pour la programmation, sélectionnez d'abord le ou les jours où cet événement de programmation se produira. Vous pouvez sélectionner : Tous les jours, les jours de la semaine (du lundi au vendredi), les week-ends (samedi et dimanche) ou des jours spécifiques de la semaine.

De...

Saisissez l'heure à laquelle vous souhaitez que l'événement débute. L'heure doit être au format 24 heures, de 00:00 à 23:59. Si vous souhaitez qu'il s'agisse d'un événement unique plutôt que d'un événement récurrent, c'est la seule valeur horaire que vous devez saisir (laissez les options À... et *Toutes les...* vides).

À...

Saisissez l'heure à laquelle vous souhaitez que l'événement se termine. L'heure doit être au format 24 heures, de 00:01 à 23:59, et doit être supérieure à la valeur *De début....* Exemple : si la valeur*De...* était "10:00", cette valeur pourrait être comprise entre "10:01" et "23:59". Laissez cette option vide si vous souhaitez qu'il s'agisse d'un événement unique plutôt que d'un événement récurrent.

Toutes les [xx] minutes.

Il s'agit de l'intervalle de temps pendant lequel le courrier sera traité entre les heures*De début à...* et À...désignées. Laissez cette option vide si vous souhaitez qu'il s'agisse d'un événement unique plutôt que d'un événement récurrent.

Ajouter

Une fois que vous avez indiqué le (s) jour(s) et l' heure de début à..., ainsi que l'heure de fin à... et la valeur derécurrence Toutes les..., cliquez sur ce bouton pour ajouter l'événement à la programmation.

Selon vos besoins, il peut suffire d'utiliser les options de programmation simples de l' écran<u>Envoi et collecte du</u> <u>courrier</u> option contrôler les intervalles de traitement du courrier. Exemple : il est inutile d'établir une programmation spécifique avec des événements pour chaque minute de chaque jour, alors qu'il suffit de régler la barre de défilement de l'écran Programmation d'envoi et de collecte sur des intervalles d'une minute pour obtenir le même résultat. En revanche, si vous souhaitez que les intervalles de traitement soient espacés de plus d'une heure, ou seulement certains jours, vous pouvez utiliser une combinaison d'options de planification et d'heures spécifiques.

Voir :

Envoi et collecte du courrier 405 Mises à jour AntiVirus 402 Mises à jour de l'anti-spam 746

3.8 MDaemon Connector

La prise en charge de *MDaemon Connector* (MC) est une fonctionnalité sous licence disponible auprès de MDaemon Technologies. MC permet à tous vos utilisateurs qui le souhaitent d'utiliser Microsoft Outlook comme client de messagerie préféré lorsque MC est installé sur leur ordinateur. Il fournit des fonctionnalités de travail en groupe et de collaboration en connectant le client Outlook d'un utilisateur au serveur MDaemon, afin d'utiliser la messagerie électronique, le calendrier avec planification libre/occupé, le carnet d'adresses, les listes de distribution, les tâches et les notes d'Outlook.

Lorsque vous avez activé la prise en charge de MC, les écrans de MDaemon Connector sont disponibles dans la barre de menu de MDaemon, située à l'endroit suivant : Configuration | MDaemon Connector. Ce compte est utilisé pour activer et configurer MC et pour autoriser des comptes spécifiques à l'utiliser.

Pour plus d'informations, ou pour acquérir la fonctionnalité MDaemon Connector, visitez la page <u>MDaemon ConnectorMDaemon</u> à l'<u>adresse</u> <u>www.mdaemon.comwww.mdaemon.com.</u>

Voir :

Paramètres de serveur MC | Paramètres 410 Paramètres des serveurs | Comptes 412 Paramètres du client MC 413

3.8.1 Paramètres du serveur MC

3.8.1.1 Paramètres

🧐 MDaemon Connector - Paramètres	
Paramètres du serveur MC Paramètres Comptes Paramètres du client MC	 MDaemon Connector permet aux utilisateurs d'Outlook de créer, d'administrer, de synchroniser et de partager des dossiers de calendriers, contacts et tâches. Activer MDaemon Connector Afficher tous les comptes MDaemon pour tous les utilisateurs de MDaemon Connector Tous les comptes MDaemon seront affichés dans l'interface de MDaemon Connector. afficher uniquement les comptes du domaine de l'utilisateur Créer les dossiers partagés de MDaemon Connector Cliquez sur le bouton ci-dessus pour que MDaemon crée les dossiers Contacts, Calendrier, Tâches, Notes et Documents pour chacun de vos domaines.
	OK Annuler Appliquer Aide

MDaemon Connector

Activer le support MDaemon Connector

Cochez cette case pour Activer le support de MDaemon Connector (MC). Vos utilisateurs ne pourront pas utiliser les fonctionnalités de MC si cette option n'est pas activée.

Les utilisateurs MDaemon Connector peuvent voir tous les comptes MDaemon

Cliquez sur cette option si vous souhaitez que tous les comptes MDaemon autorisés à se connecter via MC soient visibles dans la liste des *autorisations* qui apparaît dans MDaemon Connector sur les clients des utilisateurs. Dans cette liste, les utilisateurs de MC peuvent choisir les comptes auxquels ils souhaitent accorder l'autorisation de partager leurs éléments Outlook. Dans le cas où cette option est désactivée, la liste des*autorisations de* MDaemon Connector sera vide et les utilisateurs devront saisir les adresses électroniques manuellement. Seules les adresses appartenant à des comptes autorisés à se connecter via MC pourront partager les éléments Outlook. Si un utilisateur saisit une adresse qui n'est pas autorisée, les éléments ne seront tout simplement pas partagés avec cette adresse, à moins qu'elle ne soit autorisée à se connecter via MC à un moment donné.

...Afficher uniquement les comptes du domaine de l'utilisateur MDaemon Connector Cette option n'est disponible que si l' option *Les utilisateurs MDaemon Connector peuvent voir tous les comptes MDaemon* est activée. Cochez cette case si vous souhaitez que seuls les utilisateurs autorisés à se connecter via MC, et qui appartiennent au même domaine, apparaissent dans la liste des*autorisations de* MDaemon Connector. Les comptes appartenant à des domaines différents ne seront pas listés, même s'ils sont autorisés à se connecter via MC.

Générer des Dossiers IMAP partagés dans MDaemon Connector

Cliquez sur ce bouton pour générer un ensemble de dossiers MC pour chaque domaine. Les dossiers suivants seront générés : Contacts, Rendez-vous, Journal, Tâches et Notes.

Voir :

Paramètres des serveurs MC | Comptes 412 Paramètres du client MC 413

3.8.1.2 Comptes

🧐 MDaemon Connector - Comptes		
 Paramètres du serveur MC Paramètres Comptes Paramètres du client MC 	Comptes MD aemon Connector frank.thomas@company.test michael.mason@company.test	
	Ajouter Supprimer Autoriser tous les comptes à se connecter avec MDaemon Connector Autoriser l'accès aux comptes dès leur première utilisation de MDaemon Connector	
OK Annuler Appliquer Aide		

Comptes MDaemon Connector

Il s'agit de la liste des comptes MDaemon autorisés à partager leurs dossiers Outlook, leurs calendriers, leurs contacts, leurs notes, etc. via MDaemon Connector. Vous pouvez ajouter des comptes à la liste en utilisant les options décrites cidessous.

Nouveau compte

Pour ajouter un compte MDaemon à la liste des Comptes MDaemon Connector autorisés, sélectionnez le compte souhaité dans cette liste déroulante, puis cliquez sur *Ajouter*. Pour supprimer un compte, sélectionnez-le puis cliquez sur *Supprimer*.

Autoriser tous les comptes à se connecter avec MDaemon Connector

Pour autoriser instantanément tous les comptes MDaemon à se connecter via MDaemon Connector, cliquez sur ce bouton et tous les comptes MDaemon seront ajoutés à la liste des*Utilisateurs MDaemon Connector*.

Autoriser l'accès aux comptes dès leur première utilisation de MDaemon Connector

Cochez cette case si vous souhaitez que des comptes individuels soient ajoutés à la liste *Comptes MDaemon Connector* la première fois qu'ils se connectent à l'aide de MDaemon Connector. <u>Remarque</u> : si vous activez cette option, vous avez alors autorisé tous les comptes MDaemon à utiliser MDaemon Connector. <u>MDaemon</u> Connector. Les comptes ne seront tout simplement pas ajoutés à la liste avant la première utilisation de chacun d'entre eux.

Voir :

Paramètres de serveur MC | Paramètres 410 Paramètres du client MC 413

3.8.2 Paramètres du client MC

 Paramètres du serveur MC Paramètres du client MC Général Avancé Dossiers Envoyer/Recevoir Divers Base de données Compléments Paramètres du client MC Ces écrans permettent de configurer les paramètres du module MD aemon Connector pour les utilisateurs de tous les domaines. Ces paramètres sont poussés vers l'ensemble des utilisateurs MD aemon Connector. Utilisez le Gestionnaire de domaines si, pour un domaine donné, vous souhaitez activer/désactiver ou ignorer ces paramètres par défaut et leur attribuer des valeurs différentes (Cloud uniquement). Cliquez ici pour en savoir plus sur MD aemon Connector. Paramètres du client MC Compléments Paramètres du client MC Compléments Paramètres du client MC à ignorer les paramètres pa
Lorsque la case est décochée, les paramètres du client MC correspondant à ceux poussés sont désactivés et non modifiables.
L'édition MDaemon Private Cloud (MDPC) inclut des fonctionnalités pour les fournisseurs de services cloud. Le service de messagerie hébergée peut être acheté directement auprès de MDaemon Technologies ou de son réseau de partenaires. Cliquez ici pour en savoir plus sur les options de messagerie dans le cloud de MDaemon.

La boîte de dialogue Paramètres du client MC permet de gérer de manière centralisée les paramètres du client de vos utilisateurs MDaemon Connector (MC). Configurez chaque écran avec les paramètres clients souhaités et MDaemon poussera ces paramètres vers les écrans clients correspondants si nécessaire, à chaque fois qu'un utilisateur MC se connectera au serveur. Les Paramètres du client MC ne sont envoyés aux clients que si l'un des paramètres a changé depuis la dernière fois que le client s'est connecté et les a reçus. Si l'option "*Autoriser les utilisateurs MC à ignorer les paramètres poussés*" est autorisée, les utilisateurs peuvent ignorer tous les paramètres poussés sur leurs clients individuels. Si cette option est désactivée, tous les écrans des clients sont alors verrouillés ; les utilisateurs de MC ne peuvent apporter aucune modification.

Pour permettre certains réglages qui doivent être différents pour chaque utilisateur ou domaine, les Paramètres clients MC prennent en charge des macros telles que \$USERNAME\$, \$EMAIL\$ et \$DOMAIN\$. Ces macros seront converties en données spécifiques à l'utilisateur ou au domaine lors de la transmission des paramètres à un client. Veillez à ne pas placer de valeurs statiques dans les champs qui devraient utiliser une macro, comme par exemple "Frank Thomas" dans le champ Votre nom. Pour vous faciliter la tâche, l' écran<u>Général</u> and comporte un bouton Références des macros qui affiche une liste simple des macros prises en charge.

Pour ceux qui utilisent MDaemon Private Cloud (MDPC), il existe une autre boîte de dialogue Paramètres du client MC dans le <u>Gestionnaire de domaines</u> (184), qui permet de contrôler les paramètres du client MDaemon Connector pour chaque domaine.

Cette fonctionnalité est désactivée par défaut et n'est prise en charge que dans la version 4.0.0 ou supérieure du client MDaemon Connector.

Paramètres du client MC

Pousser les paramètres client vers les utilisateurs MC

Activez cette option si vous souhaitez envoyer les paramètres préconfigurés dans les écrans des Paramètres clients MC à vos utilisateurs MC lorsqu'ils se connectent. Les Paramètres du client MC ne sont envoyés aux clients que si l'un des paramètres a été modifié depuis la dernière fois que le client s'est connecté et les a reçus. Cette option est désactivée par défaut.

Autoriser les utilisateurs MC à ignorer les paramètres poussés

Si cette option est activée, les utilisateurs peuvent remplacer n'importe quel paramètre poussé sur leurs clients individuels. Si elle est désactivée, tous les écrans des clients sont verrouillés ; les utilisateurs MDaemon Connector ne peuvent rien y changer.

Le fait d'autoriser les utilisateurs à remplacer les paramètres transmis n'empêchera pas le serveur de transmettre les modifications futures aux clients. Exemple : si un utilisateur modifie l'un de ses paramètres MDaemon Connector et que l'administrateur modifie ensuite l'un des écrans des Paramètres clients MC sur le serveur, tous les Paramètres clients MC seront poussés vers le client de cet utilisateur lors de sa prochaine connexion au serveur. Par conséquent, même les paramètres que l'utilisateur avait précédemment ignorés seront modifiés pour correspondre aux paramètres du serveur.

Découverte automatique des paramètres MC

Lors de la première configuration de MDaemon Connector sur le client, les utilisateurs peuvent cliquer sur le bouton *"Tester et obtenir les paramètres des comptes"* dans l'écran Général après avoir saisi leur *nom d'utilisateur* et leur *mot de passe*. MDaemon Connector tente alors de valider les informations d'identification et de récupérer automatiquement les Informations du compte sur le serveur.

Pour se connecter au serveur, le client essaie d'abord les valeurs FQDN courantes. Pour IMAP, il essaie de s'authentifier sur mail.<domaine> (par exemple mail.exemple.com) en utilisant le port SSL dédié, puis le port non-SSL avec TLS. Si cela échoue, il répète le même processus pour imap.<domaine>, puis <domaine>, et enfin, imap.mail.<domaine>. Si toutes les tentatives échouent, une connexion non chiffrée est tentée pour ces mêmes emplacements.

Pour SMTP, il essaie mail.<domaine> en utilisant les ports 587, 25, puis 465, d'abord en utilisant SSL, puis TLS. Cette opération est répétée pour smtp.<domaine>, <domaine>, puis smtp.mail.<domaine>. Si toutes les tentatives échouent, une connexion non chiffrée est tentée pour ces mêmes emplacements.

Si MDaemon Connector parvient à s'authentifier, les informations sur les serveurs entrant et sortant ainsi que les informations SSL & TLS sont configurées automatiquement.

Voir :

 Paramètres de serveur MC | Paramètres
 410

 Paramètres des serveurs | Comptes
 412

 Paramètres du client MC | Général
 415

3.8.2.1 Général

🧐 MDaemon Connector - Général		—
	Infos utilisateur	
⊕ Paramétres du serveur MC	Votre nom :	\$USERNAME\$
Général	Société :	
Avancé	E-mail :	\$EMAIL\$
Dossiers Envoyer/Recevoir Divers Base de données Compléments	Paramètres de compte Nom d'affichage: Infos serveur Courrier entrant (IMAP) Courrier sortant (SMTP) Infos identifiant de conne Nom d'utilisateur :	Outlook Connector for MDaemon \$FQDN\$ \$FQDN\$ xion \$EMAIL\$ ✓ Retenir le mot de passe
	La plupart de ces champs n données d'un champ et MD. défaut correspondant.	écessitent des macros. Effacez les aemon y intégrera le paramètre par
		OK Annuler Appliquer Aide

Si vous avez activé l'option "*Pousser les paramètres* du client *vers les utilisateurs MC*" dans l' écran <u>Paramètres clients MC</u>^[413], les paramètres de cet écran seront poussés vers l'écran correspondant du client MDaemon Connector chaque fois qu'un utilisateur MDaemon Connector se connectera au serveur. Les Paramètres du client MC ne sont envoyés aux clients que lorsque l'un des paramètres a changé depuis la dernière fois que le client s'est connecté et les a reçus. La plupart des champs de cet écran doivent contenir des macros plutôt que des valeurs statiques. Voir <u>Références des macros</u>^[417]

Infos utilisateur

Votre nom

Par défaut, cette option utilise la macro \$USERNAME\$, qui insère le Prénom et le Les nom de l'utilisateur. Ceux-ci apparaissent dans l'en-tête From des messages de l'utilisateur.

Organisation

Votre nom d'entreprise ou d'organisation peut être inséré dans cet espace facultatif.

Adresse électronique

Non par défaut, cette option utilise la macro \$EMAIL\$, qui insère l'adresse électronique de l'utilisateur. Cette adresse apparaît dans l'en-tête "From" des messages de l'utilisateur. Celle-ci apparaît dans l'en-tête From des messages de l'utilisateur.

Paramètres des comptes

Nom d'affichage

Ce nom est affiché dans Outlook afin que l'utilisateur puisse identifier le compte qu'il utilise. Ce compte est utile pour les utilisateurs qui ont plusieurs comptes dans leur profil. Seul l'utilisateur voit cette information. Paramètres par défaut : MDaemon Connector.

Infos serveur

Courrier entrant (IMAP)

Il s'agit du serveur auquel les clients MC accèdent pour collecter et gérer le courrier électronique de chaque utilisateur. Non (Paramètres par défaut) par "MDaemon Connector".

Courrier sortant (SMTP)

Il s'agit du serveur auquel les clients MC se connecteront pour envoyer les messages sortants de vos utilisateurs. Il s'agit souvent du même que le Serveur Courrier entrant (IMAP) ci-dessus. Non (Paramètres par défaut).

Infos identifiant de connexion

Nom d'utilisateur

Il s'agit du nom d'utilisateur nécessaire pour accéder et gérer le compte de messagerie MDaemon de chaque utilisateur. Il s'agit généralement de l'*adresse e-mail* indiquée ci-dessus. Non (par défaut), il est défini sur \$EMAIL\$.

Retenir le mot passe

Par défaut, les clients MDaemon Connector sont configurés pour enregistrer le mot de passe de l'utilisateur, de sorte que lorsque Outlook est lancé, il se connecte automatiquement au compte de messagerie sans demander d'informations d'identification. Désactivez cette option si vous souhaitez demander aux utilisateurs de saisir leur mot de passe au démarrage d'Outlook.

Références des macros

Pour permettre certains réglages qui doivent être différents pour chaque utilisateur ou domaine, les Paramètres clients MC prennent en charge des macros telles que \$USERNAME\$, \$EMAIL\$ et \$DOMAIN\$. Ces macros seront converties en données spécifiques à l'utilisateur ou au domaine lors de la transmission des paramètres à un client. Veillez à ne pas placer de valeurs statiques dans les champs qui devraient utiliser une macro, comme par exemple "Frank Thomas" dans le champ Votre nom. Si vous le faites, chaque utilisateur de MC qui se connecte à MDaemon aura pour nom "Frank Thomas". Cliquez sur le bouton Références des macros pour afficher la liste des macros disponibles :

\$USERNAME\$	Cette macro insère la valeur de l'option " <i>Prénom et nom</i> " sous l'écran Informations générales du compte de l'utilisateur . [765] Elle est équivalente à : "\$USERFIRSTNAME\$ \$USERLASTNAME\$"
ŞEMAIL	Insère l'adresse électronique de l'utilisateur. Cette adresse e-mail de l'utilisateur est équivalente à : "\$USERFIRNAME\$ \$USERLASTNAME\$". Cela équivaut à : "\$mailbox\$@\$domain" : \$MAILBOX\$@\$DOMAIN\$.
\$MAILBOX\$	Cette macro insère le Nom de Votre compte.
NOM DE L'UTILISATEUR	Cette macro résout le prénom du titulaire du compte.
\$USERFIRSTNAMELC\$ CETTE MACRO RÉSOUT LE PRÉNOM DU TITULAIRE DU COMPTE.	Cette macro résout le prénom du titulaire du compte, en lettres minuscules.
NOM DE FAMILLE DE L'UTILISATEUR	Cette macro permet d'obtenir le nom de famille du titulaire du compte.
\$USERLASTNAMELC\$ CETTE MACRO PERMET DE TROUVER LE NOM DE FAMILLE DU TITULAIRE DU COMPTE, EN LETTRES MINUSCULES.	Cette macro permet de trouver le nom de famille du titulaire du compte, en lettres minuscules.
\$USERFIRSTINITIAL	Cette macro permet d'obtenir la première lettre du prénom du titulaire du compte.
\$USERFIRSTINITIALLC\$ (PREMIER PRÉNOM DU TITULAIRE DU COMPTE)	Cette macro permet d'obtenir la première lettre du prénom du titulaire du compte, en minuscules.

<pre>\$USERLASTINITIAL\$ Cette macro permet d'obtenir la première lettre du (DERNIÈRE LETTRE INITIALE DE L'UTILISATEUR)</pre> Cette macro permet d'obtenir la première lettre du Prénom et du nom du titulaire du compte.
\$USERLASTINITIALLC\$Cette macro permet d'obtenir la première lettre du (NOM DE FAMILLE DE L'UTILISATEUR)Prénom et du nom du titulaire du compte, en minuscules.
<pre>\$MAILBOXFIRSTCHARSn\$ (boîte aux lettres - première lettre du nom de famille) où "n" est un nombre compris entre 1 et 10. Cette macro se développe jusqu'aux "n" premiers caractères du Nom de la BAL.</pre>
\$DOMAIN Insère le <u>domaine de la</u> 765 BAL du compte <u>.</u> 765
\$DOMAINIP\$Cette macro se résout en adresse IPv4domaine auquel le compte appartient.
<pre>\$DOMAINIP6\$ CETTE MACRO RÉSOUT L'ADRESSE IPV4 ASSOCIÉE AU DOMAINE AUQUEL LE COMPTE APPARTIENT.</pre> Cette macro permet d'obtenir l' <u>adresse IPv6</u> [187] associée au domaine auquel le compte appartient.
\$FQDNInsère le nom de domaine pleinement qualifié, ou leNom d'hôte SMTP1871, du domaine auquel le compteappartient.
\$PRIMARYDOMAIN\$Cette macro permet de résoudre le nom de domaine par défaut de MDaemon.
\$PRIMARYIP\$ CETTECette macro renvoie à l' adresse IPv4associée auMACRO RÉSOUT LE NOM DE MDAEMON.domaine par défaut de MDaemon.
PRIMARYIP6\$ CETTE MACRO RÉSOUT L'ADRESSE IPV4 ASSOCIÉE AU DOMAINE PAR DÉFAUT DE MDAEMON.

Voir :

Paramètres du client MC 413 Paramètres de serveur MC | Paramètres 410 Paramètres des serveurs MC | Comptes 412

3.8.2.2 Avancé

Si vous avez activé l'option "*Pousser les paramètres* du *client vers les utilisateurs MC*" dans l' écran <u>Paramètres clients MC</u> [413], les paramètres de cet écran seront poussés vers l'écran correspondant du client MDaemon Connector chaque fois qu'un utilisateur MDaemon Connector se connectera au serveur. Les Paramètres du client MC ne sont envoyés aux clients que si l'un des paramètres a été modifié depuis la dernière fois que le client s'est connecté et les a reçus.

Serveur entrant (IMAP)

Utiliser une connexion sécurisée (SSL)

Cochez cette case si vous souhaitez que les clients utilisent une connexion sécurisée (SSL) lorsqu'ils se connectent au serveur Courrier entrant (IMAP). Activer cette option changera automatiquement le paramètre Port en "993", qui est le port SSL par défaut.

Utiliser TLS (Transport Layer Security)

Cochez cette case si vous souhaitez que les clients utilisent une connexion TLS sécurisée lorsqu'ils se connectent au serveur Courrier entrant (IMAP).

Port

Il s'agit du port sur lequel les clientsMC se connecteront à votre serveur Courrier entrant (IMAP). Non par défaut, il est fixé à 143 pour les connexions IMAP ou à 993 pour les connexions IMAP cryptées par SSL.

Serveur sortant (SMTP)

Utiliser une connexion sécurisée (SSL)

Cochez cette case si vous voulez que les clientsMC utilisent une connexion sécurisée (SSL) lorsqu'ils se connectent au Serveur sortant (SMTP). Activer cette option changera automatiquement le paramètre Port en "465", qui est le port SSL par défaut.

Utiliser TLS (Transport Layer Security)

Cochez cette case si vous voulez que les clientsMC utilisent une connexion TLS sécurisée lorsqu'ils se connectent au Serveur sortant (SMTP).

Port

Il s'agit du port sur lequel les clientsMC se connecteront à votre Serveur sortant (SMTP). Non par défaut, il est fixé à 25 pour les connexions SMTP ou à 465 pour les connexions SMTP cryptées par SSL.

Authentification SMTP

Aucune authentification requise par le serveur SMTP.

Par défaut, les utilisateurs doivent utiliser des identifiants de connexion valides pour s'authentifier lorsqu'ils se connectent au Serveur sortant (SMTP) pour envoyer un message e-mail.

Utiliser la même authentification que celle du serveur entrant

Par défaut, les clientsMC s'authentifieront en utilisant les mêmes identifiants de connexion pour le serveur (SMTP) sortant que pour le serveur (IMAP) entrant.

Utiliser l'authentification SMTP

Utilisez cette option si vous souhaitez exiger de vos utilisateursMC qu'ils utilisent des références d'authentification différentes lors de l'envoi de messages, comme cela peut être nécessaire lors de l'utilisation d'un serveur de messagerie différent pour le courrier sortant.

Voir :

Paramètres du client MC 413

Paramètres de serveur MC | Paramètres 410 Paramètres des serveurs | Comptes 412

3.8.2.3 Dossiers

Si vous avez activé l'option "*Pousser les paramètres* du client*vers les utilisateurs MC*" sur l'écran <u>Paramètres clients MC</u> [413], les paramètres de cet écran seront poussés vers l'écran correspondant du client MDaemon Connector chaque fois qu'un utilisateur MDaemon Connector se connectera au serveur. Les Paramètres du client MC ne sont envoyés aux clients que si l'un des paramètres a changé depuis la dernière fois que le client s'est connecté et les a reçus.

Liste des dossiers

Afficher tous les dossiers

Dans Outlook, la liste des dossiers affiche par défaut tous les dossiers auxquels l'utilisateur MDaemon Connector a accès sur le serveur de messagerie.

Afficher seulement les dossiers souscrits

Sélectionnez cette option si vous souhaitez que la liste des dossiers d'Outlook n'affiche que les dossiers auxquels l'utilisateur est abonné.

Charger les dossiers PIM de manière synchrone

Dans la plupart des cas, cette option ne doit pas être cochée, ce qui signifie que l'utilisateur de MDaemon Connector peut continuer à utiliser Outlook pendant que MDaemon Connector charge le contenu des dossiers PIM (c'est-à-dire les dossiers qui ne sont pas des dossiers de courrier, tels que : Contacts, Calendriers et Tâches). Si vous cochez cette case, l'utilisation d'Outlook sera bloquée jusqu'à ce que toutes les données aient été chargées. En règle générale, cette option n'est nécessaire que lorsque des applications tierces tentent d'accéder au contenu des dossiers PIM.

Charger les dossiers IMAP de manière synchrone

Dans la plupart des cas, cette option ne doit pas être cochée, ce qui signifie que l'utilisateur de MDaemon Connector peut continuer à utiliser Outlook pendant que MDaemon Connector charge le contenu des dossiers courrier IMAP de l'utilisateur. Si vous cochez cette case, l'utilisation d'Outlook sera bloquée jusqu'à ce que toutes les données aient été chargées. En général, cette option n'est nécessaire que lorsque des applications tierces tentent d'accéder au contenu des dossiers courrier.

Voir :

Paramètres du client MC 413 Paramètres de serveur MC | Paramètres 410 Paramètres des serveurs | Comptes 412

3.8.2.4 Envoyer/Recevoir

🧐 MDaemon Connector - Envoyer/Recevoir	
Paramètres du serveur MC Paramètres du client MC Général Avancé Dossiers Envoyer/Recevoir Divers Base de données Compléments	Paramètres d'envoi/réception I félécharger uniquement les en-têtes Afficher l'indicateur de progression lors du chargement des messages Seuil de l'indicateur (nombre de messages) 50 Autoriser l'annulation du téléchargement des messages Inclure tous les dossiers dans l'envoi/réception Vérifier le courrier dans des dossiers sélectionnés lors de l'envoi/réception Programmer un envoi/réception automatique toutes les 5 minutes
	OK Annuler Appliquer Aide

Si vous avez activé l'option "*Pousser les paramètres* du client*vers les utilisateurs MC*" sur l'écran<u>Paramètres clients MC</u> [413], les paramètres de cet écran seront poussés vers l'écran correspondant du client MDaemon Connector chaque fois qu'un utilisateur MDaemon Connector se connectera au serveur. Les Paramètres du client MC ne sont envoyés aux clients que si l'un des paramètres a changé depuis la dernière fois que le client s'est connecté et les a reçus.

Préférences d'envoi/réception

Télécharger les en-têtes TO: : dans l'en-tête FROM

Par défaut, lorsque MDaemon Connector effectue une opération d'envoi/réception et trouve de nouveaux messages, il télécharge uniquement les en-têtes du message (To, From, Subject, etc.) pour les afficher dans la liste des messages. Le message complet n'est pas téléchargé tant qu'il n'est pas affiché.

Afficher l'indicateur de progression lors du chargement des messages

MDaemon Connector affiche un indicateur de progression lors du téléchargement d'un grand nombre de messages. Décochez cette case si vous ne souhaitez pas afficher l'indicateur de progression.

Seuil de l'indicateur (nombre de messages)

Lorsque l'option*Afficher l'indicateur de progression...* est activée, l'indicateur de progression s'affiche lorsque le nombre de messages téléchargés est égal ou supérieur à ce seuil.

Autoriser l'annulation du téléchargement des messages

Cochez cette case si vous souhaitez que les utilisateurs de MDaemon Connector puissent annuler le téléchargement pendant que MDaemon Connector télécharge un message volumineux.

Inclure tous les dossiers dans l'envoi/réception

Sélectionnez cette option si vous souhaitez que MDaemon Connector vérifie dans tous les dossiers du courrier s'il y a de nouveaux messages lorsqu'il effectue une action d'envoi/réception pour le compte de l'utilisateur.

Vérifier le courrier dans des dossiers sélectionnés lors de l'envoi/réception

Sélectionnez cette option si vous souhaitez que MDaemon Connector vérifie les dossiers spécifiés de l'utilisateur à la recherche de nouveaux messages lorsqu'il effectue une action d'envoi/réception sur le compte.

Programmer un envoi/réception automatique toutes les [xx] minutes

Utilisez cette option si vous souhaitez effectuer un envoi/réception à un intervalle donné.

Voir :

 Paramètres du client MC
 413

 Paramètres du serveur MC | Paramètres
 410

 Paramètres des serveurs | Comptes
 412

3.8.2.5 Divers

🧐 MDaemon Connector - Divers	×
MDaemon Connector - Divers Paramètres du serveur MC Paramètres du client MC Général Avancé Dossiers Envoyer/Recevoir Divers Base de données Compléments	Options de confirmation Si une demande de confirmation de lecture arrive pour un message entrant? Me demander avant d'envoyer une réponse Toujours envoyer une réponse Ne jamais envoyer de réponse Options du cache local Pousser les paramètres du cache local vers les utilisateurs MC Stocker le cache local des messages dans un emplacement personnalisé Nom de fichier : Stocker les pièces jointes dans un emplacement personnalisé Chemin : Utilisez des macros et variables d'environnement afin de garantir des emplacements uniques pour chaque compte MC dans chaque profil Dutlook.
	 Envoyer les requêtes de rendez-vous au format iCalendar Activer les mises à jour automatiques
	OK Annuler Appliquer Aide

Si vous avez activé l'option "*Pousser les paramètres* du client*vers les utilisateurs MC*" dans l' écran<u>Paramètres clients MC</u> (413), les paramètres de cet écran seront poussés vers l'écran correspondant du client MDaemon Connector chaque fois qu'un utilisateur MDaemon Connector se connectera au serveur. Les Paramètres du client MC ne sont envoyés aux clients que si l'un des paramètres a changé depuis la dernière fois que le client s'est connecté et les a reçus.

Gérer les options de réception

Les messages entrants contiennent parfois un en-tête spécial permettant de demander qu'un message automatisé soit renvoyé à l'expéditeur pour l'informer que vous avez lu le message. Paramétrez cette option pour indiquer comment vous souhaitez que MDaemon Connector traite les messages qui demandent des confirmations de lecture.

Me demander l'autorisation avant d'envoyer une réponse

Choisissez cette option si vous souhaitez que les utilisateurs soient invités à envoyer ou non le message de confirmation de lecture chaque fois qu'ils ouvrent un message qui le demande.

Toujours envoyer une réponse

Sélectionnez cette option si vous souhaitez envoyer automatiquement un message de confirmation de lecture chaque fois qu'un utilisateur ouvre un message qui le demande.

Ne jamais envoyer de réponse

Sélectionnez cette option si vous ne souhaitez pas que MDaemon Connector réponde aux demandes de confirmation de lecture.

Options du cache local

Les options de cette section déterminent l'emplacement spécifique du cache local des messages de l'Utilisateur MDaemon Connector et l'endroit où les pièces jointes sont enregistrées.



Ces options requièrent que l'utilisateur MDaemon Connector de l'utilisateur doit être la version 4.5.0 ou une version plus récente.

Pousser les paramètres du cache local vers les utilisateurs MC

Par défaut, MDaemon n'envoie pas ces paramètres au client MDaemon Connector. Cochez cette case si vous souhaitez qu'ils y soient transférés. Le client MC déplacera les fichiers locaux de leur emplacement actuel vers l'emplacement par défaut, ou vers un emplacement personnalisé si vous en spécifiez un dans les options personnalisées ci-dessous.

Stocker le cache local des messages dans un emplacement personnalisé | Nom de fichier

Indiquez un Chemin du cache local et un nom de fichier pour le cache si vous souhaitez que le client MC déplace les fichiers locaux vers un emplacement personnalisé. Les variables d'environnement et les macros doivent être utilisées pour garantir un emplacement unique pour chaque utilisateur. Exemple :

%APPDATA%\Alt-N\Outlook Connector 2.0\Accounts\%OUTLOOKPROFILE% \OUTLOOKEMAIL%\LocalCache.db

Stocker les pièces jointes dans un emplacement personnalisé | Chemin des pièces jointes

Si vous souhaitez personnaliser l'emplacement du dossier dans lequel le client MC stocke les pièces jointes, indiquez un chemin d'accès ici. Les variables d'environnement et les macros doivent être utilisées pour garantir un emplacement unique pour chaque utilisateur.

Envoyer les requêtes de rendez-vous au format iCalendar

Cochez cette case si vous souhaitez que MC envoie les requêtes de rendez-vous au format iCalendar (iCal).

Activer les mises à jour automatiques

Non par défaut, MC sera mis à jour automatiquement dès qu'une nouvelle version sera disponible. Décochez cette case si vous ne souhaitez pas que les mises à jour soient automatiques.

Voir :

Paramètres du client MC 413 Paramètres de serveur MC | Paramètres 410 Paramètres des serveurs MC | Comptes 412

3.8.2.6 Base de données

MDaemon Connector - Base de données	
Paramètres du serveur MC Paramètres du client MC Général Avancé Dossiers Envoyer/Recevoir Divers Base de données Compléments	Nettoyage & Compression de la base de données Image: Nettoyer la base de données à la fermeture d'Outlook Supprimer le corps des messages de plus de 30 jours (0=jamais) Compresser la base de données Image: Occupie compresser la base de données à la fermeture d'Outlook Compresser la base de données à la fermeture d'Outlook Configuration Image: Me demander si la base de données doit être nettoyée/compressée à la fermeture d'Outlook Nettoyer/compresser à la fermeture tous les 7 jours (0=toujours)
	OK Annuler Appliquer Aide

Si vous avez activé l'option "*Pousser les paramètres* du client*vers les utilisateurs MC*" sur l'écran <u>Paramètres clients MC</u> [413], les paramètres de cet écran seront poussés vers l'écran correspondant du client MDaemon Connector chaque fois qu'un utilisateur MDaemon Connector se connectera au serveur. Les Paramètres du client MC ne sont envoyés aux clients que si l'un des paramètres a changé depuis la dernière fois que le client s'est connecté et les a reçus.

Nettoyer et Compresser la base de données

Nettoyer la base de données à la fermeture d'Outlook

Pour préserver l'espace disque et améliorer les performances, MDaemon Connector est configuré par défaut pour supprimer le corps des messages lorsque vous fermez Outlook. Cette opération ne supprime pas les en-têtes des messages et n'affecte pas les messages originaux stockés sur le serveur ; elle supprime simplement le corps des anciens messages mis en cache localement. Lorsque vous ouvrez un ancien message qui a été nettoyé dans le passé, le corps du message est à nouveau téléchargé sur votre ordinateur. En outre, seuls les corps des messages électroniques sont purgés ; cela n'affecte pas les contacts, les calendriers, les tâches, les journaux ou les notes. Désactivez cette option si vous ne souhaitez pas nettoyer la base de données à la fermeture.

Supprimer le corps des messages de plus de [xx] jours (0 = jamais)

Cette option permet de déterminer l'ancienneté d'un message pour que son corps soit purgé lors de l'arrêt d'Outlook. Non (par défaut), un message doit dater de plus de 30 jours pour être nettoyé. Son âge est basé sur la date de modification du message. Utilisez "0" dans cette option si vous ne souhaitez jamais qu'ils soient nettoyés.

Compresser la base de données

Compresser la base de données à la fermeture d'Outlook

Pour préserver l'espace disque et améliorer les performances, MDaemon Connector est configuré par défaut pour compacter et défragmenter le fichier de la base de données des messages mis en cache localement lorsque l'utilisateur ferme Outlook. Outlook doit cependant s'arrêter proprement pour que l'action de compactage se produise ; si Outlook se bloque ou si vous utilisez le Gestionnaire des tâches pour | Terminer la tâche ", la base de données ne sera pas compactée. Vous pouvez utiliser les options de la section Configuration ci-dessous pour déterminer la fréquence à laquelle cela se produira et si vous serez invité à le faire avant que cela ne se produise.

Configuration

Me demander de nettoyer/compacter lors de la fermeture d'Outlook

Utilisez cette option si vous souhaitez que les utilisateurs soient invités à purger ou à compacter le fichier de la base de données lors de l'arrêt d'Outlook. Si l'utilisateur clique sur **Oui**, MDaemon Connector effectuera le compactage ou la purge, en affichant un indicateur de progression. Décochez cette case si vous ne voulez pas que les utilisateurs soient invités à le faire ; à l'arrêt, MDaemon Connector commencera à purger ou à compacter la base de données automatiquement, en affichant un indicateur de progression.

Nettoyer/compresser à la fermeture tous les [xx] jours (0=toujours)

Cette option permet de définir la fréquence à laquelle MDaemon Connector purge ou compacte la base de données à l'arrêt. Non par défaut, cette option est définie sur 7 jours, ce qui signifie que le processus de nettoyage/compactage sera exécuté à l'arrêt tous les sept jours. Attribuez la valeur "0" à cette option si vous souhaitez que la base de données soit nettoyée et compactée à chaque fois qu'un utilisateur ferme Outlook.

Voir :

 Paramètres du client MC
 413

 Paramètres du serveur MC | Paramètres
 410

 Paramètres des serveurs MC | Comptes
 412

3.8.2.7 Signature

🧐 MDaemon Connector - Signature	×
MC Server Settings MC Client Settings General Advanced Folders Send/Receive Miscellaneous Database Signature Add-ins	Signature Options Push client signature to Outlook. Make it the default signature for new messages Make it the default signature for replies/forwards Signature name: MDaemon-\$EMAIL\$ Set the signature text at Setup Server Settings Default Client Signatures and/or Setup Domain Manager <domain> Client Signatures.</domain>
	Ok Cancel Apply Help

Si vous avez activé l'option "*Envoyer les paramètres clients aux utilisateurs MC* " dans l'écran <u>Paramètres clients MC</u> [413], les paramètres sélectionnés dans cet écran seront envoyés à l'écran Signatures (situé dans Outlook sous **Fichier | Options | Courrier | Signatures**) chaque fois qu'un utilisateur de MDaemon Connector se connectera au serveur. Cette fonctionnalité nécessite MDaemon Connector 6.5.0 ou une version plus récente.

Options de signature

Transmettre la signature client à Outlook

Activez cette option si vous souhaitez envoyer la <u>signature client par défaut</u> [138] (ou la <u>signature client</u> [216] spécifique au domaine , si elle a été créée) à vos utilisateurs MDaemon Connector. Désignez un nom pour la signature dans l' option*Nom de la signature* ci-dessous.

Utiliser comme signature par défaut pour les nouveaux messages

Cochez cette case si vous souhaitez que la signature client soit la signature par défaut utilisée pour les nouveaux messages.

Utiliser comme signature par défaut pour les réponses/transferts

Cochez cette case si vous souhaitez que la signature du client soit utilisée par défaut pour répondre aux messages et les transférer.

Nom de la signature :

Il s'agit du nom donné à la signature poussée vers le compte de messagerie de l'utilisateur MDaemon Connector dans Outlook. Par défaut, le nom de la signature est : "MDaemon-\$EMAIL\$". La macro \$EMAIL\$ sera convertie en adresse électronique de l'utilisateur. Exemple : "MDaemon-Frank.Thomas@company.test"

Voir :

Paramètres du client MC 413 Paramètres de serveur MC | Paramètres 410 Paramètres des serveurs MC | Comptes 412 Signatures client par défaut 138 Gestionnaire de domaines | Signatures des clients 216

3.8.2.8 Compléments

🛒 Paramètres du serveur MC	Compléments Outlook	Compléments Outlook		
 Paramètres du client MC Général Avancé Dossiers Envoyer/Recevoir Divers Base de données Compléments 	Nom du complément	Action		
	Nom du complément : Ajouter Action par défaut Action par défaut pour les compléments : [,	Action : Désactiver Autoriser		

Dans l'écran Compléments, vous pouvez gérer l'état des compléments Outlook utilisés par vos utilisateurs MDaemon Connector (MC). Vous pouvez autoriser l'utilisation normale de l'un ou de tous les compléments, ou vous pouvez désactiver ceux que vous choisissez. Cette fonction peut être particulièrement utile dans les cas où vous savez qu'un complément spécifique est en conflit avec MDaemon Connector, ce qui vous permet de le désactiver pour éviter tout problème. La fonction Compléments nécessite MDaemon Connector 5.0 ou une version plus récente.

Compléments Outlook

Dans cette boîte, vous trouverez la liste des modules d'extension Outlook de vos utilisateurs et l'action attribuée à chacun d'entre eux : *Désactiver, Autoriser* ou *Défaut*. Dans le cas où un utilisateur MC démarre Outlook, le client MC envoie la liste des compléments de l'utilisateur à MDaemon et désactive ensuite ces compléments. MDaemon et désactive alors tous ceux qui ont été réglés sur qui ont été réglés sur *Désactivé*. Les add-ins définis sur *Autoriser* ne seront pas modifiés. Dans les paramètres *Non par défaut*, l'action par défaut pour les modules complémentaires est utilisée.



MDaemon Connector ne peut gérer les modules d'extension Outlook que pour les utilisateurs qui ont défini leur compte MDaemon Connector comme compte par défaut dans Microsoft Outlook.

Ajouter, supprimer et modifier des compléments

Ajouter un complément

Pour ajouter un complément à la liste, tapez *le Nom du complément* tel qu'il apparaît dans Outlook, définissez l'*Action* et cliquez sur **Ajouter**. Cette option est utile si vous connaissez un complément que vous souhaitez gérer, mais qu'aucun utilisateur ne s'est encore connecté et n'a installé ce complément.

Suppression d'un complément

Pour supprimer un complément de la liste, sélectionnez-le et cliquez sur Supprimer.

Définition de l'action d'un complément

Pour modifier un complément, sélectionnez-le, utilisez la liste déroulante pour définir son *action* et cliquez sur **Ajouter**.

Action par défaut

Action par défaut pour les compléments.

Définissez cette option sur *Autoriser* ou *Désactiver*. Si vous choisissez *Autoriser*, MDaemon Connector ne désactivera par défaut que les compléments que vous avez spécifiquement définis comme "*Désactiver*". Tous les autres compléments ne seront pas affectés. Lorsque cette option est définie sur *Désactiver*, MDaemon Connector désactive automatiquement tous les modules d'extension, à l'exception de ceux que vous avez spécifiquement définis sur*Autoriser*.

Voir :

Paramètres du client MC 413 Paramètres de serveur MC | Paramètres 410 Paramètres des serveurs | Comptes 412

3.9 Service de cluster

Le service de cluster de MDaemon est conçu pour partager votre configuration entre deux ou plusieurs serveurs MDaemon sur votre réseau. Cela vous permet d'utiliser du matériel ou des logiciels d'équilibrage de charge pour distribuer votre charge de courrier électronique sur plusieurs serveurs MDaemon, ce qui peut améliorer la vitesse et l'efficacité en réduisant la congestion et la surcharge du réseau et en maximisant vos ressources de courrier électronique. Cela permet également d'assurer la redondance de vos systèmes de messagerie au cas où l'un de vos serveurs subirait une panne matérielle ou logicielle.

Voici un certain nombre d'éléments à prendre en compte lorsque vous décidez de mettre en place ou non un cluster MDaemon sur votre réseau :

Nœuds

Un cluster MDaemon comporte un nœud principal et des nœuds secondaires. Un serveur MDaemon sera désigné comme primaire et tous les autres comme secondaires.

- Le serveur MDaemon agissant en tant que nœud primaire voit sa configuration répliquée sur tous les autres nœuds. Si vous accédez à un nœud secondaire et que vous modifiez la configuration, ces modifications seront écrasées. Par conséquent, la plupart des options de configuration ne sont pas accessibles dans l'interface utilisateur sur les nœuds secondaires.
- Le service de cluster ne réplique pas les Dossiers Boîtes Publics ou les Dossiers Publics aux Lettres entre les nœuds ; tous les nœuds partagent le même ensemble de Dossiers Publics. Les Dossiers courrier de l'utilisateur et les Dossiers publics doivent se trouver à un emplacement de votre réseau accessible à tous les nœuds.
- Toute modification apportée au courrier électronique sur un nœud secondaire est envoyée au nœud principal, puis tous les autres nœuds sont informés de la modification.
- L'API XML sur les nœuds secondaires est en lecture seule.
- Chaque nœud du cluster doit se trouver sur le même réseau. Il est déconseillé d'utiliser le service de cluster pour regrouper des serveurs situés à des endroits différents.
- Dans le cluster, chaque nœud doit exécuter la même version de MDaemon.
- Chaque nœud de la grappe a besoin de sa propre clé MDaemon.

Routage

MDaemon ne gère pas le routage du trafic vers ou depuis des nœuds spécifiques. Nous vous recommandons d'utiliser un équilibreur de charge tiers pour gérer le routage du trafic.

Dans votre équilibreur de charge, des sessions collantes sont nécessaires pour que tout le trafic provenant de la même IP soit acheminé vers le même hôte. Les sessions collantes sont particulièrement importantes pour le trafic MDRA, Webmail et XMPP car elles ne sont pas encore compatibles avec les clusters, ce qui signifie que les informations de session ne sont pas transmises entre les nœuds. Pour faire face à cette limitation :

- Toutes les connexions MDRA doivent être acheminées vers le nœud principal.
- Lorsque quelqu'un se connecte à Webmail sur un serveur spécifique, tout le trafic pour cette session doit être acheminé vers ce même serveur.
- Le trafic du Webmail et du XMPP doit être acheminé vers le même serveur pour que les fonctions de chat intégrées au Webmail fonctionnent.
- Tout le trafic XMPP doit être acheminé vers le même nœud, sinon les utilisateurs se connectant à des serveurs différents ne pourront pas discuter entre eux.
- Compte tenu des points ci-dessus, nous recommandons que l'ensemble du trafic HTTP et XMPP soit acheminé vers le nœud principal, car il s'agit de la configuration la plus simple et la moins susceptible de causer des problèmes. Si vous n'utilisez pas certaines de ces fonctionnalités, vous pouvez toutefois modifier votre configuration (bien que des sessions collantes soient toujours nécessaires).

Boîtes aux lettres et dossiers

Les Dossiers publics & partagés, les Dossiers publics et certains autres dossiers doivent être stockés dans un chemin partagé accessible par chaque nœud de la grappe. Paramètre "Se souvenir de moi" Si vous utilisez un chemin UNC, vous devrez exécuter le service MDaemon en tant qu'utilisateur ayant accès à l'emplacement du réseau.

- Vous devez mettre à jour manuellement les chemins d'accès à votre boîte aux lettres et à vos dossiers et déplacer le contenu des dossiers vers l'emplacement accessible par le cluster. Il ne s'agit pas d'une fonction automatisée que MDaemon peut effectuer pour vous lors de la mise en place du clustering. Le service de cluster met à jour le fichier MDaemon.ini avec les chemins d'accès aux boîtes aux lettres et aux Dossiers publics que vous avez indiqués dans la configuration du service de cluster.
- Le répertoire Lockfiles doit être déplacé vers un emplacement partagé. Vous pouvez autoriser le service de clustering à le faire automatiquement ou le faire manuellement en modifiant la clé LockFiles dans la section [Directories] du fichierMDaemon.ini. Si vous autorisez le service de clustering à le faire pour vous, le répertoire LockFiles sera situé sous le chemin de la boîte aux lettres réseau.
- Le répertoire PEM doit également être déplacé vers un emplacement partagé. Pour ce faire, copiez le dossier IMAP partagés dans le nouvel emplacement, modifiez la clé PEM dans la section [Directories] du fichierMDaemon.ini et redémarrez MDaemon.
- Le nouveau modèle de compte sera mis à jour avec le chemin d'accès à la boîte aux lettres fourni dans la configuration du service de cluster.

Écran dynamique

 L'<u>Écran dynamique</u> anvoie toutes les demandes au nœud de serveur primaire, et les données du nœud primaire sont répliquées sur les nœuds secondaires.
Si le nœud principal est hors ligne, les nœuds secondaires utilisent leur propre configuration de filtrage dynamique, qui doit être identique à la configuration du nœud principal au moment où il a été mis hors ligne. Lorsque le nœud primaire est remis en ligne, toutes les modifications apportées à l'Écran dynamique par les serveurs secondaires sont écrasées.

Certificats

- Les certificats SSL sont automatiquement répliqués du nœud principal vers les nœuds secondaires.
- MDaemon réplique également ses <u>paramètres de certificat</u> [614]. Dans le cluster, chaque nœud/serveur tentera d'utiliser le même certificat. Si un nœud n'a pas le bon certificat, tout le trafic SSL & TLS/HTTPS échouera sur ce nœud.
- Les options LetsEncrypt de MDaemon ne prennent pas en charge les nœuds secondaires pour le moment.

Autre

- <u>Liens vers les pièces jointes</u> ne peut pas être utilisé dans un cluster et est donc désactivé lorsque vous activez le clustering.
- <u>Mises à jour automatiques</u> [533] doit être désactivé.
- <u>La liaison entre le Nom du domaine et l'adresse IP</u> [187] doit être désactivée.
- Tous les nœuds d'une grappe doivent être réglés sur le même fuseau horaire et exactement à la même heure. Si le fuseau horaire n'est pas le même, ou si les heures sont décalées de plus d'une seconde, un avertissement sera consigné dans le journal de la grappe.

Configuration du service de cluster

Suivez les étapes suivantes pour configurer votre service de cluster :

- 1. Assurez-vous d'avoir mis à jour tous les chemins d'accès aux Boîtes aux Lettres et ajusté les chemins d'accès aux Dossiers publics. Le serveur principal doit utiliser un emplacement de stockage réseau pour ces données et doit pouvoir y accéder sans problème avant de poursuivre.
- 2. Tous les certificats appropriés doivent être installés sur chaque nœud.
- 3. Installez MDaemon sur un nœud secondaire en utilisant une clé unique.
- 4. Sur le nœud principal, allez dans **Configuration | Service de cluster**.
- Cliquez avec le bouton droit de la souris sur la liste des serveurs enregistrés, puis cliquez sur Ajouter un nouveau serveur MDaemon à la grappe (l'opération peut être lente car le serveur recherche les serveurs disponibles sur le réseau).
- 6. Dans *Nom du serveur*, entrez le nom NETBIOS, l'adresse IP ou le nom DNS du nœud secondaire sur lequel MDaemon est installé, ou sélectionnez le serveur dans la liste déroulante (ilpeut y avoir un délai car il recherche les serveurs disponibles sur le réseau).

- 7. Cliquez sur **Ok**.
- 8. Vérifiez dans le journal Plugins / Cluster que les deux serveurs ont bien été connectés et que la réplication a bien lieu.
- Allez dans Configuration | Service de cluster sur le nœud secondaire pour confirmer qu'il liste maintenant les nœuds primaire et secondaire sous Serveurs enregistrés.
- 10. Configurez votre matériel ou logiciel d'équilibrage de charge pour acheminer le trafic vers le cluster comme indiqué ci-dessus.

Voir :

Service de cluster | Options/personnaliser Service de cluster | Chemins réseau partagés Service de cluster | Diagnostics

3.9.1 Options/personnalisation

Options/Personnaliser

Cluster Service f	or MDaemon		
□ Enable the Clu Primary Options □ Enable real-t □ Mirror Queue Retain Packa Secondary Options Min. Replication Min. Replication Retain Packa	Shared Network Patients Shared Network Patients States Service States to Secondaries ages for: 1,440 • ons on interval: 30 • ckages for: 1,440 • cka	hs Diagno	Requirements / Restrictions The following options are enforced when using the cluster service. Disable Automatic Update Installation Disable Attachment Linking Disable Domain Name to IP Binding
-Registered Serv	vers ne local server to Prima	ry Role	
Server Name VDI-MIKE	Node Type Status Primary Current	Node # 1	Server ID L: {f754081f-c5d4-4d6a-b85a-d60203a1485a} 01
<			>
		OK	Cancel Apply Help

Activer le service de cluster

Cliquez sur ce bouton pour activer le service de cluster.

Options primaires

Activer la signalisation en temps réel

Non par défaut, chaque fois qu'un changement se produit sur le nœud primaire, celui-ci envoie un signal de réplication aux nœuds secondaires, pour les avertir qu'ils doivent effectuer une demande de réplication afin de synchroniser les paramètres entre les nœuds.

Miroir des états de la file d'attente vers les nœuds secondaires

Cochez cette case si vous souhaitez vous assurer que si vous modifiez l'état d'une file d'attente (c.-à-d. gelée ou dégelée) sur le nœud principal, cet état sera également modifié sur les nœuds secondaires.

Options secondaires

Intervalle de réplication [xx] minutes

Cette option détermine la durée pendant laquelle un nœud secondaire attendra un signal de réplication de la part du nœud primaire avant d'effectuer une demande de réplication. Non (par défaut), cette valeur est fixée à 30 minutes.

Serveurs enregistrés

Cette option affiche tous les nœuds de votre cluster de serveurs MDaemon.

Promouvoir le serveur local au rôle primaire

Dans le nœud secondaire que vous souhaitez promouvoir, sélectionnez le nœud dans la liste et cliquez sur **Promouvoir**. Le nouveau nœud primaire devrait alors informer l'ancien nœud primaire de rejoindre le cluster en tant que nœud secondaire. Pour les configurations comportant plusieurs nœuds secondaires, les nœuds secondaires supplémentaires devront être supprimés et réajoutés au cluster.

Ajouter un nouveau serveur MDaemon à la grappe

Pour ajouter un nouveau serveur MDaemon au cluster, cliquez avec le bouton droit de la souris sur la liste des serveurs et cliquez sur **Ajouter un nouveau serveur MDaemon au cluster**. Dans l'écran qui s'ouvre, saisissez le nom NETBIOS, l'adresse IP ou le nom DNS du serveur sur lequel MDaemon est installé, ou sélectionnez-le dans la liste déroulante. Il se peut qu'il y ait un délai car le système cherche des serveurs disponibles sur le réseau.

Voir :

<u>Service de cluster</u> बित्ती <u>Service de cluster | Chemins d'accès réseau partagés</u> बित्ती <u>Service de cluster | Diagnostics</u> बित्ती

3.9.2 Chemins d'accès partagés

Chemins d'accès réseau partagés

Cluster Service for MDaemor	n	- • ×
Options/Customize Shared Net	work Paths Diagnostics	
Enable Shared Network Path	editing (required if this is the first node of a cluster)	
Set all network paths using	g a common MDaemon Network Share	
Root <u>M</u> Daemon Share:	\\VDI-MIKE\MDaemon	Browse
Set all network paths individual	idually	
Mail Folders:	\\VDI-MIKE\MDaemon\Users	Browse
Public folders:	\\VDI-MIKE\MDaemon\Public Folders	Browse
Lock files:	\\VDI-MIKE\MDaemon\LockFiles	Browse
Private <u>K</u> eys:	\\VDI-MIKE\MDaemon\PEM	Browse
<u>M</u> ail Archives:	\\VDI-MIKE\MDaemon\Archives	Browse
List Digests:	\\VDI-MIKE\MDaemon\Digests	Browse
<u>G</u> ateways:	\\VDI-MIKE\MDaemon\Gateways	Browse
Enable Multi-Node Mail	Routing	
Queue Folders:	C:\MDaemon\Queues	Browse
	OK Cancel Apply	Help

Activer l'édition des chemins réseau partagés (obligatoire si c'est le premier nœud d'une grappe)

Filtrez les options de cet écran pour définir les chemins réseau partagés qui seront utilisés par le cluster MDaemon. Cette option est requise sur le premier nœud de la grappe afin que les chemins réseau partagés puissent être répliqués sur les autres nœuds.

Définir tous les chemins d'accès réseau à l'aide d'un partage réseau MDaemon commun Choisissez cette option si vous souhaitez placer tous les chemins d'accès réseau partagés sous un seul partage réseau commun. Dans ce cas, tous les chemins d'accès sont définis sur les valeurs par défaut et tous les contrôles de chemin d'accès sont en lecture seule.

Définir tous les chemins d'accès au réseau individuellement

Choisissez cette option si vous souhaitez définir chaque chemin d'accès réseau partagé individuellement. Exemple : si vous souhaitez stocker des dossiers courrier et des archives de courrier à différents emplacements du réseau.

Activer le routage de courrier multi-nœuds

Utilisez l'option Multi-Node Mail Routing si vous souhaitez partager les files d'attente de courrier entre les nœuds du cluster. Le fait que plusieurs serveurs traitent et distribuent les messages leur permet de répartir le travail plus équitablement et d'éviter que les messages ne restent bloqués dans les files d'attente des serveurs en panne.

Voir :

Service de cluster | Options/personnaliser 434 Service de cluster | Diagnostics 438

3.9.3 Diagnostics

Diagnostics

Cluster Service	for MDaemo	n 🗖 🗖 💌
Options/Customize	e Shared Net	twork Paths Diagnostics
Logging Log lev	el Debug	✓ View / Analyze Log
Advanced Op	otions	Minimum debugger log level Debug ~
Log Proce	ss Memory Co m Wide Perfor	unters No more than every 3600 seconds mance Information (30-3600)
Process Dumps	r based proces	ss dumps Prefix dump files with ClstrSvc e dumps on
Value	DumpCount	LogEntry
0xC135FE00 0xC135FE01 0xC135FE04 0xC135FE08	3 3 3 3	The API installed does not match the API level being called for. (N The procedure called has been deprecated. An attempt to read or write to the specified memory would result Access Denied (MD_ACCESSDENIED)
0xC135FE0C < €	3	COM error thrown: Result: %1 Description: %2
		OK Cancel Apply Help

Pas de journalisation

Niveau de journalisation

Six niveaux de journalisation sont pris en charge, de la plus grande à la plus petite quantité de données enregistrées :

- Déboga Il s'agit du niveau de journalisation le plus complet. Il enregistre toutes les entrées disponibles et n'est généralement utilisé que pour diagnostiquer un problème ou lorsque l'administrateur souhaite obtenir des informations détaillées.
 - **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.
- AvertisLes avertissements, les erreurs, les erreurs critiques et lessementévénements de démarrage/arrêt sont consignés dans le journal.
 - **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Critiqu Les erreurs critiques et les événements de démarrage/arrêt sont e journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.

Visualiser/Analyser le journal

Cliquez sur ce bouton pour ouvrir la fenêtre de visualisation du journal du système MDaemon Advanced. Non (par défaut) Pas de journalisation dans :".. \NMDaemon\Logs\"

Options avancées

Niveau minimal du journal de débogage

Il s'agit du niveau minimal de la journalisation à envoyer au débogage. Les niveaux de journalisation disponibles sont les mêmes que ceux décrits ci-dessus.

Enregistrer les compteurs de mémoire du processus

Cochez cette case pour consigner dans le fichier journal les informations relatives à la mémoire, aux gestionnaires et aux threads spécifiques au processus. Ceci est utile pour trouver des pistes potentielles et des problèmes d'allocation de ressources. Les entrées du journal ne seront émises que si les données ont changé depuis la dernière fois qu'elles ont été journalisées.

Pas de journalisation des informations sur les performances de l'ensemble du système

Cochez cette case si vous souhaitez consigner dans le fichier journal des informations sur les performances de l'ensemble du système. Ceci est utile pour trouver des pistes potentielles et des problèmes d'allocation de ressources. Les entrées journal ne seront émises que si les données ont changé depuis la dernière fois qu'elles ont été journalisées.

Pas plus de toutes les [xx] secondes

Cette option permet de définir la fréquence à laquelle les informations relatives aux processus et aux performances seront journalisées.

Fichiers dumpers

Créer un dump du processus en cas d'erreur

Activez cette option si vous souhaitez générer des Fichiers dumps à chaque fois que survient un avertissement ou une erreur spécifique que vous avez désigné cidessous.

Inclure les informations du tas dans les dumps

Non (par défaut), les informations du tas sont incluses dans les Fichiers dumps. Décochez cette case si vous ne souhaitez pas les inclure.

Préfixe des fichiers dump

Les noms des fichiers dumpiers commenceront par ce texte.

Erreurs/avertissements à partir desquels générer des fichiers dumps

Cliquez avec le bouton droit de la souris sur cette zone et utilisez les options*Ajouter/Modifier/Supprimer une entrée...* pour gérer la liste des erreurs ou des avertissements qui déclencheront des vidages de processus. Pour chaque entrée, vous pouvez spécifier le nombre de Fichiers dumps autorisés avant qu'elle ne soit désactivée.

Voir :

<u>Service de cluster</u> बिआ <u>Service de cluster | Options/personnaliser</u> बिअ <u>Service de cluster | Chemins d'accès réseau partagés</u> बिऔ

3.10 ActiveSync

3.10.1 Système

Policy Ma	nager	A	ccounts	Clients	Groups	Client Types
System	Tuning	5	Security	Diagnostics	Protocol Restrict	ions Domain
∠ Enable t	ne ActiveSy	nc proto	ocol	Service Status:	Inactive	
MDASMam	t.dll 22.0.	0.3rc1	2022-04-20	0T11:39:22.0007		^
MDAirSync	.dll 22.0.	0.4rc1	2022-04-20	0T11:39:12.000Z		
MDASRes.	dll 22.0.	0.1rc1	2022-04-20	0T11:39:22.000Z		
MdXml.dll	22.0.	0.1rc1	2022-04-20	DT11:39:28.000Z		
Duraharan	University of		and Anti-			Ŧ
Purchase,	Upgrade, o	r Renew	an Actives	<u>ync license</u>		
ictiveSync I	license stati	IS:				
The produk		undial.				~
me produc	ct license is	valid.				
The produc	ct license is	valid.				¥
User Inter	face Optior le editing of le all "Are y te Quick Acc Sync servic : protocol. 1	advanc ou sure ess Set allows his allow	ed policy opt ?" confirmation up Menu Iter a variety of ws for clients	tions on prompts ms mail dients to com to synchronize em	municate with MDae ail, calendars, task:	emon via the s, contacts and

MDaemon prend en charge "ActiveSync for MDaemon", un serveur ActiveSync overthe-air (OTA) sous licence séparée. Ce serveur est capable de synchroniser le courrier électronique et les données PIM d'un utilisateur (c'est-à-dire les contacts, les calendriers et les tâches) entre son compte MDaemon/Webmail et un appareil compatible avec ActiveSync.

Si vous activez ActiveSync pour MDaemon la première fois en utilisant une clé d'évaluation, il fonctionnera pendant 30 jours. Si vous souhaitez continuer à l'utiliser, vous pouvez acquérir une clé de licence à l'adresse suivante <u>www.mdaemon.com</u> ou de votre distributeur/revendeur local.

ActiveSync est une extension de service web qui ne fonctionne que sur les ports **80** (pour http) et **443** (pour https). Il s'agit d'une exigence de l'implémentation d'ActiveSync. Si ActiveSync est activé et que vous utilisez le serveur web intégré du Webmail, mais qu'il ne fonctionne pas sur le port 80 ou 443, alors il commencera automatiquement à fonctionner sur le port 80 en plus des autres ports que vous avez configurés <u>sur les écrans</u> <u>342</u> <u>Serveur Web</u> <u>339</u> et <u>SSL & HTTPS.</u> <u>342</u> Si vous utilisez un autre serveur pour le Webmail, tel que IIS, vous devez le configurer manuellement pour qu'il utilise le port 80 ou 443.

Si vous avez l'intention d'exécuter ActiveSync sous IIS, vous devez appeler la DLL ActiveSync (MDAirSync.dll) lorsque "/Microsoft-Server-ActiveSync" est demandé. C'est cette requête que tous les clients ActiveSync utiliseront. Certaines versions d'IIS n'ont pas cette capacité sans télécharger, installer et configurer un logiciel tiers.

Toutes les premières synchronisations avec ActiveSync sont des synchronisations à sens unique entre le serveur et l'appareil. Lors de la première synchronisation avec ActiveSync, vous perdrez les données relatives à l'appareil. Il s'agit d'une exigence de la mise en œuvre d'ActiveSync. Vous devez donc sauvegarder les données de votre appareil avant d'utiliser ActiveSync pour la première fois. La plupart des Terminaux ActiveSync avertissent l'utilisateur que "**les données de l'appareil seront perdues**", mais certains ne le font pas.

Activer/Désactiver ActiveSync

Cliquez sur *Activer le protocole ActiveSync* pour activer ActiveSync pour MDaemon. Vous pouvez ensuite utiliser les Options des<u>domaines</u> actives pour déterminer si le service est disponible pour tous vos domaines ou pour certains d'entre eux.

Options de l'interface utilisateur

Activer les options les options avancées

Activer cette option si vous souhaitez que l'onglet Paramètres avancés soit visible dans l'<u>Éditeur de politiques ActiveSync</u> [471]. Il contient divers paramètres avancés de stratégie qui, dans la plupart des cas, n'auront pas besoin d'être modifiés. Cette option est désactivée par défaut.

Désactiver toutes les invites de confirmation "Êtes-vous sûr ?

Non par défaut, lorsque vous modifiez certains paramètres ActiveSync, une invite vous demande si vous êtes sûr de vouloir effectuer la modification. Cochez cette case si vous souhaitez désactiver ces invites.

Créer des éléments de menu de configuration à accès rapide

Si vous activez cette option, le menu Configuration | ActiveSync de l'interface de l'application MDaemon sera modifié, en ajoutant des liens vers le moniteur des connexions ActiveSync et le Log Viewer/Analyzer. **Remarque :** lorsque cette option est désactivée, ces outils restent accessibles en cliquant avec le bouton droit sur **ActiveSync** sous Serveurs dans le volet Stats de l'interface d'application.

Service de découverte automatique 75

MDaemon prend en charge le <u>service AutoDiscovery</u> [75⁻], qui permet aux utilisateurs de configurer un compte ActiveSync avec seulement leur adresse e-mail et leur mot de passe, sans avoir besoin de connaître le nom d'hôte du serveur ActiveSync. AutoDiscovery nécessite l' activation de<u>HTTPS</u> [342].

Voir :

Mon compte | ActiveSyncActiveSync | DomainesSSL & HTTPS342Serveur Web339

3.10.2 Réglages

Policy Mar	nager	Accounts	Clients	G	roups	Client T	ypes
System	Tuning	Security	Diagnostics	s Proto	ocol Restricti	ons D	omains
-Ping / Syna	: Wait Folder N	Ionitoring					
M	laximum timeo	ut (seconds)	2700 🚔	Minimum	timeout (sec	onds) 120	-
Folder	monitor interv	al (seconds)	30 🛓	Max	imum # of fo	olders 204	8
Memory Us	age						
	Maximum ite	ms per Sync	100	Maximum r	esponse size	(MB) 32	•
				PIM cache	timeout (min	utes) 10	
Character 11							
Storage Us	age chive XMLAVB		ith errors				
	Retain ar	chived XML/WB	XML requests a	nd responses	for 3	days	;
XML/WBX	ML Archive Lo	cation					
Defau	lt Logs Directo	ry	0	ActiveSync C	lient Directo	ry	
			Remove ina	ctive clients a	after 0	▲ days	
<u>G</u> lobal	Client Settings	Defaults					

Cet écran contient des options avancées qui, dans la plupart des cas, n'auront pas besoin d'être ajustées. Il contient également un bouton permettant d'ouvrir la boîte de dialogue<u>Global Paramètres client Defaults</u> [447], afin d'ajuster les paramètres par défaut utilisés pour les clients ActiveSync.

Délai de surveillance des dossiers Ping/Sync Wait

Délai d'expiration max. (1200-7200 secondes)

Il s'agit du délai maximum pendant lequel MDaemon ActiveSync Service (MDAS) attendra la surveillance d'un dossier avant de renvoyer une réponse au client. La valeur par défaut est de 2700 secondes (soit 45 minutes).

Délai d'expiration min. (120-480 secondes)

Il s'agit du délai minimum pendant lequel le MDAS surveille un dossier avant de renvoyer une réponse au client. La valeur par défaut est de 120 secondes. Si

nécessaire, vous pouvez réduire le nombre de connexions au serveur en augmentant cette valeur, car le client se connectera moins souvent en raison du temps d'attente plus long.

Intervalle de surveillance des dossiers (30-120 secondes)

Il s'agit du nombre de secondes pendant lesquelles le service ActiveSync attendra entre deux surveillances de dossiers. Non (paramètres par défaut).

Nombre max. de dossierssurveillés

Il s'agit du nombre max. de dossiers surveillés que chaque client ActiveSync est autorisé à surveiller. La valeur par défaut est 2048.

Utilisation de la mémoire

Nombre maximum d'éléments par synchronisation

Dans cette option, il s'agit du nombre maximum d'éléments que le service ActiveSync renverra au client en réponse à une demande de synchronisation. L'utilisation d'une valeur inférieure dans cette option peut réduire l'utilisation de la mémoire sur un serveur occupé, mais elle nécessitera plus de connexions et de bande passante. Elle peut également réduire la durée de vie de la batterie, car les appareils peuvent avoir besoin d'effectuer davantage de requêtes pour obtenir toutes les modifications lors d'une synchronisation. Des valeurs plus élevées dans cette option augmentent l'utilisation de la mémoire et sont plus susceptibles de provoquer des erreurs de communication. La valeur par défaut de 100 est généralement un bon compromis. Il convient toutefois de noter que les clients spécifieront la valeur qu'ils préfèrent, ce qui pourrait effectivement abaisser cette valeur pour certains d'entre eux. Si un client demande une valeur supérieure à la valeur maximale, c'est cette dernière qui sera utilisée.

Taille max de la réponse (Mo)

Il s'agit de la taille max autorisée d'une réponse à une demande de synchronisation émanant d'un client. Avant de traiter un élément donné pour la synchronisation serveur-client, la taille actuelle de la réponse est vérifiée et si elle est supérieure ou égale à cette valeur, la collection est signalée qu'il y a plus de changements disponibles et aucun élément ne sera ajouté à la réponse. Cette fonction est utile pour les serveurs qui contiennent régulièrement de nombreuses pièces jointes volumineuses dans leurs messages électroniques.

Expiration des données PIM en cache (5-60 minutes)

Comme les contacts, documents, événements et autres données PIM sont souvent statiques et ne reçoivent qu'occasionnellement des mises à jour de la part des clients, le MDAS met ces données en cache pour réduire l'activité du disque. Cependant, elles sont automatiquement rechargées lorsque les données changent sur le disque. Cette valeur détermine la durée de mise en cache des données de l'utilisateur depuis le Dernier accès.

Utilisation du stockage

Archiver automatiquement les requêtes XML/WBXML avec des erreurs

Dans le cas où vous avez désactivé les options d'*Archiver les requêtes et les réponses [XML* | *WBXML*] sur l'écran<u>Paramètres clients</u> (447), cette option archivera

quand même les requêtes XML ou WBXML qui posent problème. Seules les demandes qui provoquent des erreurs seront archivées. Cette option est activée par défaut.

Conserver les requêtes et réponses WBXML archivées pendant [xx] jours

Il s'agit du nombre de jours pendant lesquels les réponses archivées automatiquement seront conservées. Elles sont conservées pendant 3 jours par défaut.

Emplacement de l'archive XML/WBXML

Répertoire de journaux par défaut (par défaut)

Les fichiers de demandes et d'erreurs XML/WBXML auto-archivés seront stockés dans le Répertoire journaux de MDaemon par défaut.

Répertoire du client ActiveSync

Choisissez cette option si vous souhaitez stocker les fichiers dans le répertoire du client ActiveSync Debug de l'utilisateur.

Supprimer les clients inactifs au bout de [xx] jours

C'est le nombre de jours qu'un <u>périphérique ActiveSync</u> will peut passer sans se connecter au MDAS avant d'être supprimé. Lorsque le périphérique est supprimé, sa configuration et ses Aucuns accès ne sont pris en compte. Si le périphérique se connecte à nouveau, MDaemon réagira comme s'il s'agissait d'un nouveau périphérique qui n'a jamais été utilisé sur le serveur. Si une stratégie est en place pour le <u>domaine</u> 402 ou le <u>compte</u> 479, il sera contraint de procéder à un reprovisionnement , à une synchronisation initiale des dossiers et à une nouvelle synchronisation de tous les dossiers auxquels il est abonné. Cette option permet d'éviter à votre serveur de conserver des informations pour des périphériques anciens et inutilisés. L'option est réglée sur 31 jours par défaut. Lorsqu'elle est définie sur "0", les terminaux ne seront pas supprimés, quelle que soit la durée de leur inactivité.

Paramètres clients globaux par défaut

Cliquez sur ce bouton pour ouvrir la boîte de dialogue<u>Paramètres du client ActiveSync</u> <u>globaux</u>[447], afin de configurer les paramètres par défaut à utiliser pour les clients ActiveSync.

Notifications ActiveSync

Notifications de retour de synchronisation

Le service ActiveSync peut notifier les administrateurs si un client envoie de manière répétée/fréquente des clés de synchronisation expirées dans les opérations de synchronisation.

Ces notifications informent simplement l'administrateur que le serveur a émis un rollback pour une collection donnée parce qu'un client a fait une demande de synchronisation avec la dernière clé de synchronisation expirée. Le sujet indique "Client ActiveSync utilisant une clé de synchronisation expirée". Cela peut être dû à un problème de réseau ou au contenu précédemment envoyé au client dans cette

collection. Dans certains cas, l'ID de l'élément sera présent, cela dépend simplement du fait que la synchronisation précédente sur cette collection a envoyé ou non des éléments.

Les avertissements de retour en arrière ne signifient pas que le client est désynchronisé, mais que le client a le potentiel de se désynchroniser et que notre système interne l'a détecté. Les avertissements de retour en arrière sont émis pour une collection au maximum une fois par période de 24 heures. Les clés suivantes peuvent être modifiées dans l'en-tête [System] du fichier \MDaemon\Data\AirSync.ini:

- Non par défaut) [System] SendRollbackNotifications=[0|1|Yes|No|True| False] (Non par défaut)
- [System] RollbackNotificationThreshhold=[1-254] : Le nombre de rollbacks qui doivent se produire sur une collection donnée avant qu'une notification ne soit envoyée à l'administrateur. Nous recommandons une valeur d'au moins 5 ici, car les problèmes de réseau jouent un rôle dans ce domaine. (Non par défaut)
- [System] RollbackNotificationCCUser=[0|1|Yes|No|True|False] : Il faut ou non envoyer un CC à l'utilisateur dont le client a envoyé la clé de synchronisation expirée. (Non (par défaut))

Notifications de messages corrompus ActiveSync

Le service ActiveSync peut notifier les administrateurs si un message particulier ne peut pas être traité. Dans ce cas, les notifications sont envoyées en temps réel pour informer l'administrateur qu'un élément de courrier n'a pas pu être analysé et qu'il n'est pas possible de poursuivre l'action sur cet élément. L'Objet du message indique "Notification de message corrompu". Dans les versions précédentes, ces éléments pouvaient entraîner un plantage. Dans la plupart des cas, le contenu du fichier msg ne sera pas une donnée MIME. Si c'est le cas, il est probablement corrompu. Vous pouvez choisir d'envoyer ces notifications à l'utilisateur concerné à l'aide de la clé CMNCCUser afin qu'il sache qu'un courriel illisible est arrivé dans sa boîte aux lettres. Dans ce cas, l'action appropriée consiste à déplacer le fichier msg désigné de la boîte aux lettres de l'utilisateur et à l'analyser afin de déterminer pourquoi il ne peut pas être analysé et comment il est arrivé à exister dans l'état où il se trouve. Les clés suivantes peuvent être modifiées dans l'en-tête [System] du fichier \MDaemon\Data\AirSync.ini:

- Non par défaut) [System] SendCorruptMessageNotifications=[Yes|No|1|0| True|False] (Default is Enabled)
- Non par défaut : [System] CMNCCUser==[0|1|Yes|No|True|False] (Non par défaut)

Voir :

ActiveSync " Diagnostics 457

3.10.2.1 Paramètres client

La page Paramètres clients répertorie les profils de paramètres ActiveSync par défaut qui ont été configurés pour ActiveSync. Vous pouvez créer et modifier des profils de paramètres clients pour : Global, <u>Domaines</u> [216], <u>Groupes</u> [497], <u>Comptes</u> [479], <u>Types de</u> <u>terminaux</u> [504] et <u>Clients</u> [488] (c'est-à-dire les périphériques) dans leurs boîtes de dialogue respectives.

Client Settings: Global	×
General FolderSync Options Content Handling	
Troubleshooting	
Archive transactions as XML WBXML	
Client Options	
Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation	
New clients require administrative approval	
Max dients per user Unlimited \checkmark	
Bandwidth reset Day 0 (Never) \checkmark	
Security	
Allow clients provisioned/managed by other servers	
Preview Runtime Settings OK Cancel Image: Construction of the setting	elp ninate

Cet écran contient les paramètres globaux pour la gestion des clients ActiveSync. Il existe des paramètres clients correspondants sous les autres pages d'ActiveSync, telles que <u>Domaines</u> (402), <u>Comptes</u> (479) et <u>Clients</u> (488), pour définir ces options par domaine, par compte et par client respectivement. Les paramètres globaux sont définis sur des valeurs spécifiques, mais les paramètres de domaine, de compte, de client et autres sont par défaut définis sur Héritage. sont par défaut réglés pour *hériter* des paramètres de leurs options parentales respectives. Par conséquent, la modification d'un paramètre sur cet écran modifiera effectivement le même paramètre sur tous les écrans enfants, ce qui vous autorise par défaut à gérer tous les clients du serveur en ne modifiant que les paramètres de cet écran. Inversement, la modification d'un paramètre sur un écran enfant remplacera son paramètre parent, ce qui vous permettra de modifier les

paramètres au niveau du domaine, du compte ou autre si nécessaire. Si nécessaire, vous pouvez modifier les paramètres au niveau du domaine, du compte ou à un autre niveau.

Comme les <u>Politiques</u> [470], qui sont assignées à l'appareil et régissent généralement ce que l'appareil peut faire, les Paramètres Client régissent ce que le serveur fera en ce qui concerne diverses options liées au client, telles que : régir le nombre de clients ActiveSync séparés qu'un compte peut utiliser, si oui ou non les Dossiers Publics seront synchronisés avec les dossiers personnels du compte, si oui ou non inclure le dossier d'expéditeurs autorisés de l'utilisateur, et ainsi de suite. Expéditeurs autorisés de l'utilisateur, etc.

Général

Résolution des problèmes

Niveau de journalisation

ActiveSync for MDaemon prend en charge six niveaux de journalisation, du plus élevé au plus faible :

- Déboga Il s'agit du niveau de journalisation le plus complet. Il consigne toutes les entrées disponibles et n'est généralement utilisé que pour diagnostiquer un problème.
 - **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.
- **Avertis** Les avertissements, les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont consignés dans le journal.
- **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- **Critiqu** Les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.
- **Hériter** Non (par défaut), le niveau journalisation est hérité de la hiérarchie des Paramètres clients. Ainsi, les clients héritent leurs paramètres des Types de clients, les Types de clients des Comptes, les Comptes des Groupes, etc. Le Paramètres globaux du client pour cette option est déterminé par le paramètre de niveau de journalisation dans le dialogue<u>Diagnostics</u> [457].

Archiver les transactions en [XML | WBXML]

Utilisez les options d'archivage*XML...* et *WBXML* si vous souhaitez enregistrer ces données, qui peuvent parfois être utiles à des fins de débogage. Les options globales sont désactivées par défaut.

Valider/corriger l'intégrité du fichier mrk PIM

Cette option exécute un processus de validation et de correction des données PIM du client afin de rechercher les problèmes connus susceptibles d'empêcher une synchronisation correcte, tels que des UID iCal en double ou des champs facultatifs vides. L'option globale est désactivée par défaut.

Options client

Appliquer les restrictions de protocole

Activez cette option si vous souhaitez refuser les connexions de tout client qui tente d'utiliser un protocole autre que les *Versions du protocole autorisées* spécifiées pour le client. Non (par défaut), cette option est désactivée, ce qui signifie que les restrictions de protocole n'empêchent pas un client d'utiliser un protocole différent ; elles indiquent simplement au client quels protocoles utiliser. Si un client tente malgré tout d'utiliser un protocole restreint, MDaemon autorisera quand même la connexion. Pour plus d'informations, voir <u>Restrictions de protocole</u> [459] pour plus d'informations.

Répondre à 'Get/UserInformation' en utilisant l'alias de l'identifiant comme 'adresse SMTP principale'

Dans ce cas, le service peut renvoyer un Alias/une adresse secondaire en tant qu'adresse primaire en réponse à une requête de type Configurer/Gérer/Informations sur l'utilisateur. Cela permet de contourner un problème causé par une mise à jour postérieure à iOS9.x qui faisait que les clients ne pouvaient pas envoyer de courrier à l'aide d'un alias. L'utilisation de cette option résulte en une réponse non conforme aux spécifications à Settings/Get/UserInformation.

Les nouveaux clients doivent recevoir l'autorisation de l'administrateuravant de synchroniser.

Activez cette option si vous souhaitez que les nouveaux clients soient autorisés par un administrateur avant de pouvoir commencer à se synchroniser avec un compte. La liste <u>Clients</u> indique tous les clients en attente d'autorisation, et l'administrateur peut les autoriser à partir du même écran. Ce paramètre est Non (par défaut).

Max. clients par utilisateur

Si vous souhaitez limiter le nombre de clients ActiveSync ou de terminaux qui peuvent être associés à un compte MDaemon, indiquez le nombre souhaité dans cette option. L'option globale est réglée sur "illimité" par défaut. Cette option est disponible sur les écrans Paramètres clients globaux, de domaine et de compte, et non sur les écrans Clients individuels.

Jour de réinitialisation de la bande passante

Utilisez cette option si vous souhaitez réinitialiser les statistiques d'utilisation de la bande passante pour les Terminaux ActiveSync un jour précis de chaque mois. L'événement de réinitialisation a lieu dans le cadre du processus de maintenance nocturne normal et est consigné dans le journal du système comme les autres routines de maintenance. L'option globale est réglée sur "0 (Jamais)" par défaut, ce qui signifie que les statistiques d'utilisation ne seront jamais réinitialisées. Paramétrez les options enfant sur un jour différent si, par exemple, vous souhaitez que le jour de réinitialisation coïncide avec la date de réinitialisation de la facturation de l'opérateur

sans fil d'un utilisateur ou d'un client.

Sécurité

Exclure du Filtrage de pays

Activez cette option dans l'écran des paramètres d'un client ActiveSync si vous souhaitez que l'appareil puisse filtrer l' <u>écran de localisation</u> (100). Cela permet à un utilisateur valide de continuer à accéder à son compte via ActiveSync lorsque, par exemple, il se rend à un endroit où les tentatives d'authentification sont bloquées. Pour que l'appareil soit exempté, il doit s'être connecté et authentifié via ActiveSync dans le délai configuré dans le paramètre<u>Supprimer les clients inactifs après ce</u> <u>nombre de jours</u> (443) situé dans l'écran Régètres.

Autoriser dynamiquement l'adresse distante

Si vous excluez un pays du Filtrage de l'emplacement, activez cette option si vous souhaitez également autoriser l'adresse IP distante à partir de laquelle il se connecte. Cela peut s'avérer utile pour autoriser d'autres clients susceptibles de se connecter à partir de la même adresse IP.

Autoriser les clients gérés par d'autres serveurs

Par défaut, lorsque le serveur ActiveSync envoie des données de provisionnement/des spécificités de politiques à un client et que celui-ci signale qu'il est également géré par un autre serveur ActiveSync, le client sera toujours autorisé à se connecter à MDaemon. Dans ce cas, il n'y a aucun moyen de s'assurer que les spécificités de votre politique seront appliquées lorsqu'elles entrent en conflit avec la politique de l'autre serveur ActiveSync. En général, les clients utilisent par défaut l'option la plus restrictive en cas de conflit. Désactivez cette option si vous ne souhaitez pas autoriser ces clients à se connecter.

Interdire les réinitialisations aux paramètres d'usine

Si cette option est activée (On/Oui), il ne sera pas possible d'**effacer complètement** un client ActiveSync. Si vous souhaitez pouvoir effectuer un Effacer complètement à distance sur un client, vous devez d'abord désactiver cette option. L'option est désactivée par défaut. Pour plus d'informations, voir : <u>Effacer</u> <u>complètement un client ActiveSync</u> sur la page Clients.

Options FolderSync

Options de dossier

Exclure

Dossier Expéditeurs bloqués autorisés/ bloqués

Par défaut, les dossiers Expéditeurs autorisés et Dossiers Expéditeurs bloqués de l'utilisateur ne sont pas synchronisés avec les périphériques. Ils ne sont généralement utilisés par MDaemon que dans le cadre de la prévention automatique du spam. C'est pourquoi ils n'ont pas besoin d'être affichés sur les appareils en tant que contacts.

Dossiers de courrier personnalisés (Non par défaut)

Par défaut, tous les Dossiers de courrier créés par l'utilisateur et par défaut peuvent être synchronisés avec le terminal. Activez cette option si vous souhaitez que seuls les dossiers courrier par défaut soient synchronisés, c'est-àdire la Boîte de réception, les Éléments envoyés, les Éléments supprimés, les Brouillons, etc. Aucun dossier créé par l'utilisateur ne sera inclus. Cette option est désactivée par défaut.

Dossiers PIM personnalisés non (par défaut)

Par défaut, tous les dossiers PIM de l'utilisateur (contacts, calendrier, notes, tâches, etc.) sont synchronisés avec l'appareil. Activez cette option si vous souhaitez que seuls les dossiers PIM par défaut soient synchronisés. Exemple : si cette option est activée et qu'un utilisateur possède plusieurs dossiers de calendrier, seul le calendrier par défaut sera synchronisé. Cette option est désactivée par défaut.

Inclure

Arborescence Dossiers publics

Cochez cette case si vous souhaitez que les <u>Dossiers publics</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers publics</u> auxquels il a accès. Cette option est autorisée par défaut.

Navigation dans les dossiers publics (affiche les noms de dossiers)

Non par défaut, pour qu'un client puisse synchroniser un sous-dossier public ou y accéder, le compte doit disposer de l'<u>autorisation de Recherche</u> [327] pour le sousdossier (c'est-à-dire le dossier enfant) et tous les <u>Dossiers publics</u> [325] parents situés au-dessus. Si le compte n'a pas l'autorisation de voir les dossiers parents, il ne peut pas non plus voir le dossier enfant, même s'il en a l'autorisation. Activez cette option si vous souhaitez autoriser le client à accéder à ces dossiers enfants. **Par nom : l** 'activation de cette option doit nécessairement révéler les noms des dossiers parents au client, ce qui pourrait être considéré comme un risque de sécurité. Cette option est désactivée par défaut.

Nombre max de Dossiers publics

Utilisez cette option si vous souhaitez limiter le nombre de Dossiers publics autorisés sur le périphérique. Lorsqu'une limite est définie, le serveur parcourt la liste des dossiers jusqu'à ce que la limite soit atteinte, puis plus aucun dossier n'est envoyé à l'appareil. Il n'existe aucun moyen de garantir l'ordre dans lequel les dossiers seront traités. Non (paramètres par défaut).

Dossiers IMAP partagés

Cochez cette case si vous souhaitez que les <u>dossiers partagés</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers partagés</u> auxquels il a accès. Cette option est autorisée par défaut.

Gestion du contenu

Options de gestion des e-mails

Créer des tâches/rappels pour les e-mails avec indicateurs

Cette option permet à MDaemon de rappeler à l'utilisateur les éléments marqués, en créant un élément de tâche pour chaque courrier électronique marqué. lorsque le client le demande. L'option globale de ce contrôle est activée par défaut.

Toujours envoyer les mises à jour de réunion lorsque l'événement est modifié

Certains clients n'envoient pas correctement les e-mails de mise à jour des réunions lorsqu'ils modifient une réunion. Cette option indique au service ActiveSync d'envoyer une mise à jour de la réunion lorsqu'un élément de la réunion est mis à jour par l'organisateur. Cette option ne doit être définie que pour les <u>clients</u> and et les <u>types de clients</u> qui n'envoient pas correctement les mises à jour de réunion, sous peine d'envoyer des mises à jour de réunion en double. Par conséquent, cette option n'est disponible que dans les pages de paramètres pour les Clients et les Types de clients.

Demander des confirmations de lecture pour tous les e-mails envoyés

Activez cette option si vous souhaitez que le serveur demande des confirmations de lecture pour tous les courriers envoyés par un client. Cette option est désactivée par défaut.

Envoyer des confirmations de lecture du serveur lorsque le courrier est marqué comme lu et lorsque l'expéditeur le demande.

Activez cette option si vous souhaitez que le serveur prenne en charge les demandes de confirmation de lecture et délivre un accusé de réception de lecture lorsqu'un message est marqué comme lu par un client. Cette option est désactivée par défaut.

Envoyer avec l'alias spécifié dans ReplyTo

Certains clients peuvent ne pas autoriser un expéditeur à envoyer du courrier à l'aide d'un alias. Cette fonctionnalité a été ajoutée au <u>protocole Exchange ActiveSync</u> (EAS) (453) 16.x, mais certains clients ne supportent pas la version 16.x. Par exemple, Outlook pour Windows n'utilise que EAS 14.0, et bien qu'il permette à un utilisateur de spécifier une autre adresse pour l'envoi, le message généré ne reflète pas correctement les choix de l'utilisateur. Cette faculté permet d'utiliser le champ ReplyTo pour envoyer l'e-mail, à condition que l'adresse ReplyTo soit un <u>alias</u> <u>valide</u> (1994) pour cet utilisateur. L'option globale est activée par défaut.

Fusionner virtuellement les contacts publics et les contacts par défaut

Activez cette option si vous souhaitez fusionner les contacts publics avec les contacts par défaut de l'utilisateur sur le terminal. Il s'agit uniquement d'une fusion virtuelle, c'est-à-dire qu'ils ne sont pas réellement copiés dans le dossier des

contacts de l'utilisateur. Cela peut être utile sur les clients qui ne prennent pas en charge les recherches dans la liste d'adresses globale (GAL). Non (par défaut).

Dossiers Expéditeurs bloqués lors du déplacement d'un courrier dans le dossier Courriers indésirables

Si cette option est activée, lorsqu'un client déplace un e-mail vers le dossier Courriers indésirables du compte, le service ajoute l'adresse SENDER\$ - adresse de l'expéditeur de cet e-mail au dossier Contacts des expéditeurs bloqués.

Forcer l'envoi des réponses aux réunions lorsqu'une demande de réunion est acceptée/déclinée, etc.

Dans cette option, lorsqu'un client accepte, refuse ou choisit une action en réponse à une demande de réunion, le service envoie une réponse à l'organisateur de la réunion. Cette fonction est destinée aux clients spécifiques qui n'envoient pas correctement ces mises à jour eux-mêmes.

Aperçu des paramètres effectifs

Ce bouton est disponible sur tous les écrans des Paramètres clients enfant (c.-à-d. <u>domaines</u> [422], <u>comptes</u> [479] et <u>clients</u> [488]). Non (par défaut), les options de ces écrans sont définies pour hériter de leurs paramètres d'un écran parent. Utilisez cette fonction pour voir quels paramètres sont actuellement appliqués à l'écran affiché.

Voir :

ActiveSync | Domaines 462 ActiveSync | Comptes 479 ActiveSync | Clients 488

3.10.3 Sécurité

Policy Manager Accoun	ts Clients	Groups	Client Types
ystem Tuning Securi	ty Diagnostics	Protocol Res	trictions Domain
Blocked Clients The following dients are denied acc Matching Entry Type	ess Client ex Client ex Matchir 12345 Microso Outlook Windov	d Clients empt from policie: ng Ei C oft.Outlook.15 U c/15* U vsMail C vsOutlook15 C	s htry Type lient ID ser-Agent ser-Agent lient Type lient Type
			Delete Entry

Bloqués Clients

Utilisez cette option pour empêcher un Types de clients, un ID client ou un agent utilisateur spécifique d'accéder au serveur ActiveSync de MDaemon.

Ajouter une Entrée bloquée

Pour ajouter une entrée à la liste, cliquez sur **Ajouter une entrée**, indiquez les informations sur le périphérique, puis cliquez sur **Ok**. Vous pouvez obtenir les informations sur le périphérique à partir du périphérique lui-même ou des Fichiers journaux ActiveSync si le périphérique s'est connecté au serveur ActiveSync de MDaemon.

Add Blocked Entry	×
Blocking a client prevents it from performing any operations on the server. List Entry Type A specific client using its client id. Multiple clients using their device type string. Wildcards (* and ?) allowed Multiple clients using their User-Agent string. Wildcards (* and ?) allowed	
Enter client ID or pattern matching string:	
OK Cancel Help	

Vous pouvez bloquer un périphérique facilement à partir de la boîte de dialogue <u>Clients</u> (488). Cliquez avec le bouton droit de la souris sur un client dans la liste, puis cliquez sur **Bloquer ce client**.

Suppression d'une Entrée bloquée

Pour supprimer des entrées, sélectionnez une ou plusieurs entrées dans la liste et cliquez sur **Supprimer l'entrée**. Vous serez invité à confirmer l'action avant qu'elles ne soient supprimées.

Clients exemptés

Utilisez cette option pour exempter un Type du terminal, un ID client ou un Agent utilisateur spécifique des restrictions deprovisionnement ou de <u>politique.</u> 470

Ajouter un Client exempté

Pour ajouter une entrée à la liste, cliquez sur **Ajouter une entrée**, indiquez les informations sur le périphérique, puis cliquez sur **Ok**. Vous pouvez obtenir les informations sur le périphérique à partir du périphérique lui-même ou des Fichiers journaux ActiveSync si le périphérique s'est connecté au serveur ActiveSync de MDaemon.

Add Policy Exemption	×
Exempting a client from policies allows it to bypass any assigned policies List Entry Type A specific client using its client id. Multiple clients using their device type string. Wildcards (* and ?) allowed Multiple clients using their User-Agent string. Wildcards (* and ?) allowed	
Enter client ID or pattern matching string: OK Cancel Help	

Vous pouvez facilement exempter un périphérique à partir de la boîte de dialogue <u>Clients</u> (488). Cliquez avec le bouton droit de la souris sur un client dans la liste, puis cliquez sur **Exempter ce client des politiques**.

Supprimer une entrée exemptée

Pour supprimer des entrées, sélectionnez une ou plusieurs entrées dans la liste et cliquez sur **Supprimer l'entrée**. Vous serez invité à confirmer l'action avant qu'elles ne soient supprimées.

Voir :

Clients | ActiveSync 488

3.10.4 Diagnostics

Policy Manage	er A	Accounts	Clients	Groups	Client Ty	pes
System 1	Tuning	Security	Diagnostics	Protocol Restric	ctions Dor	nain
Logging						
Loa lev	el None	~		View	/ Analyze Log	
				1121	, rindifice cog	
- Advanced Op	otions		Minimum debugge	r log level None		\sim
			No more	then every 250		
	ss Memory Co	unters	INO MORE	than every 360	seconds	
Log Syste	m Wide Perfor	mance Inform	mation	(30-	3600)	
Process Dumps						
Process Dumps	r based proces	ss dumps		🗹 Indude h	eap information	
Process Dumps	r based proces	ss dumps	Prefix dump	Include h	eap information	
Process Dumps	r based proces	ss dumps e dumps on	Prefix dump	Include h	eap information nc	
Process Dumps Enable error Errors / Warnin Value	r based proces gs to generat DumpCount	ss dumps e dumps on LogEntry	Prefix dump	Include h	eap information nc	^
Process Dumps Enable error Errors / Warnin Value 0xC131FFFF	r based proces gs to generat DumpCount 3	ss dumps e dumps on LogEntry	Prefix dump	Indude h	eap information nc	^
Process Dumps Enable error Errors / Warnin Value 0xC131FFFF 0xC135FE00	r based proces gs to generat DumpCount 3 3	ss dumps e dumps on LogEntry The API ins	Prefix dump	Include h of files with AirSyn	eap information nc eing called for. (1	^
Process Dumps Enable error Errors / Warnin Value 0xC131FFFF 0xC135FE00 0xC135FE01	r based proces gs to generat DumpCount 3 3 3	e dumps on LogEntry The API ins The procedi	Prefix dump talled does not mat ure called has been	Include h o files with AirSyn ch the API level be o deprecated.	eap information nc eing called for. (1	^
Process Dumps Enable error Value 0xC131FFFF 0xC135FE00 0xC135FE01 0xC135FE04	gs to generat DumpCount 3 3 3 3	e dumps on LogEntry The API ins The procedu	Prefix dump talled does not mat ure called has been to read or write to	Include h o files with AirSyn ch the API level be o deprecated. the specified mem	eap information nc eing called for. () nory would result	^
Process Dumps Enable error Value 0xC131FFFF 0xC135FE00 0xC135FE01 0xC135FE04 0xC135FE08	gs to generat DumpCount 3 3 3 3 3 3 3	e dumps on LogEntry The API ins The proced An attempt Access Den	Prefix dump talled does not mat ure called has been to read or write to ied (MD_ACCESSDE	Include h o files with AirSyn the API level be o deprecated. the specified mem ENIED)	eap information nc eing called for. () nory would result	^
Process Dumps Enable error Value 0xC131FFFF 0xC135FE00 0xC135FE01 0xC135FE04 0xC135FE08	gs to generat DumpCount 3 3 3 3 3	e dumps on LogEntry The API ins The proced An attempt Access Den	Prefix dump talled does not mat ure called has been to read or write to ied (MD_ACCESSD	Include h offiles with AirSyn the API level be of deprecated. the specified mem ENIED)	eap information	~
Process Dumps Enable error Value 0xC131FFFF 0xC135FE00 0xC135FE01 0xC135FE04 0xC135FE08	gs to generat DumpCount 3 3 3 3	e dumps on LogEntry The API ins The proced An attempt Access Den	Prefix dump talled does not mat ure called has been to read or write to ied (MD_ACCESSDE	Include h offiles with AirSyn the API level be of deprecated. the specified ment ENIED)	eap information nc eing called for. () nory would result	*

Cet écran contient des options avancées qui, dans la plupart des cas, ne devront pas être utilisées, sauf si vous essayez de diagnostiquer un problème ou si vous êtes en contact avec le support technique.

Journalisation et archivage

Cette section contient la configuration globale du niveau de journalisation d'ActiveSync. Les <u>Paramètres clients de domaine</u> abilitation de journalisation est configuré sur "Utiliser les paramètres Nonètres par défaut", hériteront de ce paramètre à partir de cette section.

Niveau de journalisation

Six niveaux de journalisation sont pris en charge, de la plus grande à la plus petite quantité de données enregistrées :

- Déboga Il s'agit du niveau de journalisation le plus complet. Il enregistre toutes les entrées disponibles et n'est généralement utilisé que pour diagnostiquer un problème ou lorsque l'administrateur souhaite obtenir des informations détaillées.
 - **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.

Avertis	Les avertissements, les erreurs, les erreurs critiques et les
sement	événements de démarrage/arrêt sont consignés dans le journal.

- **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- **Critiqu** Les erreurs critiques et les événements de démarrage/arrêt sont e journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.

Visualiser/Analyser le journal

Cliquez sur ce bouton pour ouvrir la fenêtre de visualisation du journal du système MDaemon Advanced. Non (par défaut) Pas de journalisation dans :".. \NMDaemon\Logs\"

Options avancées

Niveau minimal du journal de débogage

Il s'agit du niveau minimal de la journalisation à envoyer au débogage. Les niveaux de journalisation disponibles sont les mêmes que ceux décrits ci-dessus.

Enregistrer les compteurs de mémoire du processus

Cochez cette case pour consigner dans le fichier journal les informations relatives à la mémoire, aux gestionnaires et aux threads spécifiques au processus. Ceci est utile pour trouver des pistes potentielles et des problèmes d'allocation de ressources. Les entrées du journal ne seront émises que si les données ont changé depuis la dernière fois qu'elles ont été journalisées.

Pas de journalisation des informations sur les performances de l'ensemble du système

Cochez cette case si vous souhaitez consigner dans le fichier journal des informations sur les performances de l'ensemble du système. Ceci est utile pour trouver des pistes potentielles et des problèmes d'allocation de ressources. Les entrées journal ne seront émises que si les données ont changé depuis la dernière fois qu'elles ont été journalisées.

Pas plus de toutes les [xx] secondes

Cette option permet de définir la fréquence à laquelle les informations relatives aux processus et aux performances seront journalisées.

Fichiers dumpers

Créer un dump du processus en cas d'erreur

Activez cette option si vous souhaitez générer des Fichiers dumps à chaque fois que survient un avertissement ou une erreur spécifique que vous avez désigné cidessous.

Inclure les informations du tas dans les dumps

Non (par défaut), les informations du tas sont incluses dans les Fichiers dumps. Décochez cette case si vous ne souhaitez pas les inclure.

Préfixe des fichiers dump

Les noms des fichiers dumpiers commenceront par ce texte.

Erreurs/avertissements à partir desquels générer des fichiers dumps

Cliquez avec le bouton droit de la souris sur cette zone et utilisez les options*Ajouter/Modifier/Supprimer une entrée...* pour gérer la liste des erreurs ou des avertissements qui déclencheront des vidages de processus. Pour chaque entrée, vous pouvez spécifier le nombre de Fichiers dumps autorisés avant qu'elle ne soit désactivée.

Voir :

ActiveSync | Réglages 443

3.10.5 Restrictions de protocoles

Policy Ma	nager	Accounts		Client	s	Grou	lps	Clie	ent Types
System	Tuning	Security	C	iagnostic	s	Protoco	Restrict	tions	Domain
Filter			2.5	12.0	12.1	14.0	14.1	16.1	
Default			x	x	x	x	x	x	
motorola-D	ROIDRAZR*		x		x				
Outlook-iO	S-Android/*		x	x	X	X			
SAMSUNG	*7500*		X		X				
A Protocol R does not ma rebooted, a	estriction MU ke an OPTIO nd the accour	ST be present a NS request, the	at the t Accou d so that	ime the c int should at it make	lient mal l be rem es the re	kes an O oved fro quired O	PTIONS m the dia PTIONS	request. ent, the o request t	If the clier lient o the
server. This	will instruct th	ne client of wha	at Proto	ocol Versi	ons are a	available	to it.		

Restrictions de protocole pour les périphériques

Utilisez les options situées sous "ActiveSync | Restrictions de protocoles" pour indiquer à certains clients et périphériques qu'ils sont limités à des protocoles ActiveSync spécifiques. Cela s'avère utile lorsque, par exemple, un certain type de périphérique s'avère avoir un support peu fiable pour un protocole mais un support fiable pour un autre. En utilisant la boîte de dialogue<u>Ajouter/Modifier une restriction de protocole</u> ^[461], vous pouvez définir des restrictions basées sur l'Agent utilisateur ou le Type de terminal, et restreindre les terminaux à n'importe laquelle des versions de protocole ActiveSync suivantes : 2.5, 12.0, 12.1, 14.0, 14.1 et 16.1.

Non (par défaut), les restrictions de protocole n'empêchent pas un client d'essayer d'utiliser un protocole différent ; elles indiquent au client quels protocoles utiliser. Si un client tente malgré tout d'utiliser un protocole restreint, MDaemon autorise la connexion. Si vous souhaitez refuser les connexions qui tentent d'utiliser des protocoles restreints, utilisez l' option *Appliquer les restrictions de protocole* dans la boîte de dialogue<u>Paramètres clients</u>

Cliquez avec le bouton droit de la souris sur une entrée de la liste pour ouvrir un menu contextuel proposant les options suivantes :

Créer une restriction de protocole.

Cliquez sur cette option pour ouvrir la boîte de dialogue<u>Ajouter/Modifier une</u> <u>restriction de protocole</u> (461) (voir ci-dessous), utilisée pour ajouter vos restrictions de protocole.

Modifier une restriction de protocole

Pour modifier une restriction de protocole, double-cliquez sur une entrée de la liste (ou cliquez avec le bouton droit de la souris et choisissez **Modifier la restriction de protocole**). Dans l'éditeur de restrictions, après avoir effectué les modifications souhaitées, cliquez sur **OK**.

Supprimer une restriction de protocole

Pour supprimer une restriction de protocole, double-cliquez sur une entrée de la liste (ou cliquez avec le bouton droit de la souris et sélectionnez **Supprimer la restriction de protocole**). Cliquez sur **Oui** pour confirmer votre décision de supprimer la restriction.

Add/Edit Protocol Restriction							
User-Agent or Device Type Filter. Wildcards (* and ?) allowed							
Allowed Protocol Versions							
Version 2.5							
Version <u>1</u> 2.0							
Version 1 <u>2</u> .1							
✓ Version 1 <u>4</u> .0							
✓ Version 14.1							
✓ Version 1 <u>6</u> .1							
OK Cancel Help							

Ajouter/Modifier une restriction de protocole

Filtre sur l'agent utilisateur ou le type de terminal

Saisissez l'Agent utilisateur ou le Type de terminal auquel la restriction s'appliquera. Dans l'identification de l'agent, MDaemon utilise jusqu'au premier caractère " / " inclus de la chaîne, s'il y en a un. Si ce n'est pas le cas, toute la chaîne est utilisée. Si vous ne connaissez pas le nom exact de l'Agent utilisateur ou du Device Type, une fois que le client s'est connecté à MDaemon ActiveSync (MDAS), vous pouvez aller sur l' écran<u>Clients</u> aller, sélectionner le client dans la liste et cliquer sur Détails. Vous pouvez également trouver ces infos en examinant directement le fichier journal de MDAS.

Versions du protocole autorisées

Cliquez sur chaque protocole que vous souhaitez prendre en charge pour le périphérique ou l'agent. Lorsque le client spécifié se connecte à MDaemon, il est invité à utiliser uniquement les protocoles que vous avez sélectionnés.

3.10.6 Domaines

462

Policy Manager		Accounts		Clients		Groups	Client Types
System	Tuning Security		Diagnostics		s Protocol Restrictions Domain		
Right-Click on	or press t	ne Context-	Menu	on an item ke	ey to m	ake modifications	
Domain	ActiveSyr	nc Enabled	Setti	ngs defined	Assig	ned Policy	
company.test	Enabled		Yes		<no policy="" set=""></no>		
example.com	Enabled		No		<no< td=""><td>Policy Set></td><td></td></no<>	Policy Set>	
Enable all do	mains unle	ss explicitly	enable	ed or disabled	ł		

Utilisez cet écran pour gérer les paramètres ActiveSync de vos <u>domaines</u> 1841. Vous pouvez activer ou désactiver ActiveSync pour chaque domaine, attribuer une <u>politique</u> <u>ActiveSync</u> 4701 par défaut , gérer les paramètres client par défaut et gérer les périphériques associés au domaine.

Activer/Désactiver ActiveSync pour des domaines spécifiques

Pour définir l'état d'ActiveSync pour un domaine spécifique :

- 1. Cliquez avec le bouton droit de la souris sur un domaine dans la liste.
- Cliquez sur Activer, Désactiver ou Défaut. Si vous choisissez "Défaut", l'option "Activer tous les domaines sauf s'ils sont explicitement activés ou désactivés" déterminera si ActiveSync est activé ou non pour le domaine.

Pour utiliser ActiveSync, vous devez correctement configurer un client ActiveSync sur le périphérique de l'utilisateur. Pour obtenir des instructions sur la façon de procéder, suivez la procédure suivante <u>Acheter, mettre à niveau ou réviser</u> <u>IesActiveSync pour MDaemon</u> sur l'écran d'<u>ActiveSync pour</u> <u>MDaemon</u>^[441] et faites défiler vers le bas jusqu'aux instructions de configuration de l'appareil.

Non (par défaut ActiveSync)

Les domaines dont la colonne ActiveSync activé est définie sur Activé/Désactivé (défaut) obtiennent leur paramètre ActiveSync à partir de l'état de l'option : Activer tous les domaines sauf s'ils sont explicitement activés ou désactivés. Lorsque cette option est activée, ActiveSync est activé par défaut dans tous les domaines. Lorsqu'elle est désactivée, ActiveSync sera désactivé par défaut. Le fait de paramétrer un domaine spécifiquement sur Activé ou Désactivé remplacera le paramètre par défaut.

Si vous changez le paramètre ActiveSync activé d'un domaine en **Désactivé**, une boîte de confirmation s'ouvrira pour vous demander si vous souhaitez retirer tout accès ActiveSync à tous les utilisateurs de ce domaine. Choisissez **Non** si vous souhaitez permettre aux utilisateurs du domaine qui utilisent actuellement ActiveSync de continuer à l'utiliser. Si vous choisissez **Oui**, ActiveSync sera alors désactivé pour tous les utilisateurs de ce domaine.

Modifier les paramètres clients d'un domaine

Cliquez avec le bouton droit de la souris sur un domaine pour gérer les Paramètres clients de ce domaine. Par défaut, ces paramètres sont hérités de l'écran "<u>Paramètres</u> <u>clients globaux</u>[447]". Voir <u>Gestion des Paramètres clients d'un domaine ci-dessous.</u>

Attribuer une Politique ActiveSync par défaut

Pour appliquer une Politique ActiveSync par défaut à un domaine :

- 1. Cliquez avec le bouton droit de la souris sur un domaine dans la liste.
- 2. Cliquez sur **Appliquer politique**.
- Dans "Politique à attribuer", sélectionnez la politique souhaitée dans la liste déroulante (pour gérer les politiques disponibles, voir le <u>Gestionnaire de</u> <u>politiques</u> 470).
- 4. Cliquez sur **OK**.

□ Gestion des paramètres clients d'un domaine

L'écran Paramètres clients du domaine vous permet de gérer les paramètres par défaut des comptes et des clients associés au domaine.

Client Settings: company.test	×
General FolderSync Options Content Handling	
Troubleshooting Log level Use inherited or default Archive transactions as XML WBXML Validate/correct PIM mrk file integrity	
Client Options Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation New clients require administrative approval	
Max clients per user Use inherited or default \vee Bandwidth reset Day Use inherited or default \vee	
Security Allow clients provisioned/managed by other servers Disallow Factory Reset Wipes 	
Preview Runtime Settings OK Cancel Help Image: Construction of the setting of the setti	e

Non (par défaut), toutes les options de cet écran sont définies sur "Utiliser les paramètres hérités ou par défaut", ce qui signifie que chaque option sera définie à partir de l'option correspondante de l' écran <u>Paramètres clients globaux</u> [447]. De même, les écrans des Paramètres des <u>comptes de</u> [479] ce domaine hériteront de leurs paramètres de cet écran, puisque l'écran des Paramètres des clients du domaine est leur écran parent. Toute modification apportée aux options de cet écran sera répercutée sur ces écrans. En dessous, les Paramètres des Types de clients ont des écrans de paramètres qui héritent de leurs paramètres des paramètres au niveau du compte, et enfin, les <u>clients</u> [466] individuels ont également leurs propres paramètres. Cette configuration vous permet d'apporter des modifications à tous les comptes et clients d'un domaine en modifiant simplement cet écran, tout en vous permettant de remplacer ces paramètres pour n'importe quel compte ou client si nécessaire.

Général

Résolution des problèmes

Niveau de journalisation

ActiveSync for MDaemon prend en charge six niveaux de journalisation, du plus élevé au plus faible :

- Déboga Il s'agit du niveau de journalisation le plus complet. Il consigne toutes les entrées disponibles et n'est généralement utilisé que pour diagnostiquer un problème.
 - **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.
- AvertisLes avertissements, les erreurs, les erreurs critiques et lessementévénements de démarrage/arrêt sont consignés dans le journal.
 - **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- **Critiqu** Les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.
- **Hériter** Non (par défaut), le niveau journalisation est hérité de la hiérarchie des Paramètres clients. Ainsi, les clients héritent leurs paramètres des Types de clients, les Types de clients des Comptes, les Comptes des Groupes, etc. Le Paramètres globaux du client pour cette option est déterminé par le paramètre de niveau de journalisation dans le dialogue<u>Diagnostics</u> [457].

Archiver les transactions en [XML | WBXML]

Utilisez les options d'archivage*XML...* et *WBXML* si vous souhaitez enregistrer ces données, qui peuvent parfois être utiles à des fins de débogage. Les options globales sont désactivées par défaut.

Valider/corriger l'intégrité du fichier mrk PIM

Cette option exécute un processus de validation et de correction des données PIM du client afin de rechercher les problèmes connus susceptibles d'empêcher une synchronisation correcte, tels que des UID iCal en double ou des champs facultatifs vides. L'option globale est désactivée par défaut.

Options client

Appliquer les restrictions de protocole

Activez cette option si vous souhaitez refuser les connexions de tout client qui tente d'utiliser un protocole autre que les *Versions du protocole autorisées*

spécifiées pour le client. Non (par défaut), cette option est désactivée, ce qui signifie que les restrictions de protocole n'empêchent pas un client d'utiliser un protocole différent ; elles indiquent simplement au client quels protocoles utiliser. Si un client tente malgré tout d'utiliser un protocole restreint, MDaemon autorisera quand même la connexion. Pour plus d'informations, voir <u>Restrictions de protocole</u> of pour plus d'informations.

Répondre à 'Get/UserInformation' en utilisant l'alias de l'identifiant comme 'adresse SMTP principale'

Dans ce cas, le service peut renvoyer un Alias/une adresse secondaire en tant qu'adresse primaire en réponse à une requête de type Configurer/Gérer/Informations sur l'utilisateur. Cela permet de contourner un problème causé par une mise à jour postérieure à iOS9.x qui faisait que les clients ne pouvaient pas envoyer de courrier à l'aide d'un alias. L'utilisation de cette option résulte en une réponse non conforme aux spécifications à Settings/Get/UserInformation.

Les nouveaux clients doivent recevoir l'autorisation de l'administrateuravant de synchroniser.

Activez cette option si vous souhaitez que les nouveaux clients soient autorisés par un administrateur avant de pouvoir commencer à se synchroniser avec un compte. La liste <u>Clients</u> indique tous les clients en attente d'autorisation, et l'administrateur peut les autoriser à partir du même écran. Ce paramètre est Non (par défaut).

Max. clients par utilisateur

Si vous souhaitez limiter le nombre de clients ActiveSync ou de terminaux qui peuvent être associés à un compte MDaemon, indiquez le nombre souhaité dans cette option. L'option globale est réglée sur "illimité" par défaut. Cette option est disponible sur les écrans Paramètres clients globaux, de domaine et de compte, et non sur les écrans Clients individuels.

Jour de réinitialisation de la bande passante

Utilisez cette option si vous souhaitez réinitialiser les statistiques d'utilisation de la bande passante pour les Terminaux ActiveSync un jour précis de chaque mois. L'événement de réinitialisation a lieu dans le cadre du processus de maintenance nocturne normal et est consigné dans le journal du système comme les autres routines de maintenance. L'option globale est réglée sur "0 (Jamais)" par défaut, ce qui signifie que les statistiques d'utilisation ne seront jamais réinitialisées. Paramétrez les options enfant sur un jour différent si, par exemple, vous souhaitez que le jour de réinitialisation coïncide avec la date de réinitialisation de la facturation de l'opérateur sans fil d'un utilisateur ou d'un client.

Sécurité

Exclure du Filtrage de pays

Activez cette option dans l'écran des paramètres d'un client ActiveSync si vous souhaitez que l'appareil puisse filtrer l' <u>écran de localisation</u> . Cela permet à un utilisateur valide de continuer à accéder à son compte via ActiveSync lorsque, par exemple, il se rend à un endroit où les tentatives d'authentification sont bloquées. Pour que l'appareil soit exempté, il doit s'être connecté et authentifié via ActiveSync dans le délai configuré dans le paramètre<u>Supprimer les clients inactifs</u> après ce nombre de jours 43 situé dans l'écran Régètres.

Autoriser dynamiquement l'adresse distante

Si vous excluez un pays du Filtrage de l'emplacement, activez cette option si vous souhaitez également autoriser l'adresse IP distante à partir de laquelle il se connecte. Cela peut s'avérer utile pour autoriser d'autres clients susceptibles de se connecter à partir de la même adresse IP.

Autoriser les clients gérés par d'autres serveurs

Par défaut, lorsque le serveur ActiveSync envoie des données de provisionnement/des spécificités de politiques à un client et que celui-ci signale qu'il est également géré par un autre serveur ActiveSync, le client sera toujours autorisé à se connecter à MDaemon. Dans ce cas, il n'y a aucun moyen de s'assurer que les spécificités de votre politique seront appliquées lorsqu'elles entrent en conflit avec la politique de l'autre serveur ActiveSync. En général, les clients utilisent par défaut l'option la plus restrictive en cas de conflit. Désactivez cette option si vous ne souhaitez pas autoriser ces clients à se connecter.

Interdire les réinitialisations aux paramètres d'usine

Si cette option est activée (On/Oui), il ne sera pas possible d'**effacer complètement** un client ActiveSync. Si vous souhaitez pouvoir effectuer un Effacer complètement à distance sur un client, vous devez d'abord désactiver cette option. L'option est désactivée par défaut. Pour plus d'informations, voir : <u>Effacer</u> <u>complètement un client ActiveSync</u> sur la page Clients.

Options FolderSync

Options de dossier

Exclure

Dossier Expéditeurs bloqués autorisés/ bloqués

Par défaut, les dossiers Expéditeurs autorisés et Dossiers Expéditeurs bloqués de l'utilisateur ne sont pas synchronisés avec les périphériques. Ils ne sont généralement utilisés par MDaemon que dans le cadre de la prévention automatique du spam. C'est pourquoi ils n'ont pas besoin d'être affichés sur les appareils en tant que contacts.

Dossiers de courrier personnalisés (Non par défaut)

Par défaut, tous les Dossiers de courrier créés par l'utilisateur et par défaut peuvent être synchronisés avec le terminal. Activez cette option si vous souhaitez que seuls les dossiers courrier par défaut soient synchronisés, c'està-dire la Boîte de réception, les Éléments envoyés, les Éléments supprimés, les Brouillons, etc. Aucun dossier créé par l'utilisateur ne sera inclus. Cette option est désactivée par défaut.

Dossiers PIM personnalisés non (par défaut)

Par défaut, tous les dossiers PIM de l'utilisateur (contacts, calendrier, notes, tâches, etc.) sont synchronisés avec l'appareil. Activez cette option si vous souhaitez que seuls les dossiers PIM par défaut soient synchronisés. Exemple : si

cette option est activée et qu'un utilisateur possède plusieurs dossiers de calendrier, seul le calendrier par défaut sera synchronisé. Cette option est désactivée par défaut.

Inclure

Arborescence Dossiers publics

Cochez cette case si vous souhaitez que les <u>Dossiers publics</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers publics</u> auxquels il a accès. Cette option est autorisée par défaut.

Navigation dans les dossiers publics (affiche les noms de dossiers)

Non par défaut, pour qu'un client puisse synchroniser un sous-dossier public ou y accéder, le compte doit disposer de l'<u>autorisation de Recherche</u> [327] pour le sous-dossier (c'est-à-dire le dossier enfant) et tous les <u>Dossiers publics</u> [325] parents situés au-dessus. Si le compte n'a pas l'autorisation de voir les dossiers parents, il ne peut pas non plus voir le dossier enfant, même s'il en a l'autorisation. Activez cette option si vous souhaitez autoriser le client à accéder à ces dossiers enfants. **Par nom : l** 'activation de cette option doit nécessairement révéler les noms des dossiers parents au client, ce qui pourrait être considéré comme un risque de sécurité. Cette option est désactivée par défaut.

Nombre max de Dossiers publics

Utilisez cette option si vous souhaitez limiter le nombre de Dossiers publics autorisés sur le périphérique. Lorsqu'une limite est définie, le serveur parcourt la liste des dossiers jusqu'à ce que la limite soit atteinte, puis plus aucun dossier n'est envoyé à l'appareil. Il n'existe aucun moyen de garantir l'ordre dans lequel les dossiers seront traités. Non (paramètres par défaut).

Dossiers IMAP partagés

Cochez cette case si vous souhaitez que les <u>dossiers partagés</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers partagés</u> auxquels il a accès. Cette option est autorisée par défaut.

Gestion du contenu

Options de gestion des e-mails

Créer des tâches/rappels pour les e-mails avec indicateurs

Cette option permet à MDaemon de rappeler à l'utilisateur les éléments marqués, en
créant un élément de tâche pour chaque courrier électronique marqué. lorsque le client le demande. L'option globale de ce contrôle est activée par défaut.

Toujours envoyer les mises à jour de réunion lorsque l'événement est modifié

Certains clients n'envoient pas correctement les e-mails de mise à jour des réunions lorsqu'ils modifient une réunion. Cette option indique au service ActiveSync d'envoyer une mise à jour de la réunion lorsqu'un élément de la réunion est mis à jour par l'organisateur. Cette option ne doit être définie que pour les <u>clients</u> and et les <u>types de clients</u> qui n'envoient pas correctement les mises à jour de réunion, sous peine d'envoyer des mises à jour de réunion en double. Par conséquent, cette option n'est disponible que dans les pages de paramètres pour les Clients et les Types de clients.

Demander des confirmations de lecture pour tous les e-mails envoyés

Activez cette option si vous souhaitez que le serveur demande des confirmations de lecture pour tous les courriers envoyés par un client. Cette option est désactivée par défaut.

Envoyer des confirmations de lecture du serveur lorsque le courrier est marqué comme lu et lorsque l'expéditeur le demande.

Activez cette option si vous souhaitez que le serveur prenne en charge les demandes de confirmation de lecture et délivre un accusé de réception de lecture lorsqu'un message est marqué comme lu par un client. Cette option est désactivée par défaut.

Envoyer avec l'alias spécifié dans ReplyTo

Certains clients peuvent ne pas autoriser un expéditeur à envoyer du courrier à l'aide d'un alias. Cette fonctionnalité a été ajoutée au <u>protocole Exchange</u> <u>ActiveSync (EAS)</u> 16.x, mais certains clients ne supportent pas la version 16.x. Par exemple, Outlook pour Windows n'utilise que EAS 14.0, et bien qu'il permette à un utilisateur de spécifier une autre adresse pour l'envoi, le message généré ne reflète pas correctement les choix de l'utilisateur. Cette faculté permet d'utiliser le champ ReplyTo pour envoyer l'e-mail, à condition que l'adresse ReplyTo soit un <u>alias</u> <u>valide</u> pour cet utilisateur. L'option globale est activée par défaut.

Fusionner virtuellement les contacts publics et les contacts par défaut

Activez cette option si vous souhaitez fusionner les contacts publics avec les contacts par défaut de l'utilisateur sur le terminal. Il s'agit uniquement d'une fusion virtuelle, c'est-à-dire qu'ils ne sont pas réellement copiés dans le dossier des contacts de l'utilisateur. Cela peut être utile sur les clients qui ne prennent pas en charge les recherches dans la liste d'adresses globale (GAL). Non (par défaut).

Dossiers Expéditeurs bloqués lors du déplacement d'un courrier dans le dossier Courriers indésirables

Si cette option est activée, lorsqu'un client déplace un e-mail vers le dossier Courriers indésirables du compte, le service ajoute l'adresse SENDER\$ - adresse de l'expéditeur de cet e-mail au dossier Contacts des expéditeurs bloqués.

Forcer l'envoi des réponses aux réunions lorsqu'une demande de réunion est acceptée/déclinée, etc.

Dans cette option, lorsqu'un client accepte, refuse ou choisit une action en réponse

à une demande de réunion, le service envoie une réponse à l'organisateur de la réunion. Cette fonction est destinée aux clients spécifiques qui n'envoient pas correctement ces mises à jour eux-mêmes.

Aperçu des paramètres effectifs

Ce bouton est disponible sur tous les écrans des Paramètres clients enfant (c.-à-d. <u>domaines</u> [462], <u>comptes</u> [479] et <u>clients</u> [488]). Non (par défaut), les options de ces écrans sont définies pour hériter de leurs paramètres d'un écran parent. Utilisez cette fonction pour voir quels paramètres sont actuellement appliqués à l'écran affiché.

Voir :

 Gestion de domaines " Paramètres du client ActiveSync 226

 Gestion de domaines | Clients ActiveSync 252

 Gestionnaire de politiques ActiveSync | Clients ActiveSync 470

3.10.7 Gestionnaire de politiques

					_			
System	Tuning	Security	Diagn	ostics	Prot	ocol Restrictio	ons	Domain
Policy Ma	inager	Accounts	C	ients	(Groups	Clie	ent Types
<u>s</u>	elect Domain	company.test			\sim	<u>R</u> efresh		
Right-Clid	k on or press t	he Context-Mer	u on an ite	m key to m	ake m	odifications		
Policy Nan	ne		Usage #	Policy ID				
Unsecured	ł		0	{0000000	0-000	0-0000-0000-0	-000000	000000}
4 Digit PIN	Required		0	{0000000	0-000	0-0001-0000-	-000000	000000}
Password	Required		0	{0000000	0-000	0-0002-0000	-000000	000000}
New Policy	/ 2017-04-19T	17:29:54.968Z	0	{762ba64	9-4fd0)-40d7-bbfd-4	45d 1baa	2276b}
New Policy	/ 2017-04-19T	17:17:44.462Z	0	{7c4e2ed	4-4d8	9-4223-9770-	f4a9bcd	7780d}
		F	OK	Ca	ncel	App	v	Help

Utilisez cet écran pour gérer les Politiques ActiveSync qui peuvent être attribuées aux terminaux des utilisateurs pour régir diverses options. Des politiques prédéfinies sont fournies, et vous pouvez créer, modifier et supprimer les vôtres. Des politiques par défaut peuvent être attribuées <u>par domaine</u> 462 et par <u>compte</u> 479, et des politiques peuvent être appliquées à des clients spécifiques. <u>des clients spécifiques</u> 252.

Tous les Terminaux ActiveSync ne reconnaissent pas ou n'appliquent pas les Politiques de manière cohérente. Certains peuvent ignorer les politiques ou certains éléments de politique, et d'autres peuvent nécessiter un redémarrage de l'appareil avant que les changements ne prennent effet. De plus, lorsqu'on tente d'attribuer une nouvelle politique à un terminal, elle ne sera pas appliquée à ce dernier avant sa prochaine connexion au serveur ActiveSync ; les politiques ne peuvent pas être "poussées" vers le terminal jusqu'à ce qu'il se connecte.

Politiques ActiveSync

Cliquez avec le bouton droit de la souris sur la liste pour ouvrir le menu contextuel avec les options suivantes :

Créer une stratégie

Cliquez sur cette option pour ouvrir l'<u>Éditeur de politiques ActiveSync</u> (471), utilisé pour créer et modifier vos politiques.

Supprimer

Pour supprimer une politique, sélectionnez une politique personnalisée dans la liste, puis cliquez sur **Supprimer**. Cliquez sur **Oui** pour confirmer l'action. Les règles prédéfinies ne peuvent pas être supprimées.

Modifier vos politiques

Pour modifier une politique, cliquez avec le bouton droit de la souris sur une politique personnalisée de la liste, puis cliquez sur **Modifier la politique**. Dans l'éditeur de politique, après avoir effectué les modifications souhaitées, cliquez sur **OK**. Les politiques prédéfinies ne peuvent pas être modifiées.

Afficher l'utilisation d'une politique

Cliquez avec le bouton droit de la souris sur une stratégie, puis choisissez cette option pour afficher une liste de tous les domaines, comptes et clients configurés pour utiliser cette stratégie.

Éditeur de politiques ActiveSync

L'Éditeur de politiques ActiveSync comporte quatre onglets : Général, Mots de passe, Sync et Paramètres avancés. L'onglet Paramètres avancés est caché à moins que vous n'activiez <u>Activer les options avancées de la politique</u> [441], situé sur l'écran Système ActiveSync System.

Général

Cet écran vous permet de donner un nom et une description à votre politique. Vous pouvez également prévisualiser le document XML de la politique.

Editing Policy: New Policy 2022-04-27T17:31:44.749Z {26a3ef60-bcee-415e-9225-d461	×
General Passwords Sync Advanced Settings	
Administrative Name New Policy 2022-04-27T17:31:44.749Z	
Description	
~	
Preview Policy Document	
OK Cancel Help	

Nom administratif

Par nom

Indiquez ici un nom pour votre politique personnalisée.

Description

Utilisez cette zone pour décrire votre politique personnalisée. Cette description apparaît dans la boîte de dialogue Appliquer une politique lors de la sélection d'une politique à appliquer à un domaine, un compte ou un client.

Prévisualiser le document de politique

Cliquez sur ce bouton pour prévisualiser le document de politique XML pour cette politique.

■ Mots de passe

Les options mot passe et les mots requis pour la politique sont désignés dans cet onglet.

Editing Policy: New Policy 2022-04-27T17:31:4	4.749Z {26a3ef60-bcee-415e-9225-d461.	×
General Passwords Sync Advanced Setting	js	
Require password Allow dient to save 'Recovery Password' to	server	
Password Type	Password Strength	
Simple PIN	Minimum length	*
Complex/Alpha-Numeric	Complexity level 1	*
Password Options Number of recent passwords Minute	Days until password expires 0	
Failed password attempts before client wipe	s or enters 'Timed Lockout Mode'	
ОК	Cancel He	þ

Exigences relatives aux mots passe

Cochez cette case si vous souhaitez exiger un mot de passe sur le périphérique. Elle est désactivée par défaut.

Activer le Mot de passe de récupération de l'appareil sur le serveur

Activez cette option si vous souhaitez autoriser les clients à utiliser l'option "Mot de passe de récupération" d'ActiveSync, qui permet à un appareil d'enregistrer un mot de passe de récupération temporaire sur le serveur pour déverrouiller l'appareil en cas d'oubli du mot de passe. L'administrateur peut trouver ce mot de passe de récupération dans les <u>détails du</u> appareils. La plupart des appareils ne prennent pas en charge cette fonction.

Type de mot de passe

Code PIN simple

La mise en œuvre de cette option dépend largement du terminal, mais le fait de sélectionner *Code PIN simple* comme type de mot de passe signifie généralement qu'aucune restriction ou exigence de complexité n'est imposée au mot de passe du terminal, à l'exception de l' option*Longueur minimale du mot de passe* ci-dessous. Autoriser les mots de passe simples tels que : "111", "aaa", "1234", "ABCD", etc.

Complexe/Alpha-Numérique

Utilisez cette option de politique si vous souhaitez exiger des mots de passe de périphérique plus complexes et plus sûrs que l'option *Code PIN simple*. Utilisez l'option*Niveau du complexité* ci-dessous pour définir exactement le degré de

complexité du mot de passe. Il s'agit de la sélection par défaut lorsqu'un mot de passe est demandé par la politique.

Force du mot de passe

Longueur minimale

Utilisez cette option pour définir le nombre minimum de caractères que le mot de passe du périphérique doit contenir, de 1 à 16. Cette option est définie sur "1" par défaut.

Niveau de complexité

Cette option permet de définir le niveau de complexité requis pour les mots de passe de périphérique*complexes/alphanumériques*. Le niveau correspond au nombre de types de caractères différents que le mot de passe doit contenir : lettres majuscules, lettres minuscules, chiffres et caractères non alphanumériques (tels que la ponctuation ou les caractères spéciaux). Vous pouvez exiger de 1 à 4 types de caractères. Exemple : si cette option est définie sur "2", le mot de passe doit contenir au moins deux des quatre types de caractères : majuscules et chiffres, majuscules et minuscules, chiffres et symboles, etc. Cette option est fixée à "1" par défaut.

Options de mot de passe

Jours avant expiration du mot passe (0=jamais)

Il s'agit du nombre de jours autorisés avant que le mot de passe de l'appareil ne doive être modifié. Cette option est désactivée par défaut (définie sur "0").

Nombre de mots de passe récents retenus/refusés par le dispositif (0 = aucune)

Utilisez cette option si vous souhaitez empêcher le périphérique de réutiliser un nombre spécifié d'anciens mots de passe. Exemple : si cette option est réglée sur "2" et que vous modifiez le mot de passe de votre appareil, vous ne pourrez pas le remplacer par l'un des deux derniers mots de passe utilisés. Cette option est désactivée par défaut (paramètres par défaut).

Minutes d'inactivité avant le verrouillage de l'appareil (0 = jamais)

Il s'agit du nombre de minutes pendant lesquelles un appareil peut rester sans intervention de l'utilisateur avant de se verrouiller. Cette option de mot passe est désactivée par défaut (réglée sur "0").

Effacer le terminal ou passer en mode Verrouillage temporaire après des tentatives échouées consécutives.

Lorsque cette option est activée et que l'utilisateur échoue le nombre de tentatives échouées, le terminal se verrouille pendant un certain temps ou efface toutes les données, en fonction du terminal. Cette option est désactivée par défaut.

Tentatives échouées de mot de passe avant que l'appareil ne s'efface ou ne passe en mode "Verrouillage temporaire".

Lorsque l'option"*Effacer l'appareil…*" ci-dessus est activée et qu'un utilisateur échoue à ce nombre de tentatives de mot de passe, l'appareil

sera effacé ou le "mode de verrouillage temporisé" sera déclenché, en fonction de l'appareil.

Synchronisation

Cet écran contient divers paramètres régissant les e-mails au format HTML, autorisant les pièces jointes, limitant le nombre de caractères à transférer et les délais maximums de synchronisation du courrier et du calendrier.

Editing Policy: New Policy 2022-04-27T17:31:44.749Z {26a3ef60-bcee-415e-9225-d461	×
General Passwords Sync Advanced Settings	
Mail Settings ✓ Allow HTML email ✓ Allow attachments Maximum attachment size in bytes (0=no limit) 0 • Maximum characters of text body to transfer (-1=no limit) -1 • Maximum characters of HTML body to transfer (-1=no limit)	
Maximum timeframe of mail to synchronize All ~	
Calendar Maximum historical timeframe of calendar to sync All ✓	
OK Cancel Help	

Paramètres du courrier

Autoriser les e-mails au format HTML

Non (par défaut), les e-mails au format HTML peuvent être synchronisés/envoyés aux clients ActiveSync. Décochez cette case si vous souhaitez envoyer uniquement du texte brut.

Autoriser pièces jointes

Autorise le téléchargement des pièces jointes sur terminal. Cette option est activée par défaut.

Taille maximale des pièces jointes en octets (0 = pas de limite) (0=pas de limite)

Il s'agit de la taille maximale de la pièce jointe qui peut être téléchargée automatiquement sur l'appareil. Aucune taille limite n'est fixée pour cette option par défaut (0=pas de limite).

Caractères max du corps du texte à transférer (-1 = pas de limite)

Ce nombre maximum de caractères dans le corps des messages électroniques au format texte brut qui seront envoyés au client. Si le corps du message contient plus de caractères que ce qui est autorisé, le corps sera tronqué jusqu'à la limite spécifiée. Non (par défaut) par défaut, aucune limite n'est fixée (option fixée à "-1"). Si la valeur de l'option est "0", seul l'en-tête du message est envoyé.

Caractères max du corps HTML à transférer (-1 = pas de limite)

Il s'agit du nombre maximum de caractères dans le corps des e-mails au format HTML qui seront envoyés au client. Si le corps du message contient plus de caractères que ce qui est autorisé, le corps sera tronqué jusqu'à la limite spécifiée. Non (par défaut), aucune limite n'est fixée (option fixée à "-1"). Si la valeur de l'option est "0", seul l'en-tête du message est envoyé.

Période max. de synchronisation des e-mails

Il s'agit de la quantité de courrier électronique passé, par plage de dates à partir d'aujourd'hui, qui peut être synchronisée par l'appareil. Non (par défaut), cette option est réglée sur "Tous", ce qui signifie que tous les courriels peuvent être synchronisés, quelle que soit leur ancienneté.

Calendrier

Période max. de synchronisation du calendrier à synchroniser

Il s'agit de l'intervalle de temps à partir d'aujourd'hui pendant lequel les entrées de calendrier passées peuvent être synchronisées par l'appareil. Non (par défaut) est réglé sur "Tous", ce qui signifie que toutes les entrées passées peuvent être synchronisées, quelle que soit leur ancienneté.

Paramètres avancés

L'onglet Paramètres avancés contient des options régissant les types de connexions autorisées, l'activation de certaines applications, le stockage et le cryptage, ainsi que l'itinérance.

Editing Policy: New Policy 2022-04-27T17:31:4	4.749Z {26a3ef60-bcee-415e-9225-d461 ×
General Passwords Sync Advanced Setting	js
Connections Allowed Bluetooth Yes ~ WIFI Infrared (IrDA)	Storage Require dient encryption Allow storage card Require storage card encryption Desktop sync
Applications Web browser enabled Camera enabled Consumer email enabled POP/IMAP email enabled	 Remote Desktop enabled Unsigned applications allowed Unsigned installers allowed Text messaging enabled
Roaming	
ОК	Cancel Help

Cet onglet est caché à moins que vous n'activiez <u>Activer l'édition des options</u> <u>de politique avancées</u> [441], situé sur l'écranServeur ActiveSync for MDaemon.

Connexions autorisées

Bluetooth

Cette option permet d'indiquer si les connexions Bluetooth sont autorisées ou non sur l'appareil. Vous pouvez choisir **Oui** pour autoriser les connexions Bluetooth, **Non** pour les empêcher, ou **Mains** libres pour restreindre le Bluetooth à la fonction Mains libres uniquement. Cette option est réglée sur **Oui (Paramètres** par défaut).

WIFI

Connexions autorisées. Non (par défaut).

Infrarouge (IrDA)

Connexions autorisées Infrarouge (IrDA). Activé par défaut.

Partage internet (point d'accès mobile)

Cette option permet à l'appareil d'utiliser le partage internet (point d'accès mobile). Elle est activée par défaut.

Stockage

Demander encodage du terminal

Cliquez sur cette option si vous souhaitez demander l'encodage du terminal. Tous les appareils n'appliquent pas le cryptage. Cette option est désactivée par défaut.

Autoriser les cartes de stockage

Autorise l'utilisation d'une carte de stockage dans l'appareil. Cette option est activée par défaut.

Exiger le chiffrement des cartes de stockage

Utilisez cette option si vous souhaitez exiger le chiffrement d'une carte de stockage. Cette option est désactivée par défaut.

Synchronisation du bureau

Autorise Desktop ActiveSync sur l'appareil. Non (par défaut).

Applications

Navigateur web activé

Autorise l'utilisation d'un navigateur sur l'appareil. Cette option n'est pas prise en charge sur certains appareils et peut ne pas s'appliquer aux navigateurs tiers. Elle est activée par défaut.

Appareil photo activé

Autorise l'utilisation d'un appareil photo sur l'appareil. Cette option est activée par défaut.

Messagerie perso activée

L'appareil permet à l'utilisateur de configurer un compte de courrier électronique personnel. Lorsqu'elle est désactivée, les types de comptes ou de services de messagerie interdits dépendent entièrement du client ActiveSync concerné. Cette option est activée par défaut.

Courrier POP/IMAP activé

Permet l'accès au courrier électronique POP ou IMAP. Cette option est activée par défaut.

Bureau distant activé

Permet au client d'utiliser le Bureau à distance. Non (par défaut).

Applications non signées autorisées

Cette option permet d'utiliser des applications non signées sur le périphérique. Cette option est activée par défaut.

Programmes d'installation non signés autorisés

Cette option autorise l'exécution de programmes d'installation non signés sur l'appareil. Cette option est activée par défaut.

Messagerie texte activée

Cette option autorise l'envoi de messages texte sur le terminal. Ce texte est activé par défaut.

Itinérance

Exiger une synchronisation manuelle en itinérance

Utilisez cette option de politique si vous souhaitez exiger que le terminal se synchronise manuellement en cas d'itinérance. Autoriser la synchronisation automatique en itinérance pourrait augmenter les coûts de données pour le terminal, en fonction de son opérateur et de son plan de données. Cette option est désactivée par défaut.

3.10.8 Comptes

System	Tuning	Se	curity	Diagr	nostics	Pro	otocol Restrict	ions	Domain
Policy Ma	nager	Aco	counts		Clients		Groups	C	lient Types
S	elect Domain	compa	any.test			\sim	<u>R</u> efresh		
[•] Right-Click	on or press t	he Con	text-Men	u on an a	ccount key	to ma	ke modificatio	ins	
Account			Settings	defined	Assigned	Policy			
bill.farmer	@company.te	st	No		<no polic<="" td=""><td>y Set:</td><td>></td><td></td><td></td></no>	y Set:	>		
frank.thon	nas@company	.test	No		<no polic<="" td=""><td>y Set?</td><td>></td><td></td><td></td></no>	y Set?	>		
michael.ma	ason@compan	y.test	No		<no polic<="" td=""><td>y Set></td><td>></td><td></td><td></td></no>	y Set>	>		
Eind ☑ Authorize ─Summary	user: e all accounts	upon fi	rst access	s via Activ	Ac VeSync pro	dd tocol	R <u>e</u> voke A	ll Listed	Accounts
3 /	Unlimited Ac	tiveSyr	ic licenses	; in use			3 in this	domain	

Utilisez cet écran pour désigner les comptes autorisés à utiliser ActiveSync. Vous pouvez autoriser ou révoquer des comptes manuellement, ou configurer MDaemon pour qu'il les autorise automatiquement, un par un, au fur et à mesure que chaque compte se connecte à l'aide d'ActiveSync.

Autoriser manuellement des comptes

Dans l'écran Comptes, sélectionnez un domaine dans la liste déroulante *Sélectionner le domaine*, puis cliquez sur **Ajouter** pour autoriser manuellement un ou plusieurs de ses comptes à utiliser ActiveSync. La boîte de dialogue Sélection d'utilisateurs s'ouvre alors pour rechercher et sélectionner les comptes.

	_		
Select Users, Groups	or Bui	ilt-In Objects	>
Select these object	Users		Object Types
From these domains:	comp	any.test	Locations
Common Queries			
Name contains	s:		Find Now
Email contains	s:		
Description contains			
Include Disabled Acco	ounts		
		Halp	Cancel
Search Results		Пар	Cancer
Name	Туре	Email	
🗌 🗕 Randy Peterman	User	randy.peterman@company.test	
😹 Sir Smith	User	sir.smith@company.test	

A partir de ces domaines

Cette liste répertorie le domaine que vous avez sélectionné dans l' option*Sélectionnez le domaine sur l*'écran Comptes. Vous pouvez chercher des utilisateurs de ce domaine.

Requêtes courantes

Utilisez les options de cette section pour limiter votre recherche en spécifiant tout ou partie du nom de l'utilisateur, son adresse électronique ou le contenu de la Description du compte. Laissez ces champs vides si vous souhaitez que les résultats de la recherche contiennent tous les utilisateurs du domaine sélectionné.

Inclure les comptes désactivés

Cochez cette case si vous souhaitez inclure les <u>comptes désactivés</u> dans votre recherche.

Rechercher maintenant

Une fois que vous avez spécifié tous vos critères de recherche, cliquez sur **Rechercher maintenant** pour effectuer la recherche.

Résultats de la recherche

Dans les résultats de la recherche, sélectionnez les utilisateurs souhaités et cliquez sur **OK** pour les ajouter à la liste des comptes autorisés.

Révocation de comptes

Pour révoquer l'autorisation d'un compte à utiliser ActiveSync, cliquez avec le bouton droit de la souris sur un compte dans la liste et cliquez sur **Révoquer l'autorisation ActiveSync**. Si vous souhaitez retirer tous les comptes, cliquez sur le bouton **Retirer tous les comptes de la liste**.

> Si vous avez activé l'option Autoriser tous les comptes lors du premier accès via le protocole ActiveSync, la révocation de l'accès à un compte le supprimera de la liste, mais la prochaine fois qu'un appareil se connectera pour le compte, il sera à nouveau autorisé.

Autoriser les comptes première fois qu'ils se connectent avec ActiveSync

Cochez cette case si vous souhaitez autoriser les comptes automatiquement, un par un, chaque fois qu'ils se connectent à MDaemon en utilisant ActiveSync.

Attribuer une Politique ActiveSync

Pour appliquer une <u>Politique</u> 470 attribuée au compte :

- 1. Cliquez avec le bouton droit de la souris sur un compte dans la liste.
- 2. Cliquez sur **Appliquer politique**.
- 3. Dans "Politique à attribuer", sélectionnez la politique souhaitée dans la liste déroulante (pour gérer les politiques disponibles, consultez le <u>Gestionnaire de politiques</u> [470]).
- 4. Cliquez sur **OK**.

Cette politique sera attribuée à tout nouveau terminal qui se connectera pour ce compte.

Chercher dans la liste des comptes autorisés

Si vous disposez d'un grand nombre de comptes autorisés à utiliser ActiveSync, vous pouvez utiliser la boîte**Rechercher un utilisateur pour** rechercher un compte spécifique dans la liste. Il suffit de taper les premières lettres de l'adresse électronique du compte pour sélectionner l'utilisateur.

Paramètres clients des comptes

Cliquez avec le bouton droit de la souris sur un compte et cliquez sur **Personnaliser les paramètres clients** pour gérer les Paramètres clients du compte. Ces paramètres seront appliqués à tous les clients ActiveSync qui se connectent pour le compte.

Client Settings	: frank.thomas@c	ompany.test	×
General Fo	lderSync Options	Content Handling	
– Troublesh Ar	nooting Log leve chive transactions a	Use inherited or default S INT WBXML Validate/correct PIM mrk file integrity	
Client Op Enforce Response	tions e protocol restrictior nd with logon alias a ients require adminis	ıs s 'PrimarySmtpAddress' in Get/UserInformation ıtrative approval	
E	Max clients per user Bandwidth reset Day	Use inherited or default \sim Use inherited or default \sim	
Security Exemp Dyna Allow o Disallo	ot from Location Scre amically allow remote clients provisioned/m w Factory Reset Wip	en address anaged by other servers bes	
Pre-	view Runtime Setting	IS OK Cancel Help	te

Non (par défaut), toutes les options de cet écran sont définies sur "Utiliser les paramètres Hériter du compte du compte", ce qui signifie que si le compte est membre d'un groupe, les paramètres de chaque option seront appliqués à tous les clients ActiveSync qui se connectent pour le compte. groupe 497, les paramètres de chaque option seront repris des Paramètres clients de ce groupe. Si le compte ne fait pas partie d'un groupe, ou si aucun Paramètres clients n'est configuré pour ce groupe, chaque option sera définie à partir de l'option correspondante de l' écran Paramètres clients du domaine. 226 Toute modification apportée aux paramètres de cet écran sera répercutée sur cet écran. Inversement, toute modification apportée à cet écran remplacera les paramètres du groupe ou du domaine pour ce compte.

Général

Résolution des problèmes

Niveau de journalisation

ActiveSync for MDaemon prend en charge six niveaux de journalisation, du plus élevé au plus faible :

- Déboga Il s'agit du niveau de journalisation le plus complet. Il consigne toutes les entrées disponibles et n'est généralement utilisé que pour diagnostiquer un problème.
 - **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.
- **Avertis** Les avertissements, les erreurs, les erreurs critiques et les **sement** événements de démarrage/arrêt sont consignés dans le journal.
- **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Critiqu Les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.
- **Hériter** Non (par défaut), le niveau journalisation est hérité de la hiérarchie des Paramètres clients. Ainsi, les clients héritent leurs paramètres des Types de clients, les Types de clients des Comptes, les Comptes des Groupes, etc. Le Paramètres globaux du client pour cette option est déterminé par le paramètre de niveau de journalisation dans le dialogue<u>Diagnostics</u>[457].

Archiver les transactions en [XML | WBXML]

Utilisez les options d'archivage*XML...* et *WBXML* si vous souhaitez enregistrer ces données, qui peuvent parfois être utiles à des fins de débogage. Les options globales sont désactivées par défaut.

Valider/corriger l'intégrité du fichier mrk PIM

Cette option exécute un processus de validation et de correction des données PIM du client afin de rechercher les problèmes connus susceptibles d'empêcher une synchronisation correcte, tels que des UID iCal en double ou des champs facultatifs vides. L'option globale est désactivée par défaut.

Options client

Appliquer les restrictions de protocole

Activez cette option si vous souhaitez refuser les connexions de tout client qui tente d'utiliser un protocole autre que les *Versions du protocole autorisées* spécifiées pour le client. Non (par défaut), cette option est désactivée, ce qui signifie que les restrictions de protocole n'empêchent pas un client d'utiliser un protocole différent ; elles indiquent simplement au client quels protocoles utiliser. Si un client tente malgré tout d'utiliser un protocole restreint, MDaemon autorisera quand même la connexion. Pour plus d'informations, voir <u>Restrictions de protocole</u> [459] pour plus d'informations.

Répondre à 'Get/UserInformation' en utilisant l'alias de l'identifiant comme 'adresse SMTP principale'

Dans ce cas, le service peut renvoyer un Alias/une adresse secondaire en tant qu'adresse primaire en réponse à une requête de type Configurer/Gérer/Informations sur l'utilisateur. Cela permet de contourner un problème causé par une mise à jour postérieure à iOS9.x qui faisait que les clients ne pouvaient pas envoyer de courrier à l'aide d'un alias. L'utilisation de cette option résulte en une réponse non conforme aux spécifications à Settings/Get/UserInformation.

Les nouveaux clients doivent recevoir l'autorisation de l'administrateuravant de synchroniser.

Activez cette option si vous souhaitez que les nouveaux clients soient autorisés par un administrateur avant de pouvoir commencer à se synchroniser avec un compte. La liste <u>Clients</u> indique tous les clients en attente d'autorisation, et l'administrateur peut les autoriser à partir du même écran. Ce paramètre est Non (par défaut).

Max. clients par utilisateur

Si vous souhaitez limiter le nombre de clients ActiveSync ou de terminaux qui peuvent être associés à un compte MDaemon, indiquez le nombre souhaité dans cette option. L'option globale est réglée sur "illimité" par défaut. Cette option est disponible sur les écrans Paramètres clients globaux, de domaine et de compte, et non sur les écrans Clients individuels.

Jour de réinitialisation de la bande passante

Utilisez cette option si vous souhaitez réinitialiser les statistiques d'utilisation de la bande passante pour les Terminaux ActiveSync un jour précis de chaque mois. L'événement de réinitialisation a lieu dans le cadre du processus de maintenance nocturne normal et est consigné dans le journal du système comme les autres routines de maintenance. L'option globale est réglée sur "0 (Jamais)" par défaut, ce qui signifie que les statistiques d'utilisation ne seront jamais réinitialisées. Paramétrez les options enfant sur un jour différent si, par exemple, vous souhaitez que le jour de réinitialisation coïncide avec la date de réinitialisation de la facturation de l'opérateur sans fil d'un utilisateur ou d'un client.

Sécurité

Exclure du Filtrage de pays

Activez cette option dans l'écran des paramètres d'un client ActiveSync si vous souhaitez que l'appareil puisse filtrer l' <u>écran de localisation</u> [609]. Cela permet à un utilisateur valide de continuer à accéder à son compte via ActiveSync lorsque, par exemple, il se rend à un endroit où les tentatives d'authentification sont bloquées. Pour que l'appareil soit exempté, il doit s'être connecté et authentifié via ActiveSync dans le délai configuré dans le paramètre<u>Supprimer les clients inactifs</u> <u>après ce nombre de jours</u> [443] situé dans l'écran Régètres.

Autoriser dynamiquement l'adresse distante

Si vous excluez un pays du Filtrage de l'emplacement, activez cette option si vous souhaitez également autoriser l'adresse IP distante à partir de laquelle il se connecte. Cela peut s'avérer utile pour autoriser d'autres clients susceptibles de se connecter à partir de la même adresse IP.

Autoriser les clients gérés par d'autres serveurs

Par défaut, lorsque le serveur ActiveSync envoie des données de provisionnement/des spécificités de politiques à un client et que celui-ci signale qu'il est également géré par un autre serveur ActiveSync, le client sera toujours autorisé à se connecter à MDaemon. Dans ce cas, il n'y a aucun moyen de s'assurer que les spécificités de votre politique seront appliquées lorsqu'elles entrent en conflit avec la politique de l'autre serveur ActiveSync. En général, les clients utilisent par défaut l'option la plus restrictive en cas de conflit. Désactivez cette option si vous ne souhaitez pas autoriser ces clients à se connecter.

Interdire les réinitialisations aux paramètres d'usine

Si cette option est activée (On/Oui), il ne sera pas possible d'**effacer complètement** un client ActiveSync. Si vous souhaitez pouvoir effectuer un Effacer complètement à distance sur un client, vous devez d'abord désactiver cette option. L'option est désactivée par défaut. Pour plus d'informations, voir : <u>Effacer</u> <u>complètement un client ActiveSync</u> with sur la page Clients.

Options FolderSync

Options de dossier

Exclure

Dossier Expéditeurs bloqués autorisés/ bloqués

Par défaut, les dossiers Expéditeurs autorisés et Dossiers Expéditeurs bloqués de l'utilisateur ne sont pas synchronisés avec les périphériques. Ils ne sont généralement utilisés par MDaemon que dans le cadre de la prévention automatique du spam. C'est pourquoi ils n'ont pas besoin d'être affichés sur les appareils en tant que contacts.

Dossiers de courrier personnalisés (Non par défaut)

Par défaut, tous les Dossiers de courrier créés par l'utilisateur et par défaut peuvent être synchronisés avec le terminal. Activez cette option si vous souhaitez que seuls les dossiers courrier par défaut soient synchronisés, c'està-dire la Boîte de réception, les Éléments envoyés, les Éléments supprimés, les Brouillons, etc. Aucun dossier créé par l'utilisateur ne sera inclus. Cette option est désactivée par défaut.

Dossiers PIM personnalisés non (par défaut)

Par défaut, tous les dossiers PIM de l'utilisateur (contacts, calendrier, notes, tâches, etc.) sont synchronisés avec l'appareil. Activez cette option si vous souhaitez que seuls les dossiers PIM par défaut soient synchronisés. Exemple : si cette option est activée et qu'un utilisateur possède plusieurs dossiers de calendrier, seul le calendrier par défaut sera synchronisé. Cette option est désactivée par défaut.

Inclure

Arborescence Dossiers publics

Cochez cette case si vous souhaitez que les Dossiers publics auxquels un

utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers publics</u> auxquels il a accès. Cette option est autorisée par défaut.

Navigation dans les dossiers publics (affiche les noms de dossiers)

Non par défaut, pour qu'un client puisse synchroniser un sous-dossier public ou y accéder, le compte doit disposer de l'<u>autorisation de Recherche</u> [327] pour le sous-dossier (c'est-à-dire le dossier enfant) et tous les <u>Dossiers publics</u> [325] parents situés au-dessus. Si le compte n'a pas l'autorisation de voir les dossiers parents, il ne peut pas non plus voir le dossier enfant, même s'il en a l'autorisation. Activez cette option si vous souhaitez autoriser le client à accéder à ces dossiers enfants. **Par nom : l** 'activation de cette option doit nécessairement révéler les noms des dossiers parents au client, ce qui pourrait être considéré comme un risque de sécurité. Cette option est désactivée par défaut.

Nombre max de Dossiers publics

Utilisez cette option si vous souhaitez limiter le nombre de Dossiers publics autorisés sur le périphérique. Lorsqu'une limite est définie, le serveur parcourt la liste des dossiers jusqu'à ce que la limite soit atteinte, puis plus aucun dossier n'est envoyé à l'appareil. Il n'existe aucun moyen de garantir l'ordre dans lequel les dossiers seront traités. Non (paramètres par défaut).

Dossiers IMAP partagés

Cochez cette case si vous souhaitez que les <u>dossiers partagés</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers partagés</u> ⁷⁹⁶ auxquels il a accès. Cette option est autorisée par défaut.

Gestion du contenu

Options de gestion des e-mails

Créer des tâches/rappels pour les e-mails avec indicateurs

Cette option permet à MDaemon de rappeler à l'utilisateur les éléments marqués, en créant un élément de tâche pour chaque courrier électronique marqué. lorsque le client le demande. L'option globale de ce contrôle est activée par défaut.

Toujours envoyer les mises à jour de réunion lorsque l'événement est modifié

Certains clients n'envoient pas correctement les e-mails de mise à jour des réunions lorsqu'ils modifient une réunion. Cette option indique au service ActiveSync d'envoyer une mise à jour de la réunion lorsqu'un élément de la réunion est mis à jour par l'organisateur. Cette option ne doit être définie que pour les <u>clients</u> [485] et

les <u>types de clients</u> [504] qui n'envoient pas correctement les mises à jour de réunion, sous peine d'envoyer des mises à jour de réunion en double. Par conséquent, cette option n'est disponible que dans les pages de paramètres pour les Clients et les Types de clients.

Demander des confirmations de lecture pour tous les e-mails envoyés

Activez cette option si vous souhaitez que le serveur demande des confirmations de lecture pour tous les courriers envoyés par un client. Cette option est désactivée par défaut.

Envoyer des confirmations de lecture du serveur lorsque le courrier est marqué comme lu et lorsque l'expéditeur le demande.

Activez cette option si vous souhaitez que le serveur prenne en charge les demandes de confirmation de lecture et délivre un accusé de réception de lecture lorsqu'un message est marqué comme lu par un client. Cette option est désactivée par défaut.

Envoyer avec l'alias spécifié dans ReplyTo

Certains clients peuvent ne pas autoriser un expéditeur à envoyer du courrier à l'aide d'un alias. Cette fonctionnalité a été ajoutée au <u>protocole Exchange</u> <u>ActiveSync (EAS)</u> [459] 16.x, mais certains clients ne supportent pas la version 16.x. Par exemple, Outlook pour Windows n'utilise que EAS 14.0, et bien qu'il permette à un utilisateur de spécifier une autre adresse pour l'envoi, le message généré ne reflète pas correctement les choix de l'utilisateur. Cette faculté permet d'utiliser le champ ReplyTo pour envoyer l'e-mail, à condition que l'adresse ReplyTo soit un <u>alias</u> <u>valide</u> [84] pour cet utilisateur. L'option globale est activée par défaut.

Fusionner virtuellement les contacts publics et les contacts par défaut

Activez cette option si vous souhaitez fusionner les contacts publics avec les contacts par défaut de l'utilisateur sur le terminal. Il s'agit uniquement d'une fusion virtuelle, c'est-à-dire qu'ils ne sont pas réellement copiés dans le dossier des contacts de l'utilisateur. Cela peut être utile sur les clients qui ne prennent pas en charge les recherches dans la liste d'adresses globale (GAL). Non (par défaut).

Dossiers Expéditeurs bloqués lors du déplacement d'un courrier dans le dossier Courriers indésirables

Si cette option est activée, lorsqu'un client déplace un e-mail vers le dossier Courriers indésirables du compte, le service ajoute l'adresse SENDER\$ - adresse de l'expéditeur de cet e-mail au dossier Contacts des expéditeurs bloqués.

Forcer l'envoi des réponses aux réunions lorsqu'une demande de réunion est acceptée/déclinée, etc.

Dans cette option, lorsqu'un client accepte, refuse ou choisit une action en réponse à une demande de réunion, le service envoie une réponse à l'organisateur de la réunion. Cette fonction est destinée aux clients spécifiques qui n'envoient pas correctement ces mises à jour eux-mêmes.

Aperçu des paramètres effectifs

Ce bouton est disponible sur tous les écrans des Paramètres clients enfant (c.-à-d. <u>domaines</u> 462, <u>comptes</u> 479 et <u>clients</u> 488). Non (par défaut), les options de ces écrans sont définies pour hériter de leurs paramètres d'un écran parent. Utilisez cette fonction pour voir quels paramètres sont actuellement appliqués à l'écran affiché.

Voir :

ActiveSync | Paramètres client 447 ActiveSync | Domaines 462 ActiveSync | Clients 488 Comptes | Paramètres du client ActiveSync 820 Comptes | Clients ActiveSync 827

3.10.9 Clients

System	Tuning	Se	curity	Diagnostics	;	Prot	ocol Restrictio	ons Domains
Policy Ma	anager	Acc	ounts	Clients		0	Groups	Client Types
S Right-Clic	elect Domain k on or press	compa the Con	iny.test text-Menu	on an accoun	t key to	- mak	<u>R</u> efresh e modification	s
Email Add	ress		Client Typ	e			Client ID	
bill, farmer	@company.te	est	Windows	Dutlook 15			48E708C28E	654AC3A31AB629
frank.tho	nas@compan	v.test	iPad				AppIDMR 11X(05F182
frank thomas@company.test			SAMSLINGSCHT747				SEC192C55E	9C4C8A
frank.thomas@company.test			WindowsQutlook15			9090756BDAE942CFA4F56DFDI		
michael.mason@company.test			Collector 1.0 (Requires Approval)			al)	TIVANb7b552669e51cf8660b80	
michael.m	ason@compa	nv.test	Windows	Dutlook 15		<u></u>	C44088A6A7	6341F192B25668
<								>
Filter C	lient Listing to	All (dients				\sim	

Cet écran contient une entrée pour chaque client ActiveSync associé au domaine sélectionné. Double-cliquez sur une entrée pour afficher plus de détails sur le client. Cliquez avec le bouton droit de la souris sur une entrée pour ouvrir le menu contextuel, à partir duquel vous pouvez personnaliser ses paramètres client, afficher des statistiques et exécuter diverses autres fonctions.

ActiveSync Client)
Email Address	frank.thomas@company.test	^
Domain	company.test	
Client Type	iPad	
Client ID	14A65AD03AA182FADF712A69	
User Agent	UA_iPad/9.6.9.8	
Client Model	iPad 4.22	
IMEI	528514162102	
Friendly Name	Frank's iPad	
Operating System	Fizzbin Mobile Systems 20.0	
Operating System Language	en-us	
Phone Number	8175559876	
Mobile Operator	Example Wireless Ltd.	
IP Address	192.168.0.100	
Last GMT Logon Time	2023-01-03T16:43:28.000Z (2023-01-03 10:43:28)	
Protocol Version	16.1	
Effective Policy	<no policy="" set=""></no>	
Device Wipe Requested	No	
Account Only Wipe Requested	No	
Authorization Time Stamp	2022-06-10T19:13:58.420Z (2022-06-10 14:13:58)	
Authorization made by	MDAirSync	
192.168.0.100	2023-01-03T16:00:00.000Z (2023-01-03 10:00:00)	~

Détails du client ActiveSync

Double-cliquez sur une entrée, ou cliquez avec le bouton droit de la souris sur l'entrée et cliquez sur **Voir les détails du client**, pour ouvrir la boîte de dialogue Détails du client. Cet écran filtre les informations relatives au client, telles que son Type de client, son ID client, l'heure de sa dernière connexion, etc.

Paramètres clients

Cliquez avec le bouton droit de la souris sur un client et cliquez sur **Personnaliser les paramètres du client** pour gérer ses Paramètres clients. Par défaut, ces paramètres sont hérités des paramètres du Type de client, mais ils peuvent être ajustés comme vous le souhaitez. Voir <u>Gérer les paramètres des clients d'un appareilGérer les</u>

Attribuer une Politique ActiveSync attribuée

Pour Attribuer une <u>Politique</u> 470 du terminal : Cliquez avec le bouton droit de la souris sur le terminal dans la liste:

- 1. Cliquez avec le bouton droit de la souris sur un périphérique dans la liste.
- 2. Cliquez sur **Appliquer politique**. La boîte de dialogue Appliquer une politique s'ouvre.
- 3. Cliquez sur la liste déroulante**Politique à appliquer** et choisissez la politique souhaitée.
- 4. Cliquez sur OK.

Statistiques de

Cliquez avec le bouton droit de la souris sur une entrée, puis cliquez sur **Afficher les statistiques** pour ouvrir la boîte de dialogue Statistiques du client, qui contient diverses statistiques d'utilisation pour le client.

Réinitialiser les statistiques

Si vous souhaitez réinitialiser les statistiques d'un client, cliquez avec le bouton droit de la souris sur le client, cliquez sur **Réinitialiser les statistiques**, puis sur **OK** pour confirmer l'action.

Suppression d'un client ActiveSync

Pour supprimer un client ActiveSync, cliquez avec le bouton droit de la souris sur le client et cliquez sur **Supprimer**, puis sur **Oui**. Cela supprimera le client de la liste et toutes les informations de synchronisation le concernant dans MDaemon. Dans ce cas, si à l'avenir le compte utilise ActiveSync pour synchroniser le même client, MDaemon traitera le client comme s'il n'avait jamais été utilisé sur le serveur ; toutes les données du client devront être resynchronisées avec MDaemon.

Effacer complètement un client ActiveSync

Lorsqu'une politique 470 a été appliquée à un client ActiveSync sélectionné, et que le client l'a appliquée et a répondu, il y aura une option d'Effacement complètement disponible pour ce client. Si c'est le cas, cliquez avec le bouton droit de la souris sur le client (ou sélectionnez-le si vous utilisez MDRA) et cliquez sur **Effacer complètement**. Lors de la prochaine connexion du client, MDaemon lui demandera d'effacer toutes les données ou de restaurer les paramètres par défaut. Selon le client, cela peut supprimer tout ce qu'il contient, y compris les applications téléchargées. En outre, tant que l'entrée ActiveSync du client existe, MDaemon continuera d'envoyer la demande d'effacement chaque fois que ce périphérique se connectera à l'avenir. Si, à un moment donné, vous souhaitez supprimer le client, assurez-vous de l'ajouter d'abord à la liste de blocage 454, afin qu'il ne puisse plus se connecter à l'avenir. Enfin, si un terminal effacé est récupéré et que vous souhaitez l'autoriser à se connecter à nouveau, vous devez le sélectionner et cliquer sur **Annuler les actions "Effacer"**. Vous devez également le supprimer de la Liste de blocage.

Effacement du compte d'un client ActiveSync

Pour effacer les données de messagerie et de PIM du compte du client ou de l'appareil, cliquez avec le bouton droit de la souris et cliquez sur **Account Wipe Account Mail and PIM from client (Effacer le courrier et le PIM du client)**. L' option *Effacer le compte* est similaire à l' option*Effacer complètement* expliquée ci-dessus, mais au lieu d'effacer toutes les données, elle effacera uniquement les données du compte, telles que ses e-mails, entrées de calendrier, contacts et autres. Le reste, comme les applications, les photos ou la musique, est laissé en l'état.

Autoriser le client

Si l'option "Les nouveaux clients nécessitent une autorisation administrative" de l' écran <u>Paramètres du client ActiveSync</u> [447] est réglée sur l'autorisation, sélectionnez un client et cliquez sur Approuver le client pour la synchronisation, pour l'autoriser à se synchroniser avec le serveur.

Gérer les paramètres clients d'un terminal

L'écran Paramètres clients au niveau de l'appareil vous autorise à gérer les paramètres d'un appareil spécifique.

Troubleshooting Log level Use inherited or default Archive transactions as XML WBXML Validate/correct PIM mrk file integrity Client Options Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation	
Troubleshooting Log level Use inherited or default Archive transactions as XML WBXML Validate/correct PIM mrk file integrity Client Options Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation	
Log level Use inherited or default Archive transactions as XML WBXML Validate/correct PIM mrk file integrity Client Options Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation	
Archive transactions as XML WBXML Validate/correct PIM mrk file integrity Client Options Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation	
Validate/correct PIM mrk file integrity Client Options Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation	
Client Options Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation	
Client Options Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation	
 Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation 	
Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation	
Bandwidth reset Day Use inherited or default	
Security	
Exempt from Location Screen	
Dynamically allow remote address	
Allow clients provisioned/managed by other servers	
Disallow Eactory Reset Wipes	

Non (par défaut), toutes les options de cet écran sont définies sur "Utiliser les paramètres hérités ou par défaut", ce qui signifie que chaque option est paramétrée à partir de l'option correspondante de l' écran<u>Paramètres clients de Types clients</u>. Toute modification apportée aux paramètres de cet écran sera répercutée sur cet écran. Inversement, toute modification apportée à cet écran remplacera le paramètre du type de clients pour ce terminal.

Général

Résolution des problèmes

Niveau de journalisation

ActiveSync for MDaemon prend en charge six niveaux de journalisation, du plus élevé au plus faible :

DébogaIl s'agit du niveau de journalisation le plus complet. Il consignegetoutes les entrées disponibles et n'est généralement utilisé que

pour diagnostiquer un problème.

- **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.
- **Avertis** Les avertissements, les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont consignés dans le journal.
- **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- **Critiqu** Les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.
- **Hériter** Non (par défaut), le niveau journalisation est hérité de la hiérarchie des Paramètres clients. Ainsi, les clients héritent leurs paramètres des Types de clients, les Types de clients des Comptes, les Comptes des Groupes, etc. Le Paramètres globaux du client pour cette option est déterminé par le paramètre de niveau de journalisation dans le dialogue<u>Diagnostics</u>[457].

Archiver les transactions en [XML | WBXML]

Utilisez les options d'archivage*XML...* et *WBXML* si vous souhaitez enregistrer ces données, qui peuvent parfois être utiles à des fins de débogage. Les options globales sont désactivées par défaut.

Valider/corriger l'intégrité du fichier mrk PIM

Cette option exécute un processus de validation et de correction des données PIM du client afin de rechercher les problèmes connus susceptibles d'empêcher une synchronisation correcte, tels que des UID iCal en double ou des champs facultatifs vides. L'option globale est désactivée par défaut.

Options client

Appliquer les restrictions de protocole

Activez cette option si vous souhaitez refuser les connexions de tout client qui tente d'utiliser un protocole autre que les *Versions du protocole autorisées* spécifiées pour le client. Non (par défaut), cette option est désactivée, ce qui signifie que les restrictions de protocole n'empêchent pas un client d'utiliser un protocole différent ; elles indiquent simplement au client quels protocoles utiliser. Si un client tente malgré tout d'utiliser un protocole restreint, MDaemon autorisera quand même la connexion. Pour plus d'informations, voir <u>Restrictions de protocole</u> [459] pour plus d'informations.

Répondre à 'Get/UserInformation' en utilisant l'alias de l'identifiant comme 'adresse SMTP principale'

Dans ce cas, le service peut renvoyer un Alias/une adresse secondaire en tant

qu'adresse primaire en réponse à une requête de type Configurer/Gérer/Informations sur l'utilisateur. Cela permet de contourner un problème causé par une mise à jour postérieure à iOS9.x qui faisait que les clients ne pouvaient pas envoyer de courrier à l'aide d'un alias. L'utilisation de cette option résulte en une réponse non conforme aux spécifications à Settings/Get/UserInformation.

Les nouveaux clients doivent recevoir l'autorisation de l'administrateuravant de synchroniser.

Activez cette option si vous souhaitez que les nouveaux clients soient autorisés par un administrateur avant de pouvoir commencer à se synchroniser avec un compte. La liste <u>Clients</u> indique tous les clients en attente d'autorisation, et l'administrateur peut les autoriser à partir du même écran. Ce paramètre est Non (par défaut).

Max. clients par utilisateur

Si vous souhaitez limiter le nombre de clients ActiveSync ou de terminaux qui peuvent être associés à un compte MDaemon, indiquez le nombre souhaité dans cette option. L'option globale est réglée sur "illimité" par défaut. Cette option est disponible sur les écrans Paramètres clients globaux, de domaine et de compte, et non sur les écrans Clients individuels.

Jour de réinitialisation de la bande passante

Utilisez cette option si vous souhaitez réinitialiser les statistiques d'utilisation de la bande passante pour les Terminaux ActiveSync un jour précis de chaque mois. L'événement de réinitialisation a lieu dans le cadre du processus de maintenance nocturne normal et est consigné dans le journal du système comme les autres routines de maintenance. L'option globale est réglée sur "0 (Jamais)" par défaut, ce qui signifie que les statistiques d'utilisation ne seront jamais réinitialisées. Paramétrez les options enfant sur un jour différent si, par exemple, vous souhaitez que le jour de réinitialisation coïncide avec la date de réinitialisation de la facturation de l'opérateur sans fil d'un utilisateur ou d'un client.

Sécurité

Exclure du Filtrage de pays

Activez cette option dans l'écran des paramètres d'un client ActiveSync si vous souhaitez que l'appareil puisse filtrer l' <u>écran de localisation</u> [609]. Cela permet à un utilisateur valide de continuer à accéder à son compte via ActiveSync lorsque, par exemple, il se rend à un endroit où les tentatives d'authentification sont bloquées. Pour que l'appareil soit exempté, il doit s'être connecté et authentifié via ActiveSync dans le délai configuré dans le paramètre<u>Supprimer les clients inactifs</u> <u>après ce nombre de jours</u> [443] situé dans l'écran Régètres.

Autoriser dynamiquement l'adresse distante

Si vous excluez un pays du Filtrage de l'emplacement, activez cette option si vous souhaitez également autoriser l'adresse IP distante à partir de laquelle il se connecte. Cela peut s'avérer utile pour autoriser d'autres clients susceptibles de se connecter à partir de la même adresse IP.

Autoriser les clients gérés par d'autres serveurs

Par défaut, lorsque le serveur ActiveSync envoie des données de

provisionnement/des spécificités de politiques à un client et que celui-ci signale qu'il est également géré par un autre serveur ActiveSync, le client sera toujours autorisé à se connecter à MDaemon. Dans ce cas, il n'y a aucun moyen de s'assurer que les spécificités de votre politique seront appliquées lorsqu'elles entrent en conflit avec la politique de l'autre serveur ActiveSync. En général, les clients utilisent par défaut l'option la plus restrictive en cas de conflit. Désactivez cette option si vous ne souhaitez pas autoriser ces clients à se connecter.

Interdire les réinitialisations aux paramètres d'usine

Si cette option est activée (On/Oui), il ne sera pas possible d'**effacer complètement** un client ActiveSync. Si vous souhaitez pouvoir effectuer un Effacer complètement à distance sur un client, vous devez d'abord désactiver cette option. L'option est désactivée par défaut. Pour plus d'informations, voir : <u>Effacer</u> <u>complètement un client ActiveSync</u> will sur la page Clients.

Options FolderSync

Options de dossier

Exclure

Dossier Expéditeurs bloqués autorisés/ bloqués

Par défaut, les dossiers Expéditeurs autorisés et Dossiers Expéditeurs bloqués de l'utilisateur ne sont pas synchronisés avec les périphériques. Ils ne sont généralement utilisés par MDaemon que dans le cadre de la prévention automatique du spam. C'est pourquoi ils n'ont pas besoin d'être affichés sur les appareils en tant que contacts.

Dossiers de courrier personnalisés (Non par défaut)

Par défaut, tous les Dossiers de courrier créés par l'utilisateur et par défaut peuvent être synchronisés avec le terminal. Activez cette option si vous souhaitez que seuls les dossiers courrier par défaut soient synchronisés, c'està-dire la Boîte de réception, les Éléments envoyés, les Éléments supprimés, les Brouillons, etc. Aucun dossier créé par l'utilisateur ne sera inclus. Cette option est désactivée par défaut.

Dossiers PIM personnalisés non (par défaut)

Par défaut, tous les dossiers PIM de l'utilisateur (contacts, calendrier, notes, tâches, etc.) sont synchronisés avec l'appareil. Activez cette option si vous souhaitez que seuls les dossiers PIM par défaut soient synchronisés. Exemple : si cette option est activée et qu'un utilisateur possède plusieurs dossiers de calendrier, seul le calendrier par défaut sera synchronisé. Cette option est désactivée par défaut.

Inclure

Arborescence Dossiers publics

Cochez cette case si vous souhaitez que les <u>Dossiers publics</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers publics</u> auxquels il a accès. Cette option est autorisée par défaut.

Navigation dans les dossiers publics (affiche les noms de dossiers)

Non par défaut, pour qu'un client puisse synchroniser un sous-dossier public ou y accéder, le compte doit disposer de l'<u>autorisation de Recherche</u> [327] pour le sous-dossier (c'est-à-dire le dossier enfant) et tous les <u>Dossiers publics</u> [325] parents situés au-dessus. Si le compte n'a pas l'autorisation de voir les dossiers parents, il ne peut pas non plus voir le dossier enfant, même s'il en a l'autorisation. Activez cette option si vous souhaitez autoriser le client à accéder à ces dossiers enfants. **Par nom : l** 'activation de cette option doit nécessairement révéler les noms des dossiers parents au client, ce qui pourrait être considéré comme un risque de sécurité. Cette option est désactivée par défaut.

Nombre max de Dossiers publics

Utilisez cette option si vous souhaitez limiter le nombre de Dossiers publics autorisés sur le périphérique. Lorsqu'une limite est définie, le serveur parcourt la liste des dossiers jusqu'à ce que la limite soit atteinte, puis plus aucun dossier n'est envoyé à l'appareil. Il n'existe aucun moyen de garantir l'ordre dans lequel les dossiers seront traités. Non (paramètres par défaut).

Dossiers IMAP partagés

Cochez cette case si vous souhaitez que les <u>dossiers partagés</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers partagés</u> auxquels il a accès. Cette option est autorisée par défaut.

Gestion du contenu

Options de gestion des e-mails

Créer des tâches/rappels pour les e-mails avec indicateurs

Cette option permet à MDaemon de rappeler à l'utilisateur les éléments marqués, en créant un élément de tâche pour chaque courrier électronique marqué. lorsque le client le demande. L'option globale de ce contrôle est activée par défaut.

Toujours envoyer les mises à jour de réunion lorsque l'événement est modifié

Certains clients n'envoient pas correctement les e-mails de mise à jour des réunions lorsqu'ils modifient une réunion. Cette option indique au service ActiveSync d'envoyer une mise à jour de la réunion lorsqu'un élément de la réunion est mis à jour par l'organisateur. Cette option ne doit être définie que pour les <u>clients</u> and et les <u>types de clients</u> out qui n'envoient pas correctement les mises à jour de réunion, sous peine d'envoyer des mises à jour de réunion en double. Par conséquent, cette option n'est disponible que dans les pages de paramètres pour les Clients et les Types de clients.

Demander des confirmations de lecture pour tous les e-mails envoyés

Activez cette option si vous souhaitez que le serveur demande des confirmations de lecture pour tous les courriers envoyés par un client. Cette option est désactivée par défaut.

Envoyer des confirmations de lecture du serveur lorsque le courrier est marqué comme lu et lorsque l'expéditeur le demande.

Activez cette option si vous souhaitez que le serveur prenne en charge les demandes de confirmation de lecture et délivre un accusé de réception de lecture lorsqu'un message est marqué comme lu par un client. Cette option est désactivée par défaut.

Envoyer avec l'alias spécifié dans ReplyTo

Certains clients peuvent ne pas autoriser un expéditeur à envoyer du courrier à l'aide d'un alias. Cette fonctionnalité a été ajoutée au <u>protocole Exchange</u> <u>ActiveSync (EAS)</u> [459] 16.x, mais certains clients ne supportent pas la version 16.x. Par exemple, Outlook pour Windows n'utilise que EAS 14.0, et bien qu'il permette à un utilisateur de spécifier une autre adresse pour l'envoi, le message généré ne reflète pas correctement les choix de l'utilisateur. Cette faculté permet d'utiliser le champ ReplyTo pour envoyer l'e-mail, à condition que l'adresse ReplyTo soit un <u>alias</u> <u>valide</u> [84] pour cet utilisateur. L'option globale est activée par défaut.

Fusionner virtuellement les contacts publics et les contacts par défaut

Activez cette option si vous souhaitez fusionner les contacts publics avec les contacts par défaut de l'utilisateur sur le terminal. Il s'agit uniquement d'une fusion virtuelle, c'est-à-dire qu'ils ne sont pas réellement copiés dans le dossier des contacts de l'utilisateur. Cela peut être utile sur les clients qui ne prennent pas en charge les recherches dans la liste d'adresses globale (GAL). Non (par défaut).

Dossiers Expéditeurs bloqués lors du déplacement d'un courrier dans le dossier Courriers indésirables

Si cette option est activée, lorsqu'un client déplace un e-mail vers le dossier Courriers indésirables du compte, le service ajoute l'adresse SENDER\$ - adresse de l'expéditeur de cet e-mail au dossier Contacts des expéditeurs bloqués.

Forcer l'envoi des réponses aux réunions lorsqu'une demande de réunion est acceptée/déclinée, etc.

Dans cette option, lorsqu'un client accepte, refuse ou choisit une action en réponse à une demande de réunion, le service envoie une réponse à l'organisateur de la réunion. Cette fonction est destinée aux clients spécifiques qui n'envoient pas correctement ces mises à jour eux-mêmes.

Aperçu des paramètres effectifs

Ce bouton est disponible sur tous les écrans des Paramètres clients enfant (c.-à-d. <u>domaines</u> 42, <u>comptes</u> 47) et <u>clients</u> 48). Non (par défaut), les options de ces écrans sont définies pour hériter de leurs paramètres d'un écran parent. Utilisez cette fonction pour voir quels paramètres sont actuellement appliqués à l'écran affiché.

Voir :

ActiveSync | Paramètres du client 447 ActiveSync | Domaines 462 ActiveSync | Comptes 479

3.10.10 Groupes

System	Tuning	Security	Diagnostics	Protocol Restriction	ns Domains
Policy	Manager	Accounts	Clients	Groups	Client Types
Group	Settings define	d			
Dept A	No				
Dept B	Yes				

Si vous souhaitez définir des Paramètres client ActiveSync personnalisés pour un <u>groupe de</u> comptes, utilisez cet écran pour gérer ces paramètres. Tous les groupes sont répertoriés ici, et l'entrée de chaque groupe indique si des paramètres personnalisés ont été définis pour lui. Pour modifier les Paramètres clients d'un groupe, double-cliquez sur le groupe ou cliquez avec le bouton droit de la souris sur le groupe et cliquez sur **Personnaliser les paramètres clients**.

Paramètres clients d'un groupe

Client Settings: Security Group: Dept A	×
General FolderSync Options Content Handling	
Troubleshooting Log level Use inherited or default \checkmark	
Archive transactions as 🔳 XML 🔳 WBXML Validate/correct PIM mrk file integrity	
Client Options Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation	
New clients require administrative approval	
Max dients per user Use inherited or default \sim	
Bandwidth reset Day Use inherited or default \sim	
Security Exempt from Location Screen Dynamically allow remote address Allow clients provisioned/managed by other servers Disallow Factory Reset Wipes	
OK Cancel Help	te

Par défaut, chaque paramètre client d'un groupe est défini de manière à hériter de l'état des Paramètres clients du Domaine - Domaine de l'utilisateur . 2261 La modification d'un paramètre de groupe remplacera le paramètre de domaine pour tout compte membre du groupe. Si vous ne souhaitez pas que les Paramètres client du groupe s'appliquent à un membre du groupe ou à un périphérique spécifique, vous pouvez alors remplacer les paramètres du groupe en modifiant les Paramètres client pour le <u>Compte 479</u>, le <u>Type de client</u> 5041 ou le <u>Client</u> 4881.

Général

Résolution des problèmes

Niveau de journalisation

ActiveSync for MDaemon prend en charge six niveaux de journalisation, du plus élevé au plus faible :

- Déboga Il s'agit du niveau de journalisation le plus complet. Il consigne toutes les entrées disponibles et n'est généralement utilisé que pour diagnostiquer un problème.
 - **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.
- **Avertis** Les avertissements, les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont consignés dans le journal.
- **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Critiqu Les erreurs critiques et les événements de démarrage/arrêt sont e journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.
- **Hériter** Non (par défaut), le niveau journalisation est hérité de la hiérarchie des Paramètres clients. Ainsi, les clients héritent leurs paramètres des Types de clients, les Types de clients des Comptes, les Comptes des Groupes, etc. Le Paramètres globaux du client pour cette option est déterminé par le paramètre de niveau de journalisation dans le dialogue<u>Diagnostics</u> [457].

Archiver les transactions en [XML | WBXML]

Utilisez les options d'archivage*XML...* et *WBXML* si vous souhaitez enregistrer ces données, qui peuvent parfois être utiles à des fins de débogage. Les options globales sont désactivées par défaut.

Valider/corriger l'intégrité du fichier mrk PIM

Cette option exécute un processus de validation et de correction des données PIM du client afin de rechercher les problèmes connus susceptibles d'empêcher une synchronisation correcte, tels que des UID iCal en double ou des champs facultatifs vides. L'option globale est désactivée par défaut.

Options client

Appliquer les restrictions de protocole

Activez cette option si vous souhaitez refuser les connexions de tout client qui tente d'utiliser un protocole autre que les *Versions du protocole autorisées* spécifiées pour le client. Non (par défaut), cette option est désactivée, ce qui signifie que les restrictions de protocole n'empêchent pas un client d'utiliser un protocole différent ; elles indiquent simplement au client quels protocoles utiliser. Si un client tente malgré tout d'utiliser un protocole restreint, MDaemon autorisera quand même la connexion. Pour plus d'informations, voir <u>Restrictions de protocole</u> pour plus d'informations.

Répondre à 'Get/UserInformation' en utilisant l'alias de l'identifiant comme 'adresse SMTP principale'

Dans ce cas, le service peut renvoyer un Alias/une adresse secondaire en tant qu'adresse primaire en réponse à une requête de type Configurer/Gérer/Informations sur l'utilisateur. Cela permet de contourner un problème causé par une mise à jour postérieure à iOS9.x qui faisait que les clients ne pouvaient pas envoyer de courrier à l'aide d'un alias. L'utilisation de cette option résulte en une réponse non conforme aux spécifications à Settings/Get/UserInformation.

Les nouveaux clients doivent recevoir l'autorisation de l'administrateuravant de synchroniser.

Activez cette option si vous souhaitez que les nouveaux clients soient autorisés par un administrateur avant de pouvoir commencer à se synchroniser avec un compte. La liste <u>Clients</u> indique tous les clients en attente d'autorisation, et l'administrateur peut les autoriser à partir du même écran. Ce paramètre est Non (par défaut).

Max. clients par utilisateur

Si vous souhaitez limiter le nombre de clients ActiveSync ou de terminaux qui peuvent être associés à un compte MDaemon, indiquez le nombre souhaité dans cette option. L'option globale est réglée sur "illimité" par défaut. Cette option est disponible sur les écrans Paramètres clients globaux, de domaine et de compte, et non sur les écrans Clients individuels.

Jour de réinitialisation de la bande passante

Utilisez cette option si vous souhaitez réinitialiser les statistiques d'utilisation de la bande passante pour les Terminaux ActiveSync un jour précis de chaque mois. L'événement de réinitialisation a lieu dans le cadre du processus de maintenance nocturne normal et est consigné dans le journal du système comme les autres routines de maintenance. L'option globale est réglée sur "0 (Jamais)" par défaut, ce qui signifie que les statistiques d'utilisation ne seront jamais réinitialisées. Paramétrez les options enfant sur un jour différent si, par exemple, vous souhaitez que le jour de réinitialisation coïncide avec la date de réinitialisation de la facturation de l'opérateur sans fil d'un utilisateur ou d'un client.

Sécurité

Exclure du Filtrage de pays

Activez cette option dans l'écran des paramètres d'un client ActiveSync si vous souhaitez que l'appareil puisse filtrer l' <u>écran de localisation</u> . Cela permet à un utilisateur valide de continuer à accéder à son compte via ActiveSync lorsque, par exemple, il se rend à un endroit où les tentatives d'authentification sont bloquées. Pour que l'appareil soit exempté, il doit s'être connecté et authentifié via ActiveSync dans le délai configuré dans le paramètre<u>Supprimer les clients inactifs après ce</u> <u>nombre de jours</u> [443] situé dans l'écran Régètres.

Autoriser dynamiquement l'adresse distante

Si vous excluez un pays du Filtrage de l'emplacement, activez cette option si vous souhaitez également autoriser l'adresse IP distante à partir de laquelle il se connecte. Cela peut s'avérer utile pour autoriser d'autres clients susceptibles de se connecter à partir de la même adresse IP.

Autoriser les clients gérés par d'autres serveurs

Par défaut, lorsque le serveur ActiveSync envoie des données de provisionnement/des spécificités de politiques à un client et que celui-ci signale qu'il est également géré par un autre serveur ActiveSync, le client sera toujours autorisé à se connecter à MDaemon. Dans ce cas, il n'y a aucun moyen de s'assurer que les spécificités de votre politique seront appliquées lorsqu'elles entrent en conflit avec la politique de l'autre serveur ActiveSync. En général, les clients utilisent par défaut l'option la plus restrictive en cas de conflit. Désactivez cette option si vous ne souhaitez pas autoriser ces clients à se connecter.

Interdire les réinitialisations aux paramètres d'usine

Si cette option est activée (On/Oui), il ne sera pas possible d'**effacer complètement** un client ActiveSync. Si vous souhaitez pouvoir effectuer un Effacer complètement à distance sur un client, vous devez d'abord désactiver cette option. L'option est désactivée par défaut. Pour plus d'informations, voir : <u>Effacer</u> <u>complètement un client ActiveSync</u> with a page Clients.

Options FolderSync

Options de dossier

Exclure

Dossier Expéditeurs bloqués autorisés/ bloqués

Par défaut, les dossiers Expéditeurs autorisés et Dossiers Expéditeurs bloqués de l'utilisateur ne sont pas synchronisés avec les périphériques. Ils ne sont généralement utilisés par MDaemon que dans le cadre de la prévention automatique du spam. C'est pourquoi ils n'ont pas besoin d'être affichés sur les appareils en tant que contacts.

Dossiers de courrier personnalisés (Non par défaut)

Par défaut, tous les Dossiers de courrier créés par l'utilisateur et par défaut peuvent être synchronisés avec le terminal. Activez cette option si vous souhaitez que seuls les dossiers courrier par défaut soient synchronisés, c'est-àdire la Boîte de réception, les Éléments envoyés, les Éléments supprimés, les Brouillons, etc. Aucun dossier créé par l'utilisateur ne sera inclus. Cette option est désactivée par défaut.

Dossiers PIM personnalisés non (par défaut)

Par défaut, tous les dossiers PIM de l'utilisateur (contacts, calendrier, notes, tâches, etc.) sont synchronisés avec l'appareil. Activez cette option si vous souhaitez que seuls les dossiers PIM par défaut soient synchronisés. Exemple : si cette option est activée et qu'un utilisateur possède plusieurs dossiers de calendrier, seul le calendrier par défaut sera synchronisé. Cette option est désactivée par défaut.

Inclure

Arborescence Dossiers publics

Cochez cette case si vous souhaitez que les **Dossiers publics** auxquels un

utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers publics</u> auxquels il a accès. Cette option est autorisée par défaut.

Navigation dans les dossiers publics (affiche les noms de dossiers)

Non par défaut, pour qu'un client puisse synchroniser un sous-dossier public ou y accéder, le compte doit disposer de l'<u>autorisation de Recherche</u> [327] pour le sousdossier (c'est-à-dire le dossier enfant) et tous les <u>Dossiers publics</u> [325] parents situés au-dessus. Si le compte n'a pas l'autorisation de voir les dossiers parents, il ne peut pas non plus voir le dossier enfant, même s'il en a l'autorisation. Activez cette option si vous souhaitez autoriser le client à accéder à ces dossiers enfants. **Par nom : l** 'activation de cette option doit nécessairement révéler les noms des dossiers parents au client, ce qui pourrait être considéré comme un risque de sécurité. Cette option est désactivée par défaut.

Nombre max de Dossiers publics

Utilisez cette option si vous souhaitez limiter le nombre de Dossiers publics autorisés sur le périphérique. Lorsqu'une limite est définie, le serveur parcourt la liste des dossiers jusqu'à ce que la limite soit atteinte, puis plus aucun dossier n'est envoyé à l'appareil. Il n'existe aucun moyen de garantir l'ordre dans lequel les dossiers seront traités. Non (paramètres par défaut).

Dossiers IMAP partagés

Cochez cette case si vous souhaitez que les <u>dossiers partagés</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers partagés</u> auxquels il a accès. Cette option est autorisée par défaut.

Gestion du contenu

Options de gestion des e-mails

Créer des tâches/rappels pour les e-mails avec indicateurs

Cette option permet à MDaemon de rappeler à l'utilisateur les éléments marqués, en créant un élément de tâche pour chaque courrier électronique marqué. lorsque le client le demande. L'option globale de ce contrôle est activée par défaut.

Toujours envoyer les mises à jour de réunion lorsque l'événement est modifié

Certains clients n'envoient pas correctement les e-mails de mise à jour des réunions lorsqu'ils modifient une réunion. Cette option indique au service ActiveSync d'envoyer une mise à jour de la réunion lorsqu'un élément de la réunion est mis à jour par l'organisateur. Cette option ne doit être définie que pour les <u>clients</u> as et les <u>types de clients</u> ou n'envoient pas correctement les mises à jour de réunion, sous peine d'envoyer des mises à jour de réunion en double. Par conséquent, cette option n'est disponible que dans les pages de paramètres pour les Clients et les Types de clients.

Demander des confirmations de lecture pour tous les e-mails envoyés

Activez cette option si vous souhaitez que le serveur demande des confirmations de lecture pour tous les courriers envoyés par un client. Cette option est désactivée par défaut.

Envoyer des confirmations de lecture du serveur lorsque le courrier est marqué comme lu et lorsque l'expéditeur le demande.

Activez cette option si vous souhaitez que le serveur prenne en charge les demandes de confirmation de lecture et délivre un accusé de réception de lecture lorsqu'un message est marqué comme lu par un client. Cette option est désactivée par défaut.

Envoyer avec l'alias spécifié dans ReplyTo

Certains clients peuvent ne pas autoriser un expéditeur à envoyer du courrier à l'aide d'un alias. Cette fonctionnalité a été ajoutée au <u>protocole Exchange ActiveSync</u> (EAS) (453) 16.x, mais certains clients ne supportent pas la version 16.x. Par exemple, Outlook pour Windows n'utilise que EAS 14.0, et bien qu'il permette à un utilisateur de spécifier une autre adresse pour l'envoi, le message généré ne reflète pas correctement les choix de l'utilisateur. Cette faculté permet d'utiliser le champ ReplyTo pour envoyer l'e-mail, à condition que l'adresse ReplyTo soit un <u>alias</u> valide (1994) pour cet utilisateur. L'option globale est activée par défaut.

Fusionner virtuellement les contacts publics et les contacts par défaut

Activez cette option si vous souhaitez fusionner les contacts publics avec les contacts par défaut de l'utilisateur sur le terminal. Il s'agit uniquement d'une fusion virtuelle, c'est-à-dire qu'ils ne sont pas réellement copiés dans le dossier des contacts de l'utilisateur. Cela peut être utile sur les clients qui ne prennent pas en charge les recherches dans la liste d'adresses globale (GAL). Non (par défaut).

Dossiers Expéditeurs bloqués lors du déplacement d'un courrier dans le dossier Courriers indésirables

Si cette option est activée, lorsqu'un client déplace un e-mail vers le dossier Courriers indésirables du compte, le service ajoute l'adresse SENDER\$ - adresse de l'expéditeur de cet e-mail au dossier Contacts des expéditeurs bloqués.

Forcer l'envoi des réponses aux réunions lorsqu'une demande de réunion est acceptée/déclinée, etc.

Dans cette option, lorsqu'un client accepte, refuse ou choisit une action en réponse à une demande de réunion, le service envoie une réponse à l'organisateur de la réunion. Cette fonction est destinée aux clients spécifiques qui n'envoient pas correctement ces mises à jour eux-mêmes.

Aperçu des paramètres effectifs

Ce bouton est disponible sur tous les écrans des Paramètres clients enfant (c.-à-d. <u>domaines</u> هوالله (<u>comptes</u> عليه) et <u>clients</u> معاليه). Non (par défaut), les options de ces écrans sont définies pour hériter de leurs paramètres d'un écran parent. Utilisez cette fonction pour voir quels paramètres sont actuellement appliqués à l'écran affiché.

Voir :

ActiveSync | DomainesActiveSync | ComptesActiveSync | Clients479ActiveSync | Clients488

3.10.11 Types de clients

System Tunir	g Security	Diagnostics	Protocol Restriction	s Domains
Policy Manager	Accounts	Clients	Groups	Client Types
Client Type	Settings defined	State		
Collector_1.0	Yes	<normal></normal>		
iPad	No	<normal></normal>		
SAMSUNGSGHI747	No	<normal></normal>		
WindowsOutlook15	No	<policyexempt></policyexempt>		

Si vous souhaitez définir des Paramètres du client ActiveSync personnalisés pour un type de client ActiveSync spécifique, utilisez cet écran pour gérer ces paramètres. Les Types de clients de tous les <u>clients actuellement autorisés à</u> abilitiser ActiveSync sont listés ici, et l'entrée de chaque Type de client indique si ses paramètres ont été définis ou non. Pour modifier les Paramètres clients d'un Type de client, double-cliquez sur l'entrée, ou cliquez dessus avec le bouton droit de la souris et cliquer avec le bouton droit de la souris et cliquer avec le bouton droit de la souris sur une entrée pour supprimer les paramètres personnalisés ou pour ajouter ou supprimer le Type client de la liste ActiveSync Liste d'autorisation ou Liste <u>d'Exceptions</u> 454.
Client Settings: Client Type: iPad X
General FolderSync Options Content Handling
Troubleshooting Log level Use inherited or default Archive transactions as XML WBXML Validate/correct PIM mrk file integrity
Client Options Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation New clients require administrative approval Bandwidth reset Day Use inherited or default
Security Exempt from Location Screen Dynamically allow remote address Allow clients provisioned/managed by other servers Disallow Factory Reset Wipes
OK Cancel Help Image: Construction of the second s

Types de clients Paramètres clients

Par défaut, chaque paramètre client Client Type est défini pour hériter de l'état des <u>Paramètres clients du compte</u> [820]. La modification d'un paramètre Client-Type remplacera le paramètre du compte pour tout compte utilisant un client de ce Type. Si vous ne souhaitez pas que les Paramètres Client-Type s'appliquent à un client spécifique, vous pouvez remplacer les <u>Paramètres Client</u> [488]-Type en modifiant les <u>Paramètres Client de</u> [488] ce <u>client</u>. [488]

Général

Résolution des problèmes

Niveau de journalisation

ActiveSync for MDaemon prend en charge six niveaux de journalisation, du plus élevé au plus faible :

Déboga Il s'agit du niveau de journalisation le plus complet. Il consigne

- **ge** toutes les entrées disponibles et n'est généralement utilisé que pour diagnostiquer un problème.
- **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.
- **Avertis** Les avertissements, les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont consignés dans le journal.
- **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Critiqu Les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.
- **Hériter** Non (par défaut), le niveau journalisation est hérité de la hiérarchie des Paramètres clients. Ainsi, les clients héritent leurs paramètres des Types de clients, les Types de clients des Comptes, les Comptes des Groupes, etc. Le Paramètres globaux du client pour cette option est déterminé par le paramètre de niveau de journalisation dans le dialogue<u>Diagnostics</u> [457].

Archiver les transactions en [XML | WBXML]

Utilisez les options d'archivage*XML...* et *WBXML* si vous souhaitez enregistrer ces données, qui peuvent parfois être utiles à des fins de débogage. Les options globales sont désactivées par défaut.

Valider/corriger l'intégrité du fichier mrk PIM

Cette option exécute un processus de validation et de correction des données PIM du client afin de rechercher les problèmes connus susceptibles d'empêcher une synchronisation correcte, tels que des UID iCal en double ou des champs facultatifs vides. L'option globale est désactivée par défaut.

Options client

Appliquer les restrictions de protocole

Activez cette option si vous souhaitez refuser les connexions de tout client qui tente d'utiliser un protocole autre que les *Versions du protocole autorisées* spécifiées pour le client. Non (par défaut), cette option est désactivée, ce qui signifie que les restrictions de protocole n'empêchent pas un client d'utiliser un protocole différent ; elles indiquent simplement au client quels protocoles utiliser. Si un client tente malgré tout d'utiliser un protocole restreint, MDaemon autorisera quand même la connexion. Pour plus d'informations, voir <u>Restrictions de protocole</u> [459] pour plus d'informations.

Répondre à 'Get/UserInformation' en utilisant l'alias de l'identifiant comme 'adresse SMTP principale'

Dans ce cas, le service peut renvoyer un Alias/une adresse secondaire en tant qu'adresse primaire en réponse à une requête de type Configurer/Gérer/Informations sur l'utilisateur. Cela permet de contourner un problème causé par une mise à jour postérieure à iOS9.x qui faisait que les clients ne pouvaient pas envoyer de courrier à l'aide d'un alias. L'utilisation de cette option résulte en une réponse non conforme aux spécifications à Settings/Get/UserInformation.

Les nouveaux clients doivent recevoir l'autorisation de l'administrateuravant de synchroniser.

Activez cette option si vous souhaitez que les nouveaux clients soient autorisés par un administrateur avant de pouvoir commencer à se synchroniser avec un compte. La liste <u>Clients</u> indique tous les clients en attente d'autorisation, et l'administrateur peut les autoriser à partir du même écran. Ce paramètre est Non (par défaut).

Max. clients par utilisateur

Si vous souhaitez limiter le nombre de clients ActiveSync ou de terminaux qui peuvent être associés à un compte MDaemon, indiquez le nombre souhaité dans cette option. L'option globale est réglée sur "illimité" par défaut. Cette option est disponible sur les écrans Paramètres clients globaux, de domaine et de compte, et non sur les écrans Clients individuels.

Jour de réinitialisation de la bande passante

Utilisez cette option si vous souhaitez réinitialiser les statistiques d'utilisation de la bande passante pour les Terminaux ActiveSync un jour précis de chaque mois. L'événement de réinitialisation a lieu dans le cadre du processus de maintenance nocturne normal et est consigné dans le journal du système comme les autres routines de maintenance. L'option globale est réglée sur "0 (Jamais)" par défaut, ce qui signifie que les statistiques d'utilisation ne seront jamais réinitialisées. Paramétrez les options enfant sur un jour différent si, par exemple, vous souhaitez que le jour de réinitialisation coïncide avec la date de réinitialisation de la facturation de l'opérateur sans fil d'un utilisateur ou d'un client.

Sécurité

Exclure du Filtrage de pays

Activez cette option dans l'écran des paramètres d'un client ActiveSync si vous souhaitez que l'appareil puisse filtrer l' <u>écran de localisation</u> . Cela permet à un utilisateur valide de continuer à accéder à son compte via ActiveSync lorsque, par exemple, il se rend à un endroit où les tentatives d'authentification sont bloquées. Pour que l'appareil soit exempté, il doit s'être connecté et authentifié via ActiveSync dans le délai configuré dans le paramètre<u>Supprimer les clients inactifs après ce</u> nombre de jours 443 situé dans l'écran Régètres.

Autoriser dynamiquement l'adresse distante

Si vous excluez un pays du Filtrage de l'emplacement, activez cette option si vous souhaitez également autoriser l'adresse IP distante à partir de laquelle il se connecte. Cela peut s'avérer utile pour autoriser d'autres clients susceptibles de se connecter à partir de la même adresse IP.

Autoriser les clients gérés par d'autres serveurs

Par défaut, lorsque le serveur ActiveSync envoie des données de provisionnement/des spécificités de politiques à un client et que celui-ci signale qu'il est également géré par un autre serveur ActiveSync, le client sera toujours autorisé à se connecter à MDaemon. Dans ce cas, il n'y a aucun moyen de s'assurer que les spécificités de votre politique seront appliquées lorsqu'elles entrent en conflit avec la politique de l'autre serveur ActiveSync. En général, les clients utilisent par défaut l'option la plus restrictive en cas de conflit. Désactivez cette option si vous ne souhaitez pas autoriser ces clients à se connecter.

Interdire les réinitialisations aux paramètres d'usine

Si cette option est activée (On/Oui), il ne sera pas possible d'**effacer complètement** un client ActiveSync. Si vous souhaitez pouvoir effectuer un Effacer complètement à distance sur un client, vous devez d'abord désactiver cette option. L'option est désactivée par défaut. Pour plus d'informations, voir : <u>Effacer</u> <u>complètement un client ActiveSync</u> with a page Clients.

Options FolderSync

Options de dossier

Exclure

Dossier Expéditeurs bloqués autorisés/ bloqués

Par défaut, les dossiers Expéditeurs autorisés et Dossiers Expéditeurs bloqués de l'utilisateur ne sont pas synchronisés avec les périphériques. Ils ne sont généralement utilisés par MDaemon que dans le cadre de la prévention automatique du spam. C'est pourquoi ils n'ont pas besoin d'être affichés sur les appareils en tant que contacts.

Dossiers de courrier personnalisés (Non par défaut)

Par défaut, tous les Dossiers de courrier créés par l'utilisateur et par défaut peuvent être synchronisés avec le terminal. Activez cette option si vous souhaitez que seuls les dossiers courrier par défaut soient synchronisés, c'est-àdire la Boîte de réception, les Éléments envoyés, les Éléments supprimés, les Brouillons, etc. Aucun dossier créé par l'utilisateur ne sera inclus. Cette option est désactivée par défaut.

Dossiers PIM personnalisés non (par défaut)

Par défaut, tous les dossiers PIM de l'utilisateur (contacts, calendrier, notes, tâches, etc.) sont synchronisés avec l'appareil. Activez cette option si vous souhaitez que seuls les dossiers PIM par défaut soient synchronisés. Exemple : si cette option est activée et qu'un utilisateur possède plusieurs dossiers de calendrier, seul le calendrier par défaut sera synchronisé. Cette option est désactivée par défaut.

Inclure

Arborescence Dossiers publics

Cochez cette case si vous souhaitez que les **Dossiers publics** auxquels un

utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers publics</u> auxquels il a accès. Cette option est autorisée par défaut.

Navigation dans les dossiers publics (affiche les noms de dossiers)

Non par défaut, pour qu'un client puisse synchroniser un sous-dossier public ou y accéder, le compte doit disposer de l'<u>autorisation de Recherche</u> [327] pour le sousdossier (c'est-à-dire le dossier enfant) et tous les <u>Dossiers publics</u> [325] parents situés au-dessus. Si le compte n'a pas l'autorisation de voir les dossiers parents, il ne peut pas non plus voir le dossier enfant, même s'il en a l'autorisation. Activez cette option si vous souhaitez autoriser le client à accéder à ces dossiers enfants. **Par nom : l** 'activation de cette option doit nécessairement révéler les noms des dossiers parents au client, ce qui pourrait être considéré comme un risque de sécurité. Cette option est désactivée par défaut.

Nombre max de Dossiers publics

Utilisez cette option si vous souhaitez limiter le nombre de Dossiers publics autorisés sur le périphérique. Lorsqu'une limite est définie, le serveur parcourt la liste des dossiers jusqu'à ce que la limite soit atteinte, puis plus aucun dossier n'est envoyé à l'appareil. Il n'existe aucun moyen de garantir l'ordre dans lequel les dossiers seront traités. Non (paramètres par défaut).

Dossiers IMAP partagés

Cochez cette case si vous souhaitez que les <u>dossiers partagés</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers partagés</u> auxquels il a accès. Cette option est autorisée par défaut.

Gestion du contenu

Options de gestion des e-mails

Créer des tâches/rappels pour les e-mails avec indicateurs

Cette option permet à MDaemon de rappeler à l'utilisateur les éléments marqués, en créant un élément de tâche pour chaque courrier électronique marqué. lorsque le client le demande. L'option globale de ce contrôle est activée par défaut.

Toujours envoyer les mises à jour de réunion lorsque l'événement est modifié

Certains clients n'envoient pas correctement les e-mails de mise à jour des réunions lorsqu'ils modifient une réunion. Cette option indique au service ActiveSync d'envoyer une mise à jour de la réunion lorsqu'un élément de la réunion est mis à jour par l'organisateur. Cette option ne doit être définie que pour les <u>clients</u> at les <u>types de clients</u> qui n'envoient pas correctement les mises à jour de réunion, sous

peine d'envoyer des mises à jour de réunion en double. Par conséquent, cette option n'est disponible que dans les pages de paramètres pour les Clients et les Types de clients.

Demander des confirmations de lecture pour tous les e-mails envoyés

Activez cette option si vous souhaitez que le serveur demande des confirmations de lecture pour tous les courriers envoyés par un client. Cette option est désactivée par défaut.

Envoyer des confirmations de lecture du serveur lorsque le courrier est marqué comme lu et lorsque l'expéditeur le demande.

Activez cette option si vous souhaitez que le serveur prenne en charge les demandes de confirmation de lecture et délivre un accusé de réception de lecture lorsqu'un message est marqué comme lu par un client. Cette option est désactivée par défaut.

Envoyer avec l'alias spécifié dans ReplyTo

Certains clients peuvent ne pas autoriser un expéditeur à envoyer du courrier à l'aide d'un alias. Cette fonctionnalité a été ajoutée au <u>protocole Exchange ActiveSync</u> (EAS) (453) 16.x, mais certains clients ne supportent pas la version 16.x. Par exemple, Outlook pour Windows n'utilise que EAS 14.0, et bien qu'il permette à un utilisateur de spécifier une autre adresse pour l'envoi, le message généré ne reflète pas correctement les choix de l'utilisateur. Cette faculté permet d'utiliser le champ ReplyTo pour envoyer l'e-mail, à condition que l'adresse ReplyTo soit un <u>alias</u> valide (1994) pour cet utilisateur. L'option globale est activée par défaut.

Fusionner virtuellement les contacts publics et les contacts par défaut

Activez cette option si vous souhaitez fusionner les contacts publics avec les contacts par défaut de l'utilisateur sur le terminal. Il s'agit uniquement d'une fusion virtuelle, c'est-à-dire qu'ils ne sont pas réellement copiés dans le dossier des contacts de l'utilisateur. Cela peut être utile sur les clients qui ne prennent pas en charge les recherches dans la liste d'adresses globale (GAL). Non (par défaut).

Dossiers Expéditeurs bloqués lors du déplacement d'un courrier dans le dossier Courriers indésirables

Si cette option est activée, lorsqu'un client déplace un e-mail vers le dossier Courriers indésirables du compte, le service ajoute l'adresse SENDER\$ - adresse de l'expéditeur de cet e-mail au dossier Contacts des expéditeurs bloqués.

Forcer l'envoi des réponses aux réunions lorsqu'une demande de réunion est acceptée/déclinée, etc.

Dans cette option, lorsqu'un client accepte, refuse ou choisit une action en réponse à une demande de réunion, le service envoie une réponse à l'organisateur de la réunion. Cette fonction est destinée aux clients spécifiques qui n'envoient pas correctement ces mises à jour eux-mêmes.

Aperçu des paramètres effectifs

Ce bouton est disponible sur tous les écrans des Paramètres clients enfant (c.-à-d. <u>domaines</u> المحكة (محكة), <u>comptes</u> (محكة) et <u>clients</u> (محكة). Non (par défaut), les options de ces écrans sont définies pour hériter de leurs paramètres d'un écran parent. Utilisez cette fonction pour voir quels paramètres sont actuellement appliqués à l'écran affiché.

Voir :

ActiveSync | Comptes 479 ActiveSync | Clients 488 ActiveSync | Sécurité 454

3.11 Indexation des messages

3.11.1 Options/Personnaliser

Message Indexing for MDaemon	- • ×
Options/Customize Diagnostics	
Daily Maintenance Options Maintain search indexes in mailboxes Inboxes Only All mail folders Maintain search indexes in public folders	
Index messages in Mailboxes Index messages in Public Folders Maximum # of worker threads: 20	
Cluster Options	
Daily Maintenance Node : VDI-MIKE V	
Realtime Indexing Node : VDI-MIKE V	
OK Cancel Apply	Help

La boîte de dialogue Indexation des messages est utilisée pour la configuration de la maintenance en temps réel et nocturne des index de recherche utilisés par Webmail, ActiveSync et MDaemon Remote Admin.

Options de maintenance quotidienne

Les options de cette section régissent l'indexation des recherches de nuit.

Maintenir les index de recherche dans les boîtes aux lettres

Cochez cette case si vous souhaitez conserver les index de recherche dans les dossiers de vos boîtes aux lettres. Vous pouvez choisir de le faire pour les boîtes de réception uniquement ou pour tous les dossiers courrier.

Maintenir les index de recherche dans les Dossiers publics

Activer cette option si vous souhaitez maintenir des index de recherche dans vos <u>Dossiers publics</u> [325]. Vous pouvez également spécifier un nombre maximum de fils de discussion qui seront autorisés à travailler simultanément sur ces index.

Indexation en temps réel

Indexer les messages dans les boîtes aux lettres

Activez cette option si vous souhaitez effectuer une indexation en temps réel dans les boîtes aux lettres, afin que les index de recherche soient toujours à jour.

Indexation des messages dans les Dossiers publics

Cochez cette case si vous souhaitez effectuer une indexation de recherche en temps réel dans les <u>Dossiers publics</u> 325 .

Options de regroupement

Si vous utilisez le clustering, utilisez les options de cette section pour désigner les nœuds du cluster qui seront dédiés à la maintenance quotidienne de l'indexation et à l'indexation en temps réel.

3.11.2 Diagnostics

Message Index	ing for MDae	mon	X
Options/Customize	Diagnostics	3	
Logging Log lev	el Info	View / Analyze Log	
- Advanced Op	tions	Minimum debugger log level Debug ~	·
Process Dumps	r based proces	ss dumps Prefix dump files with MdMbSrch	
Value	DumpCount	LogEntry	^
0xC135FE00 0xC135FE01 0xC135FE04 0xC135FE08 0xC135FE02	3 3 3 3 3	The API installed does not match the API level being called for. (No The procedure called has been deprecated. An attempt to read or write to the specified memory would result Access Denied (MD_ACCESSDENIED) COM error thrown: Result: %1 Description: %2	~
<		OK Cancel Apply He	≥lp

Cet écran contient des options avancées qui, dans la plupart des cas, n'auront pas besoin d'être utilisées, sauf si vous essayez de diagnostiquer un problème avec l'indexation des messages ou si vous êtes en contact avec le support technique.

Pas de journalisation

Niveau de journalisation

Six niveaux de journalisation sont pris en charge, de la plus grande à la plus petite quantité de données enregistrées :

- Déboga Il s'agit du niveau de journalisation le plus complet. Il enregistre toutes les entrées disponibles et n'est généralement utilisé que pour diagnostiquer un problème ou lorsque l'administrateur souhaite obtenir des informations détaillées.
 - **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par

défaut.

Avertis	Les avertissements, les erreurs, les erreurs critiques et les
sement	événements de démarrage/arrêt sont consignés dans le journal.

- **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Critiqu Les erreurs critiques et les événements de démarrage/arrêt sont e journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.

Visualiser/Analyser le journal

Cliquez sur ce bouton pour ouvrir la fenêtre de visualisation du journal du système MDaemon Advanced. Non (par défaut) Pas de journalisation dans :".. \NMDaemon\Logs\"

Options avancées

Niveau minimal du journal de débogage

Il s'agit du niveau minimal de journalisation à envoyer au débogage. Les niveaux de journalisation disponibles sont les mêmes que ceux décrits ci-dessus.

Fichiers dumpers

Créer un dump du processus en cas d'erreur

Activez cette option si vous souhaitez générer des Fichiers dumps à chaque fois que survient un avertissement ou une erreur spécifique que vous avez désigné cidessous.

Inclure les informations du tas dans les dumps

Non (par défaut), les informations du tas sont incluses dans les Fichiers dumps. Décochez cette case si vous ne souhaitez pas les inclure.

Préfixe des fichiers dump

Les noms des fichiers dumpiers commenceront par ce texte.

Erreurs/avertissements à partir desquels générer des fichiers dumps

Cliquez avec le bouton droit de la souris sur cette zone et utilisez les options*Ajouter/Modifier/Supprimer une entrée…* pour gérer la liste des erreurs ou des avertissements qui déclencheront des vidages de processus. Pour chaque entrée, vous pouvez spécifier le nombre de Fichiers dumps autorisés avant qu'elle ne soit désactivée.

Voir :

Écran dynamique | Options/Personnalisation

3.12 Service API XML

Cette boîte de dialogue contient divers paramètres de gestion pour le service API XML de MDaemon. Pour en savoir plus sur la bibliothèque d'API de MDaemon et sur l'intégration de vos applications personnalisées à MDaemon, consultez le document suivant : **MD-API.html** (situé dans le dossier \...\NMDaemon\NDocs\NAPI).

Système

XML A	API Mana	gement		—		×
System	Address	Restrictions	Diagnostics			
MdMg	mtWS.dll	24.0.0.1rc1	2024-05-15T12:58:38.000Z			
MDAS	Res.dll	24.0.0.1rc1	2024-05-15T12:58:18.000Z			
MdXm	il.dll	24.0.0.1rc1	2024-05-15T12:58:40.000Z			
MdUs	er.dll	24.0.0rc1	2024-05-15T12:56:58.000Z			
MdCa	lendar.dll	24.0.0rc1	2024-05-15T12:56:42.000Z			
15 15 Disa	▲ da ▲ Se ■ ble all "Area	ys of Settings conds betwee e you sure?" (Editor backup retention n maintenance thread interval onfirmation prompts			
			OK Cancel	Apply	He	ln

Archiver les requêtes et les réponses XML

Activez cette option si vous souhaitez enregistrer toutes les demandes et réponses XML afin de pouvoir diagnostiquer les problèmes qui peuvent survenir.

Activer la mise en cache de la Liste de cache globale (Dossier public)

Utilisez cette option si vous souhaitez autoriser l'API à conserver les Listes d'adresses globales (Dossiers publics) des domaines en cache, afin d'améliorer les performances. Cette option est activée par défaut.

[xx] seconde Délai d'attente pour la session de connexion

Cette option détermine le nombre de secondes avant qu'un jeton de connexion à l'API n'expire s'il n'est pas utilisé.

[xx] jours de conservation des sauvegardes de l'éditeur de paramètres

Cette option détermine le nombre de jours pendant lesquels les sauvegardes de l'Éditeur/INIfile et de l'Éditeur/HiWater doivent être conservées, afin que les modifications puissent être annulées/réinitialisées via l'action "récupérer".

[xx] Intervalle de secondes entre les fils de maintenance

Il s'agit du nombre de secondes pendant lesquelles le fil de maintenance dort avant de vérifier la présence de nouvelles tâches de maintenance telles que le nettoyage d'anciens répertoires et fichiers.

Désactiver toutes les invites de confirmation "Êtes-vous sûr ?

Cochez cette case si vous souhaitez désactiver toutes les invites de confirmation "Êtes-vous sûr ?" afin de rationaliser les actions de l'interface utilisateur.

XML API Management	– 🗆 X
System Address Restrictions Diagnostics	
Allowed Addresses	Blocked Addresses
 Allow all Trusted IP addresses Allow all LAN IP addresses Allow all Dynamic Allow List addresses 	Deny all IP addresses not specifically allowed
OK	Cancel Apply Help

Adresses autorisées

Cliquer avec le bouton droit de la souris pour ajouter une nouvelle adresse IP/masque à la liste des adresses autorisées. Ces adresses sont autorisées à se connecter à l'API.

Autoriser toutes les adresses IP autorisées

Cochez cette case si vous souhaitez autoriser toutes les adresses<u>IP autorisées</u> a se connecter à l'API.

Allow all LAN IP Addresses (Autoriser toutes les adresses IP locales)

Cochez cette case si vous souhaitez autoriser toutes les adresses<u>IP locales</u> à se connecter à l'API.

Allow all Dynamic Allow Liste d'autorisations addresses (Autoriser toutes les adresses de la Liste dynamique)

Cochez cette case si vous souhaitez autoriser toutes les adresses<u>autorisées</u> <u>dynamiquement</u> a se connecter à l'API.

Adresses bloquées

Cliquez avec le bouton droit de la souris pour ajouter ou modifier des adresses IP dans cette liste. Ces adresses IP ne peuvent pas se connecter à l'API.

Deny all Adresses IP not specifically allowed (Refuser toutes les adresses IP non spécifiquement autorisées)

Lorsque cette case est cochée, les seules adresses IP autorisées à se connecter à l'API sont celles qui sont spécifiquement autorisées à se connecter via les paramètres des Adresses autorisées.

Diagnostics

ystem Address	Restrictions	Diagnostics						
Logging								
Log lev	el Critical	~			View /	Analyze	e Log	
- Advanced Or	tions							
narancea op			Minimum deb	ugger log leve	Debug		\sim	
	ss Memory Co	unters	No	more than eve	erv 3600		econds	
	m Wide Derfor	mance Infor	nation		(30-3	600)		
	m while Perior	mance milon						
Process Dumps	r based proces	ss dumps	Prefix	dump files with	include he	ap inforr	mation	
Process Dumps	r based proces	ss dumps e dumps on	Prefix	dump files with	indude hei	ap inforr	mation	
Process Dumps Enable erro Errors / Warnin Value	r based proces ngs to generate DumpCount	ss dumps e dumps on LogEntry	Prefix	dump files wit	Include hea	ap inforr	mation	
Process Dumps Enable erro Errors / Warnin Value 0xC135FE00	r based proces ngs to generate DumpCount 3	ss dumps e dumps on LogEntry The API ins	Prefix talled does no	dump files with	Include hei	ap inforr	d for. (N	
Process Dumps Enable erro Errors / Warnin Value 0xC135FE00 0xC135FE01	r based proces ngs to generate DumpCount 3 3	e dumps on LogEntry The API ins The proced	Prefix talled does no ure called has	dump files with t match the AF been depreca	Include her n PI level bei ted.	ap inforr	d for. (N	
Process Dumps Enable erro Errors / Warnin Value 0xC135FE00 0xC135FE01 0xC135FE04	r based proces ngs to generate DumpCount 3 3 3	e dumps on LogEntry The API ins The proced An attempt	Prefix talled does no ure called has to read or wr	dump files with t match the AF been depreca ite to the speci	Include her PI level bein ted.	ap inforr ng called	d for. (N	
Process Dumps Enable error Value 0xC135FE00 0xC135FE01 0xC135FE04 0xC135FE08	r based proces ngs to generate DumpCount 3 3 3 3	e dumps on LogEntry The API ins The proced An attempt Access Den	Prefix talled does no ure called has to read or wr ied (MD_ACC6	dump files with t match the AF been depreca ite to the speci SSDENIED)	Include her PI level bei ted. ified memo	ap inforr ng callec	d for. (N	
Process Dumps Enable error Value 0xC135FE00 0xC135FE01 0xC135FE04 0xC135FE08 0xC135FE08	r based proces ngs to generate DumpCount 3 3 3 3 3 3 3	e dumps on LogEntry The API ins The proced An attempt Access Den This functio	Prefix talled does no ure called has to read or wr ied (MD_ACCI n has been di	dump files with t match the AF been depreca ite to the speci SSDENIED) scontinued for	Include her PI level bei ted. ified memo	ap inforr ng callec ry would relopme	d for. (N d result nt	
Process Dumps Enable error Value 0xC135FE01 0xC135FE01 0xC135FE04 0xC135FE08 0xC135FE08 0xC135FE00	r based proces ngs to generate DumpCount 3 3 3 3 3 3	e dumps on LogEntry The API ins The proced An attempt Access Den This functio	Prefix talled does no ure called has to read or wr ied (MD_ACC n has been di	dump files with t match the AF been depreca ite to the speci ESSDENIED) scontinued for	Include her PI level bei ted. ified memo future dev	ap inforr ng callec ry would relopme	d for. (N d result nt	
Process Dumps Enable error Value 0xC135FE00 0xC135FE01 0xC135FE04 0xC135FE08 0xC135FE08 0xC135FE00	r based proces ngs to generate DumpCount 3 3 3 3 3	e dumps on LogEntry The API ins The proced An attempt Access Den This functio	Prefix talled does no ure called has to read or wr ied (MD_ACCE n has been di	dump files with t match the AF been depreca ite to the speci ESSDENIED) scontinued for	Include her PI level bei ted. ified memo	ap inforr ng callec ry would velopme	d for. (N d result nt	

Pas de journalisation

Niveau de journalisation

Six niveaux de journalisation sont pris en charge, de la plus grande à la plus petite quantité de données enregistrées :

- Déboga Il s'agit du niveau de journalisation le plus complet. Il enregistre toutes les entrées disponibles et n'est généralement utilisé que pour diagnostiquer un problème ou lorsque l'administrateur souhaite obtenir des informations détaillées.
 - **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.
- AvertisLes avertissements, les erreurs, les erreurs critiques et lessementévénements de démarrage/arrêt sont consignés dans le journal.
- **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- **Critiqu** Les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.

Visualiser/Analyser le journal

Cliquez sur ce bouton pour ouvrir la fenêtre de visualisation du journal du système MDaemon Advanced. Non (par défaut) Pas de journalisation dans :".. \NMDaemon\Logs\"

Options avancées

Niveau minimal du journal de débogage

Il s'agit du niveau minimal de la journalisation à envoyer au débogage. Les niveaux de journalisation disponibles sont les mêmes que ceux décrits ci-dessus.

Enregistrer les compteurs de mémoire du processus

Cochez cette case pour consigner dans le fichier journal les informations relatives à la mémoire, aux gestionnaires et aux threads spécifiques au processus. Ceci est utile pour trouver des pistes potentielles et des problèmes d'allocation de ressources. Les entrées du journal ne seront émises que si les données ont changé depuis la dernière fois qu'elles ont été journalisées.

Pas de journalisation des informations sur les performances de l'ensemble du système

Cochez cette case si vous souhaitez consigner dans le fichier journal des informations sur les performances de l'ensemble du système. Ceci est utile pour trouver des pistes potentielles et des problèmes d'allocation de ressources. Les entrées journal ne seront émises que si les données ont changé depuis la dernière fois qu'elles ont été journalisées.

Pas plus de toutes les [xx] secondes

Cette option permet de définir la fréquence à laquelle les informations relatives aux processus et aux performances seront journalisées.

Fichiers dumpers

Créer un dump du processus en cas d'erreur

Activez cette option si vous souhaitez générer des Fichiers dumps à chaque fois que survient un avertissement ou une erreur spécifique que vous avez désigné cidessous.

Inclure les informations du tas dans les dumps

Non (par défaut), les informations du tas sont incluses dans les Fichiers dumps. Décochez cette case si vous ne souhaitez pas les inclure.

Préfixe des fichiers dump

Les noms des fichiers dumpiers commenceront par ce texte.

Erreurs/avertissements à partir desquels générer des fichiers dumps

Cliquez avec le bouton droit de la souris sur cette zone et utilisez les options*Ajouter/Modifier/Supprimer une entrée...* pour gérer la liste des erreurs ou des avertissements qui déclencheront des vidages de processus. Pour chaque entrée, vous pouvez spécifier le nombre de Fichiers dumps autorisés avant qu'elle ne soit désactivée.

3.13 Préférences

3.13.1 Préférences

3.13.1.1 Interface utilisateur

🧐 Preferences - UI	
Preferences - UI Preferences System Disk Fixes Headers Updates Miscellaneous Windows Service	Start MD aemon Start MD aemon in the system tray full screen in a default window Always keep icon on task bar UI Settings USe small display font Show Apply button result Preserve root node mail counts Preserve server on/off states Expand UI tree nodes Expand List Manager tree nodes Update message counts in UI Split session pane Center all UI dialogs Use colors in UI logs MDSTATS use in single instance List Manager includes Sustem lists
	MDSTATS runs in single instance List Manager includes System lists ✓ MDSTATS shows sub-folders ✓ Show/Log Subject data Configuration session shows this many bytes of old logs 15000 Number of accounts shown in UI controls (0=show all) 0 Number of domains shown in UI controls (0=show all) 0 Number of lines shown before main log windows clear 5000 Number of lines logged before session windows clear 250 Path or executable name of my favorite text file editor: Browse Dk Cancel Applu

De...

...dans la barre d'état système

Choisissez cette option si vous ne souhaitez pas afficher l'interface deMDaemonau démarrage. L'icône de MDaemon apparaîtra tout de même dans la barre d'état système.

...plein écran

Choisissez cette option si vous souhaitezque l'interface deMDaemonsoit maximisée au démarrage.

...dans une fenêtre par défaut

Choisissez cette option si vous souhaitezque l'interface deMDaemonapparaisse dans une fenêtre par défaut au démarrage.

Toujours garder l'icône dans la barre des tâches

Dans cette option, MDaemon démarrera minimisé dans la barre des tâches, et il apparaîtra à la fois dans la barre des tâches et dans la barre d'état système lorsqu'il sera minimisé. Décochez cette case si vous ne souhaitez pas que MDaemon apparaisse dans la barre des tâches de Windows lorsqu'il est réduit ; seule l'icône de la barre d'état système sera visible.

Paramètres de l'interface utilisateur

Utiliser une petite police d'affichage

Active la petite police d'affichage dans les fenêtres Suivi des événements et Session.

Afficher le résultat du bouton Appliquer

Non (par défaut), lorsque vous cliquez sur le bouton Appliquer dans une boîte de dialogue, une boîte de message s'ouvre pour confirmer que les modifications apportées aux paramètres de la boîte de dialogue ont été enregistrées. Décochez cette case si vous souhaitez appliquer les modifications sans afficher le message.

Conserver les comptes de courrier du nœud racine

Activez cette option si vous souhaitez sauvegarder les compteurs du nœud racine lors des redémarrages du serveur. Les compteurs du nœud racine sont listés dans la section "Statistiques" du volet Stats de l'interface graphique principale deMDaemon.

Conserver les états marche/arrêt du serveur

Si cette option est activée, MDaemon s'assurera que l'état de ses serveurs (activés ou désactivés) reste le même après un redémarrage.

Développer les nœuds de l'arborescence de l'interface utilisateur

Cochez cette case si vous souhaitez que les nœuds de l'arborescence de navigation dans le volet gauche des différentes boîtes de dialogue soient développés automatiquement. Cela ne s'applique pas au <u>Gestionnaire listes de diffusion</u>²⁶¹. Si vous souhaitez développer automatiquement les nœuds de l'arborescence de la liste de diffusion, utilisez l' option*Gérer liste de diffusion* ci-dessous.

Développer les nœuds de l'arborescence du gestionnaire de liste

Cochez cette case si vous souhaitez que les 281 nœuds de l'arborescence de navigation<u>du Gestionnaire de listes de 281</u> diffusion dans le volet de gauche soient développés automatiquement.

Actualiser les compteurs de messages dans l'interface utilisateur

Dans cette option, MDaemon doit vérifier le disque pour compter les messages en attente dans les files d'attente.

Diviser le volet de session

Activez cette option si vous souhaitez que l'onglet Sessions de l'interface principale de MDaemon soit séparé des autres onglets dans son propre volet. La modification de ce paramètre nécessite un Redémarrage de l'interface utilisateur de MDaemon, et l'option du menu Windows permettant de passer d'un volet à l'autre ne sera plus disponible.

Centrer toutes les boîtes de dialogue de l'interface utilisateur

Non (par défaut), toutes les boîtes de dialogue sont centrées sur l'écran lorsqu'elles sont ouvertes, plutôt que de se chevaucher. Filtrez cette case à cocher si vous

souhaitez que les boîtes de dialogue se chevauchent, mais cela peut occasionnellement les faire sortir partiellement de l'écran ou les rendre hors cadre.

Utiliser des couleurs dans les pas de journalisation de l'interface utilisateur

Cette option permet de coloriser le texte affiché dans plusieurs des onglets<u>Suivi des</u> <u>événements et Journalisation de le 172</u> 'interface utilisateur de MDaemon. Elle est activée par défaut. Pour la modifier, il faudra redémarrer l'interface de MDaemon avant qu'elle ne prenne effet. Voir : <u>Pas de journalisation des sessions en couleur</u> [162] pour plus d'informations.

Le gestionnaire de listes inclut les listes du système

Activez cette option si vous souhaitez afficher les listes de diffusion générées par le système de MDaemon (par exemple Everyone@ et MasterEveryone@) dans le <u>Gestionnaire de diffusion</u> [281]. Les listes générées par le système ont un nombre limité d'éléments disponibles pour la configuration par l'utilisateur. Lorsque cette option est désactivée, les listes système seront cachées mais toujours disponibles pour l'utilisation. Cette option est désactivée par défaut.

MDSTATS s'exécute dans une seule instance

Cochez cette case si vous ne souhaitez pas que plusieurs copies du<u>gestionnaire de</u> <u>files d'attente et de statistiques de</u> MDaemon puissent s'exécuter en même temps. Si vous tentez de lancer le gestionnaire alors qu'il est déjà en cours d'exécution, la fenêtre active sera simplement celle de l'instance en cours d'exécution.

MDSTATS affiche les sous-dossiers

Cochez cette case si vous souhaitez que le <u>gestionnaire de files d'attente et de</u> <u>statistiques</u> affiche les sous-dossiers contenus dans les différentes files d'attente et les dossiers courrier des utilisateurs.

Afficher/enregistrer les données du sujet

Par défaut, les données de la ligne Subject : sont affichées dans les onglets de l'interface utilisateur de MDaemon et écrites dans les fichiers journaux. Dans le cas des listes de diffusion, un mot de passe peut être inséré par l'utilisateur dans la ligne Objet. Il est donc recommandé de désactiver cette option. Il est donc recommandé de désactiver cette option.

La session de configuration affiche ce nombre d'octets d'anciens journaux.

Lors de l'exécution d'une session de configuration, il s'agit de la quantité maximale de données de journalisation qui sera affichée dans un onglet de<u>suivi des événements</u> et de journalisation [72]. Le paramètre par défaut est de 15 000 octets.

Nombre de comptes affichés dans les contrôles de l'interface utilisateur (0 = tout)

Dans cette option est indiqué le nombre maximum de comptes qui seront affichés dans les listes déroulantes de diverses boîtes de dialogue. De plus, lorsque la valeur de cette option est inférieure au nombre de comptes existants, les options "Modifier le compte " et " Supprimer le compte " n'apparaîtront plus dans le menu Comptes ; vous ne pourrez modifier et supprimer des comptes qu'en utilisant le <u>Gestionnaire de comptes</u> [762]. Vous devez redémarrer MDaemon pour que les modifications soient prises en compte. Le paramètre par défaut est "0", ce qui signifie que tous les comptes sont affichés.

Nombre de domaines affichés dans les contrôles de l'interface utilisateur (0 = tout) Il s'agit du nombre maximum de domaines qui seront affichés dans l'interface graphique principale, quel que soit le nombre de domaines existants. Après avoir modifié cette valeur, vous devez redémarrer MDaemon en cours pour que les modifications soient visibles. Le Domaine par défaut est "0", ce qui signifie que tous les domaines sont affichés.

Nombre de lignes affichées avant l'effacement des fenêtres du journal principal Il s'agit du nombre maximum de lignes qui seront affichées dans les fenêtres de journalisation de l'écran principal. Lorsque ce nombre de lignes est atteint, la fenêtre est effacée. Cela n'a aucune incidence sur le fichier journal ; seul l'affichage est effacé.

Nombre de lignes journalisées avant l'effacement des fenêtres de session Il s'agit du nombre maximum de lignes qui apparaîtront dans chaque <u>fenêtre de</u> <u>session</u> avant qu'elle ne soit effacée. Ce paramètre n'a aucune incidence sur le fichier journal.

Chemin du fichier ou nom de l'exécutable de mon éditeur de texte préféré Notepad.exe est l'éditeur de texte général que l'interface utilisateur de MDaemon lance par défaut en cas de besoin. Si vous préférez utiliser un autre éditeur de texte, indiquez ici son chemin d'accès ou le nom de son exécutable.

3.13.1.2 Système

🧐 Préférences - Système		×
Préférences Interface utilisateur Système Oisque Correctifs En-têtes Mises à jour Divers Service Windows	Alias du compte système MDaemon Extension par défaut des pièces jointes Caractère de délimitation du nom de connexion I Exiger l'adresse e-mail complète pour l'authend Nom du dossier spam par défaut Code de représentation des caractères des messages générés automatiquement Objet des messages de bienvenue : Bienvenue dans le système de messagerie MDaa Démarrer la maintenance & le nettoyage quotidie I Diviser en sous-répertoires	MDaemon .eml \$ (en plus de '@') ification sur les serveurs Junk E-mail iso-8859-1 emon du domaine \$DOMAIN ns à 12 am
	OK	Annuler Appliquer Aide

Alias du compte MDaemon de la boîte aux lettres du système [adresse]

Cette adresse électronique est celle à partir de laquelle les messages générés par le système seront envoyés. Les confirmations d'abonnement, les messages de notification d'état de livraison (DSN), divers autres messages de notification, etc. sont tous des messages système.

Extension défaut des pièces jointes)

Les messages générés par le système seront créés à l'aide de cette extension. C'est également l'extension attribuée aux pièces jointes incluses dans les messages générés par le système. Exemple : si MDaemon génère un message d'alerte au postmaster à propos d'un message spécifique, il joindra ce message avec cette valeur comme extension de fichier.

Caractère de délimitation de la connexion par défaut (10 caractères maximum)

Lorsqu'une adresse électronique est utilisée comme paramètre de connexion au compte, ce caractère ou cette chaîne de caractères peut être utilisé(e) à la place de "@". Cela peut s'avérer nécessaire pour certains utilisateurs dont les clients de messagerie ne prennent pas en charge "@" dans le champ À :. Exemple : si vous utilisez "\$" dans ce champ, les utilisateurs peuvent se connecter en utilisant "user1@example.com" ou "user1\$example.com".

Demander l'adresse e-mail complète pour l'authentification sur les serveurs

Les serveurs POP et IMAP de MDaemon exigent par défaut que vous utilisiez votre adresse électronique complète pour vous connecter à MDaemon. Si vous souhaitez autoriser les connexions par boîte aux lettres uniquement (par exemple, "user1" au lieu de "user1@example.com"), vous pouvez désactiver cette option, mais elle n'est pas recommandée car les connexions par boîte aux lettres uniquement sont ambiguës lorsque MDaemon dessert plusieurs domaines.

Dossier spam par défaut

Utilisez ce texte pour indiquer le nom par défaut du dossier spam que MDaemon peut créer automatiquement pour vos utilisateurs. Le nom par défaut est " Courrier indésirable " pour correspondre à la valeur par défaut de divers autres produits largement diffusés.

Code de représentation des caractères des messages générés automatiquement Indiquez le jeu de caractères que vous souhaitez utiliser pour les messages générés automatiquement. Le paramètre par défaut est iso-8859-1.

Sujet du message de bienvenue aux nouveaux comptes :

MDaemon envoie généralement un "message de bienvenue "aux nouveaux comptes. Ce texte apparaît dans l'en-tête "Subject" dumessage.Le message de bienvenue est construit à partir du fichier NEWUSERHELP.DAT contenu dans le dossier ... \MDaemon\app, et cet objet du message peut contenir toutes les macros autorisées dans les <u>scripts de réponse automatique</u>.

Démarrer la maintenance et le nettoyage quotidiens à [1-12] [am/pm]

Cette option permet de définir l'heure à laquelle la maintenance et le nettoyage quotidiens sont effectués. Le paramètre par défaut et recommandé est 12 heures.

Quelle que soit l'heure définie pour cette option, certains événements quotidiens auront toujours lieu à minuit, comme la maintenance des fichiers journaux et l'exécution de midnight.bat.

Déplacer les dossiers courrier du compte lorsque les valeurs du domaine ou de la BAL changent

Si cette case est activée, lorsque vous modifiez un Nom de domaine ou une boîte aux lettres, les dossiers courrier des comptes concernés seront déplacés vers le nouvel emplacement. Sinon, MDaemon continuera à utiliser les anciens noms de dossiers courrier.

Diviser en sous-dossiers

Cochez cette case si vous souhaitez activer le hachage des répertoires - MDaemon hachera certains répertoires en créant jusqu'à 65 sous-répertoires. Le hachage peut augmenter les performances de certains sites à fort volume, mais peut les dégrader légèrement pour les sites MDaemon classiques. Cette option est désactivée par défaut.

3.13.1.3 Disque

🧐 Préférences - Disque	
Préférences Interface utilisateur Système Correctifs En-têtes Mises à jour Divers Service Windows	 Activer le moteur de vérification d'espace disque Envoyer une alerte à Postmaster@example.com lorsque l'espace disque passe en dessous de 1000 Mo Désactiver automatiquement les services TCP/IP si l'espace disque disponible est inférieur à 100 Mo Les disques suivants sont vérifiés (ex. : C, D, E) Ne remplissez pas ce champ si vous souhaitez vérifier uniquement le disque du répertoire APP. Figer la file entrante après ce nombre d'erreurs 0 Nettoyage et Sauvegarde Supprimer les fichiers de la file des messages erronés de plus de (en jours, 0=jamais) 0 Sauvegarder les fichiers de configuration à minuit Fichiers à sauvegarder *INII*.DATI*.SUPI*.MBFI*.RSPI*.GRPI*.CF Séparez plusieurs fichiers par le caractère « I ». Les caractères jokers sont acceptés. Les sauvegardes sont conservées dans le dossier Backup. Supprimer les sauvegardes de plus de (jours, 0=jamais) 0 Limiter l'accès au dossier MDaemon aux comptes Administrateurs, Opérateurs de sauvegarde et Système
	OK Annuler Appliquer Aide

Activer le moteur de vérification de l'espace disque

Activez cette case à cocher si vous souhaitez que MDaemon surveille l'espace disque disponible sur le lecteur où se trouvemDaemon.exe.

Envoyer une notification à [utilisateur ou adresse] lorsque l'espace disque libre est inférieur à [xx] Mo.

En utilisant cette option, vous pouvez configurer MDaemon pour qu'il envoie un message de notification à l'utilisateur ou à l'adresse de votre choix lorsque l'espace disque passe en dessous d'un certain niveau. La valeur par défaut est de 1000 MO.

MDaemon désactivera automatiquement les services TCP/IP si l'espace disque libre est inférieur à [xx] Mo.

Activez cette fonctionnalité si vous souhaitez que MDaemon désactive les services TCP/IP si l'espace disque libre passe en dessous d'un certain niveau. La valeur par défaut est de 100 MO.

Les disques suivants sont vérifiés (ex : C, D, E)

Utilisez cette option si vous souhaitez surveiller l'espace disque disponible sur plusieurs disques, en spécifiant la lettre du lecteur pour chacun d'entre eux. Si vous laissez cette option vide, seul le disque remplissez ce champ souhaitez vérifieruniquement le disque du répertoire APPde MDaemon.

Figer la file d'attente entrante après ce nombre d'erreurs de disque consécutives (0 = jamais)

Si ce nombre d'erreurs de disque se produit lors du traitement de la file entrante, MDaemon interrompt le traitement de la file jusqu'à ce que vous résolviez le problème. Un e-mail est placé dans la boîte aux lettres du postmaster lorsque cet arrêt se produit.

Nettoyage et sauvegarde du disque

Supprimer les fichiers de la file des messages erronés de plus de (en jours, 0=jamais) Utilisez cette option si vous souhaitez que MDaemon supprime les anciens fichiers de la file d'attente des messages erronés lorsqu'ils sont plus anciens que le nombre de jours spécifié. Si vous ne souhaitez pas supprimer les messages automatiquement, utilisez "0" dans cette option.

Sauvegarder les fichiers de configuration à minuit

Cochez cette case si vous souhaitez archiver tous les fichiers de configuration de MDaemon à minuit chaque nuit dans le répertoire Backups.

Fichiers à sauvegarder

Utilisez cette zone de texte pour spécifier exactement les fichiers et les extensions de fichiers à sauvegarder. Les caractères joker sont autorisés et chaque nom de fichier ou extension doit être séparé par le caractère "|".

Supprimer les sauvegardes datant de plus de ce nombre de jours (0=jamais)

Utilisez cette option si vous souhaitez supprimer automatiquement les anciens fichiers à sauvegarder. Les fichiers plus anciens que le nombre de jours spécifié seront supprimés dans le cadre du nettoyage quotidien de minuit. Le paramètre par défaut est "0", ce qui signifie que les anciens fichiers de sauvegarde ne seront pas supprimés.

Limiter l'accès au dossier MDaemon aux comptes Administrateurs, Opérateurs de sauvegarde et Système

Cliquez sur ce bouton pour limiter l'accès au dossier MDaemon et à ses sous-dossiers aux comptes/groupes Windows suivants : Administrateurs, Opérateurs de sauvegarde et SYSTÈME.

3.13.1.4 Correctifs



Supprimer CRLFCRLF à la fin du corps des messages

Certains clients de messagerie ont des difficultés à afficher les messages qui se terminent par des Carriage Return Line Feeds (CRLFCRLF) consécutifs. Lorsque cette case est cochée, MDaemon supprime les séquencesCRLFCRLFCONSÉcutives de la fin du corps du message. Cette option est activée par défaut.

Supprimer CRLF LF.CR CRCRLF à la fin des corps des messages

Non (par défaut), MDaemon supprime cette séquence à la fin des messages, car elle peut poser des problèmes à certains clients de messagerie. Décochez cette case si vous ne souhaitez pas supprimer cette séquence des messages.

Supprimer NULL & EOF mais autoriser LF.LF à la fin du corps des messages

Dans cette option, MDaemon supprime les caractères NULL et EOF à la fin du corps des messages, mais autorise les messages se terminant par LF.LF, ainsi que les messages se terminant par la séquence normale CRLF.CRLF qui signifie la fin d'un message. Cette option est activée par défaut.

Corriger les en-têtes inexacts en ajoutant "X-MD-Bad-Header :" aux en-têtes illégaux.

Lorsque cette option est activée et que MDaemon rencontre un en-tête de message incorrect, il le fait précéder de la mention "X-MD-Bad-Header :". Cette option est activée par défaut.

Copier 'Sender:' dans 'From:' si 'From:' est manquant

Certains clients de messagerie ne créent pas d'en-tête FROM : dans la composition d'un message. Dans ce cas, les informations de l'en-tête FROM : sont placées dans l'en-tête Sender :. Cela peut poser des problèmes à certains serveurs de messagerie ainsi qu'au destinataire de votre message. Pour éviter ces problèmes, MDaemon crée l'en-tête FROM : manquant en utilisant le contenu de l'en-tête Sender : lorsque cette case est cochée. Cette option est activée par défaut.

Accepter le message même si la connexion est interrompue après DATA

Si cette option est activée, MDaemon acceptera et délivrera un message même en cas d'interruption de la connexion pendant ou immédiatement après la commandeDATA au cours du processus SMTP. Cette option ne doit pas être utilisée dans des circonstances normales car elle peut entraîner des messages en double.

3.13.1.5 En-têtes

🧐 Préférences - En-têtes		×
 Préférences Interface utilisateur Système Disque Correctifs En-têtes Mises à jour Divers 	S'ils sont manquants, insérer les en-têtes Date Message-ID	Supprimer les en-têtes X-RBL-Warning X-Spam-Flag Received (messages de liste uniquement) Tous les autres en-têtes commençant par X-
Service Windows	Ajouter les en-têtes suivants Precedence: bulk (messages système X-Authenticated-Sender: (courrier auth Content-ID: (messages RAW avec piè Masquer les IP réservées lors de la créati Masquer les noms d'hôte & les IP lors de l Masquer les informations de version du lo Répondre à toutes les requêtes 'Return-R	"From: MD aemon" uniquement) entifié uniquement) ces jointes) on des en-têtes de message a création des en-têtes de messages giciel dans les réponses & les en-têtes "Received:" leceipt-To:'
		DK Annuler Appliquer Aide

S'ils manquent, insérez ces en-têtes

Date début

Si MDaemonrencontre un message qui ne contient pas d'en-tête "Date :", il en crée un et l'ajoute au fichier du message si cette option est activée. Il s'agit de la date à laquelle MDaemon reçoit le message pour la première fois, et non de la date à laquelle il a été créé par l'expéditeur. Certains clients de messagerie ne créent pas cet en-tête, et comme certains serveurs de messagerie refusent d'honorer de tels messages, cette fonctionnalité leur permettra d'être délivrés.

Message ID

Lorsqu'un message est rencontré sans en-tête "Message-ID", MDaemon en crée un et l'insère dans le message.

Si c'est le cas, il supprime les en-têtes suivants dans TO :.

Received (liste de diffusion uniquement)

Cochez cette case si vous souhaitez supprimer tous les en-têtes "Received : "existants dans les listes en-tête FROM.

Avertissement X-RBL

Cochez cette case si vous souhaitez supprimer tous les destinataires"X-RBL-Warning : " présents dans les messages. Cette option est désactivée par défaut.

Drapeau X-Spam

Activez cette option si vous souhaitez supprimer les anciens en-têtes"X-Spam-Flag : " dans les messages.

Tous les en-têtes commençant par X-.

MDaemon et d'autres serveurs de messagerie utilisent de nombreux en-têtes spécifiques au serveur, appelés en-têtes Type X, afin d'acheminer le courrier et d'effectuer diverses autres fonctions. Lorsque cette option est activée, MDaemon supprime ces en-têtes dans les messages. **Remarque**: cette option ne supprime pas les en-têtesX-RBL-Warning. Si vous souhaitez supprimer les en-têtes From, utilisez l'option "X-RBL-Warning" ci-dessus.

Ajouter ces en-têtes

Precedence : bulk (messages système uniquement)

Lorsque cette case est cochée, tous les messages générés par le système à partir de MDaemon (messages de bienvenue, messages d'alerte, messages "could not deliver", etc.) auront un en-tête "Precedence : bulk" inséré.

X-Authenticated-Sender : (courrier authentifié uniquement)

Par défaut, MDaemon ajoute l'en-tête "X-Authenticated-Sender :" aux messages qui arrivent sur une session authentifiée à l'aide de la commandeAUTH. Décochez cette case si vous ne souhaitez pas ajouter cet en-tête.

Content-ID : (messages RAW avec pièces jointes)

Cochez cette case si vous souhaitez ajouter des en-têtesMIME Content-ID aux messages créés par MDaemon à partir d'un fichier RAW contenant des pièces jointes.

Masquer les adresses IP réservées lors de la création d'en-têtes de messages

Cette option est activée par défaut et empêche les adresses IP réservées d'apparaître dans certains en-têtes de messages créés par MDaemon. Les adresses IP réservées sont les suivantes : 127.0.0.*, 192.168.*.*, 10.*.*.* et 172.16.0.0/12. Si vous souhaitez également masquer les IP de vos domaines (y compris les domaines LAN) dans les en-têtes, vous pouvez définir manuellement le commutateur suivant dans le fichier app\MDaemon.ini de MDaemon : [Special] HideMyIP: [Oui (Non (par défaut)).

Masquer les noms d'hôte et les IP dans la création des en-têtes de message

Cliquez sur cette option si vous souhaitez omettre les noms d'hôte ou les adresses IP dans les en-têtes "Received :" lors de leur construction. Cette option est désactivée par défaut.

Masquer l'identification de la version du logiciel dans les réponses et les en-têtes "Received :".

Utilisez cette option si vous souhaitez empêcher MDaemon d'indiquer la version de son logiciel et d'autres informations d'identification dans les en-têtes "Received:" ou dans les réponses à diverses requêtes de protocole. Cette option est désactivée par défaut.

Répondre à toutes les requêtes 'Return-Receipt-To:'.

Cochez cette case si vous souhaitez honorer les demandes de confirmation de livraison des messages entrants et envoyer automatiquement un message de confirmation à l'expéditeur. Cette option est désactivée par défaut.

3.13.1.6 Mises à jour

Mises à jour automatiques

Grâce aux Mises à jour automatiques, vous pouvez configurer MDaemon pour qu'il informe le postmaster chaque fois qu'une mise à jour est disponible pour MDaemon, et vous pouvez le configurer pour qu'il télécharge et installe les mises à jour automatiquement. Le serveur sera toujours redémarré lorsqu'une mise à jour est installée automatiquement. Les fichiers sont téléchargés lorsque la mise à jour est détectée, mais l'installation et le redémarrage ont lieu plus tard, à l'heure que vous avez choisie. Toutes les activités d'installation sont enregistrées dans le journal système de MDaemon et le postmaster est informé lorsqu'une mise à jour a eu lieu.

Informer le postmaster lorsque de nouvelles mises à jour à jour sont disponibles Cette option permet à MDaemon d'informer le postmaster lorsqu'une mise à jour de MDaemon est disponible. MDaemon est disponible. Cette option est activée par défaut.

> LorsqueMDaemon est configuré pour se mettre à jour automatiquement, ce message n'est pas envoyé. Au lieu de cela, le postmaster est informé qu'une mise à jour a été installée, et il est informé de toute considération particulière concernant la mise à jour.

Télécharger et installer les mises à jour de MDaemon automatiquement

Cochez cette case si vous souhaitez télécharger et installer les mises à jour de MDaemon automatiquement. Les mises à jour sont téléchargées lorsqu'elles sont détectées, puis installées à l'heure indiquée ci-dessous. Cette option est désactivée par défaut.

Installer les mises à jour et redémarrer le serveur à :

Les mises à jour automatiques sont téléchargées au moment où elles sont détectées, puis stockées dans le dossier\MDaemon\Updates, mais elles ne sont pas installées avant l'heure indiquée ici. Le serveur sur lequel MDaemon est installé sera redémarré automatiquement après chaque mise à jour. Cette option est réglée sur 2 AM par défaut.

Supprimer les fichiers d'installation une fois les mises à jour terminées

Cochez cette case si vous souhaitez supprimer les fichiers d'installation d'une mise à jour terminée.

Modifier les mises à jour en attente

Lorsqu'une mise à jour est détectée et téléchargée, elle est alors mise en file d'attente en vue d'une installation ultérieure. La liste des mises à jour en attente est stockée dans le fichier QueuedUpdates.dat. Cliquez sur ce bouton pour consulter cette liste ou supprimer une mise à jour en attente.

3.13.1.7 Divers

Preferences - Miscellaneous	
Preferences UI System Disk Fixes Headers Updates Windows Service Windows Service	 Do not send welcome message to new accounts Send response to invalid command messages System generated messages are sent through the content and spam filters Forwarded messages are sent through the content and spam filters DSN messages are sent through the content and spam filters Disable subaddressing feature for all accounts Send stats report to postmaster at midnight Account export includes disk usage stats (this could greatly slow export) Messages forwarded to specific hosts do not go to the smart host on errors Copy all system generated Postmaster notifications to Global Admins Copy all system generated Postmaster notifications to Domain Admins Do not allow anyone to forward mail to foreign domains Send anonymous usage data
	Ok Cancel Apply Help

Ne pas envoyer de message de bienvenue aux nouveaux comptes

Par défaut, MDaemon génère un message de bienvenue basé sur le fichierNEWUSERHELP.DAT et le distribue aux nouveaux utilisateurs lors de la création de leur compte. Activez cette commande si vous souhaitez empêcher la génération de ce message.

Envoyer une réponse aux messages de commande invalide

Par défaut, lorsque quelqu'un envoie un e-mail au Compte système qui ne contient pas de commande valide, MDaemon ne répond pas en envoyant un e-mail "Aucune commande valide trouvée ". Activez cette option si vous souhaitez envoyer une réponse à ces e-mails.

Soumettre les messages générés automatiquement au filtre de contenu et au Filtre antispam

Par défaut, les messages générés par le système sont traités par le Filtre de contenu et le Filtre anti-spam. Désactivez cette case à cocher si vous souhaitez qu'ils soient exclus du filtre de contenu et du filtre anti-spam.

Envoyer les messages transférés via le filtre de contenu et le filtre anti-spam

Cochez cette case si vous souhaitez que les messages transférés soient transférés via le Filtre de contenu et le Filtre anti-spam. Cette option est désactivée par défaut.

Envoyer les notifications d'état de remise via le Filtre de contenu et le Filtre anti-spam Activez cette option si vous souhaitez que les <u>messages DSN</u> soient envoyés via les filtres anti-spam et de contenu. Cette option est désactivée par défaut.

Désactiver le routage par dossiers pour tous les comptes

Cliquez sur cette option si vous souhaitez désactiver globalement la fonction de fonction de sous-adressage [817]. Le sous-adressage ne sera autorisé pour aucun compte, quels que soient les paramètres de chaque compte. Le paramètre de compte pour le sous-adressage se trouve sur la page<u>Paramètres de [815]</u> l'éditeur de compte.

Envoyer le résumé des statistiques au postmaster à minuit

Non par défaut, un rapport de statistiques sera envoyé au postmaster tous les soirs à minuit. Décochez cette case si vous ne souhaitez pas que le rapport soit envoyé. Cette option correspond à l'onglet<u>Statistiques</u> 21 situé sur l'écran principal de MDaemon.

L'exportation de comptes inclut les statistiques d'utilisation du disque (cela peut ralentir considérablement l'exportation)

Non (par défaut), les exportations de comptes n'incluent pas le nombre de fichiers sur le disque et l'espace consommé. Si vous souhaitez inclure ces informations dans les exportations, activez cette case à cocher. Cela risque toutefois de ralentir considérablement les exportations.

Les messages transférés à des hôtes spécifiques ne sont pas envoyés aux hôtes intelligents en cas d'erreurs ! TRANSFÉRER LEESSAGE !

Les Paramètres de transfert avancés de l'écran <u>Transfert de l</u>⁽⁷⁸⁰⁾Éditeur de comptes permettent de configurer les comptes de manière à ce qu'ils transfèrent les messages à un hôte intelligent spécifique plutôt que d'utiliser le processus de distribution standard de MDaemon. Par défaut, lorsque MDaemon rencontre une erreur de livraison lors d'une tentative de transfert, le message est placé dans la file d'attente des messages erronés. Activez cette option si vous souhaitez que MDaemon place le message dans la <u>File de relance</u> al pour d'autres tentatives de distribution en utilisant le processus de distribution normal de MDaemon.

Envoyer une copie des notifications du postmaster aux administrateurs globaux

Non (par défaut), les notifications générées par le système et envoyées au Postmaster seront également envoyées aux <u>Administrateurs globaux</u> [812]. Les administrateurs globaux reçoivent tout, y compris le rapport de synthèse de la file d'attente, le rapport de statistiques, les notes de mise à jour, le message " No Such User " (pour tous les domaines), les notifications d'erreurs de disque, les notifications de gel et de désactivation des comptes pour tous les domaines (qu'ils peuvent, comme les administrateurs de domaine, débloquer et réactiver), les avertissements concernant les licences et les versions de test bêta sur le point d'expirer, les rapports sur les spams, et ainsi de suite. Si vous ne souhaitez pas que vos Administrateurs globaux reçoivent ces notifications, désactivez ce paramètre.

Envoyer une copie des notifications du postmaster aux administrateurs de domaine

Par défaut, les notifications générées par le système et envoyées au Postmaster seront également envoyées aux <u>Administrateurs de domaine</u> [812]. Cependant, les Administrateurs de domaine ne peuvent recevoir que les courriels destinés à leur

domaine. Si vous ne souhaitez pas que vos Administrateurs de domaine reçoivent ces notifications, désactivez ce paramètre.

Interdire le transfert de courrier à des domaines externes

Cochez cette case si vous ne souhaitez pas autoriser le Transfert courrier à ce domaine à envoyer des e-mails en dehors du domaine. Si un utilisateur configure le Transfert de courrier de son compte pour qu'il soit envoyé à un domaine étranger, les adresses de transfert distantes sont ignorées. Ce paramètre ne s'applique qu'aux messages qui sont transférés à l'aide des options de transfert de courrier du compte. Ce paramètre s'applique uniquement aux messages qui sont transférés à l'aide des options de transfert de courrier du rabi

Envoyer des données d'utilisation anonymes

Par défaut, le serveur MDaemon envoie des données d'utilisation anonymes à MDaemon Technologies, afin d'améliorer le produit et ses fonctionnalités pour mieux répondre aux besoins de nos clients. Désactivez cette option si vous ne souhaitez pas nous envoyer ces informations d'utilisation anonymes. Voir notre <u>politique de</u> <u>confidentialité</u> pour plus d'informations.

3.13.2 Service Windows

₩indows Service	
Windows Service The name of the service is "MDaemon" Dependencies Start ser Remove Auto Manual Disa	rvice omatically nually abled
New dependency Add Remon The MD aemon service runs under the SYSTEM account by account does not have permission to access networked driv different account enter the account credentials below. Icocal System account This account:	ive service y default. This ves. To specify a
Logon name Password Domain Leave the Domain field blank to logon to the default domain.	1.

Service Windows

Lorsque MDaemon fonctionne en tant que service, sonnom est "MDaemon".

Dépendances

Utilisez cette option pour désigner tout service dont vous souhaitez exiger le fonctionnement **avant le** démarrage du service MDaemon.

De...

Il s'agit de l'état initial du service : démarrage automatique, démarrage manuel ou désactivé.

Installer/Supprimer le service

Cliquez sur ce bouton pour installer ou supprimer le service MDaemon.

Accès aux ressources réseau

Lorsque MDaemon est exécuté en tant que service Windows, il s'exécute par défaut sous le compte SYSTEM. Si ce compte n'a pas accès aux périphériques réseau, MDaemon ne pourra pas accéder au courrier si vous souhaitez le stocker sur d'autres ordinateurs de votre réseau local. En d'autres termes, MDaemon ne pourra pas accéder au courrier si vous souhaitez le stocker sur d'autres ordinateurs de votre réseau local, à moins que vous ne fournissiez les informations d'identification d'un compte pouvant être utilisé pour permettre au service MDaemon d'accéder aux partages du réseau. Si vous devez le faire, vous pouvez créer un compte utilisateur Windows spécialement conçu pour exécuter MDaemon avec les restrictions que vous souhaitez, mais qui a accès aux partages de réseau que vous voulez que MDaemon puisse utiliser. De plus, toutes les applications lancées par MDaemon utiliseront les mêmes informations d'identification.

Votre nom Identifiant

Votre nom est l'Identifiant du compte Windows sous lequel le service MDaemon doit s'exécuter.

Mot de passe

Il s'agit dumot de passe ducompte Windows.

Domaine

Il s'agit du domaine Windows sur lequel le compte réside. Laissez ce champ vide pour vous connecter au domaine par défaut.

3.14 eM Client

Cette page n'est disponible que dans l' interface web de<u>MDaemon</u> <u>Remote Admin</u> (MDRA).

Vous pouvez utiliser cette page pour gérer vos licences **eM Client** directement dans MDRA. A partir de cette page, les administrateurs globaux de MDaemon peuvent demander des licences eM Client, acheter des licences supplémentaires et gérer les

activations. eM Client est un excellent client de messagerie doté de toutes les fonctionnalités et d'une interface propre et facile à utiliser. Il offre également des fonctionnalités pour les calendriers, les tâches, les contacts, les notes et le chat. Il est disponible pour Windows et macOS (il existe également des clients gratuits pour Android et iOS). Pour en savoir plus sur la façon dont eM Client peut être exploité avec MDaemon, consultez : <u>https://mdaemon.com/pages/emclient-for-emaileM Client for Email.</u>

Licence eM Client

Les administrateurs globaux peuvent utiliser cette option pour demander une licence eM Client avec 3 activations client/appareil GRATUITES. Pour ce faire, utilisez la liste déroulante pour sélectionner le domaine MDaemon auquel vous souhaitez associer la licence, et cliquez sur **Demander une Licence** ci-dessous. Le "postmaster@[domaine sélectionné]" recevra un e-mail de MDaemon contenant un code de vérification pour confirmer qu'il s'agit bien d'une adresse valide à laquelle vous avez accès. Ce code expirera dans 24 heures. Dans le formulaire **Informations d'enregistrement de la licence**, après avoir saisi le code pour valider l'adresse e-mail "postmaster@" du domaine, remplissez le formulaire **Informations d'enregistrement de la licence** et cliquez sur **Soumettre**.

La licence sera associée au domaine sélectionné et vous permettra d'activer gratuitement jusqu'à trois clients sous la licence de ce domaine. Si vous hébergez plusieurs domaines sur votre serveur MDaemon, vous pouvez utiliser cette fonctionnalité pour demander une licence avec trois activations gratuites pour chacun de vos domaines. Les licences sont associées à des domaines organisationnels tels que "exemple.com". Exemple : tout sous-domaine, tel que "sub1.example.com", doit être couvert par la licence "example.com". Si vous souhaitez acheter plus de licences ou étendre une licence existante pour couvrir plus d'activations de licences, vous pouvez le faire en cliquant sur le bouton**\$ Acheter des licences** cidessus.

Licences

Cette zone contient une liste de toutes vos licences eM Client. Chaque entrée indique le domaine auquel elle est associée, la clé d'activation de la licence, le nombre de clients activés, ainsi que les dates d'émission et d'expiration. Sélectionnez une licence et cliquez sur **Copier la Clé d'activation dans le Copier-caisse** si vous devez la copier/coller dans un client/appareil ou l'envoyer à quelqu'un pour qu'il active un client. Dans le cas où une licence est sélectionnée, la liste de toutes les activations associées à cette licence sera affichée dans la section Activations de licences ci-dessous.

Activations de Licence

Cette zone affiche des Informations sur chaque activation associée à la licence sélectionnée ci-dessus. Elle répertorie le compte auquel elle est associée, sa date d'activation, son état actuel et d'autres informations. Cliquez sur n'importe quelle entrée pour **activer**, **désactiver** ou **supprimer l'** activation de ce client.
Section

4 Menu Sécurité

MDaemon est équipé d'un ensemble complet de fonctions et de contrôles de sécurité. Cliquez sur Sécurité dans labarre de menus de MDaemonpour accéder aux fonctions de sécurité suivantes :

- <u>Health Check</u> [st] Cette page fournit une liste pratique des paramètres de sécurité importants consolidés sur une seule page, et elle affiche la valeur actuelle de chaque paramètre ainsi que sa valeur par défaut. Lorsque ces valeurs diffèrent, le paramètre est mis en surbrillance afin que les Administrateurs globaux puissent rapidement passer en revue ces paramètres particuliers. Si nécessaire, les administrateurs peuvent sélectionner n'importe lequel de ces paramètres pour revenir à sa valeur par défaut, ou ils peuvent cliquer sur un lien à côté de n'importe quel paramètre pour passer à la page où se trouve ce paramètre. Dans ce cas, les administrateurs peuvent facilement annuler la dernière modification apportée sur la page Health Check. Ils peuvent également afficher les Modifications apportées à cette session navigateur, puis annuler des modifications spécifiques. Note : Cette option n'est disponible que dans l' interface web deMDaemon Remote Admin (MDRA) [376].
- AntiVirus all MDaemon AntiVirus peut vous aider à stopper les virus informatiques véhiculés par le courrier électronique en fournissant le plus haut niveau de protection intégrée disponible pour les clients de MDaemon. Il attrape, met en quarantaine, répare et/ou supprime tout message électronique contenant un virus. AntiVirus contient également une fonction appelée Protection instantanée, qui peut être utilisée pour vous protéger contre certaines épidémies de spam, d'hameçonnage et de virus qui peuvent parfois être ignorées par les autres mesures de sécurité traditionnelles, basées sur le contenu et les signatures.
- Filtre de contenu (a) un système de Filtrage de contenu très polyvalent et entièrement multithread vous permet de personnaliser le comportement du serveur en fonction du contenu des messages entrants et sortants. Vous pouvez insérer et supprimer des en-têtes, ajouter des pieds de page aux messages, supprimer des pièces jointes, envoyer des copies à d'autres utilisateurs, faire en sorte qu'un message instantané soit envoyé à quelqu'un, exécuter un programme suivant, et bien d'autres choses encore.
- Filtre anti-spam [725] utilise la technologie de filtrage des messages pour examiner de manière heuristique les messages électroniques afin de calculer un "score". Ce score est utilisé pour déterminer la probabilité qu'un message soit un spam. Sur la base de cette détermination, le serveur peut alors prendre certaines mesures telles que refuser ou marquer le message. Voir aussi : <u>Pièges</u> à spam [758]
- Liste blocage DNS [751] Vous permet de spécifier plusieurs services de listes blocage DNS qui seront vérifiés chaque fois que quelqu'un essaiera d'envoyer un message à votre serveur. Si l'IP de connexion est répertoriée par l'un de ces hôtes, le message sera refusé. Refususe les connexions provenant de cette IP permet de contrôler la nature des messages envoyés à votre serveur.
- <u>Contrôle des relais</u> permet de contrôler l'action de MDaemon lorsqu'un message qui n'est ni en provenance ni à destination d'une adresse locale arrive sur votre serveur de messagerie.

- **Bouclier IP** 5551: si un Nom de domaine spécifié dans cette liste tente de se connecter à votre serveur, son adresse IP doit correspondre à celle que vous lui avez attribuée.
- **Reverse Lookup** [548] MDaemon peut interroger les serveurs DNS pour vérifier la validité des noms de domaine et des adresses signalés dans les messages entrants. Les commandes de cet écran permettent de refuser les messages suspects ou d'y insérer un en-tête spécial. Les données de la recherche inversée seront également signalées dans les pas de journalisation de MDaemon.
- **POP avant SMTP** 552 les contrôles de cet écran permettent de requérir que chaque utilisateur accède d'abord à sa boîte aux lettres avant d'être autorisé à envoyer un message via MDaemon, authentifiant ainsi que l'utilisateur est un titulaire de compte valide et qu'il est autorisé à utiliser le système de messagerie.
- Écran d'IP Nom d'<u>hôte</u> 553 & IP : Domaine ou adresse IP qui seront considérés comme des exceptions aux règles de relais listées dans l'écran Contrôle des relais.
- <u>Authentification SMTP</u> [558] utilisé pour définir plusieurs options qui indiquent comment MDaemon se comportera lorsqu'un utilisateur envoyant un message à MDaemon a ou n'a pas été authentifié au préalable.
- SPF sol La plupart des domaines publient des enregistrements MX pour identifier les machines qui peuvent recevoir du courrier pour eux, mais cela n'identifie pas les emplacements autorisés à envoyer du courrier pour eux. Sender Policy Framework (SPF) est un moyen par lequel les domaines peuvent également publier des enregistrements "MX inversés" pour identifier les emplacements autorisés à envoyer des messages.
- DomainKeys Identified Mail set DomainKeys Identified Mail (DKIM) est un système de vérification par e-mail qui peut être utilisé pour empêcher l'usurpation d'identité. Il peut également être utilisé pour garantir l'intégrité des messages entrants, en s'assurant que le message n'a pas été modifié entre le moment où il a quitté le serveur de messagerie de l'expéditeur et celui où il est parvenu au vôtre. Pour ce faire, on utilise un système de paires de clés publiques/privées cryptées. Les messages entrants sont signés à l'aide d'une clé privée et les messages entrants voient leur signature vérifiée en les testant avec la clé publique publiée sur le serveur DNS de l'expéditeur.
- <u>Certification</u> La Certification des messages est un processus par lequel une entité se porte garante ou "certifie" la bonne conduite d'une autre entité en matière de courrier électronique. La fonction de Certification est avantageuse car elle permet de s'assurer que les messages ne seront pas soumis par erreur ou inutilement à l'analyse du Filtre anti-spam. Elle permet également de réduire les ressources nécessaires au traitement de chaque message.
- Liste d'autorisation d'expéditeurs (Sender Liste (Sender Liste)) de blocage) liste des adresses qui ne sont pas autorisées à envoyer du trafic de messagerie par l'intermédiaire de votre serveur.
- <u>Écran IP</u> sert à désigner les adresses IP à partir desquelles vous autoriserez ou refuserez les connexions à votre serveur.
- <u>Écran d'hôte</u> and permet de désigner les hôtes (noms de domaine) à partir desquels vous autoriserez ou refuserez les connexions à votre serveur.

- Écran dynamique Grâce à l'Écran dynamique, MDaemon peut suivre le comportement des connexions entrantes afin d'identifier les activités suspectes et de réagir en conséquence. Vous pouvez <u>bloquer</u> al les connexions d'<u>une</u> adresse IP al (ou d'une plage d'adresses) lorsqu'elle échoue à l'authentification un certain nombre de fois dans un laps de temps donné. Vous pouvez également <u>bloquer les comptes</u> ou tentent de s'authentifier lorsqu'ils échouent trop souvent et trop rapidement.
- <u>SSL & TLS</u> [613] MDaemon prend en charge le protocole Secure Sockets Layer (SSL) pour les protocoles SMTP, POP et IMAP, ainsi que pour le serveur web du Webmail. SSL est la méthode standard pour sécuriser les communications Internet entre le serveur et le client.
- **Protection contre la rétrodiffusion BAL** La rétrodiffusion fait référence aux messages de réponse que vos utilisateurs reçoivent pour des e-mails qu'ils n'ont jamais envoyés. Ce phénomène se produit lorsque des messages de spam ou des messages envoyés par des virus contiennent une adresse Return-Path falsifiée. La protection contre la rétrodiffusion permet d'éviter ce phénomène en garantissant que seuls les Notifications d'état de livraison et les Répondeurs automatiques légitimes sont livrés à vos comptes, en utilisant une méthode de hachage à clé privée pour générer et insérer un code spécial sensible au temps dans l'adresse de retour des messages sortants de vos utilisateurs.
- <u>Régulation de la bande passante</u> [337] La fonction de Régulation de la bande passante vous permet de contrôler la consommation de la bande passante utilisée par MDaemon. Vous pouvez contrôler la vitesse à laquelle les sessions ou les services progressent, en définissant des taux différents pour chacun des principaux services de MDaemon par domaine, y compris les domaines et les passerelles de domaine.
- **Tarpitting** [41] permet de ralentir délibérément une connexion une fois qu'un certain nombre de commandes RCPT ont été reçues de l'expéditeur d'un message. Cette technique vise à décourager les spammeurs d'essayer de vous envoyer des e-mails en masse non sollicités. L'hypothèse sous-jacente à cette technique est que si les spammeurs mettent un temps anormalement long à envoyer chaque message, cela les dissuadera d'essayer de recommencer à l'avenir.
- **Greylisting** [43] Le greylisting est une technique de lutte contre le spam qui exploite le fait que les serveurs SMTP réessayent de livrer tout message qui reçoit un code d'erreur temporaire (c.-à-d. "réessayez plus tard"). Grâce à cette technique, lorsqu'un message arrive d'un expéditeur qui ne figure pas sur la liste d'autorisation ou qui est inconnu, son expéditeur, son destinataire et l'adresse IP du serveur d'envoi sont enregistrés, puis le message est refusé par Greylisting avec un code d'erreur temporaire au cours de la session SMTP. . then, when the legitimate servers attempt to deliver the messages again a few minutes later, they will be accepted. Étant donné que les spammeurs n'effectuent généralement pas d'autres tentatives de livraison, le Greylisting peut contribuer à réduire considérablement le nombre de spams reçus par vos utilisateurs.
- **IP locales** [647]: cet écran permet de répertorier les adresses IP qui résident sur votre réseau local (LAN). Ces adresses IP sont donc traitées comme du trafic local aux fins de la régulation de la bande passante et peuvent être exemptées de diverses autres restrictions en matière de sécurité et de prévention du spam.

 <u>Politique du site</u> 648: permet de créer une politique du site qui sera transmise aux serveurs d'envoi au début de chaque session de courrier SMTP. Un exemple de Politique du site courante est : "Ce serveur ne fait pas de relais".

4.1 Health Check

Cette page fournit une liste pratique des paramètres de sécurité importants consolidés sur une seule page, et affiche la valeur actuelle et la valeur par défaut de chaque paramètre. Lorsque ces valeurs diffèrent, le paramètre est mis en surbrillance afin que les Administrateurs globaux puissent rapidement examiner ces paramètres particuliers et les restaurer à leurs valeurs par défaut si nécessaire. Chaque groupe de paramètres est accompagné d'une icône de raccourci qui permet d'accéder à la page où se trouvent ces paramètres. En outre, vous pouvez également afficher une liste de tous les Changements Health Check apportés à cette session du navigateur, et annuler l'un de ces changements si nécessaire. **Note :** Cette fonctionnalité n'est disponible que dans l' interface web de<u>MDaemon Remote Admin (MDRA</u> [376]).

Restaurer les paramètres (Paramètres par défaut)

Pour Restaurer les paramètres par défaut :

- 1. Cliquez sur un ou plusieurs paramètres souhaités.
- 2. Cliquez sur **Restaurer les paramètres par défaut** dans la barre d'outils.

Annuler la dernière action

Cliquez sur **Annuler dernière action** dans la barre d'outils si vous utilisez Health Check pour effectuer une modification et que vous souhaitez ensuite l'annuler immédiatement.

Révision/annulation des Changements de session

Cliquez sur **Modifications apportées à cette** session pour consulter la liste des modifications apportées au Health Check au cours de la session du navigateur. Si vous souhaitez annuler l'une des modifications répertoriées, cochez la case située à côté de l'une d'entre elles et cliquez sur **Annuler sélection**. Si vous souhaitez effacer la liste des changements de session, cliquez sur **Effacer**. Cette opération ne modifie aucun paramètre et ne peut être annulée.

Les valeurs par défaut de ces paramètres de sécurité ne sont pas nécessairement celles qui conviennent le mieux à votre configuration particulière. Soyez prudent lorsque vous utilisez Health Check pour effectuer des modifications.

4.2 Gestionnaire de sécurité

4.2.1 Paramètres de sécurité

4.2.1.1 Contrôle de relais

🧐 Paramètres de sécurité - Contrôle de relais	
 Paramètres de sécurité - Contrôle de relais Contrôle de relais Vérification inverse POP avant SMTP Hôtes autorisés IP autorisées Authentification de l'expéditeur Analyse SSL & TLS Autres 	Interdire le relais du courrier Interdire le relais du courrier Interdire le message est destiné à un alias connu Interdire le message provient d'une session SMTP authentifiée Insauf si le message provient d'une IP ou d'un hôte autorisés Insauf si le message provient d'une passerelle Exiger une valeur SMTP MAIL valide si elle utilise un domaine local Insauf si le message provient d'une IP autorisée Exiger une valeur SMTP RCPT valide si elle utilise un domaine local Insauf si le message provient d'une IP autorisée Exiger une valeur SMTP RCPT valide si elle utilise un domaine local Insauf si le message provient d'une IP autorisée Insauf si le message provient d'une session SMTP authentifiée Insauf si le message provient d'une IP autorisée
	OK Annuler Appliquer Aide

Utilisez le contrôle des relais sous Sécurité | Paramètres de sécurité | Contrôle des relais pour définir la manière dont votre serveur réagit au relayage du courrier. Lorsqu'un message arrivant à votre serveur de messagerie ne provient pas d'une adresse locale et n'y est pas destiné, il est demandé à votre serveur de relayer (c'està-dire de délivrer) le message pour le compte d'un autre serveur. Si vous ne souhaitez pas que votre serveur relaie le courrier pour des utilisateurs inconnus, vous pouvez utiliser les paramètres fournis ici pour le contrôler.

> Le fait de relayer du courrier électronique sans discernement pour d'autres serveurs peut entraîner le blocage de votre domaine par un ou plusieurs serveurs. bloqué par un ou plusieurs <u>services DNS-BL</u> [751]. Le relais ouvert est fortement déconseillé car les spammeurs exploitent les serveurs ouverts pour dissimuler leurs traces.

Relais du courrier

Ne pas autoriser le relais de messages

Lorsque cette option est activée, MDaemon refuse de prendre en charge les messages qui proviennent d'un utilisateur non local et qui lui sont destinés.

... sauf s'ils sont adressés à un Alias connu

Cochez cette case si vous souhaitez que MDaemon relaie le courrier pour les <u>alias</u> [84], quels que soient vos paramètres de relais.

...sauf s'il est envoyé via une session SMTP authentifiée

Lorsque cette case est cochée, MDaemon relaie toujours le courrier lorsqu'il est envoyé via une session SMTP authentifiée.

...sauf s'il est envoyé à partir d'un hôte ou d'une IP autorisée

Activez cette option si vous souhaitez autoriser le relais lorsque le courrier provient d'un Hôtes autorisés ou d'une Adresse IP autorisée.

...sauf s'il est envoyé par un utilisateur de passerelle

Activer cette option si vous souhaitez que MDaemon autorise le relais du courrier par le biais de passerelles de domaine, quels que soient vos paramètres Relayer. Cette fonctionnalité est désactivée par défaut et n'est pas recommandée.

Vérification des comptes

L'adresse SMTP MAIL doit exister si elle utilise un domaine local.

Cochez cette option si vous souhaitez vérifier que la valeur MAIL transmise au cours du processus SMTP pointe vers un compte valide lorsqu'elle est censée provenir d'un domaine ou d'une passerelle locale.

...sauf s'il est envoyé via une session SMTP authentifiée

Cliquez sur cette option si vous souhaitez exempter un message de l' option*SMTP MAIL address must exist...* lorsqu'il est envoyé via une session SMTP authentifiée.

...sauf s'il est envoyé à partir d'un hôte ou d'une IP autorisés

Cliquez sur cette option si vous souhaitez exempter un message de l 'option*SMTP MAIL address must exist*... lorsqu'il est envoyé à partir d'une adresse IP autorisée.

L'adresse SMTP RCPT doit exister si elle utilise un domaine local

Cliquez sur cette option si vous souhaitez vérifier que la valeur RCPT transmise au cours du processus SMTP pointe vers un compte valide réel lorsqu'elle est censée provenir d'un domaine local.

...sauf s'il est envoyé via une session SMTP authentifiée

Cliquez sur cette option si vous souhaitez exempter un message de l' option*SMTP RCPT address must exist...* lorsqu'il est envoyé via une session SMTP authentifiée.

...sauf s'il est envoyé à partir d'un hôte ou d'une IP autorisés

Cliquez sur cette option si vous souhaitez exempter un message de l 'option*SMTP RCPT address must exist*... lorsqu'il est envoyé à partir d'une adresse IP autorisée.

4.2.1.2 Vérification inverse

Security Manager - Reverse Lookups		×
Security Settings Relay Control	Perform PTR lookup on inbound SMTP connections Send 501 and close connection if no PTR record exists (caution) Send 501 and close connection if no PTR record match Exempt authenticated sessions Exe Perform lookup on HELO/EHLO domain	mpt list
Sender Authentication Screening SSL & TLS Other	Send 501 and close connection on forged identification (caution) Refuse to accept mail if a lookup returns 'domain not found' send 501 error code (normally sends 451 error code) and then close the connection ✓ Exempt authenticated sessions	mpt list
	Perform lookup on domain passed in the MAIL command Send 501 and close connection on forged identification (caution) Refuse to accept mail if a lookup returns no MX records (caution) Refuse to accept mail if a lookup returns 'domain not found' send 501 error code (normally sends 451 error code) and then close connection Exe	mpt list
	Ok Cancel Apply	Help

Les options de cet écran permettent de configurer MDaemon pour qu'il effectue une recherche inversée sur le domaine transmis dans les commandes HELO/EHLO et MAIL. Lors de cette recherche, MDaemon tente d'obtenir toutes les adresses IP des enregistrements MX et A pour le domaine en question. Dans ce cas, l'adresse IP du serveur qui établit la connexion est comparée à cette liste afin de déterminer si l'expéditeur utilise une identité falsifiée.

Vous pouvez également effectuer des recherches inversées sur les enregistrements de pointeurs (PTR) des adresses IP entrantes. Si vous utilisez cette option, la connexion peut être interrompue ou un en-tête d'avertissement peut être inséré dans le message si l'adresse IP entrante ne contient pas d'enregistrement PTR.

Enfin, il est généralement accepté que l'acceptation du courrier provenant de sources qui s'identifient en utilisant un domaine qui n'existe pas soit facultative. C'est pourquoi il existe un commutateur qui vous permet de refuser les messages pour lesquels le processus de recherche inversée renvoie un message "domaine non trouvé" du serveur DNS. Dans ce cas, MDaemon renvoie un code d'erreur 451, refuse d'accepter le message, puis autorise la poursuite de la session SMTP. Cependant, si vous souhaitez renvoyer un code d'erreur501, fermer la connexion ou faire les deux, d'autres commutateurs sont prévus à cet effet.

Les adresses IP autorisées et localhost (127.0.0.1) sont toujours exemptées des recherches inversées.

Effectuer une recherche PTR sur les connexions SMTP entrantes

Activez cette option si vous souhaitez que MDaemon effectue des recherches d'enregistrements de pointeurs sur toutes les connexions SMTP en entrée.

...envoyer 501 et fermer la connexion si aucun enregistrement PTR n'existe (attention)

Si cette case est cochée, MDaemon enverra un code d'erreur501 (erreur de syntaxe dans les paramètres ou les arguments) et fermera la connexion si aucun enregistrement PTR n'existe pour le domaine.

...envoyer 501 et fermer la connexion si aucun enregistrement PTR ne correspond Si cette case est cochée, MDaemon enverra un code d'erreur501 (erreur de syntaxe dans les paramètres ou les arguments) et fermera la connexion si le résultat de la recherche d'un enregistrement PTR ne correspond pas.

Exempter les sessions authentifiées

Si vous souhaitez différer la recherche PTR sur les connexions SMTP entrantes jusqu'à la fin de la commande SMTP MAIL' afin de savoir si la connexion utilise l'authentification ou non, cochez cette option.

Liste des exceptions

Cliquez sur ce bouton pour ouvrir la liste d'exemption de la recherche PTR Exempter des IP, dans laquelle vous pouvez spécifier les adresses IP qui seront exemptées des recherches inversées PTR.

Effectuer la recherche sur le domaine HELO/EHLO

Cochez cette case si vous souhaitez qu'une recherche soit effectuée sur le Nom de domaine qui est signalé pendant la partie HELO/EHLO de la session. La commande HELO/EHLO est utilisée par le client (machine émettrice) pour s'identifier auprès du serveur. Le nom de domaine transmis par le client dans cette commande est utilisé par le serveur pour remplir la partie from de l 'en-têteReceived.

...envoyer 501 et fermer la connexion en cas de fausse identification (attention) Cochez cette case si vous voulez qu'un code d'erreur 501 soit envoyé et que la connexion soit fermée lorsque le résultat de la recherche semble être une fausse identification.



Lorsque le résultat d'une recherche inversée indique que le serveur utilise une identification falsifiée, ce résultat peut souvent être incorrect. Il est très fréquent que les serveurs de messagerie s'identifient avec des valeurs qui ne contiennent pas leurs adresses IP. Cela peut être dû à des limitations et à des restrictions imposées par les fournisseurs d'accès à Internet ou à d'autres raisons légitimes. C'est pourquoi il convient de faire preuve de prudence avant d'activer cette option. Il est probable que l'utilisation de cette option conduise votre serveur à refuser certains messages légitimes.

Refuser d'accepter le courrier si une recherche renvoie la mention "domaine non trouvé".

Dans le cas d'une recherche dont le résultat est "domaine non trouvé", l'activation de cette option entraînera le refus du message avec un code d'erreur451 (Requested action aborted : local error in processing), puis la session sera autorisée à se dérouler normalement jusqu'à son terme.

... envoyer un code d'erreur 501 (envoie normalement un code d'erreur 451)

Activez cette case à cocher si vous souhaitez que le code d'erreur envoyé en réponse à un résultat "domain not found" soit 501 (erreur de syntaxe dans les paramètres ou les arguments) au lieu de 451.

... puis fermer la connexion

Cochez cette case si vous voulez que la connexion soit fermée immédiatement au lieu d'être autorisée à progresser lorsque le résultat de la recherche inversée est "domaine non trouvé".

Exempter les sessions authentifiées

Cochez cette option si vous souhaitez différer la recherche jusqu'à la fin de la commande SMTP MAIL afin de voir si la connexion utilisera ou non l'authentification.

Liste d'exceptions

Cliquez sur ce bouton pour ouvrir la liste HELO/EHLO Lookup pour dresser la liste des adresses IP et des noms de domaine ou d'hôte des sites que vous souhaitez exclure des recherches inversées HELO/EHLO.

Effectuer une recherche sur la valeur transmise dans la commande MAIL

L'activation de ce commutateur permet d'effectuer une recherche sur le Nom de domaine transmis lors de la commande MAIL de la transaction de courrier. Dans la commandeMAIL, l'adresse transmise est censée être le chemin inverse du message et correspond généralement à la boîte aux lettres d'où provient le message. Parfois, cependant, il s'agit de l'adresse vers laquelle les messages d'erreur doivent être dirigés.

... envoyer 501 et fermer la connexion en cas de fausse identification (attention)

Cochez cette case si vous souhaitez qu'un code d'erreur 501 soit envoyé et que la connexion soit fermée lorsque le résultat d'une recherche semble être une fausse identification.

Lorsque le résultat d'une recherche inversée indique que le serveur utilise une identification falsifiée, ce résultat peut souvent être incorrect. Il est très fréquent que les serveurs de messagerie s'identifient avec des valeurs qui ne contiennent pas leurs adresses IP. Cela peut être dû à des limitations et à des restrictions imposées par les fournisseurs d'accès à Internet ou à d'autres raisons légitimes. C'est pourquoi il convient de faire preuve de prudence avant d'activer cette option. Il est probable que l'utilisation de cette option conduise votre serveur à refuser certains messages légitimes.

Refuser d'accepter du courrier si la recherche ne renvoie aucun enregistrement MX (prudence)

Cochez cette case si vous souhaitez refuser le courrier provenant de domaines qui n'ont pas d'enregistrements MX. Cette option est désactivée par défaut et doit être utilisée avec prudence, car les domaines n'ont pas besoin d'enregistrements MX pour exister, être valides ou envoyer/recevoir du courrier.

Refuser d'accepter le courrier si une recherche renvoie "domaine introuvable". Dans le cas d'une recherche dont le résultat est "domaine non trouvé", l'activation de cette option entraînera le refus du message avec un code d'erreur451 (action demandée interrompue : erreur locale dans le traitement), puis la session sera autorisée à se poursuivre normalement jusqu'à son terme.

... envoyer un code d'erreur 501 (envoie normalement un code d'erreur 451) Activez cette case à cocher si vous souhaitez que le code d'erreur envoyé en réponse à un résultat "domain not found" soit 501 (erreur de syntaxe dans les paramètres ou les arguments) au lieu de 451.

... puis fermer la connexion

Cochez cette case si vous voulez que la connexion soit fermée immédiatement au lieu d'être autorisée à progresser lorsque le résultat de la recherche inversée est "domaine non trouvé".

Liste des exceptions

Cliquez sur ce bouton pour ouvrir la liste d'exclusion de la recherche de courrier. Exceptions. Vous pouvez y désigner les adresses IP et les noms de domaine ou d'hôte des sites que vous souhaitez exempter des recherches inversées de MAIL.

4.2.1.3 POP avant SMTP



POP avant SMTP

L'expéditeur local doit avoir accédé à sa boîte aux lettres au cours des [xx] dernières minutes. [xx] dernières minutes.

Dans ce cas, chaque fois qu'un message est censé provenir d'un utilisateur local, ce compte utilisateur doit s'être connecté et avoir consulté sa boîte aux lettres locale au cours du nombre de minutes spécifié avant d'être autorisé à envoyer du courrier.

Ne pas appliquer POP avant SMTP aux messages collectés via ATRN

Cochez cette case si vous souhaitez que les messages collectés via <u>ATRN</u> resident pas soumis à la restriction POP avant SMTP.

Ne pas appliquer le protocole POP avant SMTP aux messages envoyés aux comptes locaux

Cochez cette case si vous souhaitez que les messages envoyés d'un utilisateur local à un autre soient exemptés de la restriction POP avant SMTP. Normalement, MDaemon applique cette exigence dès que l'expéditeur est connu, mais lorsque cette option est activée, MDaemon attend que le destinataire du message soit connu avant de déterminer si cette exigence est nécessaire ou non.

Ne pas appliquer POP avant SMTP aux messages provenant d'IP autorisées

Si cette case est activée, les messages arrivant d'une adresse IP répertoriée dans l'écran<u>Hôtes autorisés</u> seront exemptés de la fonction POP avant SMTP.



Vous pouvez exempter les sessions authentifiées de la restriction POP avant SMTP via une option de l' écran<u>Authentification SMTP</u> [558].

4.2.1.4 Hôtes autorisés

🧐 Paramètres de sécurité - Hôtes autorisés		—
Paramètres de sécurité Contrôle de relais Vérification inverse POP avant SMTP Hôtes autorisés Pautorisées Authentification de l'expéditeur Analyse SSL & TLS Autres	Hôtes autorisés	Supprimer
	OK Annuler	Appliquer Aide

Dans diverses boîtes de dialogue et fonctions de sécurité de MDaemon, des options vous permettent de choisir si les "Hôtes autorisés" ou les "Domaines autorisés" seront des exceptions ou des exemptions à ces options. Les hôtes que vous listez dans cet écran sont ceux auxquels ces options font référence.

Hôtes autorisés

Il s'agit de la liste des hôtes qui seront exemptés de certaines options de sécurité désignées.

Nouvel hôte autorisé

Ajoutez un nouvel hôte à la liste deshôtes autorisés.

Commentaire

Utilisez ceci pour tout texte de commentaire sur une entrée.

Ajouter

Cliquez sur ce bouton pour ajouter le nouveau domaine à laliste des Hôtes autorisés .

Supprimer

Cliquez sur ce bouton pour supprimer les entrées sélectionnées de la liste des *Hôtes autorisés*.

4.2.1.5 IP autorisées

🧐 Paramètres de sécurité - IP autorisées	×
	A design ID as here for
Paramètres de sécurité Contrôle de relais Vérification inverse POP avant SMTP Hôtes autorisés Paramètres Authentification de l'expéditeur Analyse SL & TLS Autres	Adresses IP autorisées
	OK Annuler Appliquer Aide

Dans diverses boîtes de dialogue et fonctions de sécurité de MDaemon, des options vous permettent de choisir si les " IP autorisées " seront des exceptions ou des exemptions à ces options. Les adresses IP que vous listez dans cet écran sont celles auxquelles ces options font référence.

Adresses IP autorisées

Il s'agit de la liste des adresses IP qui seront exemptées de certaines options de sécurité désignées.

Nouvelle IP autorisée

Saisissez une nouvelle adresse IP à ajouter à la liste des Adresses IP autorisées.

Commentaire

Utilisez ce texte pour tout commentaire concernant une entrée.

Ajouter

Cliquez sur ce bouton pour ajouter la nouvelle adresse IP à laliste des Adresses IP autorisées .

Supprimer

Cliquez sur ce bouton pour supprimer les entrées sélectionnées de la liste *Adresses IP autorisées*.

4.2.2 Authentification de l'expéditeur

4.2.2.1 Bouclier IP

IP Utilisez \$LOCALDOMAIN\$ pour indiquer les domaines et les passerelles locaux. Notation CIDR et caractères jokers * ? # acceptés. Ne pas appliquer le Bouclier IP aux messages envoyés à des utilisateurs locaux valides Ne pas appliquer le Bouclier IP aux sessions authentifiées Ne pas appliquer le Bouclier IP aux IP autorisées Appliquer le Bouclier IP aux alias Vérifier les adresses des en-têtes FROM avec le Bouclier IP	Paramètres de sécurité - Bouclier IP Paramètres de sécurité Authentification de l'expéditeur Authentification SMTP Authentification SPF Vérification DKIM Signature DKIM Paramètres DKIM Vérification DMARC Rapports DMARC Paramètres DMARC Certification VBR Definition VBR Defi	Avec le Bouclier IP, les domaines ci-dessous ne peuvent être utilisés dans une valeur SMTP MAIL (et optionnellement un en-tête FROM) que s'ils proviennent des IP indiquées. Activer le Bouclier IP \$LOCALDOMAIN\$, 10.0.0.0/8 \$LOCALDOMAIN\$, 172.16.0.0/12 \$LOCALDOMAIN\$, 192.168.0.0/16 \$LOCALDOMAIN\$, 127.0.0.1/8 Par défaut Domaine
	Rapports DMARC Paramètres DMARC Certification VBR Domaines acceptés Analyse SSL & TLS Autres	Image: Part défaut Domaine IP Utilisez \$LOCALDOMAIN\$ pour indiquer les domaines et les passerelles locaux. Notation CIDR et caractères jokers * ? # acceptés. Image: Ne pas appliquer le Bouclier IP aux messages envoyés à des utilisateurs locaux valides Image: Ne pas appliquer le Bouclier IP aux sessions authentifiées Image: Ne pas appliquer le Bouclier IP aux IP autorisées Image: Ne pas appliquer le Bouclier IP aux alias Image: Népliquer le Bouclier IP aux alias

Le Bouclier IP, situé dans le menu Sécurité | Paramètres de sécurité | Authentification de l'expéditeur, est une liste de noms de domaines et d'adresses IP correspondants qui seront vérifiés lors de la commandeMAIL From au cours de la session SMTP. Une session SMTP prétendant provenir d'une personne de l'un des domaines répertoriés ne sera honorée que si elle provient de l'une des adresses IP associées. Par exemple, supposons que votre nom de domaine soit example.com et que les ordinateurs de votre réseau local utilisent des adresses IP dans la plage de 192.168.0.0 à 192.168.0.255. Grâce à ces informations, vous pouvez configurer le Bouclier IP de manière à associer le Nom de domaine .com à la plage d'adresses IP 192.168.0.* (les caractères génériques sont autorisés). Si, à chaque fois qu'un ordinateur se connecte à votre serveur SMTP et déclare "MAIL

DE <someone@example.com>", la session SMTP ne se poursuivra que si l'ordinateur connecté possède une adresse IP comprise dans la plage requise de 192.168.0.0 à 192.168.0.255.

Activer le Bouclier IP

Décochez cette case si vous souhaitez désactiver le Bouclier IP. Le Bouclier IP est activé par défaut.

Nom de domaine

Saisissez le nom du domaine que vous souhaitez associer à une plage d'adresses IP spécifique. Vous pouvez également utiliser la macro *\$LOCALDOMAIN\$* pour couvrir tous les domaines locaux (y compris les passerelles). Si vous utilisez cette macro, il ne sera pas nécessaire de maintenir le Bouclier IP à jour lorsque les domaines locaux ou les passerelles changent. Par défaut, des entrées sont ajoutées au Bouclier IP associant toutes les plages d'adresses IP réservées à *\$LOCALDOMAIN\$*.

Adresse IP

Saisissez l'adresse IP que vous souhaitez associer à un nom de domaine. Vous devez saisir cette adresse sous forme décimale pointée.

Ajouter

Cliquez sur le bouton*Ajouter* pour ajouter le domaine ou l'adresse IP à la liste.

Supprimer

Cliquez sur ce bouton pour supprimer les entrées sélectionnées de la liste.

Ne pas appliquer le Bouclier IP aux messages envoyés aux utilisateurs locaux valides

Cliquez sur cette option si vous souhaitez que seuls les messages destinés à un utilisateur non local ou à un utilisateur local non valide fassent l'objet d'une vérification de concordance entre le domaine ou l'adresse IP. Cela empêchera d'autres personnes de se faire passer pour l'un de vos utilisateurs locaux afin de relayer leur courrier via votre serveur, mais cela permettra d'économiser des ressources en ne vérifiant pas les messages adressés à vos utilisateurs. Si vous activez à la fois cette option et l' option*Bouclier IP honore les alias* ci-dessous, les messages adressés à des alias valides seront également acceptés.

Ne pas appliquer le Bouclier IP aux sessions authentifiées

Lorsque cette option est activée, les restrictions du Bouclier IP ne s'appliquent pas aux utilisateurs authentifiés. Le courrier d'un utilisateur authentifié sera accepté quelle que soit l'adresse IP à partir de laquelle il se connecte. Dans le cas où un utilisateur ne s'authentifie pas et que l'accès est refusé, le message renvoyé au client SMTP sera "Authentification requise" afin de donner à l'utilisateur un indice lui permettant de résoudre le problème en configurant le client de messagerie pour qu'il utilise l'authentification avant d'envoyer un message. Cette option est activée par défaut.

Ne pas appliquer le Bouclier IP aux IP autorisées

Lorsque cette commande est activée, le Bouclier IP ne sera pas appliqué lorsque la connexion provient d'une <u>adresse IP autorisée</u> [553]. Cette option est activée par défaut.

Bouclier IP honore les alias

Activez cette option si vous souhaitez que le Bouclier IP honore les alias d'adresse lors de la vérification des boucliers de domaine ou d'adresse IP. Le Bouclier IP traduira un alias en véritable compte vers lequel il pointe et l'honorera donc s'il passe le bouclier. Si cette option n'est pas activée, le Bouclier IP traitera chaque alias comme s'il s'agissait d'une adresse indépendante du compte qu'il représente. Ainsi, si l'adresse IP d' un alias ne respecte pas le Bouclier IP, le message sera refusé. Cette option est reproduite dans l'<u>écran Paramètres</u> des alias - la modification du paramètre ici sera répercutée dans l'<u>écran Paramètres</u>.

Si vous souhaitez que les messages entrants adressés à des Alias valides soient exemptés du Bouclier IP, cliquez à la fois sur cette option et sur l' option*Ne pas appliquer le Bouclier IP aux messages envoyés à des utilisateurs locaux valides* cidessus.

Vérifier l'adresse de l'en-tête FROM par rapport au Bouclier IP

Cochez cette case si vous souhaitez que le Bouclier IP compare l'adresse figurant dans l'en-tête FROM du message en plus de celle figurant dans la valeur SMTP MAIL. Cette option est désactivée par défaut.



Utiliser cette option pourrait causer des problèmes avec certains types de messages, tels que ceux provenant de listes diffusion. Elle ne doit donc être activée que si vous êtes sûr d'en avoir besoin.

4.2.2.2 Authentification SMTP

558

💛 Security Manager - SMTP Authentication		×
Security Settings Sender Authentication IP Shield SFF Verification DKIM Verification DKIM Signing DKIM Settings DMARC Verification DMARC Reporting DMARC Settings VBR Certification Approved List SSL & TLS Other	 SMTP Authentication (AUTH) Authentication is extremely important for email security and should almost always be required. Authentication is always required when mail is sent from local account unless mail is sent to a local account unless Domain Sharing finds the sender on another server Authentication is always required when mail is sent from local IPs Credentials used must match those of the return-path address Credentials used must match those of the 'From' header address Exempt list Mail from 'postmaster', 'abuse', 'webmaster' must be authenticated Do not apply POP Before SMTP to authenticated sessions Do not allow authentication on the SMTP pott add their IP to the Dynamic Screen if they attempt it anyway 	
	Ok Cancel Apply He	lp

Authentification SMTP (AUTH)

Exiger une authentification lorsque le courrier provient de comptes locaux

Lorsque cette option est activée et qu'un message entrant prétend provenir de l'un desdomaines deMDaemon, le compte doit d'abord être authentifié ou MDaemon refusera d'accepter le message pour distribution. Cette option est activée par défaut.

...sauf si le message est destiné à un compte local

Si vous demandez une authentification requise lorsqu'un message provient d'un expéditeur local, mais que vous souhaitez ignorer la restriction d'authentification lorsque le destinataire est lui aussi local, cliquez sur cette option. Remarque : cela peut s'avérer nécessaire dans certaines situations où vous exigez que certains de vos utilisateurs utilisent des serveurs de messagerie différents pour le courrier sortant et le courrier entrant.

...sauf si le Partage de domaine trouve l'expéditeur sur un autre serveur

Par défaut, lorsque <u>le Partage de domaine</u> [113] trouve l'expéditeur sur un autre serveur, cet expéditeur sera exempté de l' option*L'authentification est toujours requise...* ci-dessus. Décochez cette case si vous souhaitez également requérir l'authentification de ces expéditeurs.

Aucune authentification requise lorsque le courrier est envoyé à partir d'IP locales Activez cette option si vous souhaitez exiger l'authentification lorsqu'un message entrants est envoyé à partir d'une adresse IP locale. Si le message n'est pas authentifié, il sera rejeté. Les IP autorisées sont exemptées et cette option est activée par défaut pour les nouvelles installations.

Les informations d'identification utilisées doivent correspondre à celles de l'adresse du chemin de retour

Dans le défaut, les paramètres utilisés lors de l'authentification SMTP doivent correspondre à ceux de l'adresse trouvée dans le chemin de retour du message. Désactivez cette option si vous ne voulez pas que le chemin de retour corresponde. Pour prendre en charge le stockage et le transfert du courrier de la passerelle, il existe une option correspondante située dans l'écran<u>Paramètres globaux de la passerelle</u> 2004 qui "Exclut le courrier de la passerelle des obligations de correspondance AUTH" par défaut.

Les informations d'identification utilisées doivent correspondre à celles de l'adresse de l'en-tête "From :".

Non par défaut, les informations d'identification utilisées lors de l'authentification SMTP doivent correspondre à celles de l'adresse figurant dans l'en-tête "From :" du message. Désactivez cette option si vous ne souhaitez pas que l'adresse dans l'en-tête FROM : corresponde. Pour prendre en charge le stockage et le transfert du courrier de la passerelle, il existe une option correspondante située dans l'écran <u>Paramètres globaux de la passerelle</u> a qui "Exclut le courrier de la passerelle des obligations de correspondance AUTH" par défaut.

Liste des exceptions

Utilisez la liste d'exemption de correspondance d'informations d'identification pour exempter une adresse des options"*Les informations d'identification utilisées doivent correspondre…*" ci-dessus. Pour être exemptée de l'option "*...must match those of the return-path* address", l'adresse exemptée doit correspondre à l'adresse du chemin de retour du message. Pour être exemptée de l'option "*...must match those of the 'From:' header address*", l'adresse exemptée doit correspondre à l'adresse du l'option "*...must match those of the 'From:' header address*", l'adresse exemptée doit correspondre à l'adresse du chemin de retour du message. Pour être exemptée doit correspondre à l'adresse doit correspondre à l'adresse doit correspondre à l'adresse doit correspondre à l'adresse doit correspondre doit correspondre à l'adresse doit correspondre à l'adresse doit correspondre à l'adresse doit correspondre à l'adresse doit correspondre doit correspondre à l'adresse doit correspondre doit correspondre doit correspondre à l'adresse doit correspondre doit correspondre à l'adresse doit correspondre do

Les messages provenant de 'Postmaster', 'abuse', 'webmaster' doivent être authentifiés Cochez cette case pour exiger que les messages provenant de l'un de vos alias ou comptes " postmaster@... ", " abuse@... " ou " webmaster@... " soient authentifiés avant que MDaemon ne les accepte. Les spammeurs et les pirates informatiques savent que ces adresses peuvent exister et peuvent donc tenter d'utiliser l'une d'entre elles pour envoyer du courrier via votre système. Cette option les empêchera, ainsi que d'autres utilisateurs non autorisés, de le faire. Cette option est reproduite dans l'écran Paramètres d' Best Alias. Si vous modifiez le paramètre ici, il sera également modifié dans cet écran.

Ne pas appliquer POP avant SMTP aux sessions authentifiées

Si vous utilisez la fonction de sécurité<u>POP avant SMTP</u> [552], vous pouvez cliquer sur cette option pour exempter les utilisateurs authentifiés de cette restriction. Un

utilisateur authentifié n'aura pas besoin de vérifier son courrier électronique avant d'envoyer des messages.

Ne pas autoriser l'authentification sur le Port SMTP

Cette option désactive la prise en charge de l'AUTH sur le Port SMTP. AUTH ne sera pas proposé dans la réponse EHLO et sera traité comme une commande inconnue si elle est fournie par le client SMTP. Ce paramètre et l'option"...ajouter leur IP à l'Écran dynamique" ci-dessous sont utiles dans les configurations où tous les comptes légitimes utilisent le port MSA ou un autre port pour envoyer du courrier authentifié. Dans ce type de configuration, on suppose que toute tentative d'authentification sur le Port SMTP doit provenir d'un pirate.

...ajouter leur IP à l'Écran dynamique s'ils tentent quand même de le faire.

Lorsque vous utilisez l'option*Ne pas autoriser l'authentification sur le port SMTP* ci-dessus, cette option ajoute à l'Écran dynamique l'adresse IP de tout client qui tente malgré tout de s'authentifier sur le port SMTP. La connexion sera également immédiatement interrompue.

4.2.2.3 Vérification SPF

🧐 Paramètres de sécurité - Vérification SPF	
 Paramètres de sécurité Authentification de l'expéditeur Bouclier IP Authentification SMTP Vérification SPF Vérification DKIM Signature DKIM Paramètres DKIM Vérification DMARC Rapports DMARC Paramètres DMARC Certification VBR Domaines acceptés Analyse SSL & TLS Autres 	 Vérification SPF Activer la vérification SPF Ne pas vérifier les messages provenant de sessions authentifiées Cela inclut les authentifications POP avant SMTP et celles du Bouclier IP. Ne pas vérifier les messages provenant d'IP autorisées Mettre les enregistrements SPF en cache Cache Liste blanche Traitement des messages Lorsque la vérification donne le résultat 'FAIL': envoyer le code d'erreur 550 puis fermer la connexion ajouter au score du Filtre anti-spam 15.0 Messages provenant d'un expéditeur valide, dont le domaine est listé dans 'Domaines approuvés' ajouter au score du Filtre anti-spam -0.5 Paramètres SPF Appliquer le traitement SPF à la valeur HELO/EHLO Insérer l'en-tête 'Received-SPF' dans les messages sauf si le résultat SPF est ''NONE'' Utiliser une adresse locale dans l'enveloppe SMTP pour le transfert des messages Nombre max. de vérifications 'void' (au moins 2)
	OK Annuler Appliquer Aide

MDaemon prend en charge le SPF (Sender Policy Framework) pour vérifier les serveurs d'envoi et se protéger contre le spoofing et le phishing, deux types courants de falsification d'e-mails dans lesquels l'expéditeur du message tente de faire croire qu'il provient de quelqu'un d'autre.

De nombreux domaines publient des enregistrements MX dans le système de noms de domaine (DNS) afin d'identifier les lieux autorisés à recevoir du courrier pour eux, mais cela ne permet pas d'identifier les lieux autorisés à *envoyer du* courrier pour eux. SPF est un moyen par lequel les domaines peuvent également publier des enregistrements d'expéditeur pour identifier les lieux autorisés à envoyer des messages. En effectuant une recherche SPF sur les messages entrants, MDaemon peut tenter de déterminer si le serveur d'envoi est autorisé à distribuer du courrier pour le domaine d'envoi supposé, et par conséquent déterminer si l'adresse de l' expéditeura été falsifiée ou " usurpée ".

Les options de cet écran permettent de configurer les paramètres SPF de votre serveur.

Pour plus d'informations sur SPF, consultez le site

http://www.open-spf.org

Vérification SPF

Activer la vérification SPF

Lorsque cette option est activée, MDaemon effectue une requête DNS pour obtenir les données de l'enregistrement SPF de l'expéditeur présumé de chaque message entrant, afin de s'assurer que le serveur d'envoi est autorisé à envoyer des messages en son nom. L'hôte vérifié par MDaemon est défini à partir de la valeurMAIL transmise lors du traitement SMTP. La vérification SPF est activée par défaut.

Ne pas vérifier les messages provenant de sessions authentifiées

Par défaut, les connexions authentifiées sont exemptées des requêtes SPF. Les sessions authentifiées comprennent celles vérifiées via l'<u>authentification SMTP</u> [552], <u>POP avant SMTP</u> [552] ou l'<u>écran IP obligatoires</u> [555]. Désactivez cette option si vous ne souhaitez pas exempter les sessions authentifiées de SPF.

Ne pas vérifier les messages provenant d'IP autorisées

Par défaut, tout message provenant d'une <u>adresse IP autorisée</u> 564 est exempté de la vérification SPF.

Mettre en cache les résultats de la vérification

Par défaut, MDaemon met temporairement en cache l'enregistrement de politique SPF de chaque domaine obtenu lors de la requête DNS. Décochez la case si vous ne souhaitez pas mettre en cache les politiques SPF.

Pas de cache

Ce bouton permet d'ouvrir le cache SPF, qui répertorie tous les enregistrements SPF actuellement mis en cache.

Liste des exceptions

Cliquez sur ce bouton pour ouvrir la liste d'exceptions SPF sur laquelle vous pouvez désigner les adresses IP, les adresses e-mail et les domaines que vous souhaitez exempter des consultations SPF. Les adresses électroniques sont comparées à l'enveloppe SMTP et non à l'en-tête From du message. Les domaines sont Les domaines sont exemptés en plaçant le mot "spf" devant le nom de domaine. MDaemon inclura l'enregistrement SPF de ce domaine dans chaque évaluation SPF à l'aide d'une balise "wlinclude: <domain>" spécifique à MDaemon. Vous pouvez ainsi faire en sorte que votre fournisseur MX de secours soit considéré comme une source SPF valide pour tous les expéditeurs.

Traitement des messages SPF

Lorsque la vérification produit un résultat FAIL :

... envoyer un code d'erreur 550

Cochez cette case si vous souhaitez qu'un code d'erreur 550 soit envoyé lorsque le résultat de la requête SPF est "Fail".

...puis fermer la connexion

Activez cette option si vous souhaitez que la connexion soit fermée immédiatement après l'envoi du code d'erreur 550.

...ajouter ceci au score du Filtre anti-spam

Indiquez le montant que vous souhaitez ajouter auscore du filtre anti-spam lorsque lemessagene passe pas la vérification SPF.

Messages provenant d'un expéditeur valide d'un domaine figurant sur la 'Domaines approuvés'

...ajouter au score du Filtre anti-spam

Indiquez le montant que vous souhaitez ajouter au score de spam d'un messagelorsque SPF confirme qu'il provient d'un domaine figurant sur la Domaines <u>approuvés</u> [553].



En règle générale, la valeur spécifiée ici doit être un nombre négatif afin que le score de spam soit réduit pour les messages approuvés.

Paramètres SPF

Appliquer le traitement SPF à la valeur HELO/EHLO

Cette option applique la vérification SPF à la valeur transmise dans la commande HELO ou EHLO au début du processus SMTP. Elle est activée par défaut.

Insérer un en-tête "Received-SPF" dans les messages

Cliquez sur cette option si vous souhaitez qu'un en-tête "Received-SPF" soit inséré dans chaque message.

... sauf si le résultat SPF est "aucun

Activer cette option si vous ne souhaitez pas que l'en-tête "Received-SPF" soit inséré dans un message lorsque le résultat de la requête SPF est "none".

Utiliser cette adresse dans l'enveloppe SMTP pour Transférer le message !

Activer cette option si vous souhaitez que tous les courriers transférés par MDaemon utilisent une adresse locale dans l'enveloppe SMTP. Cela permet de réduire les problèmes liés au transfert. Normalement, les messages transférés sont envoyés en utilisant l'adresse e-mail de l'expéditeur d'origine et non l'adresse e-mail qui effectue le transfert. Dans certaines situations, l'utilisation d'une adresse locale peut s'avérer nécessaire pour éviter que le serveur destinataire n'identifie à tort le message transféré comme ayant une adresse "usurpée". Cette option est activée par défaut.

Nombre maximal de recherches "nulles" (doit être au moins égal à 2)

Dans une requête SPF, MDaemon peut afficher un nombre maximum de résultats nuls avant de générer une erreur permanente. Une recherche vide est une recherche dont le résultat est "le domaine n'existe pas" ou "aucune réponse n'existe". Cette valeur doit être au moins égale à "2".

4.2.2.4 DomainKeys Identified Mail

DomainKeys Identified Mail (DKIM) est un système de vérification cryptographique des e-mails qui peut être utilisé pour empêcher l'usurpation d'identité (falsification de l'adresse électronique d'une autre personneafin de se faire passer pour un autre expéditeur). Dans la mesure où la plupart des courriers indésirables (spam) contiennent des adresses usurpées, la norme DKIM peut grandement contribuer à la réduction du spam, même si les spécifications n'ont pas été spécifiquement conçues pour être un outil anti-spam. La norme DKIM peut également être utilisée pour garantir l'intégrité des messages entrants, c'est-à-dire pour s'assurer que le message n'a pas été modifié entre le moment où il a quitté le serveur de messagerie qui l'a signé et celui où il est arrivé chez vous. Dans d'autres termes, grâce à la vérification cryptographique DKIM, le serveur destinataire peut être certain que le message qui arrive provient bien du serveur qui l'a signé et que personne ne l'a modifié de quelque manière que ce soit.

Dans le but de garantir la validité et l'intégrité des messages, DKIM utilise un système de paires de clés publiques et privées. Une clé publique cryptée est publiée dans lesenregistrements DNS duserveur d'envoi, puis chaque message sortant est signé par le serveur à l'aide de la clé privée cryptée correspondante. Pour les messages entrants, lorsque le serveur de réception voit qu'un message a été signé, il récupère la clé publique dans lesenregistrements DNS duserveur d'envoiet compare cette clé à lasignature cryptographique dumessagepour en déterminer la validité. Si le message entrant ne peut pas être vérifié, le serveur de réception sait qu'il contient une adresse usurpée ou qu'il a été altéré ou modifié. Un message non vérifié peut alors être rejeté ou accepté, mais son score de spam peut être modifié.

Pour configurer MDaemon afin qu'il vérifie les messages entrants signés cryptographiquement, utilisez les options proposées dans l'écran <u>Vérification DKIM</u> Pour configurer MDaemon afin qu'il signe les messages sortants, utilisez les options de l' écran <u>Signature DKIM</u> bell ces deux options se trouvent dans la section Authentification de l'expéditeur de la boîte de dialogue Paramètres de sécurité : Sécurité | Paramètres de sécurité | Authentification de l'expéditeur. Dans l'<u>interface principale</u> MDaemon, un onglet " DKIM " (situé sous l'onglet Sécurité) permet de surveiller l'activité DKIM en temps réel. Vous pouvez également journaliser l'activité DKIM à l'aide de l'option située à l'adresse : Sécurité "Paramètres du serveur "Authentification de l'expéditeur : Configuration | Paramètres du serveur | Journalisation | Paramètres.

Voir :

Vérification DKIMConnexion DKIMParamètres DKIMSol

Pour en savoir plus sur le courrier identifié par DomainKeys, consultez le <u>site</u> : http://www.dkim.org/.

4.2.2.4.1 Vérification DKIM

🧐 Paramètres de sécurité - Vérification DKIM		×
 Paramètres de sécurité Authentification de l'expéditeur Bouclier IP Authentification SMTP Vérification SPF Vérification DKIM Signature DKIM Paramètres DKIM Vérification DMARC Rapports DMARC Paramètres DMARC Certification VBR Domaines acceptés Analyse SSL & TLS Autres 	 Vérification DKIM ✓ Activer la vérification DKIM ✓ Ne pas vérifier les messages provenant de sessions authentifiées Les vérifications POP avant SMTP et celles de l'écran IP sont obligatoires. ✓ Ne pas vérifier les messages provenant d'IP autorisées Liste blanche 	
	OK Annuler Appliquer Ai	de

Cet écran permet de configurer MDaemon pour qu'il vérifie les signatures DomainKeys Identified Mail (DKIM) dans les messages entrants distants. Lorsque cette fonctionnalité est activée et qu'un message entrant a été signé cryptographiquement, MDaemon récupère la clé publique de l'enregistrement DNS du domaine figurant dans la signature, puis utilise cette clé pour tester la signature DKIM du message afin d'en déterminer la validité. Si la signature passe le test de vérification, le message passera à l'étape suivante du processus de livraison normal. En outre, si le domaine extrait de la signature figure également sur la Domaines <u>approuvés</u> [593], le score du Filtre anti-spam du message sera ajusté en conséquence.

Pour en savoir plus sur le DKIM, voir : http://www.dkim.org/

Vérification DKIM

Activer la vérification DKIM

Cliquez sur cette option pour activer la vérification DomainKeys Identified Mail des messages distants entrants.

Ne pas vérifier les messages provenant de sessions authentifiées

Cliquez sur cette option si vous souhaitez exempter les messages de la vérification cryptographique lorsque la session de messages est authentifiée. Les sessions authentifiées comprennent celles vérifiées via l'<u>authentification SMTP</u> [552] ou le <u>Bouclier IP</u> [555].

Ne pas vérifier les messages provenant d'IP autorisées

Utilisez cette option si vous souhaitez que les connexions provenant d'<u>adresses IP</u> <u>autorisées</u> soient exemptées de la vérification DKIM.

Liste d'exceptions

Cliquez sur ce bouton pour ouvrir la liste des exceptions. Les messages provenant de toutes les adresses IP indiquées dans la liste ne feront pas l'objet d'une vérification cryptographique.

En-tête Authentication-Results : dans l'en-tête FROM

Lorsqu'un message est authentifié à l'aide de SMTP AUTH, SPF, DomainKeys Identified Mail ou DMARC, MDaemon insère l'en-tête Authentication-Results dans le message, qui répertorie les résultats du processus d'authentification. Si MDaemon est configuré pour accepter les messages même en cas d'échec de l'authentification, l'en-tête Authentication-Results contiendra un code permettant d'identifier la raison de l'échec.

> Des travaux sont en cours au sein de l'IETF (Internet Engineering Task Force) sur cet en-tête et sur les protocoles d'authentification mentionnés dans cette section. Vous trouverez de plus amples informations à ce sujet sur le site web de l'IETF, à l'adresse <u>suivante</u>: http://www.ietf.org/.

En-têtes DKIM dans les listes de diffusion : TO : Par défaut, MDaemon supprime les en-têtes DKIM dans les listes de diffusion.

Par défaut, MDaemon supprime les signatures DKIM des messages entrants de la liste car ces signatures peuvent être rompues par des modifications apportées aux en-têtes ou au contenu du message pendant le traitement de la liste. Si vous souhaitez que MDaemon laisse les signatures dans les messages de liste, vous pouvez le configurer en définissant manuellement l'option suivante dans le fichierMDaemon.ini:

```
[DomainKeys]
StripSigsFromListMail=No (Oui (par défaut))
```

Voir :

<u>Courrier identifié par DomainKeys</u> <u>Connexion DKIM</u> <u>Paramètres DKIM</u> ଇ

4.2.2.4.2 Signature DKIM

🧐 Paramètres de sécurité - Signature DKIM 👘		×
 Paramètres de sécurité Authentification de l'expéditeur Bouclier IP Authentification SMTP Vérification DKIM Signature DKIM Paramètres DKIM Vérification DMARC Rapports DMARC Paramètres DMARC Certification VBR Domaines acceptés Analyse SSL & TLS Autres 	Signature DKIM Signer les messages sortants éligibles avec DKIM Signer les messages de liste de diffusion également Sélecteur par défaut MDaemon Pour créer un nouveau sélecteur, entrez simplement une valeur dans le champ. Une clé publique et une clé privée ont été créées pour ce sélecteur. Créer une clé publique et une clé privée Pour que les messages soient signés, les signatures doivent être autorisées. Définir les messages qui peuvent être signés Image: Les signatures sont autorisées pour tous les messages provenant de domaines locauter	JX.
	OK Annuler Appliquer Ai	de

Les options de l'écran Connexion DKIM permettent de configurer MDaemon pour qu'il signe les messages sortants éligibles à l'aide de DKIM, et de définir les critères d'éligibilité d'un message. Cet écran permet également de désigner des sélecteurs et de générer des clés publiques et privées adaptées à la spécification DKIM. Un Sélecteur par défaut ("MDaemon") ainsi qu'une clé publique et une clé privée par défaut sont créés automatiquement au démarrage. Toutes les clés sont uniques : elles ne sont

jamais identiques d'un site à l'autre, quel que soit le sélecteur spécifié. Non (par défaut), les clés sont générées avec une profondeur de bits sécurisée de 2048 bits.

Connexion DKIM

Signer les messages sortants éligibles à l'aide de DKIM

Cliquez sur cette option si vous souhaitez utiliser DomainKeys Identified Mail pour signer cryptographiquement certains messages sortants. Pour qu'un message soit signé, il doit répondre aux critères indiqués sous le bouton*Définir les messages qui peuvent être signés* et être reçu par MDaemon pour être délivré lors d'une session authentifiée. Il existe également une action du Filtre de contenu, "*Sign with DKIM selector*...", que vous pouvez utiliser pour faire signer les messages.

...signer les messages des listes diffusion

Cochez cette case si vous souhaitez signer cryptographiquement tous les messages de la Liste de diffusion sortants. Comme MDaemon signera tout le courrier destiné à toutes vos listes, vous n'avez pas besoin d'utiliser l'option"*Définir les messages qui peuvent être signés*" pour les autoriser à recevoir une signature cryptographique.

Sélecteur par défaut

Dans la liste déroulante, choisissez le sélecteur dont vous souhaitez utiliser la paire de clés publique/privée correspondante lors de la signature des messages. Si vous souhaitez créer une nouvelle paire de clés avec un sélecteur différent, tapez le nom du sélecteur souhaité ici et cliquez sur "Créer de nouvelles clés publiques et privées" ci-dessous. Si vous souhaitez signer certains messages à l'aide d'un autre sélecteur, désignez un sélecteur spécifique dans l'option"*Définir les messages qui sont signés*" ou créez une règle de Filtre de contenu à l'aide de l'action "Sign with DKIM selector...".

Supprimer ce sélecteur

Cliquez sur ce bouton si vous souhaitez supprimer un sélecteur. Suivez les instructions qui s'affichent à l'écran.

Créer une clé publique et une clé privée

Cliquez sur ce bouton pour générer une paire de clés publique/privée pour le sélecteur spécifié ci-dessus. Une paire de clés publique/privée sera généréepour le sélecteur, et le fichier dns_readme.txt sera généré et automatiquement ouvert. Ce fichier contient des exemples de données DKIM que vous devrez publier dans les enregistrements DNS de votre domaineen indiquant votre politique DKIM et la clé publique pour le sélecteur désigné. Le fichier répertorie des exemples pour les statuts "testing" et "not testing", et selon que vous signez tous les messages ou seulement certains messages provenant de votre domaine. Si vous testez actuellement DKIM ou ce sélecteur, vous devrez alors utiliser les informations contenues dans les entrées Testing pour la politique ou le sélecteur, en fonction de ce que vous testez. Dans le cas contraire, vous devrez utiliser les entrées "Not Testing".

Toutes les clés sont stockées au format PEM, et tous les sélecteurs et clés sont stockés dans le dossier\MDaemon\Pem de la manière suivante :

\MDaemon\Pem\<Selector>\rsa.public - clé publique pour ce sélecteur

\MDaemon\Pem\<Selector>\rsa.private - clé privée pour ce sélecteur

Les fichiers contenus dans ces dossiers ne sont pas cryptés ou cachés, mais ils contiennent des clés de cryptage privées RSA auxquelles personne ne devrait jamais avoir accès sans autorisation. Vous devez donc prendre des mesures pour sécuriser ces dossiers et sous-dossiers à l'aide des outils de votre système d'exploitation.

Définir les messages qui peuvent être signés

Si vous avez choisi de signer les messages sortants éligibles, cliquez sur ce bouton pour modifier le fichier DKSign.dat, qui contient la liste des domaines et des adresses que MDaemon utilisera pour déterminer si un message doit être signé ou non. Pour chaque adresse listée, vous devez indiquer si le message doit être Entête ou From pour qu'il puisse être signé, ou vous pouvez indiquer un autre entête tel que "Reply-To" ou " Sender ". Vous pouvez également indiquer un sélecteur pour chaque entrée, qui sera utilisé lors de la signature d'un message correspondant à cette entrée. Enfin, vous pouvez spécifier un domaine de signature facultatif à utiliser dans la balise "d=" de l'en-tête de signature. Cela peut s'avérer utile, par Exemple, lorsque plusieurs sous-domaines signent des messages. Dans ce cas, vous pouvez utiliser la balise "d=" pour indiquer aux serveurs destinataires de rechercher les clés DKIM dans l'enregistrement DNS d'un seul domaine, ce qui vous permet de gérer toutes les clés dans un seul enregistrement au lieu de devoir gérer des enregistrements distincts pour chaque sous-domaine. Les caractères génériques sont autorisés dans les domaines et les adresses.

Tous les domaines locaux sont éligibles à la Connexion

Utilisez cette option si vous souhaitez que tous les messages provenant de vos domaines locaux puissent être signés. Si vous utilisez cette option, vous n'aurez pas besoin d'enregistrer tous les messages provenant de vos domaines locaux. Si vous utilisez cette option, vous n'avez pas besoin d'ajouter vos domaines locaux à la liste d'éligibilité (c'est-à-dire au fichierDKSign.dat), à moins que vous ne souhaitiez désigner un sélecteur spécifique ou une balise "d=" à utiliser lors de la signature des messages d'un domaine spécifique. Cette option est activée par défaut.

Voir :

 DomainKeys Identified Mail

 Paramètres DKIM

 Wérification DKIM

4.2.2.4.3 Paramètres DKIM

Paramètres de signature DKIM

Les signatures expirent après [xx] jours (balise "x=", 7 jours recommandés).

Si vous souhaitez limiter le nombre de jours pendant lesquels une signature DKIM peut être considérée comme valide, activez cette option et indiquez le nombre de jours souhaité. Les messages dont la signature a expiré échoueront toujours à la vérification. Cette option correspond à la balise"x="de la signature. Cette option est activée par défaut, la valeur étant fixée à 7 jours.

Inclure l'heure de création dans la signature (balise t=)

Dans cette option, l'heure de création de la signature (balise "t=") est incluse dans la signature. Cette option est activée par défaut.

Les signatures incluent les méthodes d'interrogation (include q= tag)

Cette option est activée par défaut. Elle fait en sorte que la signature inclue la balise de la méthode d'interrogation (par exemple, "q=dns").

Les signatures incluent le décompte de la longueur du corps (include l= tag)

Activez cette option si vous souhaitez inclure la balise "body length count" dans les signatures DKIM.

Les signatures incluent le contenu de l'en-tête original (include z= tag)

Cochez cette option si vous souhaitez inclure la balise "z=" dans la signature DKIM. Cette balise contiendra une copie des en-têtes originaux dumessage.Cela peut potentiellement rendre les signatures assez volumineuses.

Les signatures incluent les rapports demandés (inclure la balise r=y)

Activez cette option si vous souhaitez inclure la balise r=y dans vos messages signés. La présence de cette balise indique aux serveurs de réception qui l'honorent que vous souhaitez recevoir d'eux des rapports d'échec AFRF lorsqu'ils rencontrent des messages censés provenir de votre domaine mais qui échouent à la vérification DKIM. Pour recevoir ces rapports, vous devez également configurer un enregistrement TXT de rapport DKIM dans le DNS de votre domaine.. Voir RFC-6651 : <u>Extensions to DomainKeys Identified Mail (DKIM) for Failure Reporting</u>, pour la syntaxe et les instructions à suivre. Cette option nécessitant des modifications du DNS, elle est désactivée par défaut.

Canonicalisation

La canonicalisation est un processus par lequel lesen-têtes et le corps dumessagesont convertis en une norme canonique et "normalisés" avant que la signature DKIM ne soit créée. Cette opération est nécessaire car certains serveurs de messagerie et systèmes de relais apportent diverses modifications sans importance au message au cours de son traitement normal, ce qui risquerait de rompre la signature si une norme canonique n'était pas utilisée pour préparer chaque message en vue de sa signature. Actuellement, deux méthodes de canonisation sont utilisées pour la signature et la vérification DKIM : Simple et Relaxed. La méthode simple est la plus stricte, car elle n'autorise que peu ou pas de modifications du message. La méthode "Relaxed" est plus indulgente que la méthode "Simple", car elle autorise plusieurs modifications sans importance.

Canonicaliser les en-têtes dans FROM: : Simple, Relaxed

Il s'agit de la méthode de canonisation utilisée pour les en-têtes du message lors de la signature du message. Simple n'autorise aucune modification des en-têtes dans les champs À :. Relaxed permet de convertir les noms des en-têtes (pas les valeurs des en-têtes) en minuscules, de convertir un ou plusieurs espaces séquentiels en un seul espace, et d'autres modifications inoffensives. Le paramètre (par défaut) est "Simple".

Canonicaliser le corps en utilisant : Simple, Détendu

Il s'agit de la méthode de canonicalisation utilisée pour le Corps du message lors de la Connexion du message. Simple ignore les lignes vides à la fin du Corps du message - aucune autre modification du corps n'est autorisée. Relaxed autorise les lignes vides à la fin du message, ignore les espaces en fin de ligne, réduit toutes les séquences d'espaces dans une même ligne à un seul caractère d'espace, ainsi que d'autres modifications mineures. Le paramètre (par défaut) est "Simple".

Paramètres de vérification DKIM

Le vérificateur tient compte de la longueur du corps (balise I=)

Dans cette option, MDaemon respecte la balise de longueur du corps lorsqu'elle figure dans la signature DKIM d'unmessage entrant.Dans le cas où la longueur réelle du corps est supérieure à la valeur contenue dans cette balise, MDaemon ne vérifie que

la quantité spécifiée dans la balise ; le reste du message n'est pas vérifié. Cela indique que quelque chose a été ajouté au message et que, par conséquent, la partie non vérifiée peut être considérée comme suspecte. Dans le cas où la longueur réelle du corps du message est inférieure à la valeur contenue dans cette balise, la signature ne passera pas la vérification (c'est-à-dire qu'elle recevra un résultat "FAIL"). Cela indique qu'une partie du message a été supprimée, ce qui fait que la longueur du corps est inférieure à la valeur spécifiée dans la balise.

Le vérificateur exige des signatures pour protéger l'en-tête "Subject".

Activez cette option si vous souhaitez que la signature DKIM des messages entrants protège l'en-tête Subject.

Les signatures valides des domaines approuvés ajoutent cette valeur au score du Filtre anti-spam :

La valeur indiquée ici sera ajoutée au score du Filtre anti-spam de tous les messages signés DKIM qui reçoivent un résultat "Pass" lorsque le domaine repris dans la signature figure dans la <u>Liste approuvée</u> [553]. Lorsque la signature d'un message est vérifiée mais que le domaine ne figure pas dans la Domaines approuvés, le score du Filtre anti-spam ne sera pas ajusté - la signature vérifiée n'aura aucun effet sur le score. Cependant, le traitement normal du Filtre anti-spam et la notation seront toujours appliqués à ce message.

> En règle générale, la valeur spécifiée ici doit être un nombre négatif afin que le score du Filtre anti-spam soit réduit pour les messages contenant une signature cryptographique valide lorsque le domaine tiré de la signature figure sur la <u>Liste</u> <u>approuvée</u> 503. La valeur par défaut de MDaemon pour cette option est -0, 5.

Voir :

<u>DomainKeys Identified Mail</u> ब्ली <u>Vérification DKIM</u> ब्ली <u>Connexion DKIM</u> ब्लि

4.2.2.5 Paramètres ARC

💛 Security Manager - ARC Settings	
Security Settings Relay Control Reverse Lookups POP Before SMTP Trusted Hosts Trusted IPs Sender Authentication P Shield SMTP Authentication	ARC Verification ARC Verification Trusted ARC Sealers
SPF Verification DKIM Verification DKIM Signing DKIM Settings ARC Settings DMARC Verification DMARC Reporting DMARC Settings WBR Certification Approved List	Domain Add ARC Signing Sign eligible outbound messages using ARC Default selector Delete New Default signing domain company.test Advanced
	Ok Cancel Apply Help

Le protocole ARC (Authenticated Received Chain) est un protocole d'authentification du courrier électronique qui permet aux serveurs de messagerie intermédiaires de signer numériquement les résultats de l'authentification d'un message. Il fournit une "chaîne de conservation" authentifiée pour un message, permettant à chaque serveur qui traite le message de voir quels serveurs précédents l'ont traité et s'il a été authentifié ou non à chaque étape. Lorsqu'un serveur de messagerie en aval effectue une <u>vérification</u> <u>DMARC</u> apprendent que <u>SPF</u> ou <u>DKIM</u> ant échoué (en raison d'un transfert ou de modifications apportées à une liste de diffusion, par exemple), il peut rechercher les résultats de l'ARC auprès d'un serveur de confiance et les utiliser pour décider d'accepter ou non le message.

Pour plus d'informations sur le protocole ARC, voir : <u>RFC 8617 : The Authenticated</u> <u>Received Chain (ARC)</u>.

Vérification ARC

Activer la vérification ARC

Cochez cette case pour activer la vérification ARC.

Scelleurs ARC de Confiance

Les Scelleurs ARC de confiance sont les domaines dont les résultats ARC sont fiables. Les résultats ARC de domaines non fiables sont ignorés lors de la <u>vérification</u> <u>DMARC</u> .

Signature ARC

Signez les messages sortants éligibles en utilisant ARC

Les messages transférés, les messages de listes de diffusion et les messages de passerelle avec résultats d'authentification peuvent être signés à l'aide de l'ARC. La signature ARC nécessite un sélecteur et un domaine de signature désignés cidessous.

Non (par défaut) sélecteur

Cette option permet de choisir le sélecteur par défaut à utiliser pour la signature ARC. Vous pouvez utiliser le même sélecteur que pour la <u>signature DKIM</u> [566] ou en créer un nouveau.

Domaine signature par défaut> Domaine signature par défaut

Sélectionnez le domaine par défaut pour la signature ARC.

Avancé

Si vous hébergez plusieurs domaines et que vous souhaitez utiliser un sélecteur ou un domaine de connexion différent pour l'un d'entre eux, cliquez sur **Avancé** pour le configurer.

4.2.2.6 DMARC

Domain-based Message Authentication, Reporting & Conformance (DMARC) est une spécification conçue pour aider à réduire les abus de messages électroniques, tels que les messages entrants de spam et de phishing qui présentent faussement leur origine dans l'en-tête FROM : du message. DMARC permet aux propriétaires de domaines d'utiliser le système de noms de domaines (DNS) pour informer les serveurs de réception de leur politique DMARC, c'est-à-dire de la manière dont ils souhaitent que ces serveurs traitent les messages censés provenir de leur domaine mais dont l'origine ne peut être authentifiée. Cette politique, qui est récupérée par le serveur de réception via une requête DNS lors du traitement du message entrant, peut indiquer que le serveur doit mettre en quarantaine ou rejeter les messages qui ne sont pas conformes à la politique, ou ne prendre aucune mesure (c'est-à-dire laisser le message se dérouler normalement). Dans l'enregistrement DNS DMARC du domaine, on peut également demander au serveur d'envoyer à certains des rapports DMARC indiquant le nombre de messages entrants censés provenir de ce domaine et précisant si l'authentification a été réussie ou échouée, avec des détails sur les échecs. Les fonctions de rapport DMARC peuvent être utiles pour déterminer l'efficacité de vos procédures d'authentification du courrier électronique et la fréquence à laquelle votre nom de domaine est utilisé dans des messages falsifiés.

Dans la section Authentification de l'expéditeur de la boîte de dialogue Paramètres de sécurité, trois écrans permettent de configurer les fonctions de vérification et de rapport DMARC de MDaemon : Vérification DMARC, Rapports DMARC et Paramètres de rapports DMARC.

Vérification DMARC 500

Dans le cadre du processus de vérification DMARC, MDaemon effectue une requête DNS DMARC sur le domaine figurant dans l'en-tête FROM : de chaque message entrant. Cela permet de déterminer si le domaine utilise ou non DMARC et, si c'est le cas, de récupérer son <u>enregistrement DNS DMARC</u> [575], qui contient sa politique et d'autres informations relatives à DMARC. En outre, DMARC utilise <u>SPF</u> [560] et <u>DKIM</u> [564] pour valider chaque message et exige qu'il réussisse au moins l'un de ces tests pour passer la vérification DMARC. Si le message passe avec succès, il sera acheminé normalement par le reste des processus de distribution et de filtrage de MDaemon. Si le message échoue, son sort est déterminé par la politique DMARC du domaine et par la façon dont vous avez configuré MDaemon pour traiter ces messages.

Si un message échoue à la vérification DMARC et que le domaine DMARC a une politique "p=none", aucune mesure punitive ne sera prise et le traitement normal des messages se poursuivra. Inversement, lorsque le domaine DMARC a une politique restrictive de "p=quarantine" ou "p=reject", MDaemon peut optionnellement filtrer le message automatiquement dans la liste de "spam" (c'est-à-dire de courrier indésirable) de l'utilisateur destinataire. Dossier de courrier indésirable (spam)de l'utilisateur destinataire. Dossier de courrier indésirable (spam)de l'utilisateur destinataire .Vous pouvez également choisir de demander à MDaemon de rejeter complètement le message lorsque le domaine utilise la stratégie"p=reject". De plus, pour les messages ayant échoué et dont la politique est restrictive, MDaemon insère l'en-tête "X-MDDMARC-Fail-policy : quarantine" ou "X-MDDMARC-Fail-policy : reject", en fonction de la politique. Cela vous permet d'utiliser le Filtre de contenu pour effectuer une action basée sur la présence de ces en-têtes, telle que l'envoi du message dans un dossier spécifique pour un examen plus approfondi.

La vérification DMARC est activée par défaut et recommandée dans la plupart des configurations de MDaemon.

Rapport DMARC 583

Lorsque MDaemon signale au DNS un enregistrement DMARC, celui-ci peut contenir des balises indiquant que le propriétaire du domaine souhaite recevoir des rapports d'échec ou d'agrégation DMARC concernant les messages prétendant provenir de ce domaine. Les options de l'écran DMARC Report permettent d'indiquer si l'on souhaite ou non envoyer les types de rapports demandés et de spécifier les Métadonnées du rapportARC que ces rapports doivent contenir. Les rapports globaux sont envoyés quotidiennement à minuit UTC et les rapports d'échec sont envoyés par message, au fur et à mesure que se produit l'incident qui déclenche le rapport. Les rapports sont toujours envoyés sous forme de fichiers XML zippés, et plusieurs outils d'analyse sont disponibles en ligne pour permettre aux destinataires de les consulter facilement.

Par défaut, MDaemon n'envoie pas de rapports globaux ou de rapports d'échec. Si vous souhaitez envoyer l'un ou l'autre type de rapport, activez les options correspondantes dans l'écran Rapports DMARC.

Paramètres DMARC 587

L'écran Paramètres DMARC contient diverses options permettant d'inclure certaines informations dans les rapports DKIM, de journaliser les enregistrements DNS DMARC et de mettre à jour le fichier de suffixes publics utilisé par MDaemon pour DMARC.

Vérification DMARC et listes de diffusion

Dans la mesure où l'objectif de DMARC est de garantir que le domaine figurant dans l'en-tête From : d'un message n'a pas été falsifié, le serveur d'envoi doit être autorisé à envoyer des messages au nom de ce domaine. Cela peut poser un problème

particulier pour les listes de diffusion, car il est courant que les listes distribuent des messages au nom de leurs membres à partir de domaines extérieurs, tout en laissant l'en-tête From : inchangé. Cela signifie que lorsqu'un serveur récepteur tente d'utiliser la vérification DMARC pour l'un de ces messages, le message aura été envoyé par un serveur qui n'est pas officiellement affilié au domaine de l'en-tête From :. Si le domaine DMARC utilise une politique DMARC restrictive, le message peut être mis en quarantaine ou même rejeté par le serveur destinataire. Dans certains cas, le destinataire peut également être retiré de la liste. Pour contourner ce problème, lorsque MDaemon constate qu'un message destiné à une liste provient d'un domaine soumis à une politique DMARC restrictive, MDaemon remplacera l'en-tête From : du message par l'adresse de la liste de diffusion. Vous pouvez également configurer MDaemon pour qu'il refuse d'accepter tout message destiné à une liste lorsqu'il provient d'un domaine soumis à une politique restrictive. Cette dernière option rendrait impossible la publication d'un message sur la liste par un utilisateur d'un domaine ayant une politique restrictive. L'option de remplacement de l'en-tête From : se trouve dans l'écran En-<u>tête de 294</u>) l'éditeur de listes de diffusion, et l'option de rejet des messages se trouve dans l'écran Paramètres. 2001 **Remarque :** Le serveur SMTP consultera la politique DMARC de l'expéditeur si nécessaire pour ces options de liste de diffusion liées à DMARC, même si la connexion est <u>exemptée du</u> mitraitement DMARC.

Utiliser DMARC pour vos domaines MDaemon

Si vous souhaitez utiliser DMARC pour l'un de vos domaines, c'est-à-dire si vous voulez que les serveurs de messagerie qui prennent en charge DMARC utilisent DMARC pour vérifier les messages qui prétendent provenir de vous, vous devez d'abord vous assurer que vous avez créé des enregistrements DNS SPF et DKIM correctement formatés pour le domaine ; au moins l'une de ces options doit fonctionner correctement pour utiliser DMARC. Si vous utilisez DKIM, vous devez également configurer les Options <u>DKIM</u> <u>Signing de</u> MDaemon pour signer les messages du domaine. En outre, vous devez créer un enregistrement DNS DMARC pour le domaine. En interrogeant le DNS pour cet enregistrement TXT spécialement formaté , le serveur de réception peut déterminer votre politique DMARC et divers paramètres facultatifs tels que : le mode d'authentification que vous utilisez, si vous souhaitez ou non recevoir des rapports globaux, l'adresse électronique à laquelle les rapports doivent être envoyés, et d'autres encore.

Une fois que vous avez correctement configuré DMARC et que vous avez commencé à recevoir des rapports DMARC XML, il existe une variété d'outils en ligne que vous pouvez utiliser pour lire ces rapports et diagnostiquer tout problème potentiel. Pour vous faciliter la tâche, un outil DMARC Reporter vous est également fourni dans le dossier \MDaemon\App\. Voir DMARCReporterReadMe.txt pour savoir comment l'utiliser.

Définition d'un enregistrement de ressource DMARC TXT

Ce qui suit est une vue d'ensemble des composants les plus élémentaires et les plus couramment utilisés d'un enregistrement DMARC. Pour des informations plus détaillées, ou pour des informations sur des configurations plus avancées, voir : www.dmarc.org.

Champ À : le propriétaire

Le champ Propriétaire (également appelé "Nom" ou "gauche") de l'enregistrement de ressource DMARC doit toujours être _dmarc, ou il peut prendre la forme

<u>_dmarc.domain.name</u> si vous souhaitez spécifier le domaine ou le sous-domaine auquel l'enregistrement s'applique.

Exemple :

Enregistrement DMARC pour le domaine **example.com**

dmarc IN TXT "v=DMARC1;p=none"

Cet enregistrement s'appliquerait aux courriels provenant de user@example.com ou de tout sous-domaine de example.com, comme user@support.example.com, user@mail.support.example.com, etc.

_dmarc.support.example.com IN TXT "v=DMARC1;p=none" Cet enregistrement ne s'appliquerait qu'aux courriels provenant de user@support.example.com, et non à ceux provenant, par exemple, de user@example.com.

_dmarc.support IN TXT "v=DMARC1;p=none" Cet enregistrement s'applique aux courriels provenant de : user@support.example.com, user@a.support.example.com, user@a.b.support.example.com, et ainsi de suite.

Balises et valeurs des enregistrements DMARC

Balises requises

Balis e	Valeur	Notes
v=	DMARC1	Dans est la balise Version, qui doit être la première balise dans la partie texte spécifique à DMARC de l'enregistrement. Bien que les valeurs des autres balises DMARC ne soient pas sensibles à la casse, la valeur de la balise v = doit être en majuscules : DMARC1 . Exemple :
		_dmarc IN TXT "v=DMARC1;p=none"
p=	aucun quarantaine rejet	Dans ce cas, il s'agit de la balise Policy, qui doit être la deuxième balise de l'enregistrement DMARC, après la balise v=. p=none signifie que le serveur de réception ne doit prendre aucune mesure en fonction des résultats de la requête DMARC. Les messages qui échouent au contrôle DMARC ne doivent pas être mis en quarantaine ou rejetés sur la base de cet échec. Ils peuvent encore être mis en quarantaine ou rejetés pour d'autres raisons, par exemple parce qu'ils ont échoué aux tests du filtre anti-spam ou à d'autres contrôles de sécurité sans rapport avec DMARC. L'utilisation


Balises optionnelles

Toutes les balises énumérées ci-dessous sont facultatives. Lorsque l'une de ces balises n'est pas utilisée dans un enregistrement, sa valeur par défaut est prise en compte.

Balis	Valeur	Remarques
-------	--------	-----------

е			
sp=	aucun quarantaine rejeter - Non (par défaut) : Si sp= n'est pas utilisé, la balisep= s'applique au domaine et aux sous- domaines.	Cette balise permet de spécifier une politique à utiliser pour es sous-domaines du domaine auquel s'applique enregistrement DMARC. Exemple : si cette balise est utilisée dans un enregistrement ayant une portée sur example.com, la politique indiquée dans la balise p= 'appliquera aux messages provenant de example.com et la politique indiquée dans la balise sp= s'appliquera aux nessages provenant des sous-domaines de example.com, els que mail.example.com. Si cette balise est omise dans enregistrement, la balise p= s'appliquera au domaine et à es sous-domaines. Exemple : 	
rua=	Liste d'adresses e- mail, séparées par des virgules, auxquelles les rapports DMARC agrégés doivent être envoyés. Les adresses doivent être saisies sous la forme d'URI : mailto:user @example.c om	Cette balise indique que vous souhaitez recevoir des rapports globaux DMARC de la part des serveurs qui reçoivent des messages se réclamant de : un expéditeur de votre domaine. Spécifiez une ou plusieurs adresses électroniques par des virgules) sous la forme : mailto:user@example.com, en séparant plusieurs adresses électroniques par des virgules . Exemple :	
		<pre></pre>	
		des rapports à une adresse située dans un autre domaine, le fichier de zone DNS de ce domaine doit également contenir un enregistrement DMARC spécial indiquant qu'il acceptera les rapports DMARC pour le domaine.	
	Non (par défaut) Si cette balise n'est pas utilisée, aucun	Exemple d'enregistrement chez example.com : _dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:non- local-user@example.net"	
		Enregistrement requis sur exemple.net : Exemple.comreportdmarc TXT "v=DMARC1"	

	rapport global ne sera envoyé.	
ruf=	Liste d'adresses électroniques , séparées par des virgules, auxquelles les rapports d'échec DMARC doivent être envoyés. Les adresses doivent être saisies en	Cette balise indique que vous souhaitez recevoir des rapports d'échec DMARC de la part des serveurs qui reçoivent des messages prétendant provenir de : un expéditeur de votre domaine, lorsque les conditions spécifiées dans la balise fo= sont remplies. Non (par défaut), lorsque aucune balise fo= n'est spécifiée, les rapports d'échec sont envoyés lorsque le message échoue à tous les contrôles de vérification DMARC (c'est-à-dire qu'il échoue à la fois à SPF et à DKIM). Spécifiez une ou plusieurs adresses e-mail par des virgules sous la forme : mailto:user@example.com, en séparant plusieurs adresses électroniques par des virgules.
	tant qu'URI sous la forme	failures@example.com"
	: mailto:user @example.c om - Non (par défaut) Si cette balise n'est pas utilisée, aucun rapport d'échec ne sera envoyé.	En règle générale, ces adresses se trouvent dans le domaine couvert par cet enregistrement. Si vous souhaitez envoyer des rapports à une adresse située dans un autre domaine, le fichier de zone DNS de ce domaine doit également contenir un enregistrement DMARC spécial indiquant qu'il acceptera les rapports DMARC pour le domaine.
		Exemple d'enregistrement chez example.com :
		_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:non- local-user@example.net"
		Enregistrement requis sur exemple.net :
		Exemple.comreportdmarc TXT "v=DMARC1"

Pour de plus amples informations sur la spécification DMARC, voir : www.dmarc.org.

Voir :

<u>Vérification DMARC</u> जिली <u>Rapport DMARC</u> जिली <u>Paramètres DMARC</u> जिली <u>Liste de diffusion | Paramètres de diffusion</u> व्रिकी <u>Liste de diffusion | En-tête :</u> व्रिथ्मे

4.2.2.6.1 Vérification DMARC

Vérification DMARC

Activer la vérification et le rapport DMARC

Si cette option est activée, MDaemon Activera les requêtes DNS DMARC sur le domaine figurant dans l'en-tête From : des messages entrants, et enverra des rapports globaux et des rapports d'échec si vous l'avez paramétré à cet effet dans l' écran <u>Rapports DMARC</u>. BARC utilise <u>SPF</u> al et <u>DKIM</u> pour valider les messages, c'est pourquoi au moins l'une de ces fonctions doit être activée pour que DMARC puisse être utilisé. La vérification et les rapports DMARC sont activés par défaut et devraient être utilisés dans la plupart des configurations de MDaemon.

Désactiver la prise en charge de DMARC pourrait entraîner une augmentation du nombre de spams, de messages d'hameçonnage ou de messages falsifiés parvenant à vos utilisateurs. Cela pourrait également entraîner le rejet de certains messages de votre Liste de diffusion par d'autres serveurs, voire l'exclusion de certains membres de vos listes. Ne désactivez DMARC que si vous êtes absolument sûr de ne pas en avoir besoin.

580

Ne pas vérifier les messages provenant de sessions authentifiées

Par défaut, MDaemon n'effectue pas de requêtes DMARC sur les messages reçus lors d'une session authentifiée. Les sessions authentifiées sont celles vérifiées par l'<u>authentification SMTP</u> [556], <u>POP avant SMTP</u> [552] et celles de l'<u>écran IP obligatoires</u> [555].

Ne pas vérifier les messages provenant d'IP autorisées

Par défaut, MDaemon n'effectue pas de requêtes DMARC sur les messages provenant d'une <u>adresse IP autorisée</u> [554].

Mettre en cache les enregistrements DMARC

Par défaut, MDaemon met en cache les données de l'enregistrement DMARC trouvées lors de la recherche DNS. Dans la mise en cache temporaire de ces informations, vous pouvez augmenter l'efficacité lors du traitement de messages similaires qui arriveront prochainement du même domaine.

Pas de cache

Ce bouton permet d'ouvrir le cache DMARC, qui répertorie tous les enregistrements DMARC actuellement mis en cache.

Liste des exceptions

Cliquez sur ce bouton pour ouvrir la liste DMARC Exceptions. Les messages provenant des adresses IP indiquées dans cette liste ne seront pas soumis à la vérification DMARC.

> La vérification DMARC honore également la <u>certification VBR</u> (500) et les Domaines<u>approuvés</u> (503), qui peuvent exempter sur la base d'identifiants DKIM vérifiés et de chemins SPF provenant de sources dignes de confiance. Exemple : si un message n'est pas vérifié par DMARC mais qu'il porte une signature DKIM valide provenant d'un domaine figurant sur la liste approuvée, il n'est pas soumis à la politique DMARC punitive (c'est-à-dire qu'il est traité comme si la politique était "p=none"). Il en va de même si la vérification du chemin SPF correspond à un domaine figurant sur la liste approuvée.

Traitement des messages DMARC

Honorer p=reject lorsque DMARC produit un résultat 'FAIL'.

Par défaut, cette option est activée, ce qui signifie que MDaemon respecte la politique DMARC p=reject lorsque le domaineFrom : d'un message a publié cette politique dans son enregistrement DMARC et que le message échoue à la vérification DMARC. Les messages qui échouent à la vérification DMARC seront refusés au cours de la session SMTP.

Lorsque cette option est désactivée et qu'un message échoue à la vérification DMARC, MDaemon insère l'en-tête"X-MDDMARC-Fail-policy : reject" dans le message au lieu de le refuser. Dans ce cas, vous pouvez utiliser le Filtre de contenu pour effectuer une action basée sur la présence de cet en-tête, par exemple envoyer le message dans un dossier spécifique pour un examen plus approfondi. En outre, vous pouvez utiliser l'option"*Filtrez les messages qui échouent au test DMARC* *dans les dossiers* spam" ci-dessous pour que le message soit placé dans le dossier spam du destinataire.

Si cette option n'est pas activée, le message peut tout de même être rejeté pour une autre raison non liée à DMARC, par exemple si le <u>score du Filtre anti-spam</u> [726] est supérieur au seuil autorisé.

Filtrer les messages qui échouent au test DMARC dans les dossiers spam

Activez cette option si vous souhaitez filtrer automatiquement les messages dans le dossier anti-spam (c'est-à-dire les courriers indésirables) du compte destinataire chaque fois qu'un message échoue à la vérification DMARC. Si ce dossier n'existe pas encore pour l'utilisateur, MDaemon en créera un si nécessaire.



Lorsqu'elle est activée, cette option n'est appliquée que si le domaine From : a publié une politique DMARC restrictive (p=quarantine ou p=reject). Lorsque le domaine publie une politique p=none, cela indique que le domaine ne fait que surveiller DMARC et qu'aucune mesure punitive ne doit être prise.

Voir :

DMARC ନେଶି Rapport DMARC ଛେଶି Paramètres DMARC ଛେଶି Liste de diffusion | Paramètres de liste de diffusion 200 Liste de diffusion | En-tête From : Dans les en-tête FROM 200 Domaines approuvés ଛେଶି

4.2.2.6.2 Rapports DMARC

Paramètres de sécurité Authentification de l'expéditeur	Rapports DMARC La vérification DMARC doit être activée pour que vous puissiez activer ces paramètres.
	Envoyer des rapports DMARC globaux Envoyer maintenant Envoyer des rapports d'échec DMARC (ces rapports sont envoyés lorsque des incidents se produisent) Accepter ce nombre de destinataires 'rua' et 'ruf' DMARC (0=pas de limite) S Envoyer une copie des rapports par e-mail à : Métadonnées des rapports DMARC Nom de l'organisation
Parametres DIMARC Certification VBR Domaines acceptés Analyse SSL & TLS	Entité chargée de produire les données des rapports. Il doit s'agir d'un de vos domaines. E-mail de contact postmaster@company.test
⊕- Autres	Adresse(s) locale(s) pouvant être contactée(s) par les destinataires des rapports en cas de problème (séparez plusieurs adresses par des virgules). Informations de contact Informations ou ressources supplémentaires pour les destinataires du rapport. Il peut s'agir de l'URL d'un site web, d'un numéro de téléphone, etc.
	Chemin de retour du rapport noreply@company.test Adresse SMTP utilisée en cas d'erreur ou de problème pendant la distribution du rapport. Utilisez noreply@ <mydomain.com> pour ignorer les problèmes de distribution.</mydomain.com>

Lorsque MDaemon interroge le DNS pour obtenir un enregistrement DMARC, celui-ci peut contenir diverses balises indiquant que le propriétaire du domaine souhaite recevoir des rapports DMARC concernant les messages prétendant provenir de ce domaine. Les options de l'écran DMARC Report permettent d'indiquer si vous souhaitez ou non envoyer des rapports DMARC globaux ou d'échec aux domaines dont les enregistrements DMARC en font la demande, et de spécifier les Métadonnées du rapport DMARC que ces rapports contiendront. Les options de cet écran ne sont disponibles que si l'option "*Activer la vérification et le rapport DMARC*" est activée dans l' écran Vérification DMARC. Iso proposée par les destinataires des rapports. Il est donc conseillé d'activer STARTTLS dans la mesure du possible.

Rapports DMARC

Envoyer des rapports DMARC agrégés

Activez cette option si vous souhaitez envoyer des rapports agrégés DMARC aux domaines qui en font la demande. Lorsqu'une requête DNS DMARC sur le domaineFrom : d'un message entrant indique que son enregistrement DMARC contient la balise "rua=" (par exemple rua=mailto:dmarc-reports@example.com), cela signifie que le propriétaire du domaine souhaite recevoir des rapports globaux DMARC. À de MDaemon stockera donc les informations DMARC relatives au domaine et aux messages entrants prétendant provenir de ce domaine. Il enregistrera les adresses électroniques auxquelles le rapport global doit être envoyé, les méthodes de vérification utilisées pour chaque message (SPF, DKIM ou les deux), la réussite ou l'échec du message, le serveur d'envoi, son adresse IP, la politique DMARC appliquée, etc. Puis, chaque jour à minuit UTC, MDaemon utilisera les données stockées pour générer le rapport de chaque domaine et l'envoyer aux adresses désignées. De l'envoi des rapports, les données DMARC stockées sont effacées et MDaemon recommence tout le processus.

> MDaemon ne prend pas en charge la balise d'intervalle de rapport DMARC (c'est-à-dire "ri=") pour les rapports globaux. MDaemon enverra des rapports globaux chaque jour à minuit UTC, à tous les domaines pour lesquels il a compilé des données DMARC depuis la dernière fois que les rapports DMARC ont été générés et envoyés.

Envoyer maintenant

Cliquez sur ce bouton si vous souhaitez générer et envoyer un lot de rapports agrégés à partir des données DMARC actuellement stockées, au lieu d'attendre que MDaemon le fasse automatiquement lors du prochain événement de lot à minuit UTC. Les rapports sont envoyés immédiatement et les données DMARC stockées sont effacées, exactement comme cela se produit chaque jour à minuit UTC. MDaemon recommencera alors à stocker les données DMARC jusqu'au prochain événement Midnight UTC, ou jusqu'à ce que vous cliquiez à nouveau sur le bouton, selon ce qui se produit en premier.

Si vous arrêtez MDaemon à ce moment-là, aucun rapport ne sera généré et les données DMARC ne seront pas effacées. La collecte des données DMARC se poursuivra lorsque MDaemon sera à nouveau opérationnel, mais les rapports ne seront pas générés et les données ne seront pas effacées avant le prochain événement de minuit UTC, ou jusqu'à ce que vous cliquiez sur le bouton"*Envoyer les rapports agrégés maintenant*".

Envoyer les rapports d'échec DMARC (les rapports sont envoyés au fur et à mesure des incidents)

Activez cette option si vous souhaitez envoyer des rapports d'échec DMARC aux domaines qui en font la demande. Lorsqu'une requête DNS DMARC sur le domaineFrom : d'un message entrant indique que son enregistrement DMARC contient la balise "ruf=" (par exemple ruf=mailto:dmarc-failure@example.com), cela signifie que le domaine souhaite recevoir des rapports d'échec DMARC. Dans les rapports agrégés, ces rapports sont créés en temps réel au fur et à mesure que les incidents qui les déclenchent se produisent, et ils contiennent de nombreux détails concernant chaque incident et les erreurs qui ont causé l'échec. Ces rapports peuvent être utilisés à des fins d'analyse judiciaire par les administrateurs du domaine afin de corriger les problèmes liés à la configuration de leur système de messagerie ou d'identifier d'autres problèmes, tels que des attaques de phishing en cours. Le type d'échec qui déclenche un rapport d'échec dépend de la valeur de la balise"fo=" dans l'enregistrement DMARC du domaine. Par défaut, un rapport d'échec ne sera généré que si tous les contrôles DMARC sous-jacents échouent (c'est-à-dire si SPF et DKIM échouent tous les deux), mais les domaines peuvent utiliser diverses valeurs de balise"fo=" pour indiquer qu'ils souhaitent recevoir les rapports uniquement en cas d'échec de SPF, uniquement en cas d'échec de DKIM, en cas d'échec de l'un ou de l'autre, ou selon une autre combinaison. Par conséquent, plusieurs Rapports d'échec peuvent être générés à partir d'un seul message en fonction du nombre de destinataires dans la balise"ruf=" de l'enregistrement DMARC, de la valeur de la balise"fo=" et du nombre d'échecs d'authentification indépendants rencontrés pour le message au cours du traitement. Si vous souhaitez limiter le nombre de destinataires auxquels MDaemon enverra un rapport donné, utilisez l'option"*Honorer jusqu'à ce nombre de destinataires DMARC 'rua' et 'ruf*" ci-dessous.

En ce qui concerne le format de rapport, MDaemon ne respecte que la baliserf=afrf (<u>Authentication Failure Reporting Using the Abuse Reporting</u>), qui est le paramètre par défaut de DMARC. Tous les rapports sont envoyés dans ce format, même si l'enregistrement DMARC d'un domaine contient la balise rf=iodef.

> Afin de prendre en charge les rapports d'échec DMARC, MDaemon est entièrement compatible avec le format DMARC : <u>RFC 5965 : An Extensible Format for Email Feedback</u>, <u>RFC</u> 6591 : Rapport d'échec d'authentification utilisant le format de rapport d', <u>RFC 6652 : Rapport d'échec d'authentification SPF</u> (Sender Policy Framework) utilisant le format de rapport d', <u>RFC 6651 : Extensions à DomainKeys Identified Mail (DKIM)</u> pour le rapport d', et <u>RFC 6692 : Ports source dans les ARF</u> (Abuse Reporting Format)RFC-6692.

Lorsque la baliseDMARC "fo=" demande de signaler les échecs liés à SPF, MDaemon envoie des rapports d'échec SPF conformément à la RFC 6522. Dans ce cas, les extensions de cette spécification doivent être présentes dans l'enregistrement SPF du domaine. Les rapports d'échec SPF ne sont pas envoyés indépendamment du traitement DMARC ou en l'absence d'extensions RFC 6522.

Lorsque la baliseDMARC "fo=" demande un rapport sur les échecs liés à la norme DKIM, MDaemon envoie des rapports d'échec DKIM conformément à la RFC 6651. Dans ce cas, les extensions de cette spécification doivent être présentes dans le champ En-tête DKIM-Signature, et le domaine doit publier un enregistrement TXT de rapport DKIM valide dans le DNS. LES RAPPORTS D'ÉCHEC DKIM ne sont pas envoyés indépendamment du traitement DMARC ou en l'absence d'extensions RFC 6651.

Honorer jusqu'à ce nombre de destinataires DMARC 'rua' et 'ruf' (0 = pas de limite) Si vous souhaitez limiter le nombre de destinataires auxquels MDaemon enverra un rapport DMARC global ou un rapport d'échec DMARC, indiquez ici le nombre maximum.

Si la balise"rua=" ou "ruf="d'un enregistrement DMARC contient plus d'adresses que la limite fixée, MDaemon enverra un rapport donné aux adresses listées, dans l'ordre, jusqu'à ce que le nombre maximum d'adresses soit atteint. Non (par défaut), aucune limite n'est fixée.

Envoyer une copie des rapports par e-mail à :

Saisissez ici une ou plusieurs adresses e-mail séparées par des virgules pour leur envoyer une copie de tous les rapports DMARC agrégés et des rapports d'échec DMARC (fo=0 ou fo=1 uniquement).

Métadonnées du rapport DMARC

Utilisez ces options pour spécifier les métadonnées de votre entreprise ou organisation, qui seront incluses dans les rapports DMARC que vous envoyez.

Nom de l'Organisation

Il s'agit de l'entité responsable de la production des rapports DMARC. Il doit s'agir de l'un de vos domaines MDaemon. Sélectionnez le domaine dans la liste déroulante.

Courriel du contact

Utilisez cette option pour spécifier les adresses électroniques locales que les destinataires du rapport peuvent contacter en cas de problèmes avec le rapport. Séparez plusieurs adresses par des virgules.

Informations de contact

Utilisez cette option pour inclure des Informations de contact supplémentaires pour les destinataires du rapport, telles qu'un site web, un numéro de téléphone, etc.

Chemin de retour du rapport

Dans cette option, il s'agit du chemin de retour SMTP (adresse de rebond) utilisé pour les messages de rapport envoyés par MDaemon, en cas de problème de livraison. Utilisez noreply@<mydomain.com> pour ignorer ces problèmes.

Voir aussi

<u>DMARC</u> (इन्डो <u>Vérification DMARC</u> (इक्डो <u>Paramètres DMARC</u> (इक्डो

4.2.2.6.3 Paramètres DMARC

Paramètres DMARC

Les en-têtes canonisés DKIM sont inclus dans les rapports d'échec DMARC

Activez cette option si vous souhaitez inclure les <u>en-têtes canonisés</u> DKIM dans les rapports d'<u>échec</u> al DMARC. Cette option est désactivée par défaut.

Le corps canonisé DKIM est inclus dans les rapports d'échec DMARC

Activez cette option si vous souhaitez inclure le <u>corps canonisé</u> BDKIM dans les <u>rapports d'échec</u> BDARC . Cette option est désactivée par défaut.

Remplacer les IP réservées par "X.X.X.X " dans les rapports DMARC

Par défaut, MDaemon remplace vos Adresses IP réservées par "x.x.x.x "dans les rapports DMARC. Désactivez cette option si vous souhaitez que vos adresses IP réservées soient visibles dans les rapports DMARC. Cette option ne s'applique pas aux données canonisées par DKIM.

Refusées si 'From' est incompatible avec DMARC

Activez cette option si vous souhaitez refuser les messages qui sont incompatibles avec les exigences DMARC concernant la construction de l'en-tête 'From'. Il s'agit de messages comportant plusieurs En-têtes From ou plusieurs adresses électroniques dans un seul En-tête From. Ces messages sont actuellement exemptés du traitement DMARC. Ce paramètre est désactivé par défaut parce que la présence de plusieurs adresses dans un seul en-tête "From" ne constitue pas techniquement une violation du protocole, mais l'activation de ce paramètre permettrait de maximiser la protection DMARC. Ce paramètre n'est appliqué que lorsque <u>la vérification DMARC</u> with the set activée.

Insérer l'en-tête " Precedence : bulk " dans les e-mails de rapport DMARC

Par défaut, MDaemon insère un en-tête de courrier en vrac dans les courriels de rapport DMARC. Décochez cette case si vous ne souhaitez pas insérer cet en-tête.

Inclure les enregistrements DMARC complets dans le fichier journal

Non par défaut, MDaemon consigne l'enregistrement DNS DMARC complet qu'il obtient lors des requêtes DNS DMARC. Désactivez cette option si vous ne souhaitez pas inclure l'enregistrement DMARC complet dans le fichier journal.

Mise à jour automatique du fichier de suffixe public s'il est plus ancien que ce nombre de jours

DMARC nécessite un fichier de suffixes publics pour déterminer de manière fiable les domaines à interroger pour les enregistrements DNS DMARC. Non (par défaut), MDaemon met automatiquement à jour son fichier de suffixes publics lorsqu'il date de plus de 15 jours. Modifiez la valeur de cette option si vous souhaitez mettre à jour le fichier de suffixes publics plus ou moins souvent. Désactivez cette option si vous ne souhaitez pas le mettre à jour automatiquement.

URL du fichier de suffixe public

Il s'agit de l'URL du fichier de suffixe public que MDaemon téléchargera pour l'utiliser dans le cadre de DMARC. Par défaut, MDaemon utilise le fichier situé à l'adresse suivante : http://publicsuffix.org/list/effective_tld_names.dat.

Mettre à jour le fichier de suffixes publics maintenant

Cliquez sur ce bouton pour mettre à jour manuellement le fichier de suffixes publics, à partir de l'*URL du fichier de suffixes publics* spécifiée ci-dessus.

Voir aussi

<u>DMARC</u> চিস্ট <u>Vérification DMARC</u> জিণী <u>Rapport DMARC</u> জিগী <u>Paramètres DKIM</u> জিগী

4.2.2.7 Certification de messages

La Certification des messages est un processus par lequel une entité se porte garante ou "certifie" la bonne conduite d'une autre entité en matière de courrier électronique. Par conséquent, lorsque cette entité de certification est une entité en laquelle un serveur de courrier électronique récepteur a confiance, les messages envoyés à partir d'un domaine qui est cautionné par cette entité peuvent être affichés avec moins de suspicion. Le serveur destinataire peut ainsi être raisonnablement assuré que le domaine d'envoi adhère à un ensemble de bonnes pratiques en matière de courrier électronique et n'envoie pas de spam ou d'autres messages problématiques. La certification est bénéfique car elle permet de s'assurer que les messages ne seront pas soumis par erreur ou inutilement à l'analyse d'un filtre anti-spam. Elle permet également de réduire les ressources nécessaires au traitement de chaque message.

MDaemon prend en charge la Certification des messages grâce au protocole de messagerie "VBR " (Vouch-By-Reference), que MDaemon Technologies a contribué à créer en participant au Conseil d'assurance du domaine (DAC). Le protocole VBR permet aux fournisseurs de services de certification (CSP) ou "certificateurs" de se porter garants des bonnes pratiques de messagerie électronique de domaines spécifiques.

Certification des messages entrants

Il est facile de configurer la fonction de Certification des messages de MDaemon pour vérifier les messages entrants. Il vous suffit de cliquer sur l'option *Activer certification pour les messages entrants* dans la boîte de dialogue Certification VBR (Sécurité | Paramètres de sécurité | Authentification de l'expéditeur | Certification VBR) et d'inclure un ou plusieurs certificateurs auxquels vous faites confiance pour se porter garant des messages entrants (par exemple, vbr. com). (par exemple, vbr.exemple.com). Vous pouvez également choisir d'exempter les messages certifiés du filtrage anti-spam ou de donner à leur score au Filtre anti-spam un ajustement bénéfique.

Certification des messages sortants

Avant de configurer MDaemon pour qu'il insère des données de certification dans les messages sortants, vous devez d'abord faire certifier votre courrier électronique par un ou plusieurs CSP.

Pour configurer votre serveur MDaemon afin qu'il utilise la Certification des messages pour votre courrier sortant, après vous être inscrit auprès d'un CSP :

- Ouvrez la boîte de dialogue Certification VBR : cliquez sur Sécurité | Paramètres de sécurité | Authentification de l'expéditeur | Certification VBR.
- 2. Cliquez sur "Insérer des données de certification dans les messages sortants".
- 3. Cliquez sur "*Configurer un domaine pour la certification des messages*": le dialogue Certification des messages s'ouvre.
- 4. Tapez le *Nom du domaine* dont les messages sortants contiendront les données de certification.
- 5. Utilisez la liste déroulante*Type de messages* pour choisir le type de messages électroniques que votre CSP accepte de certifier pour ce domaine, ou saisissez un nouveau type si le type souhaité n'est pas répertorié.
- 6. Entrez un ou plusieurs CSP qui certifieront le courrier sortant du domaine. Si vous avez plus d'un CSP, séparez-les par un espace.
- 7. Cliquez sur "OK".
- 8. Configurez votre serveur pour qu'il signe les messages sortants du domaine avec <u>DKIM</u> [563], ou veillez à ce qu'ils soient envoyés depuis un serveur approuvé par<u>SPF.</u> [560] Cette mesure est nécessaire pour garantir que le message provient

bien de vous. Un message ne peut être certifié que si le serveur de réception peut d'abord déterminer que le message est authentique.



Spécification VBR - RFC 5518 :

http://tools.ietf.org/html/rfc5518

Pour plus d'informations sur DKIM, consultez le site

http://www.dkim.org/

Voir :

Certification VBR 590

4.2.2.7.1 Certification VBR

Configure a domain for message certification Edit certification configuration file directly
--

Copyright © 1996-2025. All rights reserved. MDaemon Technologies

La boîte de dialogue Certification VBR se trouve à l'adresse suivante : Sécurité | Paramètres de sécurité | Authentification de l'expéditeur | Certification VBR : Sécurité | Paramètres de sécurité | Authentification de l'expéditeur | Certification VBR.

Certification VBR

Activer la certification des messages VBR

Cochez cette case pour activer la certification des messages entrants. Lorsque MDaemon reçoit un message entrant nécessitant une certification, il interroge les fournisseurs de services de certification (CSP) pour savoir si le message doit être considéré comme " certifié ". Si c'est le cas, le message sera exempté du Filtrage anti-spam 725 ou son score sera ajusté, selon l'option que vous avez sélectionnée cidessous.

Nom(s) d'hôte(s) du/des service(s) de certification utilisé(s) (séparez-les par des espaces) : Utilisez ce champ pour entrer les noms d'hôte des services de certification auxquels vous faites confiance. Si vous faites confiance à plusieurs services, séparez chacun d'eux par un espace.

Ne pas appliquer le Filtre anti-spam aux messages certifiés

Choisissez cette option si vous souhaitez que les messages provenant de sources certifiées soient exemptés du Filtre anti-spam.

Ne pas appliquer de politique DMARC restrictive aux messages provenant de sources certifiées

Cette option garantit que les messages vérifiés provenant de sources certifiées ne seront pas pénalisés si le domaine d'envoi publie une <u>politique DMARC</u> mestrictive (c'est-à-dire p=quarantine ou p=reject) et que le message échoue à la vérification DMARC. Cette option est activée par défaut.

Effectuer une vérification VBR même si le message entrant ne contient pas d'en-tête VBR-Info

Activez cette option si vous souhaitez effectuer des vérifications VBR même si les messages entrants ne contiennent pas l'en-tête VBR-Info. Normalement, cet en-tête est nécessaire, mais le contrôle VBR peut fonctionner sans lui. Lorsque l'en-tête est manquant, MDaemon interroge les CSP de confiance en utilisant le type de courrier " all ". Cette option est désactivée par défaut.

Les messages certifiés appliquent ce nombre de points au score du filtre anti-spam

Si vous ne souhaitez pas exempter les messages certifiés du filtrage anti-spam, utilisez cette option pour indiquer le nombre de points dont vous souhaitez ajuster le score du Filtre anti-spam du message. En règle générale, il s'agit d'un nombre négatif afin que les messages certifiés bénéficient d'un ajustement bénéfique. Le paramètre par défaut est "-3.0".

Insérer des données de certification dans les messages sortants

Cochez cette case pour insérer les données de certification dans les messages sortants. Alors, exécutez l'actionsuivante :*Configurer un domaine pour la certification des messages* pour ouvrir la boîte de dialogue Paramètres de certification afin de désigner les domaines spécifiques à certifier et les CSP qui leur sont associés.

Configurer la certification des messages pour un domaine

Après avoir activé l' option*Insérer des données certification dans les messages sortants* ci-dessus, cliquez sur ce bouton pour ouvrir la boîte de dialogue Certification des sortants. Dans cette boîte de dialogue, vous désignerez le domaine dont les messages sortants seront certifiés, les types de messages qui seront certifiés et les CSP associés au domaine.

Modifier directement le fichier de configuration de la certification

Après avoir activé l' option*Insérer les données de certification dans les messages sortants* ci-dessus, cliquez sur ce bouton pour ouvrir le fichier de configuration Vouch-by-Reference (VBR). Tous les domaines que vous avez configurés via le dialogue Paramètres de certification pour utiliser VBR seront listés dans ce fichier, ainsi que les données VBR associées. Vous pouvez utiliser ce fichier pour modifier ces entrées ou en créer de nouvelles manuellement.

Paramètres de certification

ertification Setup			×
To configure a dom the domain name, ti host name of one o	ain for message certifical ne type of mail eligible for r more certification servic	tion you must provide r certification, and the res.	
Domain name		Find	
Messages sent from	i this domain are eligible l	for certification.	
Mail type	all	~	
Use "all" unless this domain sends only messages of a specific type. Custom and vendor defined types can be used by entering them directly into the control above.			ι.
Host name(s) of services willing to certify messages of the above type sent from the above domain (space separated list):			
	C	OK Cancel	

Après avoir activé l' option *Insérer les données certification dans les messages sortants* dans la boîte de dialogue Certification, cliquez sur le bouton *Configurer un domaine pour la certification des messages* pour ouvrir la boîte de dialogue Paramètres de certification. Cette boîte de dialogue permet de désigner le domaine dont les messages sortants seront certifiés, les types de messages qui seront certifiés et les CSP associés au domaine.

Paramètres de certification

Nom de domaine

Utilisez cette option pour entrer le domaine dont les messages sortants seront certifiés.

Recherche

Si vous avez déjà configuré les paramètres de Certification des messages pour un domaine particulier, tapez le *Nom du domaine* puis cliquez sur ce bouton et les paramètres de ce domaine seront listés dans les options de la boîte de dialogue Configuration de la certification.

Type de messages

Utilisez cette liste déroulante pour choisir le Type de messages que le CSP associé a accepté de certifier pour ce domaine. Si le type n'est pas listé, vous pouvez le saisir manuellement.

Nom(s) d'hôte des services...

Entrez les noms d'hôte des CSP qui ont accepté de certifier les messages sortants du domaine (par Exemple, vbr.emailcertification.org). Si vous entrez plus d'un CSP, séparez chacun d'eux par un espace.

Voir :

Certification des messages 588

4.2.2.8 Domaines approuvés

🧐 Paramètres de sécurité - Domaines accepté:	5	×
 Paramètres de sécurité Authentification de l'expéditeur Bouclier IP Authentification SMTP Vérification DKIM Signature DKIM Paramètres DKIM Vérification DMARC Rapports DMARC Paramètres DMARC Certification VBR Domaines acceptés SSL & TLS Autres 	<pre># Domaines acceptés par SPF/Sender ID/DomainKeys/DKIM # # Pour que la signature SPF, Sender ID, DK ou DKIM # ait un effet positif sur un message, le domaine dont il provient doit figurer dans cette liste. # # spf = une signature SPF/Sender ID valide ne suffit pas pour que le domaine soit accept -dk = une signature DK ne suffit pas pour que le domaine soit approuvé # dkim = une signature DKIM valide ne suffit pas pour que le domaine soit approuvé # dkim = une signature DKIM valide ne suffit pas pour que le domaine soit approuvé # dkim = une signature DKIM valide ne suffit pas pour que le domaine soit approuvé # dkim = une signature DKIM valide ne suffit pas pour que le domaine soit approuvé # dkim = une signature DKIM valide ne suffit pas pour que le domaine soit approuvé # dkim = une signature DKIM valide ne suffit pas pour que le domaine soit approuvé # dkim = une signature DKIM valide ne suffit pas pour que le domaine soit approuvé # dkim = une signature DKIM valide ne suffit pas pour que le domaine soit approuvé # dkim = une signature DKIM valide ne suffit pas pour que le domaine soit approuvé # dkim = une signature DKIM valide ne suffit pas pour que le domaine soit approuvé # dkim = une signature DKIM valide ne suffit pas pour que le domaine soit approuvé # dkim = une signature DKIM valide ne suffit pas pour que le domaine soit approuvé # dkim = une signature DKIM valide ne suffit pas pour que le domaine soit approuvé # dkim = une sourcette is sont acceptés. Une entrée par ligne. # Exemple.com # example.com # example.org -spf -sf # example.org -spf -sf # example.org -spf -sf</pre>	*
	•	Ŧ
	OK Annuler Appliquer Aic	le

Étant donné que certains spammeurs et expéditeurs d'e-mails en masse ont commencé à utiliser SPF ou à signer les messages avec une signature DKIM valide, le fait qu'un message soit signé et vérifié ne garantit pas qu'il neserapas considéré comme du spam, même si cela assure que le message provient d'une source valide. C'est pourquoile score de spam d'un messagene sera pas abaissé à la suite d'une vérification SPF ou DKIM, à moins que le domaine repris dans la signature ne figure dans la liste approuvée. Il s'agit essentiellement d'une liste d'autorisation que vous pouvez utiliser pour désigner les domaines autorisés à voir le score de spam de leurs messages réduit lorsque ces messages entrants sont vérifiés.

Lorsqu'un message signé par l'un de ces domaines est vérifié par SPF ou DKIM, son score de spam est réduit conformément aux paramètres figurant dans les écrans<u>Vérification</u> aux paramètres figurant dans les drapeaux énumérés ci-dessous si vous souhaitez empêcher l'une ou l'autre de ces méthodes de vérification de réduire le score. Il existe également un drapeau que vous pouvez utiliser pour empêcher les messages vérifiés de passer par le Filtre anti-spam.

- -spf Ne pas réduire le score de spam pour les messages vérifiés par SPF envoyés par ce domaine.
- -dkim Neréduit pas le score de spam pour les messages vérifiés DKIM provenant de ce domaine.
- -sf Ne pas traiter les messages vérifiés de ce domaine par le Filtre anti-spam.

DMARC et les Domaines approuvés

La<u>vérification DMARC</u> willise également la Domaines approuvés, qui peut La vérification DMARC utilise également la liste approuvée, qui peut être exemptée sur la base des identifiants DKIM vérifiés et des chemins d'accès SPF provenant de sources fiables. Exemple : si un message n'est pas vérifié par DMARC mais qu'il porte une signature DKIM valide provenant d'un domaine figurant sur la liste approuvée, il n'est pas soumis à la politique DMARC punitive (c'est-à-dire qu'il est traité comme si la politique était "p=none"). Il en va de même si la vérification du chemin SPF correspond à un domaine figurant sur la liste approuvée.

4.2.3 Analyse

4.2.3.1 Liste de blocage d'expéditeurs

🤍 Security Manager - Sender Block List	
Security Settings Sender Authentication Screening Screening Screening Host Screen Host Screen SMTP Screen Hijack Detection Spambot Detection Location Screening From Header Screening SSL & TLS Other	Messages are refused if they are from addresses listed here. Image: Domains Image: All domains Image: example.com Image: company.test Image: company.test<
	Ok Cancel Apply Help

La Liste de blocage bloqués se trouve à l'adresse suivante : Sécurité | Paramètres de sécurité | Filtrer. Cette liste contient les adresses qui ne sont pas autorisées à envoyer du trafic de messagerie via votre serveur. Si une adresse de cette liste envoie un message, celui-ci sera refusé au cours de la session SMTP. Cette fonction est utile pour contrôler les utilisateurs problématiques. Les adresses peuvent être bloquées par domaine ou globalement (appliquées à tous les domaines de MDaemon).

Les messages sont refusés s'ils proviennent des adresses ci-dessous sont refusés. Les messages envoyés aux adresses sont refusés.

Cette fenêtre affiche toutes les adresses bloquées, classées par domaine.

Domaine

Sélectionnez le domaine auquel cette adresse bloquée sera associée. Dans d'autres termes, quel domaine souhaitez-vous empêcher de recevoir du courrier provenant de l'adresse spécifiée ? Sélectionnez Tous les domaines dans cette liste pour bloquer l'adresse globalement.

Adresse électronique

Saisissez l'adresse que vous souhaitez bloquer. Les caractères joker sont acceptés. Ainsi, "*@example.net" supprimera tout message provenant d'un utilisateur de "example.net", et "user1@*" supprimera tout message provenant d'une adresse commençant par "user1@", quel que soit le domaine d'où provient le message.

Ajouter

Cliquez sur ce bouton pour ajouter l'adresse désignée à la liste de blocage.

Supprimer

Cliquez sur ce bouton pour supprimer une entrée que vous avez sélectionnée dans la liste.

Vérifier les en-têtes des messages pour les adresses en-tête de la liste FROM : Par défaut, MDaemon applique l'en-tête de la liste FROM à tous les messages.

Non (par défaut), MDaemon applique la liste de blocage aux valeurs extraites des en-têtes From/Sender du message au cours de la session SMTP. Cela permet d'éviter que le message ne soit détecté ultérieurement et déplacé dans la file d'attente des messages erronés par le thread MTA.

Supprimer les messages envoyés par des expéditeurs figurant sur la liste de blocage (sinon, ils sont placés dans la file d'attente des messages indésirables).

Activer cette option si vous souhaitez que MDaemon supprime les messages entrants provenant d'Expéditeurs bloqués. Outre le courrier ordinaire, cette option s'applique également aux messages arrivant via MultiPOP et DomainPOP. Lorsque cette option est désactivée, le message est placé dans la file d'attente des messages erronés (Bad Message Queue) au lieu d'être supprimé. Cette option est désactivée par défaut.



🧐 Paramètres de sécurité - Liste noire de dest	inataires	×
 Paramètres de sécurité Authentification de l'expéditeur Analyse Liste noire d'expéditeurs Étran IP Écran d'hôte Écran SMTP Détournement de compte Robots spammeurs Filtrage de pays SSL & TLS Autres 	Les messages destinés aux adresses de cette liste Tous les domaines example.com company.test Supprimer	sont refusés Domaine Tous les domaines Adresse e-mail Caractères * et ? autorisés. Ajouter
	ОК	Annuler Appliquer Aide

La Liste de blocage de destinataires se trouve à l'adresse suivante : Sécurité | Paramètres de sécurité | Filtrer. Cette liste contient les adresses électroniques qui ne sont pas autorisées à recevoir du courrier par l'intermédiaire de votre serveur. Si une adresse de cette liste reçoit un message, celui-ci sera refusé. Les adresses peuvent être bloquées par domaine ou globalement (appliquées à tous les domaines de MDaemon). La Liste de blocage de destinataires fonctionne uniquement sur les données RCPT de l'enveloppe SMTP (pas sur les en-têtes des messages).

Les messages sont refusés s'ils sont aux adresses ci-dessous sont refusés.

Cette fenêtre affiche toutes les adresses bloquées, classées par domaine.

Domaine

Sélectionnez le domaine auquel cette adresse bloquée sera associée. Dans d'autres termes, quel domaine souhaitez-vous empêcher de recevoir du courrier pour l'adresse spécifiée ? Sélectionnez Tous les domaines dans cette liste pour bloquer l'adresse globalement.

Adresse électronique

Saisissez l'adresse que vous souhaitez bloquer. Les caractères joker sont acceptés, ainsi "*@example.net" supprimera tout message pour tout utilisateur de "example.net", et "user1@*" supprimera tout message pour toute adresse commençant par "user1@", quel que soit le domaine auquel le message est adressé.

Ajouter

Cliquez sur ce bouton pour ajouter l'adresse désignée à la liste de blocage.

Supprimer

Cliquez sur ce bouton pour supprimer une entrée que vous avez sélectionnée dans la liste.

4.2.3.3 Écran IP

🧐 Paramètres de sécurité - Écran IP		×
 Paramètres de sécurité Authentification de l'expéditeur Analyse Liste noire d'expéditeurs Liste noire de destinataires Écran IP Écran d'hôte Écran SMTP Détournement de compte Robots spammeurs Filtrage de pays SSL & TLS Autres 	Écran IP Toutes les IP 2001:0:4137:9e76:240f:c00:f5eb:d7e3 127.0.0.1	Supprimer Haut Bas Importer Nouveau Action par défaut Sélectionnez une IP ou le noeud ‹default> pour modifier l'action par défaut.
	OK A	nnuler Appliquer Aide

L'Écran IP est filtré par : Sécurité " Paramètres de sécurité | Filtres. Il permet de définir les adresses IP distantes spécifiques qui seront autorisées ou non à se connecter à vos adresses IP locales. Les adresses IP distantes que vous placez dans l'Écran IP peuvent être associées soit à toutes vos adresses IP locales, soit à des adresses IP individuelles. La notation CIDR et les caractères génériques *, # et ? sont autorisés.

Exemple :

* * * *	Correspond à n'importe quelle adresse IP.
#.#.#.#	Correspond à n'importe quelle adresse IP
192.*.*.*	Correspond à toute adresse IP commençant par 192
192.168.*.239 192.168.255.239.	Correspond aux adresses IP comprises entre 192.168.0.239 et

192.168.0.1 ?? Correspond aux adresses IP comprises entre 192.168.0.100 et 192.168.0.199.

Nouvel élément de l'Écran IP

Pour créer une nouvelle entrée d'Écran IP, cliquez sur **Nouvelle**. La boîte de dialogue Nouvelle IP s'ouvre et permet de créer l'entrée.

IP locale

Dans la liste déroulante, choisissez "Toutes les IP" ou l'IP spécifique à laquelle cet élément s'appliquera.

IP distante (CIDR, * ? et # autorisés)

Saisissez l'adresse IP distante que vous souhaitez ajouter à la liste, associée à l'IP locale désignée ci-dessus.

Acceptées connexions

En sélectionnant cette option, les adresses IP distantes spécifiées seront autorisées à se connecter à l'adresse IP locale associée.

Refuser les connexions

En sélectionnant cette option, les adresses IP distantes spécifiées ne seront PAS autorisées à se connecter à l'adresse IP locale associée. La connexion sera refusée ou abandonnée.

Ajouter

Dans les options ci-dessus, cliquez sur ce bouton pour ajouter l'entrée à la liste.

Importer

Sélectionnez une adresse IP et cliquez sur ce bouton si vous souhaitez importer des adresses IP à partir d'un fichier APF ou .htaccess. La prise en charge de ces fichiers par MDaemon est actuellement limitée à ce qui suit :

- les options "deny from" et "allow from" sont prises en charge
- seules les valeurs IP sont importées (pas les noms de domaine)
- la notation CIDR est autorisée, mais les adresses IP partielles ne le sont pas.
- Chaque ligne peut contenir un nombre quelconque d'adresses IP séparées par des espaces ou des virgules. Exemple : "deny from 1.1.1.1 2.2.2.2/16", ""3.3.3.3, 4.4.4.4, 5.5.5.5", etc.
- Les lignes starts with # sont ignorées.

Supprimer

Pour supprimer une entrée, sélectionnez-la dans la liste et cliquez sur **Supprimer**.

Non (par défaut)

Pour spécifier l'action par défaut pour les connexions provenant d'adresses IP distantes qui n'ont pas été définies, sélectionnez une adresse IP dans la liste et cliquez sur **accepter** ou **refuser**. Une fois qu'une action par défaut a été spécifiée, vous pouvez la modifier en sélectionnant le nœud "<défaut>" sous l'adresse IP, puis en sélectionnant le nouveau paramètre par défaut.

Acceptées

Lorsque cette option est choisie, les connexions provenant de cette Adresses IP qui ne sont pas spécifiquement définies dans l'Écran IP seront acceptées.

Refusées

Lorsque cette option est choisie, les connexions provenant de toutes les adresses IP qui ne sont pas spécifiquement définies dans l'Écran IP sont filtrées, ou refusées.



Paramètres de filtrage

Appliquer l'Écran IP aux connexions MSA

Cette option permet d'appliquer l'Écran IP aux connexions établies sur le port MSA du serveur. Normalement, cela n'est pas nécessaire. Ce paramètre est Non (par défaut).

4.2.3.4 Écran d'hôte

🧐 Paramètres de sécurité - Écran d'hôte		×		
 Paramètres de sécurité Authentification de l'expéditeur Analyse Liste noire d'expéditeurs Liste noire de destinataires Écran IP Écran d'hôte Écran SMTP Détournement de compte Robots spammeurs Filtrage de pays SSL & TLS Autres 	Paramètres de filtrage	Supprimer Haut Bas Nouveau Action par défaut Sélectionnez une IP ou le noeud <default> pour modifier l'action par défaut. accepter @ refuser</default>		
	Former la connexion après un refus de l'Écran d'hôte			
	Fermer la connexion après EHLO (ne pas attendre l'a El connexion après EHLO (ne pas attendre l'a	authentification)		
OK Annuler Appliquer Aide				

L'Écran d'hôte se trouve à l'adresse suivante : Sécurité | Paramètres de sécurité | Filtres. Il permet de définir quels hôtes distants seront autorisés à se connecter à vos adresses IP locales. Vous pouvez spécifier une liste d'hôtes et configurer le serveur pour qu'il n'autorise que les connexions en provenance de ces hôtes, ou vous pouvez le configurer pour qu'il refuse les connexions en provenance des hôtes répertoriés. Le filtrage des hôtes compare les valeurs EHLO et PTR déterminées au cours de la session SMTP aux valeurs spécifiées ici.

Nouvel élément de l'Écran d'hôte

Pour créer une nouvelle entrée dans l'Écran d'hôte, cliquez sur **Nouvelle**entrée . La boîte de dialogue Nouvel élément de l'Écran d'hôte s'ouvre et permet de créer l'entrée.

IP locale

Utilisez cette liste déroulante pour choisir l'adresse IP locale à laquelle l'entrée de l'Écran hôte s'appliquera. Choisissez "Toutes les adresses IP" si vous souhaitez qu'elle s'applique à toutes vos adresses IP locales.

Hôte distant (* et # acceptés)

Saisissez l'hôte distant que vous souhaitez ajouter à la liste, associé à l'IP locale désignée ci-dessus.

Acceptées connexions

La sélection de cette option signifie que l'Hôte distant spécifié sera autorisé à se connecter à l'Adresse IP locale associée.

Refuser les connexions

En sélectionnant cette option, l'Hôte distant spécifié ne sera PAS autorisé à se connecter à l'Adresse IP locale associée. La connexion sera refusée ou abandonnée.

Supprimer

Pour supprimer une entrée, sélectionnez-la dans la liste et cliquez sur Supprimer.

Non (par défaut)

Pour spécifier l'action par défaut pour les connexions provenant d'Hotes distants qui n'ont pas été définis, sélectionnez une adresse IP dans la liste et cliquez sur **Accepter** ou **Refuser**. Une fois qu'une action par défaut a été spécifiée, vous pouvez la modifier en sélectionnant le nœud "<défaut>" sous l'adresse IP, puis en sélectionnant le nouveau paramètre par défaut.

Acceptées

Lorsque cette option est choisie, les connexions en provenance de tout hôte non spécifiquement défini dans l'Écran d'hôte sont acceptées.

Refusées

Lorsque cette option est choisie, les connexions en provenance de tout hôte qui n'est pas spécifiquement défini dans l'Écran d'hôte seront refusées.



L'Écran d'hôte ne filtrera jamais les Hôtes<u>autorisés</u> 553 ou locaux.

Paramètres de filtrage

Filtrer par hôte les connexions MSA

Cette option permet d'appliquer l'Écran d'hôte aux connexions établies sur le port MSA du serveur. Ce paramètre est activé par défaut.

Filtrer la connexion en cas de Refus d'Écran d'hôte

Lorsque cette option est activée, la connexion est immédiatement filtrée en cas de refus de l'Écran d'hôte.

Interrompre la connexion après EHLO (ne pas attendre l'authentification)

Activez cette option si vous souhaitez interrompre les connexions interdites immédiatement après EHLO/HELO. Normalement, il faut attendre l'authentification. Ce paramètre est activé par défaut.

4.2.3.5 Écran SMTP

 Security Manager - SMTP Screen Security Settings Relay Control Reverse Lookups POP Before SMTP Trusted Hosts Trusted IPs Sender Authentication Screening Sender Block List Recipient Block List IP Screen Hjack Detection Spambot Detection Location Screening From Header Screening SSL & TLS Other 	SMTP Screening (requires Dynamic Screening) Block IPs that connect more than 5 times in 5 minutes (also applies to POP and IMAP) Block IPs that cause this many failed RCPTs 3 Block IPs that cause this many failed RCPTs 3 Block IPs that cause this many failed RCPTs 3 Block IPs that send this many RSETs (0 = no limit) 20 The above are subject to the Dynamic Screening allow list and block IPs for the length of time specified by the Dynamic Screening system. You can see all the IPs blocked by the above by viewing the Dynamic Screening block list. O close SMTP session after blocking IP Allow list Do not block IP when SMTP authentication is used Advanced Send notification when IP is blocked Vertication is used IP History Save IP addresses of login attempts so new and previously-failed IPs can be reported in the Screening log Forget IP addresses after this many days 365 (0 = never)
	Ok Cancel Apply Help

L'Écran SMTP permet de bloquer les adresses IP qui se connectent à MDaemon trop souvent en l'espace d'un certain nombre de minutes. Vous pouvez également bloquer les adresses qui provoquent trop d'échecs de RCPT et celles qui envoient trop de commandes RSET. L'écran SMTP nécessite un Écran dynamique et utilise la <u>Liste</u> <u>blocage dynamique</u> at la <u>Liste d'autorisation dynamique</u>.

Bloquer les IP bloquées qui se connectent plus de [X] fois en [X] minutes.

Cochez cette case si vous souhaitez bloquer temporairement les adresses IP qui se connectent à votre serveur un nombre excessif de fois au cours d'une période limitée. Indiquez le nombre de minutes et le nombre de connexions autorisées au cours de cette période. Les adresses sont bloquées pendant la durée spécifiée sur l'écran<u>Auth Failure Tracking (Suivi des échecs d'authentification)</u> Cette option s'applique également aux connexions POP et IMAP.

Bloquer les IP bloquées à l'origine de ce nombre d'échecs de RCPT

Lorsqu'une adresse IP provoque ce nombre d'erreurs "Destinataire inconnu" au cours d'une session de messagerie, elle est automatiquement bloquée pour la durée spécifiée dans l'écran<u>Auth Failure Tracking (Suivi des échecs d'authentification</u>) Des erreurs fréquentes de type "Destinataire inconnu" sont souvent un indice que l'expéditeur est un spammeur, étant donné que les spammeurs tentent généralement d'envoyer des messages à des adresses obsolètes ou incorrectes.

Bloquer les IP bloquées qui envoient autant de RSET (0 = pas de limite)

Utilisez cette option si vous souhaitez bloquer toute adresse IP qui émet le nombre désigné de commandes RSET au cours d'une seule session de courrier. Utilisez "0" si vous ne souhaitez pas fixer de limite. Il existe une option similaire dans l' écran <u>Serveurs</u> (soi), sous Paramètres des serveurs, qui peut être utilisée pour fixer une limite stricte au nombre de commandes RSET autorisées. Une adresse IP bloquée le restera pendant la durée spécifiée dans l' écran <u>Auth Failure Tracking (Suivi des</u> échecs d'authentification) (654).

Fermer la session SMTP après avoir bloqué l'IP

L'activation de cette option permet à MDaemon de fermer la session SMTP après le blocage de l'adresse IP. Cette option est activée par défaut.

Ne pas bloquer l'IP lorsque l'authentification SMTP est utilisée

Cochez cette case si vous souhaitez que les expéditeurs qui authentifient leurs sessions lentifiées avant l'envoi soient exemptés de l'Écran dynamique. Cette option est activée par défaut.

Envoyer une notification lorsque l'IP est bloquée

Par défaut, lorsqu'une adresse IP est automatiquement bloquée par le système d'Écran dynamique, les options <u>Rapports de blocage des adresses IP de l</u> best l'Écran dynamique sont utilisées pour vous avertir de cette action. Décochez cette case si vous ne souhaitez pas être averti lorsqu'une adresse IP est bloquée en raison de la fonction de filtrage SMTP.

Liste d'autorisation

Cliquez sur ce bouton pour ouvrir la <u>Liste d'autorisation dynamique</u>. Les adresses IP qui y figurent sont Exclure les adresses "De" de l'Écranran SMTP.

Optionsavancées

Ce bouton permet d'ouvrir la boîte de dialogue Écran<u>dynamique.</u>

Historique des IP

Enregistrez les adresses IP des tentatives de connexion afin que les nouvelles adresses IP et celles ayant échoué précédemment puissent être signalées dans le journal de filtrage.

Dans le défaut, les tentatives de connexion SMTP/IMAP/POP sont enregistrées, de sorte que les nouvelles adresses IP et celles qui ont échoué précédemment puissent être signalées dans le journal d'Écran.

Oubliez les adresses IP après ce nombre de jours [xxx] (0 = jamais)

Cette option permet de spécifier la durée pendant laquelle les adresses IP enregistrées seront supprimées. Elles sont sauvegardées 365 jours par défaut. Utilisez "0" dans cette option si vous ne souhaitez jamais les supprimer.

4.2.3.6 Détournement de compte

💛 Security Manager - Hijack Detection	×
Security Settings Sender Authentication Sercening Sender Block List Recipient Block List IP Screen Host Screen SMTP Screen Hijack Detection Location Screening From Header Screening SSL & TLS Other	Account Hijack Detection Some features operate only on authenticated sessions from local accounts. ↓ Limit messages sent from local IPs to 500 msgs in 30 minutes ↓ Limit messages sent from local IPs to 500 msgs in 500 minutes ↓ Limit messages sent from all other IPs to 500 msgs in 500 minutes ↓ Limit access to 5 connections from differing IPs in 30 minutes ↓ Include LAN IPs when limiting local IPs ↓ Send 50 when limit is reached (otherwise 40×1) ↓ Freeze accounts when limit is reached ↓ If an account causes 5 5xx RCPT errors within 10 minutes: ↓ Freeze the account (the admin will have to unfreeze) Exempt list
	Ok Cancel Apply Help

Détection de détournement de compte

Les options de cet écran permettent de détecter un compte MDaemon éventuellement détourné et de l'empêcher automatiquement d'envoyer des messages via votre serveur. Exemple : si un spammeur a obtenu l'adresse électronique et le mot de passe d'un compte, cette fonction peut l'empêcher d'utiliser ce compte pour envoyer des courriers indésirables en masse via votre système. Vous pouvez définir un nombre maximum de messages pouvant être envoyés par un compte en un certain nombre de minutes, en fonction de l'adresse IP à partir de laquelle il se connecte. Vous pouvez également choisir de désactiver les comptes qui atteignent cette limite. Il existe également une Exclure les adresses "À De" qui peut être utilisée pour exempter certaines adresses de cette restriction. Ce compte Piratage Detection est activé par défaut.



Le Piratage de détournement de compte ne s'applique qu'aux comptes locaux sur des sessions authentifiées, et le compte Postmaster est automatiquement exempté.

Limiter les messages envoyés à partir d'IP réservées à [xx] msgs en [xx] minutes

Cette option permet d'empêcher les comptes MDaemon qui se connectent à partir d'adresses IP réservées d'envoyer plus que le nombre de messages spécifié pendant [%MINUTES] minutes supplémentaires. Les adresses IP réservées sont pour la plupart définies par les RFC (par exemple, 127.0.0.*, 192.168.*.*, 10.*.*.*, 172.16.0.0/12, ::1, FD00::/8, FEC0::/10, et FE80::/64).

Limiter les messages envoyés depuis les IP locales à [xx] msgs en [xx] minutes

Cette option permet d'empêcher les comptes MDaemon se connectant à partir de n'importe quelle IP locale d'envoyer plus que le nombre de messages spécifié pendant le nombre de minutes indiqué. Les IP locales sont toutes les adresses IP configurées pour l'un de vos domaines MDaemon.

Limiter les messages envoyés depuis toutes les autres IP à [xx] msgs en [xx] minutes Cette option permet d'empêcher les comptes MDaemon se connectant à partir d'autres IP d'envoyer plus que le nombre de messages spécifié pendant le nombre de minutes supplémentaires.

Limiter l'accès à [xx] connexions à partir d'autres IP en [xx] minutes

Utilisez cette option pour limiter le nombre de connexions provenant d'adresses IP différentes autorisées pendant le nombre de minutes spécifié. Exemple : dans des circonstances normales, si votre compte est accédé à partir de dix adresses IP différentes en l'espace de quelques minutes, il est probable que le compte ait été piraté. Cette option est désactivée par défaut.

Inclure les IP locales dans la limitation des IP locales

Par défaut, <u>les IP locales</u> sont incluses lorsque vous utilisez l'option "*Limiter les messages envoyés à partir des IP locales…*" ci-dessus. Décochez cette case si vous ne souhaitez pas inclure les IP locales lors de la limitation des IP locales.

Envoyer 5XX lorsque la limite est atteinte (sinon 4XX)

Par défaut, lorsque l'une des limites est atteinte, MDaemon envoie un code de réponse 5XX au compte piraté. Désactivez cette option si vous souhaitez envoyer un code 4XX à la place.

Figer les comptes lorsque la limite est atteinte

Cochez cette case si vous souhaitez figer les comptes qui tentent d'envoyer un nombre de messages supérieur à la limite autorisée. Dans ce cas, le serveur envoie une erreur 552, la connexion est interrompue et le compte est immédiatement figé. Le compte figé ne pourra plus envoyer de courrier ni consulter son courrier, mais MDaemon acceptera toujours le courrier entrant pour ce compte. Enfin, lorsque le compte est figé, un e-mail est alors envoyé au postmaster à propos du compte. Si le postmaster souhaite réactiver le compte, il lui suffit de répondre au message.

Si un compte provoque [xx] erreurs RCPT 5xx dans un délai de [xx] minutes

Cette option permet de contrôler le nombre de fois qu'un compte tente d'envoyer des messages à un destinataire non valide dans un laps de temps donné. Le spam se caractérise par le fait que les messages sont souvent envoyés à un grand nombre de destinataires non valides, car le spammeur tente de les envoyer à d'anciennes adresses électroniques ou d'en deviner de nouvelles. Dans ce cas, si un compte MDaemon commence à envoyer des messages à un nombre important de destinataires non valides en peu de temps, c'est une bonne indication que le compte a été piraté et qu'il est utilisé pour envoyer du spam. L'utilisation de cette option avec l'option"*Figer les comptes...*" ci-dessous peut permettre d'arrêter un compte piraté avant qu'il ne soit trop endommagé. Dans cette option, un destinataire non valide est valide lorsqu'un code d'erreur 5xx apparaît en réponse à une commande RCPT lors de l'envoi du courrier du compte.

Figer le compte (l'administrateur devra le dégeler)

Utilisez cette option si vous souhaitez figer un compte lorsque le seuil"*Si un compte provoque [xx] erreurs RCPT 5xx*..." ci-dessus est atteint. Lorsque cela se produit, l'administrateur en sera informé par courriel, afin qu'il puisse enquêter sur le problème et débloquer le compte.

Liste des exceptions

Utilisez la *Liste des* comptes exemptés pour désigner les adresses que vous souhaitez exempter de la Détection détournement de compte. Les caractères génériques sont autorisés. Exemple :"newsletters@example.com" exempte le compte MDaemon "newsletters" de example.com, tandis que "*@newsletters.example.com" exempte tous les comptes MDaemon appartenant au domaine newsletters.example.com. Le compte Postmaster est automatiquement exempté de la Détection détournement de compte.

4.2.3.7 Robots spammeurs

Paramètres de sécurité - Robots spammeur - Paramètres de sécurité	s La détection de robots spammeurs observe les IP utilisées o un temps donné. Si trop d'IP différentes sont utilisées, vous	dans les chemins de retour pendant
Authentification de l'expéditeur	Activer la détection de robots spammeurs	
- Liste noire d'expéditeurs	Nombre max. d'IP différentes autorisées pendant l'intervalle de temps	10 Liste blanche
Liste noire de destinataires Écran IP	Intervalle de temps (minutes)	10
Ecran d'hôte Ecran SMTP Détournement de compte Robots spammeurs En Filtrage de pays SSL & TLS E Autres	 Mettre les chemins de retour en infraction sur liste noire pendant (minutes) Mettre les IP en infraction sur liste noire pendant (minutes) Réponse SMTP (laissez le champ vide pour utiliser la ré Ve pas suivre les connexions authentifiées Ne pas suivre les connexions provenant d'IP autorisit 	10 Avancé 4320 Avancé ponse par défaut) :
	ΟΚ	nnuler Appliquer Aide

La détection des spambots suit les adresses IP que chaque valeurSMTP MAIL (chemin de retour) utilise au cours d'une période donnée. Si le même chemin de retour est utilisé par un nombre excessif d'adresses IP différentes dans un court laps de temps, cela peut indiquer l'existence d'un réseau de spambots. Lorsqu'un spambot est détecté, la connexion en cours est immédiatement interrompue et la valeur du chemin de retour est optionnellement bloquée pendant une durée que vous spécifiez Vous pouvez également, à titre facultatif bloquer toutes les adresses IP bloquées pour une période déterminée.

Activer la détection des spambots

Cliquez sur cette case pour activer la détection des spambots. Elle est désactivée par défaut.

Nombre maximum d'adresses IP différentes autorisées pendant l'intervalle de temps Il s'agit du nombre d'adresses IP différentes à partir desquelles un chemin de retour donné peut se connecter pendant l'intervalle de temps spécifié.

Intervalle de temps (en minutes)

Dans ce champ, vous pouvez spécifier l'intervalle de temps (en minutes) à utiliser pour la détection des réseaux de spambots.

Liste des exceptions

Cliquez sur ce bouton pour ouvrir la liste d'exemptions de la détection de spambots Exceptions. Vous pouvez y spécifier les adresses IP, les expéditeurs et les destinataires qui sont exemptés de la détection des spambots.

Bloquer les chemins de retour offensants pendant ce nombre de minutes

Utilisez cette option si vous souhaitez bloquer les chemins de retour des spambots détectés. MDaemon n'acceptera pas les messages dont le chemin de retour est bloqué pendant le nombre de minutes indiqué. Cette option est activée par défaut.

Avancé

Cliquez sur ce bouton pour ouvrir le fichier des expéditeurs de spambots. Il affiche les chemins de retour actuellement bloquées et le nombre de minutes restantes avant qu'elles ne soient supprimées de la liste de liste de blocage.

Bloquer les IP bloquées pendant (en minutes)

Utilisez cette option si vous souhaitez bloquer les adresses IP des spambots détectés. MDaemon n'acceptera pas les messages provenant d'une adresse IP bloquée pendant le nombre de minutes indiqué. Cette option est désactivée par défaut.

Avancé

Cliquez sur ce bouton pour ouvrir le fichier des adresses IP des spambots. Il affiche les Adresses IP actuellement bloquées et le nombre de minutes restantes avant la fin de la période de blocage. actuellement bloquées et le nombre de minutes restantes avant qu'elles ne soient retirées de la liste. Liste de blocage.

Réponse SMTP (laissez le champ vide pour utiliser le paramètre par défaut)

Utilisez cette option si vous souhaitez personnaliser la réponse SMTP aux spambots qui tentent d'envoyer des messages à partir d'un chemin de retour ou d'une adresse IP bloqués. d'un chemin de retour ou d'une adresse IP bloquée. MDaemon renvoie la réponse SMTP suivante "551 5.5.1 <votre texte personnalisé>", au lieu de la réponse par défaut. Utilisez les paramètres par défaut pour utiliser la réponse par défaut de MDaemon.

Ne pas suivre les connexions si elles sont authentifiées

Par défaut, MDaemon ne suit pas les sessions<u>authentifiées</u> wi pour la détection des spambots. Décochez cette case si vous ne souhaitez pas exempter les connexions authentifiées.

Ne pas suivre les connexions provenant d'IP autorisées

Par défaut, la détection des spambots ne suit pas les connexions provenant d' adresses<u>IP autorisées.</u> Décochez cette case si vous ne souhaitez pas exclure les IP autorisées.

4.2.3.8 Filtrage de pays



Filtrage de l'emplacement

Le filtrage d'adresses est un système de blocage géographique qui permet de bloquer les connexionsSMTP, POP, IMAP, Webmail, ActiveSync, <u>AutoDiscovery</u>, XML API, MDaemon Remote Admin, CalDAV/CardDAV, XMPP et Minger provenant de régions du monde non autorisées. MDaemon détermine le pays associé à l'adresse IP de connexion, puis bloque cette connexion si elle provient d'un lieu restreint, et ajoute une ligne au journal de l'Écran IP. Pour le protocole SMTP, le filtrage des emplacements peut éventuellement bloquer uniquement les connexions utilisant AUTH. Cela s'avère utile, Exemple, si vous n'avez pas d'utilisateurs dans un pays spécifique mais que vous souhaitez tout de même pouvoir recevoir du courrier de ce pays. De cette façon, vous ne bloquerez que ceux qui tentent de se connecter à votre serveur.

Le dossier\MDaemon\Geo\ contient des fichiers de base de données qui servent de base de données principale des adresses IP des pays. Les fichiers ont été fournis par MaxMind (www.maxmind.com), et des mises à jour peuvent être téléchargées sur leur site si vous le souhaitez.

Activer le filtrage des emplacements

Le Filtrage par localisation est activé par défaut, mais aucune région ni aucun pays n'est bloqué ; MDaemon se contente de journaliser le pays ou la région de connexion. Pour bloquer un emplacement, cliquez sur la case jusqu'à ce qu'une coche apparaisse en regard de la région ou du pays que vous souhaitez bloquer. Si vous souhaitez bloquer uniquement les connexions AUTH, ce qui signifie que les connexions SMTP seront toujours autorisées, cliquez à nouveau sur la case pour qu'elle soit complètement remplie.

Tout sélectionner/Désélectionner

Dans ce bouton, vous pouvez sélectionner ou désélectionner tous les emplacements de la liste.

Afficher

Cliquez sur ce bouton pour afficher un fichier texte contenant la liste de tous les sites actuellement bloqués par le système de filtrage des sites. Si vous cochez/décochez une case dans la liste des lieux, le bouton *Afficher* ne sera disponible qu'après avoir cliqué sur **Appliquer**.

Liste d'autorisation

Ce bouton permet d'ouvrir la <u>Liste d'autorisation de l'Écran dynamique</u>, qui est également utilisée pour le filtrage de localisation. Si vous souhaitez exempter une adresse IP de l'Écran IP, cliquez sur ce bouton et indiquez l'adresse IP ainsi que la date d'expiration de l'entrée.

Ajouter l'en-tête "X-MDOrigin-Country" aux messages

Non par défaut, lorsque le filtrage d'adresses est activé, que des sites soient bloqués ou non, MDaemon insère l'en-tête "x-MDOrigin-Country" dans les messages, à des fins de filtrage du contenu ou autres. Cet en-tête contient les codes ISO 3166 à deux lettres des pays et des continents. Décochez cette case si vous ne souhaitez pas insérer l'en-tête dans les messages. **Ajouter I'IP à l'Écran Dynamique si une tentative d'AUTH est effectuée lorsque désactivé** Par défaut, l'Écran dynamique ajoutera l'IP d'une connexion SMTP à la <u>Liste de</u> <u>blocage dynamique</u> ajoutera de s'authentifier alors que l'authentification est désactivée.

4.2.3.9 Analyse de l'en-tête From



Filtrage de l'en-tête From :

Cette fonction de sécurité modifie l'en-tête "From :" des messages entrants de manière à ce que la partie de l'en-tête réservée au nom contienne à la fois le nom et l'adresse électronique. Cela permet de lutter contre une tactique couramment utilisée dans les spams et les attaques, qui consiste à faire croire que le message provient de quelqu'un d'autre. Lorsqu'ils affichent une liste de messages, les clients de messagerie n'affichent généralement que le nom de l'expéditeur au lieu du nom et de l'adresse électronique. Pour voir l'adresse électronique, le destinataire doit d'abord ouvrir le message ou effectuer une autre action, comme cliquer avec le bouton droit de la souris sur l'entrée, survoler le nom, etc. C'est pourquoi les attaquants construisent généralement un e-mail de manière à ce qu'une personne ou un nom de société légitime apparaisse dans la partie visible de l'en-tête "From :", tandis qu'une adresse électronique illégitime est cachée. Exemple : l'en-tête "From :" d'un message peut être "En-têteBank and Trust" <lightfingers.klepto@example.com>, mais votre client peut afficher uniquement "En-tête Bank and Trust" en tant qu'expéditeur. Cette fonction modifie la partie visible de l'en-tête pour afficher les deux parties. Dans l'Exemple cidessus, l'expéditeur serait désormais "Honest Bank and Trust

(lightfingers.klepto@example.com)" <lightfingers.klepto@example.com>, ce qui vous indique clairement qu'il s'agit d'un message frauduleux.

Ajouter l'adresse électronique au nom affiché

Activez cette option si vous souhaitez modifier la partie visible par le client de l'entête "From :" des messages entrants afin d'y inclure le nom et l'adresse électronique de l'expéditeur. La construction du nouvel en-tête passera de "Nom de l'expéditeur" <mailbox@example.com> à "Nom de l'expéditeur (mailbox@example.com) " <mailbox@example.com>. Ceci ne s'applique qu'aux messages destinés aux utilisateurs locaux, et cette option est désactivée par défaut. Réfléchissez bien avant d'activer cette option, car certains utilisateurs ne s'attendent pas à ce que l'en-tête From : soit modifié et ne le souhaitent pas, même si cela peut les aider à identifier des courriels frauduleux.

Placer l'adresse électronique avant le nom

Lorsque vous utilisez l'option *Ajouter l'adresse électronique à l'affichage du nom* ci-dessus, activez cette option si vous souhaitez intervertir le nom et l'adresse électronique dans l'en-tête "From :" modifié, en plaçant l'adresse électronique en premier. Dans l'exemple ci-dessus, "Nom de

l'expéditeur"<mailbox@example.com> serait remplacé par :

"mailbox@example.com (Nom de l'expéditeur)" <mailbox@example.com>.

Remplacer les adresses électroniques non concordantes dans les noms affichés par des adresses réelles

Une autre tactique utilisée dans le spam consiste à placer un nom et une adresse électronique apparemment légitimes dans la partie "display-name" de l'en-tête "From :", même s'il ne s'agit pas de l'adresse électronique d'envoi réelle. Utilisez cette option si vous souhaitez remplacer l'adresse électronique visible dans les messages de ce type par l'adresse actuelle de l'expéditeur.

Ne pas appliquer ces fonctionnalités aux messages authentifiés

Cochez cette case si vous ne souhaitez pas appliquer les options de Filtrage de l'Entête aux messages entrants qui ont été authentifiés par MDaemon.

Liste d'exceptions

Utilisez cette option pour ajouter des adresses à l'Exclure les adresses "En-tête TO :". Les messages envoyés aux adresses listées ne verront pas leurs en-têtes "From :" modifiés.
4.2.4 SSL & TLS

MDaemon prend en charge le protocole Secure Sockets Layer (SSL)/Transport Layer Security (TLS) pour les services suivants <u>SMTP, POP, IMAP</u> [614], et pour l'Administration à distance de MDaemon et le Webmail, [614] <u>MDaemon Remote Admin</u> [621] et le <u>serveur</u> <u>Webmail.</u> [617] Le protocole SSL, développé par Netscape Communications Corporation, est la méthode standard pour sécuriser les communications Internet serveur/client. Il permet l'authentification du serveur, le cryptage des données et, en option, l'authentification du client pour les connexions TCP/IP. En outre, comme le protocole SSL est intégré dans tous les principaux navigateurs actuels, il suffit d'installer un certificat numérique valide sur votre serveur pour activer les capacités SSL du navigateurlors de la connexion à MDRA ou Webmail.

Si vous vous connectez aux ports de messagerie standard via un client de messagerie au lieu d'utiliser le Webmail, MDaemon supporte l'extension STARTTLS sur TLS pour SMTP et IMAP, et l'extension STLS pour POP3. Cependant, votre client doit d'abord être configuré pour utiliser SSL, et il doit prendre en charge ces extensions - tous les clients de messagerie ne les prennent pas en charge. Utilisez les pages<u>Liste</u> <u>STARTTLS</u> et <u>Liste STARTTLS</u> [527] pour désigner les hôtes et adresses spécifiques qui ne doivent pas ou doivent, respectivement, utiliser STARTTLS.

La boîte de dialogue SSL & TLS contient également une page permettant d'activer <u>DNSSEC</u> (DNS Security Extensions), la page <u>SMTP Extensions</u> (DNS Security Extensions), la page <u>SMTP Extensions</u> (DNS Security Extensions), la page <u>Let's Encrypt</u> (DNS Security Extensity (DNS Security Extensions), la page <u>Let's</u>

Les options permettant d'activer et de configurer SSL se trouvent dans la section SSL & TLS de la boîte de dialogue Paramètres de sécurité : Sécurité | Gestionnaire de sécurité | SSL & TLS. Les paramètres du port SSL pour SMTP, POP3 et IMAP se trouvent dans l' écran Ports 106 à l'adresse suivante : Configuration | Paramètres du serveur | DNS & TLS Configuration | Paramètres du serveur | DNS & TLS Configuration | Paramètres du serveur | DNS & IPs. Les ports HTTPS pour Webmail 617 et MDaemon Remote Admin 621 sont situés sur leurs écrans respectifs.

Pour plus d'informations sur la création et l'utilisation des certificats SSL, voir :

Créer et utiliser des certificats SSL. 974

-

Le protocole SSL & TLS est traité dans la RFC-4346 : <u>The Transport Layer Security</u> (TLS) Protocol Version 1.1The

L'extension STARTTLS pour SMTP est traitée dans le document RFC-3207 : <u>SMTP</u> <u>Service Extension for Secure SMTP over Transport Layer SecuritySMTP</u>

L'utilisation de TLS avec les protocoles IMAP et POP3 entrant est traitée dans le RFC-2595 : <u>Using TLS with IMAP, POP3 and ACAPUsing</u>

DNSSEC (DNS Security Extensions) est défini dans : <u>RFC-4033</u> : <u>DNS Security</u> <u>Introduction and RequirementsRFC-4033</u> et <u>RFC-4035</u> : <u>Protocol Modifications for the</u> <u>DNS Security ExtensionsRFC-4035</u>) en tant que

Pour une description complète de RequireTLS, voir : <u>RFC 8689 : SMTP Require TLS</u>.

La prise en charge de MTA-STS est décrite dans la <u>RFC 8461 : MTA-STS Strict</u> <u>Transport Security (MTA-STS)</u>).

Les Rapports TLS sont décrits dans la RFC 8460 : SMTP Rapports TLS.

Voir :

 SSL & TLS | MDaemon
 614

 SSL & TLS | Webmail
 617

 SSL & TLS | MDaemon Remote Admin
 621

4.2.4.1 MDaemon

🧐 Paramètres de sécurité - MDaemon				×
Paramètres de sécurité Authentification de l'expéditeur Analyse SSL & TLS MDaemon Webmail MDaemon Remote Admin	Activer SSL Activer les p Le serveur S Le serveur S Les serveur Les serveur	, STARTTLS et STLS orts SSL des serveurs SMTP, IMAP, PC SMTP envoie les e-mails avec STARTTL SMTP requiert STARTTLS sur le port M s DomainPOP/MultiPOP utilisent STLS le ts à utiliser avec SSL. Sélectionnez l'éto)P3 LS lorsque c'est possible SA orsque c'est possible ile du certificat par défaut.	
Liste blanche STARTILS	Sujet	Autres noms d'hôtes	Date d'expiration	Fournisse
Liste STARTTLS DNSSEC Let's Encrypt Autres	🗹 ★ mail.comp	any.test	4/25/2021	mail.com
	•			F.
	Créer un certific	at Redémarrer les serveurs		Supprimer
		OK A	nnuler Appliquer	Aide

Activer SSL, STARTTLS et STLS

Cochez cette case pour activer la prise en charge du protocole SSL/TLS et des extensions STARTTLS et STLS. . then, choose the certificate that you want to use from the list below.

Activer les ports SSL dédiés pour les serveurs SMTP, IMAP et POP3

Activez cette option si vous souhaitez mettre à disposition les ports SSL dédiés spécifiés dans<u>Ports</u> with sous Domaine par défaut - Serveurs. Cela n'affectera pas les clients qui utilisent STARTTLS et STLS sur les ports de messagerie par défaut - cela fournit simplement un niveau supplémentaire de prise en charge de SSL.

Le serveur SMTP envoie le courrier en utilisant STARTTLS lorsque c'est possible.

Cliquez sur cette option si vous souhaitez que MDaemon tente d'utiliser l'extension STARTTLS pour chaque message SMTP qu'il envoie. Si le serveur auquel MDaemon se connecte ne prend pas en charge STARTTLS, le message sera délivré normalement sans utiliser SSL. Utilisez la liste <u>Liste STARTTLS</u> [626] si vous souhaitez empêcher l'utilisation de STARTTLS pour certains domaines.

Serveur SMTP exige STARTTLS sur le port MSA

Activez cette option si vous souhaitez exiger STARTTLS pour les connexions au serveur effectuées sur le port MSA [106].

Les serveurs DomainPOP/MultiPOP utilisent STLS dans la mesure du possible

Cochez cette case si vous souhaitez que les serveurs DomainPOP et MultiPOP utilisent l'extension STLS chaque fois que possible.

Sélectionnez le certificat à utiliser avec SSL

Cette boîte affiche vos certificats SSL. Cochez la case à côté des certificats que vous souhaitez activer. Cliquez sur l'étoile en regard de celui que vous souhaitez définir comme certificat par défaut. MDaemon prend en charge l'extension Server Name Indication (SNI) du protocole TLS, ce qui permet d'utiliser un certificat différent pour chaque nom d'hôte de votre serveur. MDaemon examine les certificats actifs et choisit celui qui contient le nom d'hôte demandé dans le champ Subject Alternative Names (vous pouvez spécifier les noms alternatifs lors de la création du certificat). Si le client ne demande pas de Nom d'hôte, ou si aucun certificat correspondant n'est trouvé, le certificat par défaut est utilisé. Double-cliquez sur un certificat pour l'ouvrir dans la boîte de dialogue Certificat de Windows afin de l'examiner (disponible uniquement dans l'interface d'application, pas dans l'administration à distance basée sur le navigateur).

Supprimer

Sélectionnez un certificat dans la liste, puis cliquez sur ce bouton pour le supprimer. Une boîte de confirmation s'ouvre et vous demande si vous êtes sûr de vouloir supprimer le certificat.

Créer un certificat

Cliquez sur ce bouton pour ouvrir la boîte de dialogue Créer un certificat SSL.

Créer un certificat SSL	
Détails du certificat	
Nom d'hôte (ex. : wc.altn.com)	mail.company.test
Nom de l'organisation/entreprise	Example Corp
Autres noms d'hôtes (séparez plusi	ieurs entrées par des virgules)
Longueur de la clé de cryptage	2048 🔹
Algorithme de hachage	SHA2 -
Pays/région	United States US 🔹
	OK Annuler

Détails du certificat

Nom d'hôte

Lors de la création d'un certificat, entrez le nom d'hôte auquel vos utilisateurs se connecteront (par exemple, "mail.example.com").

Nom de l'organisation/entreprise

Saisissez ici le nom de l'organisation ou de la société qui "possède" le certificat.

Autres noms d'hôtes (séparez plusieurs entrées par des virgules)

Si les utilisateurs se connectent à d'autres noms d'hôte et que vous souhaitez que ce certificat s'applique également à ces noms, entrez ici ces noms de domaine en les séparant par des virgules. Les caractères joker sont autorisés, ainsi "*.example.com" s'applique à tous les sous-domaines de example.com (par exemple, "wc.example.com", "mail.example.com", etc.)

MDaemon prend en charge l'extension SNI (Server Name Indication) du protocole TLS, ce qui permet d'utiliser un certificat différent pour chaque nom d'hôte de votre serveur. MDaemon examine les certificats actifs et choisit celui qui contient le nom d'hôte demandé dans son champ À :. Si le client ne demande pas de Nom d'hôte, ou si aucun certificat correspondant n'est trouvé, le certificat par défaut est utilisé.

Longueur de clé de cryptage

Choisissez la longueur de clé de cryptage souhaitée pour ce certificat. Plus la clé de cryptage est longue, plus les données transférées sont sécurisées. Notez toutefois que toutes les applications ne prennent pas en charge des longueurs de clé supérieures à 512.

Algorithme de hachage

Choisissez l'algorithme de hachage que vous souhaitez utiliser : SHA1 ou SHA2. Le paramètre par défaut est SHA2.

Pays/région

Choisissez le pays ou la région dans lequel votre serveur réside.

Redémarrer les serveurs

Cliquez sur ce bouton pour redémarrer les serveurs SMTP/IMAP/POP. Les serveurs doivent être redémarrés lorsqu'un certificat est modifié.

Voir :

SSL & TLS 613

Créer et utiliser des certificats SSL 974

4.2.4.2 Webmail

🧐 Paramètres de sécurité - Webmail				×
Paramètres de sécurité Authentification de l'expéditeur Analyse SSL & TLS MDaemon	Accepter ces types de cor HTTP uniquement HTTPS uniquement	nnexions ● HTTP et HTTPS ● HTTP redirigé en HTTPS	Port HTTPS 4	43
MDaemon Remote Admin Liste blanche STARTTLS Liste STARTTLS DNSSEC Let's Encrypt Autres	Sujet Sujet mail.company.test Créer un certificat	Autres noms d'hôtes	Date d'expiration 4/25/2021	Fournisse mail.com
		OK Annu	ler Appliquer	Aide

Le serveur Web intégré à MDaemon prend en charge le protocole Secure Sockets Layer (SSL). SSL est la méthode standard pour sécuriser les communications serveur/client

sur le web. Il permet l'authentification du serveur, le cryptage des données et, en option, l'authentification du client pour les connexions TCP/IP. En outre, la prise en charge du protocole HTTPS (c'est-à-dire HTTP sur SSL) étant intégrée dans tous les principaux navigateurs, il suffit d'installer un certificat numérique valide sur votre serveur pour activer les capacités SSL du client qui se connecte.

Les options permettant d'activer et de configurer le Webmail pour qu'il utilise HTTPS se trouvent sur l'écran SSL & HTTPS sous Activer | Services web & IM | Webmail". Cependant, pour votre commodité, ces options sont également reflétées sous "Sécurité" "Gestionnaire de sécurité" "SSL & TLS" "Webmail". | SSL & TLS | Webmail".

Pour plus d'informations sur le protocole SSL et les certificats, voir : <u>SSL &</u> <u>Certificats</u> 613



Cet écran ne s'applique au Webmail que lorsque vous utilisez leserveur Web intégré de MDaemon. Si vous configurez Webmail pour utiliser un autre serveur Web tel que IIS, ces options ne seront pas utilisées - le support SSL & HTTPS devra être configuré en utilisant les outils de l'autre serveur Web.

Accepter ces types de connexions

HTTP uniquement

Choisissez cette option si vous ne souhaitez pas autoriser les connexions HTTPS au Webmail. Seules les connexions HTTP seront acceptées.

HTTP et HTTPS

Choisissez cette option si vous souhaitez activer le support SSL dans Webmail, mais ne souhaitez pas forcer vos utilisateurs Webmail à utiliser HTTPS. Webmail écoutera les connexions sur le port HTTPS désigné ci-dessous, mais répondra toujours aux connexions http normales sur le port TCP de Webmail désigné sur l' écran<u>Serveur</u> Web

HTTPS uniquement

Choisissez cette option si vous souhaitez exiger le protocole HTTPS lors de la connexion à la messagerie Web. Webmail ne répondra qu'aux connexions HTTPS lorsque cette option est activée - il ne répondra pas aux requêtes HTTP.

HTTP redirigé vers HTTPS

Choisissez cette option si vous souhaitez rediriger toutes les connexions HTTP vers HTTPS sur le port HTTPS.

Port HTTPS

Il s'agit du port TCP que le Webmail écoutera pour les connexions SSL. Le port SSL par défaut est 443. Si le port SSL par défaut est utilisé, vous ne devrez pas inclure le numéro de port dans l'URL deWebmaillorsque vous vous connectez via HTTPS (c'est-à-dire que "https://example.com" est équivalent à "https://example.com:443").

Ce n'est pas la même chose que le port du Webmail qui est désigné sur l'écran<u>Serveur Web</u> (338) du Webmail. Si vous autorisez toujours les connexions HTTP au Webmail, ces connexions doivent utiliser cet autre port pour réussir à se connecter. Les connexions HTTPS doivent utiliser le port HTTPS.

Sélectionnez le certificat à utiliser avec HTTPS/SSL

Cette boîte affiche vos certificats SSL. Cochez la case en regard des certificats que vous souhaitez activer. Cliquez sur l'étoile en regard de celui que vous souhaitez définir comme certificat par défaut. MDaemon prend en charge l'extension Server Name Indication (SNI) du protocole TLS, ce qui permet d'utiliser un certificat différent pour chaque nom d'hôte de votre serveur. MDaemon examine les certificats actifs et choisit celui qui contient le nom d'hôte demandé dans le champ Subject Alternative Names (vous pouvez spécifier les noms alternatifs lors de la création du certificat). Si le client ne demande pas de Nom d'hôte, ou si aucun certificat correspondant n'est trouvé, le certificat par défaut est utilisé. Double-cliquez sur un certificat pour l'ouvrir dans la boîte de dialogue Certificat de Windows afin de l'examiner (disponible uniquement dans l'interface d'application, pas dans l'administration à distance basée sur le navigateur).

Supprimer

Sélectionnez un certificat dans la liste, puis cliquez sur ce bouton pour le supprimer. Une boîte de confirmation s'ouvre et vous demande si vous êtes sûr de vouloir supprimer le certificat.

Créer un certificat

Cliquez sur ce bouton pour ouvrir la boîte de dialogue Créer un certificat SSL.

Cré	ier un certificat SSL	
	Détails du certificat	
	Nom d'hôte (ex. : wc.altn.com)	mail.company.test
	Nom de l'organisation/entreprise	Example Corp
	Autres noms d'hôtes (séparez plusie	eurs entrées par des virgules)
	Longueur de la clé de cryptage	2048 🔹
	Algorithme de hachage	SHA2 -
	Pays/région	United States US 🔹
		OK Annuler

Détails du certificat

Nom d'hôte

Lors de la création d'un certificat, entrez le nom d'hôte auquel vos utilisateurs se connecteront (par exemple, "wc.example.com").

Nom de l'organisation/entreprise

Entrez ici le nom de l'organisation ou de la société qui "possède" le certificat.

Autres noms d'hôtes (séparez plusieurs entrées par des virgules)

Si les utilisateurs se connectent à d'autres noms d'hôte et que vous souhaitez que ce certificat s'applique également à ces noms, entrez ici ces noms de domaine en les séparant par des virgules. Les caractères joker sont autorisés, ainsi "*.example.com" s'applique à tous les sous-domaines de example.com (par exemple, "wc.example.com", "mail.example.com", etc.)



Longueur de clé de cryptage

Choisissez la longueur de clé de cryptage souhaitée pour ce certificat. Plus la clé de cryptage est longue, plus les données transférées sont sécurisées. Notez toutefois que toutes les applications ne prennent pas en charge des longueurs de clé supérieures à 512.

Pays/région

Choisissez le pays ou la région dans lequel votre serveur réside.

Algorithme de hachage

Choisissez l'algorithme de hachage que vous souhaitez utiliser : SHA1 ou SHA2. Le paramètre par défaut est SHA2.

Redémarrer les serveurs Web

Cliquez sur ce bouton pour redémarrer le serveur Web. Le serveur Web doit être redémarré avant qu'un nouveau certificat ne soit utilisé.

Utiliser Let's Encrypt pour gérer votre certificat

Let's Encrypt est une autorité de certification (AC) qui fournit des certificats gratuits via un processus automatisé conçu pour éliminer le processus actuellement complexe de création, de validation, de signature, d'installation et de renouvellement manuels des certificats pour les sites web sécurisés.

Dans le cadre de l'utilisation du processus automatisé de Let's Encrypt pour gérer un certificat, l' écran Let's Encrypt [632] est fourni pour vous aider à configurer et à exécuter facilement le script PowerShell inclus dans le dossier "MDaemon\LetsEncrypt". L'exécution du script permet de tout configurer pour Let's Encrypt, y compris de placer les fichiers nécessaires dans le dossier HTTP du Webmail pour relever le défi http-01. Il utilise le <u>nom d'hôte SMTP</u> [187] du <u>domaine par défaut</u> [184] comme domaine pour le certificat, inclut tout *autre nom d'hôte que* vous avez spécifié, récupère le certificat, l'importe dans Windows et configure MDaemon pour qu'il utilise le certificat pour MDaemon, Webmail et Remote Admin. Dans le dossier "MDaemon\Logs\", le script crée un fichier journal appelé LetsEncrypt.log. Ce fichier journal est supprimé et recréé à chaque fois que le script est exécuté, et il inclut la date et l'heure début du script. De plus, des e-mails de notification seront envoyés lorsque des erreurs se produisent si vous spécifiez un *E-mail de l'administrateur pour les notifications*. Voir la rubrique Let's Encrypt

Voir :

<u>SSL et certificats</u> ति। <u>Créer et utiliser des certificats SSL</u> (जन्म)

4.2.4.3 MDaemon Remote Admin

🧐 Paramètres de sécurité - MDaemon Remote	Admin			×
Paramètres de sécurité Authentification de l'expéditeur Analyse SSL & TLS MDaemon	Accepter ces types de cor HTTP uniquement HTTPS uniquement	enexions Energy HTTP et HTTPS HTTP redirigé en HTTPS Sélectionnes l'éte	Port HTTPS 4	44
Webmail MDaemon Remote Admin Liste blanche STARTTLS DNSSEC Let's Encrypt Autres	Sujet	Autres noms d'hôtes	Date d'expiration 4/25/2021	Fournisse mail.com
		ОК Алли	ler Appliquer	Aide

Le serveur Web intégré à MDaemon prend en charge le protocole SSL (Secure Sockets Layer). SSL est la méthode standard pour sécuriser les communications serveur/client sur le Web. Il permet l'authentification du serveur, le cryptage des données et, en option, l'authentification du client pour les connexions TCP/IP. En outre, la prise en charge du protocole HTTPS (c'est-à-dire HTTP sur SSL) étant intégrée dans tous les principaux navigateurs, il suffit d'installer un certificat numérique valide sur votre serveur pour activer les capacités SSL du client qui se connecte.

Les options permettant d'activer et de configurer le MDaemon Remote Admin pour utiliser HTTPS se trouvent dans l'écran SSL & HTTPS sous | Setup | Web & IM Services | MDaemon Remote Admin". Pour plus de commodité, ces options sont également reprises sous "Sécurité | Paramètres de sécurité | SSL & TLS | Administration à distance".

Pour plus d'informations sur le protocole SSL et les certificats, voir : <u>SSL &</u> <u>Certificats</u>

> Cet écran ne s'applique à l'Administration à distance que lorsque vous utilisez leserveur web intégré de MDaemon. Si vous configurez l'Administration à distance pour utiliser un autre serveur web tel que IIS, ces options ne seront pas utilisées - le support SSL/HTTPS devra être configuré en utilisant les outils de l'autre serveur web.

Accepter ces types de connexions

HTTP uniquement

Choisissez cette option si vous ne souhaitez pas autoriser de connexions HTTPS vers MDaemon Remote Admin. Seules les connexions HTTP seront acceptées.

HTTP et HTTPS

Choisissez cette option si vous souhaitez activer la prise en charge de SSL dans MDaemon Remote Admin, mais ne souhaitez pas obliger les utilisateurs de MDaemon Remote Admin à utiliser HTTPS. MDaemonRemote Admin écoutera les connexions sur le port HTTPS désigné ci-dessous, mais répondra toujours aux connexions http normales sur le port TCP de MDaemon Remote Admin désigné sur l' écran <u>Serveur</u> <u>Web</u> 377].

HTTPS uniquement

Choisissez cette option si vous souhaitez exiger le protocole HTTPS lors de la connexion au MDaemon Remote Admin. MDaemon Remote Admin ne répondra qu'aux connexions HTTPS lorsque cette option est activée - il ne répondra pas aux demandes HTTP.

HTTP redirigé vers HTTPS

Choisissez cette option si vous souhaitez rediriger toutes les connexions HTTP vers HTTPS sur le port HTTPS.

Port HTTPS

Il s'agit du port TCP que MDaemon Remote Admin écoutera pour les connexions SSL. Le port SSL par défaut est 444. Si le port SSL par défaut est utilisé, il n'est pas nécessaire d'inclure le numéro de port dans l'URL de l'administration à distancelors de la connexion via HTTPS (c'est-à-dire que "https://example.com" équivaut à "https://example.com:444").

> Il ne s'agit pas du même port que celui désigné pour le MDaemon Admin dans l'écran <u>Serveur Web</u> 3771. Si vous autorisez toujours les connexions HTTP au MDaemon Remote Admin, ces connexions doivent utiliser cet autre port pour réussir à se connecter. Les connexions HTTPS doivent utiliser le port HTTPS.

Sélectionnez le certificat à utiliser avec HTTPS/SSL

Cette boîte affiche vos certificats SSL. Cochez la case en regard des certificats que vous souhaitez activer. Cliquez sur l'étoile en regard de celui que vous souhaitez définir comme certificat par défaut. MDaemon prend en charge l'extension Server Name Indication (SNI) du protocole TLS, ce qui permet d'utiliser un certificat différent pour chaque nom d'hôte de votre serveur. MDaemon examine les certificats actifs et choisit celui qui contient le nom d'hôte demandé dans le champ Subject Alternative Names (vous pouvez spécifier les noms alternatifs lors de la création du certificat). Si le client ne demande pas de Nom d'hôte, ou si aucun certificat correspondant n'est trouvé, le certificat par défaut est utilisé. Double-cliquez sur un certificat pour l'ouvrir dans la boîte de dialogue Certificat de Windows afin de l'examiner (disponible uniquement dans l'interface d'application, pas dans l'administration à distance basée sur le navigateur).

Supprimer

Sélectionnez un certificat dans la liste, puis cliquez sur ce bouton pour le supprimer. Une boîte de confirmation s'ouvre et vous demande si vous êtes sûr de vouloir supprimer le certificat.

Créer un certificat

Cliquez sur ce bouton pour ouvrir la boîte de dialogue Créer un certificat SSL.

Créer un certificat SSL	
Détails du certificat	
Nom d'hôte (ex. : wc.altn.com)	mail.company.test
Nom de l'organisation/entreprise	Example Corp
Autres noms d'hôtes (séparez plusi	ieurs entrées par des virgules)
Longueur de la clé de cryptage	2048 🔹
Algorithme de hachage	SHA2 -
Pays/région	United States US 🔹
	OK Annuler

Détails du certificat

Nom d'hôte

Lors de la création d'un certificat, entrez le nom d'hôte auquel vos utilisateurs se connecteront (par exemple, "wc.example.com").

Nom de l'organisation/entreprise

Entrez ici le nom de l'organisation ou de la société qui "possède" le certificat.

Autres noms d'hôtes (séparez plusieurs entrées par des virgules)

Si les utilisateurs se connectent à d'autres noms d'hôte et que vous souhaitez que ce certificat s'applique également à ces noms, entrez ici ces noms de domaine en les séparant par des virgules. Les caractères joker sont autorisés, ainsi "*.example.com" s'applique à tous les sous-domaines de example.com (par exemple, "wc.example.com", "mail.example.com", etc.)

MDaemon prend en charge l'extension SNI (Server Name Indication) du protocole TLS, ce qui permet d'utiliser un certificat différent pour chaque nom d'hôte de votre serveur. MDaemon examine les certificats actifs et choisit celui qui contient le nom d'hôte demandé dans son champ À :. Si le client ne demande pas de Nom d'hôte, ou si aucun certificat correspondant n'est trouvé, le certificat par défaut est utilisé.

Longueur de clé de cryptage

Choisissez la longueur de clé de cryptage souhaitée pour ce certificat. Plus la clé de cryptage est longue, plus les données transférées sont sécurisées. Notez toutefois que toutes les applications ne prennent pas en charge des longueurs de clé supérieures à 512.

Pays/région

Choisissez le pays ou la région dans lequel votre serveur réside.

Algorithme de hachage

Choisissez l'algorithme de hachage que vous souhaitez utiliser : SHA1 ou SHA2. Le paramètre par défaut est SHA2.

Redémarrer les serveurs Web

Cliquez sur ce bouton pour redémarrer le serveur Web. Le serveur Web doit être redémarré avant qu'un nouveau certificat ne soit utilisé.

Utiliser Let's Encrypt pour gérer votre certificat

Let's Encrypt est une autorité de certification (AC) qui fournit des certificats gratuits via un processus automatisé conçu pour éliminer le processus actuellement complexe de création, de validation, de signature, d'installation et de renouvellement manuels des certificats pour les sites web sécurisés.

Dans le cadre de l'utilisation du processus automatisé de Let's Encrypt pour gérer un certificat, l' écran Let's Encrypt [622] est fourni pour vous aider à configurer et à exécuter facilement le script PowerShell inclus dans le dossier "MDaemon\LetsEncrypt". L'exécution du script permet de tout configurer pour Let's Encrypt, y compris de placer les fichiers nécessaires dans le dossier HTTP du Webmail pour relever le défi http-01. Il utilise le nom d'hôte SMTP [187] du domaine par défaut [184] comme domaine pour le certificat, inclut tout *autre nom d'hôte que* vous avez spécifié, récupère le certificat, l'importe dans Windows et configure MDaemon pour qu'il utilise le certificat pour MDaemon, Webmail et Remote Admin. Dans le dossier "MDaemon\Logs\", le script crée un fichier journal appelé LetsEncrypt.log. Ce fichier journal est supprimé et recréé à chaque fois que le script est exécuté, et il inclut la date et l'heure début du script. De plus, des e-mails de notification seront envoyés lorsque des erreurs se produisent si vous spécifiez un *E-mail de l'administrateur pour les notifications*. Voir la rubrique Let's Encrypt

Pour plus d'informations sur SSL et les certificats, voir :

<u>SSL et certificats</u> लाउँ <u>Créer et utiliser des certificats SSL</u> (जर्म)

Pour plus d'informations sur le MDaemon Remote Admin, voir :

Configuration à distance 376

MDaemon MDaemon Remote Admin | Serveur Web 377

Non (par défaut) accès Web

Mon compte | Web

Article KB : <u>Comment configurer les services Webmail, MDaemon Remote Admin,</u> <u>ActiveSync, CalDav, CardDav, AutoDiscover, MDDP, Webmail API et XML API dans IIS ?</u>

4.2.4.4 Exceptions STARTTLS

626

Paramètres de sécurité - Liste blanche START	TLS 💌
Paramètres de sécurité Authentification de l'expéditeur Analyse SSL & TLS MDaemon Webmail MDaemon Remote Admin Liste blanche STARTTLS DNSSEC Let's Encrypt Autres	# Liste blanche de STARTTLS # Les connexions SMTP à des hôtes/IP figurant sur cette liste n'utilisent pas STARTTLS. # Les connexions SMTP provenant d'hôtes/IP figurant sur cette liste ne peuvent pas utilis
	OK Annuler Appliquer Aide

Cette liste permet d'empêcher l'utilisation de pour empêcher l'utilisation de STARTTLS lors de l'envoi ou de la réception de courrier à destination ou en provenance de certains hôtes ou adresses IP.



L'extension STARTTLS pour SMTP est traitée dans la RFC-3207, qui peut être consultée à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc3207.txt

4.2.4.5 Liste STARTTLS

🧐 Paramètres de sécurité - Liste STARTTLS		×
 Paramètres de sécurité Authentification de l'expéditeur Analyse SSL & TLS MDaemon Webmail MDaemon Remote Admin Liste blanche STARTTLS DNSSEC Let's Encrypt Autres 	Liste STARTTLS obligatoire # Les connexions SMTP vers ou depuis les hôtes/IP de cette liste DOIVENT utiliser STAF #Les caractères jokers et la notation CIDR sont acceptés.	
	OK Annuler Appliquer Aid	de

Utilisez cet écran pour spécifier les hôtes, les adresses IP et les adresses MAIL FROM qui requièrent l'utilisation de l'extension STARTTLS afin d'envoyer ou de recevoir du courrier vers ou depuis votre serveur.

L'extension STARTTLS pour SMTP est traitée dans la RFC-3207, qui peut être consultée à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc3207.txt

4.2.4.6 SMTP Extensions

628

Security Manager - SMTP Extensions	SMTP Extensions SMTP Extensions Enable REQUIRETLS (RFC 8689) Cache MTA-STS (RFC 8669) Cache MTA-STS DNS records Edit Cache MTA-STS DNS records Edit Cache MTA-STS DNS records Edit Cache MTA-STS DNS records Example Corp Contact email (appears in reports) postmaster@company.test SMTP return path (used when sending reports) noreply@company.test Max recipients per report (default=5) Nereply@company.test Max recipients per report (default=5) Nereply@company.test Max recipients per report (default=5) Nereply@company.test Cache TLS reporting DNS records Edit Cache TLS reporting DNS records Edit
	Ok Cancel Apply Help

Extensions SMTP

Activer REQUIRETLS (RFC 8689)

RequireTLS vous permet de marquer les messages **pour** REQUIRETLS. Si TLS n'est pas possible (ou si les paramètres de l'échange de certificats TLS sont inacceptables), les messages seront renvoyés au lieu d'être délivrés de manière non sécurisée. Pour une description complète de RequireTLS, voir : <u>RFC 8689 : SMTP</u> <u>Require TLS</u>.

RequireTLS est activé par défaut, mais les seuls messages soumis au processus RequireTLS sont les messages spécifiquement marqués par une règle du Filtre de contenu à l'aide de la nouvelle <u>action du Filtre de contenu</u>, "Marquer*le message pour REQUIRETLS*...", ou les messages envoyés à <local-

part>+requiretls@domain.tld (par exemple,

arvel+requiretls@mdaemon.com). Tous les autres messages sont traités comme si le service était désactivé. Plusieurs conditions doivent être remplies pour qu'un message puisse être envoyé à l'aide de RequireTLS. Dans le cas où l'une d'entre elles ne serait pas respectée, le message serait renvoyé au lieu d'être envoyé en clair. Ces conditions sont les suivantes :

- RequireTLS doit être activé.
- Le message doit être marqué comme nécessitant le traitement RequireTLS, via l'action du Filtre de contenu ou l'adresse "<localpart>+requireTLS@...".

- Les recherches DNS pour les hôtes MX destinataires doivent utiliser <u>DNSSEC</u> [631] (voir ci-dessous), ou le MX doit être validé par MTA-STS.
- La connexion à l'hôte destinataire doit utiliser SSL (STARTTLS).
- Le certificat SSL de l'hôte de réception doit correspondre au nom de l'hôte MX et être lié à une autorité de certification approuvée.
- Le serveur de messagerie de réception doit prendre en charge REQUIRETLS et l'indiquer dans la réponse EHLO.

RequireTLS nécessite des vérifications DNSSEC des hôtes de l'enregistrement MX, ou le MX doit être validé par MTA-STS. Vous pouvez <u>configurer DNSSEC</u> and en spécifiant des critères selon lesquels les recherches demanderont le service DNSSEC. Le <u>Cache IP</u> and dispose d'une option permettant d'accepter les affirmations DNSSEC, et des instructions relatives au DNSSEC figurent en haut du <u>Fichier MX HOSTS</u> 1041. Enfin, le DNSSEC nécessite des serveurs DNS configurés de manière appropriée, ce qui dépasse le cadre de ce fichier d'aide.

Autoriser MTA-STS (RFC 8461)

La prise en charge de MTA-STS est activée par défaut et est décrite dans la <u>RFC</u> <u>8461 : SMTP MTA-STS Strict Transport Security (MTA-STS)</u>.

SMTP MTA Strict Transport Security (MTA-STS) est un mécanisme permettant aux fournisseurs de services de messagerie (SP) de déclarer leur capacité à recevoir des connexions SMTP sécurisées par Transport Layer Security (TLS) et de spécifier si les serveurs SMTP d'envoi doivent refuser de livrer aux hôtes MX qui n'offrent pas TLS avec un certificat de serveur de confiance. Pour configurer MTA-STS pour votre propre domaine, vous aurez besoin d'un fichier de politique MTA-STS qui peut être téléchargé via HTTPS à partir de l'URL https://mta-sts.domain.tld/.well-known/mta-sts.txt, où "domain.tld" est votre nom de domaine. Le fichier texte de la politique doit contenir des lignes au format suivant :

```
version : STSv1
mode : testing
mx : mail.domain.tld
max_age : 86400
```

Le mode peut être "none", "testing" ou "enforce". Il doit y avoir une ligne "mx" pour chacun de vos noms d'hôtes MX. Un joker peut être utilisé pour les sous-domaines, comme "*.domain.tld". L'âge maximum est exprimé en secondes. Les valeurs courantes sont 86400 (1 jour) et 604800 (1 semaine).

Un enregistrement DNS TXT est également nécessaire à _mta-sts.domain.tld, où "domain.tld" est votre nom de domaine. Dans cet enregistrement, la valeur doit correspondre au format suivant

v=STSv1 ; id=20200206T010101 ;

La valeur de "id" doit être modifiée à chaque fois que le fichier de politique est changé. Il est courant d'utiliser un horodatage pour l'identifiant.

Liste des Exceptions

Utilisez cette liste pour exempter des domaines spécifiques de MTA-STS.

Cache Enregistrements DNS MTA-STS

Par défaut, MDaemon met en cache les enregistrements DNS MTA-STS. Cliquez sur **Modifier** pour afficher ou modifier le fichier de cache actuel.

Activer les Rapports TLS (RFC 8460)

Les Rapports TLS sont désactivés par défaut et sont décrits dans la <u>RFC 8460 :</u> <u>SMTP TLS ReportingSMTP</u>.

Les Rapports TLS permettent aux domaines utilisant MTA-STS d'être notifiés en cas d'échec de la récupération de la politique MTA-STS ou de la négociation d'un canal sécurisé à l'aide de STARTTLS. Lorsque cette option est activée, MDaemon envoie un rapport quotidien à chaque domaine compatible STS auquel il a envoyé (ou tenté d'envoyer) du courrier ce jour-là. Plusieurs options permettent de configurer les informations contenues dans les rapports.

Pour configurer les Rapports TLS pour votre domaine, activez la <u>signature DKIM</u> et créez un enregistrement DNS TXT à _smtp._tls.domain.tld, où "domain.tld" est votre nom de domaine, avec une valeur au format :

v=TLSRPTv1 ; rua=mailto:mailbox@domain.tld

Où mailbox@domain.tld est l'adresse électronique où vous souhaitez que les rapports concernant votre domaine soient envoyés.

4.2.4.7 DNSSEC



L'option DNSSEC (DNS Security Extensions) permet à MDaemon d'agir en tant que résolveur stub non validant, défini dans les RFC <u>4033Lien</u> et <u>4035Lien</u> comme "une entité qui envoie des requêtes DNS, reçoit des réponses DNS et est capable d'établir un canal sécurisé avec un serveur de noms récursif sécurisé qui fournira ces services pour le compte du résolveur stub sécurisé". "Cela signifie que lors des requêtes DNS de MDaemon, il peut demander le service DNSSEC à vos serveurs DNS, en paramétrant le bit AD (Authentic Data) dans les requêtes et en le vérifiant dans les réponses. Cela peut fournir un niveau de sécurité supplémentaire pendant le processus DNS pour certains messages, mais pas tous, car le service DNSSEC n'est pas encore pris en charge par tous les serveurs DNS ou pour tous les domaines de premier niveau.

Lorsqu'il est activé, le service DNSSEC n'est appliqué qu'aux messages qui répondent à vos critères de sélection ; il peut être demandé ou exigé de manière aussi large ou aussi restreinte que vous le souhaitez. Il vous suffit de désigner les combinaisons de "Valeurs en-tête" que vous choisissez dans cet écran pour que MDaemon demande le service DNSSEC pour tous les messages correspondant à ce critère lorsqu'il effectue une requête DNS. Lorsque les résultats DNS ne contiennent pas de données authentifiées, il n'y a pas de conséquences négatives ; MDaemon revient simplement au comportement normal du DNS. Si, toutefois, vous souhaitez *exiger le* protocole DNSSEC pour certains messages, ajoutez "SECURE" à la combinaison en-tête/valeur (par exemple, To *@example.net SECURE). Pour ces messages, lorsque les résultats DNS n'incluent pas de données authentifiées, le message sera renvoyé à l'expéditeur. **Remarque :** Étant donné que les recherches DNSSEC prennent plus de temps et de

ressources, et que DNSSEC n'est pas encore pris en charge par tous les serveurs, MDaemon n'est pas configuré pour appliquer DNSSEC à chaque livraison de message par défaut. Cependant, si vous souhaitez demander l'application du DNSSEC pour chaque message, vous pouvez le faire en incluant "To *" dans vos critères.

Les journaux de session de messagerie incluront une ligne en haut si le service DNSSEC a été utilisé et "DNSSEC" apparaîtra à côté des données sécurisées dans les journaux.

MDaemon étant un stub-resolver non validant, il demandera des données authentifiées à votre serveur DNS, mais il n'a aucun moyen de vérifier de manière indépendante que les données qu'il reçoit du serveur sont sécurisées. C'est pourquoi, pour utiliser avec succès l'option DNSSEC, vous devez vous assurer que vous avez confiance dans votre connexion à votre serveur DNS. Exemple : il fonctionne sur localhost ou au sein d'un réseau local ou d'un lieu de travail sécurisé.

4.2.4.8 Let's Encrypt

🧐 Paramètres de sécurité - Let's Encrypt	
Paramètres de sécurité Authentification de l'expéditeur Analyse SSL & TLS MDaemon Webmail MDaemon Remote Admin Liste blanche STARTTLS Liste STARTTLS DNSSEC Autres	Mise à jour du script PowerShell de Let's Encrypt Activer les mises à jour Autres noms d'hôtes (séparez plusieurs entrées par des virgules) Nom de site IIS (disponible avec un serveur web externe) E-mail de l'administrateur pour les notifications E-mail de l'administrateur pour les notifications Nombre de jours entre les mises à jour (10-60) 60 Mettre à jour maintenant Jours avant la prochaine mise à jour : 60 Ligne de commande: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy Bypass "C:\MDaemon\LetsEncrypt\LetsEncrypt.ps1"
	OK Annuler Appliquer Aide

Utiliser Let's Encrypt pour gérer votre certificat

Pour supporter <u>SSL & TLS et HTTPS</u> [613] pour <u>MDaemon</u> [614] Webmail [617] et <u>MDaemon</u> [614] <u>Remote Admin</u> [627], vous avez besoin d'un certificat SSL/TLS. Les certificats sont de petits fichiers émis par une Autorité de Certification (AC) qui sont utilisés pour vérifier auprès d'un client ou d'un navigateur qu'il est connecté au serveur auquel il est destiné, et qui permettent à SSL & TLS/HTTPS de sécuriser la connexion à ce serveur. <u>Let's EncryptLet'</u> est une autorité de certification qui fournit des certificats gratuits via un processus automatisé conçu pour éliminer le processus actuellement complexe de création, de validation, de signature, d'installation et de renouvellement manuels des certificats pour les sites web sécurisés.

Dans le cadre de l'utilisation du processus automatisé de Let's Encrypt pour gérer un certificat, cet écran est fourni pour vous aider à configurer et à exécuter facilement le script PowerShell inclus dans le dossier "MDaemon\LetsEncrypt". L'exécution du script permet de tout configurer pour Let's Encrypt, y compris de placer les fichiers nécessaires dans le dossier HTTP du Webmail pour relever le défi http-01. Il utilise le nom d'hôte SMTP 187 du domaine par défaut 184 comme domaine pour le certificat, inclut tout *autre nom d'hôte que* vous avez spécifié, récupère le certificat, l'importe dans Windows et configure MDaemon pour qu'il utilise le certificat pour MDaemon, Webmail et Remote Admin. Dans le dossier "MDaemon\Logs\", le script crée un fichier journal appelé LetsEncrypt.log. Ce fichier journal est supprimé et recréé à chaque fois que le script est exécuté, et il inclut la date et l'heure début du script. De plus, des e-mails de notification seront envoyés lorsque des erreurs se produisent si vous spécifiez un *E-mail de l'administrateur pour les notifications*.

Let's Encrypt nécessite <u>PowerShell 5.1</u> et .Net Framework 4.7.2, ce qui signifie qu'il ne fonctionnera pas sous Windows 2003. De plus, <u>Webmail</u> and doit écouter sur le port 80, et le script ne fonctionnera pas si vous avez un <u>nom d'hôte SMTP</u> (187) (i.e. FQDN) configuré pour votre Domaine par défaut qui ne pointe pas vers le serveur MDaemon.

Let's Encrypt PowerShell Updates (en anglais)

Activer les mises à jour

Cochez cette case si vous souhaitez créer et mettre à jour automatiquement un certificat SSL/TLS via le script Let's Encrypt. Le certificat sera mis à jour tous les 10 à 60 jours en fonction de votre paramètre*Jours entre les mises à jour* ci-dessous.

Autres noms d'hôtes (séparez plusieurs entrées par des virgules)

Si vous souhaitez paramétrer des noms d'hôtes alternatifs dans le certificat, indiquez ces noms d'hôtes ici, en les séparant par des virgules. Il n'est pas nécessaire d'inclure le Nom d'hôte SMTP du Domaine défaut - Domaine dans cette liste. Exemple : si votre domaine par défaut est "example.com", configuré avec un nom d'hôte SMTP "mail.example.com", et que vous souhaitez utiliser un nom d'hôte alternatif "imap.example.com", vous ne devez inclure que "imap.example.com" comme nom d'hôte alternatif . Si vous ne souhaitez pas utiliser de noms d'hôtes alternatifs, laissez cette option vide. **Par nom :** si vous incluez des noms d'hôtes alternatifs, un challenge HTTP de Let's Encrypt doit être complété pour chacun d'entre eux afin de valider le contrôle de ce nom d'hôte par votre serveur. Si tous les défis n'ont pas été remplis, le processus échouera.

Nom de site IIS (disponible avec un serveur web externe)

Si vous utilisez le webmail via IIS, entrez ici le nom du site IIS. Les outils Web Scripting de Microsoft doivent être installés pour que le certificat soit automatiquement configuré dans IIS.

E-mail de l'administrateur pour les notifications

Indiquez ici l'adresse électronique de l'administrateur si vous souhaitez être averti lorsqu'une erreur se produit lors d'une mise à jour de Let's Encrypt.

Supprimer les anciens certificats (expirés depuis plus de 30 jours)

Non (par défaut), MDaemon supprimera tous les anciens certificats expirés depuis plus de 30 jours. Décochez cette case si vous ne souhaitez pas les supprimer automatiquement.

Nombre de jours entre les mises à jour (10-60)

Utilisez cette option pour spécifier la fréquence de mise à jour de votre certificat, de 10 à 60 jours. Le paramètre (par défaut) est de 60 jours.

Mettre à jour maintenant

Cliquez sur ce bouton pour exécuter immédiatement le script.

4.2.5 Autres

4.2.5.1 Retours de courrier - Présentation

Rétrodiffusion

La "rétrodiffusion" fait référence aux messages de réponse que vos utilisateurs reçoivent à des e-mails qu'ils n'ont jamais envoyés. Ce phénomène se produit lorsque des messages de spam ou des messages envoyés par des virus contiennent une adresse "Return-Path" falsifiée. Alors, quand un de ces messages est rejeté par le serveur du destinataire, ou si le destinataire a un Autorépondeur ou un message "absent du bureau"/vacances associé à son compte, le message de réponse sera alors dirigé vers l'adresse falsifiée. Il peut en résulter un grand nombre de fausses Notifications d'état de remise (DSN) ou de messages de réponse automatique qui aboutissent dans les boîtes aux lettres de vos utilisateurs. De plus, les spammeurs et les auteurs de virus profitent fréquemment de ce phénomène et l'utilisent parfois pour lancer des attaques par déni de service (DoS) contre les serveurs de messagerie, provoquant ainsi l'arrivée d'un flot de messages électroniques non valides en provenance de serveurs situés dans le monde entier.

La solution de MDaemon

Pour lutter contre la rétrodiffusion, MDaemon contient une fonctionnalité appelée Protection contre la rétrodiffusion (BP). Cette protection permet de s'assurer que seuls les Notifications d'état de remise et les Répondeurs automatiques légitimes sont envoyés à vos comptes. Elle utilise une méthode de hachage à clé privée pour générer et insérer un code spécial sensible au temps dans l'adresse "Return-Path " des messages sortants de vos utilisateurs. Ensuite, lorsque l'un de ces messages rencontre un problème de distribution et est renvoyé, ou lorsqu'une réponse automatique est reçue avec un "mailer-daemon@..." ou un chemin inverseNUL, MDaemon verra le code spécial et saura qu'il s'agit d'une véritable réponse automatique à un message qui a été exécuté par l'un de vos comptes. Si l'adresse ne contient pas le code spécial, ou si elle date de plus de sept jours, elle sera journalisée par MDaemon et pourra être rejetée.

La <u>protection contre la rétrodiffusion</u> se trouve dans le menu Sécurité de MDaemon : Sécurité | Paramètres de sécurité | Autres | Protection contre les rétrodiffusions.

La protection contre les rétrodiffusions est une implémentation de la validation des balises d'adresses de rebond (BATV). Pour en savoir plus sur BATV, consultez le site

http://www.mipassoc.org/batv/

Voir :

Protection contre la rétrodiffusion 635

4.2.5.1.1 Retours de courrier

Paramètres de sécurité - Retours de courrie	er 🗾 🗾
Paramètres de sécurité Authentification de l'expéditeur Analyse SSL & TLS Autres Régulateur de bande passante Régulateur de bande passante Domaines LAN IP LAN Politique du site	Cette fonctionnalité utilise le protocole BATV pour protéger les utilisateurs contre les "retours non sollicités". Cela se produit lorsque des spams ou virus sont envoyés avec une adresse de retour usurpée. Les propriétaires de l'adresse reçoivent alors des centaines de notifications, messages d'absence, etc. Activer la protection contre les retours de courrier non sollicités Activer la protection contre les retours de courrier non sollicités Rejeter les messages non validés par la protection contre les Inste blanche Liste blanche La protection contre les retours enregistre la détection des messages invalides. Activez l'option ci-dessus si vous souhaitez également les refuser. Créer une nouvelle clé de protection contre les retours de courrier Cette technologie inclut une clé secrète associée à une fonction de hachage afin de protéger la valeur "return path" utilisée lors de l'envoi de messages. Cela permet ensuite de distinguer les adresses légitimes des adresses usurpées. Il est recommandé de générer régulièrement une nouvelle clé afin d'éviter qu'elle ne soit piratée.
	OK Annuler Appliquer Aide

Protection contre la rétrodiffusion

Activer la protection contre la rétrodiffusion

Cochez cette case si vous souhaitez insérer un code spécial de protection contre la rétrodiffusion dans l'adresse "Return-Path " de chaque message sortant. MDaemon génère ce code spécial en utilisant la clé privée qui se trouve dans le fichier rsa.private situé dans le dossier PEM_batv\ de MDaemon, et le code est valable pendant sept jours. Tous les messages DSN entrants ou autres messages de réponse automatique (avec un chemin d'accès inverse "mailer-daemon@..." ou NULL) doivent comporter un code BP valide et non expiré, sous peine d'échouer à la vérification BP.

Si vous désactivez cette option, MDaemon n'insérera pas le code spécial de protection contre la rétrodiffusion dans les messages sortants. Il continuera cependant à vérifier les DSN entrants et les messages de réponse automatique pour s'assurer que tout message entrant avec un code valide n'est pas rejeté par erreur.

Appliquer la protection contre la rétrodiffusion aux domaines de la passerelle

Si la protection contre la rétrodiffusion est activée, cliquez sur cette option si vous souhaitez également l'appliquer aux domaines pour lesquels MDaemon joue le rôle de passerelle ou de serveur de sauvegarde (voir <u>Gestionnaire de passerelles</u> 2011).

Rejeter les messages qui échouent à la vérification de la protection contre les rétrodiffusions

Cochez cette case si vous souhaitez rejeter les DSN ou autres messages de réponse automatique qui échouent à la vérification de la protection contre la rétrodiffusion. Les messages comportant un chemin inverse "mailer-daemon@..." ou NULL seront rejetés s'ils ne contiennent pas le code spécial ou si le cycle de vie de sept jours du code a expiré. Grâce à la fiabilité de la protection contre la rétrodiffusion, il n'y a pas de faux positifs ou de "zones grises" : un message est valide ou ne l'est pas. C'est pourquoi il est possible de configurer MDaemon pour qu'il rejette les messages non valides, à condition de s'assurer que tous les messages sortants de vos comptes contiennent le code BP spécial. Dans tous les cas, le résultat de la vérification BP sera enregistré dans le fichier journal SMTP-in, même si vous choisissez de ne pas rejeter les messages qui échouent à la vérification. Les messages entrants destinés aux passerelles ne seront pas rejetés, sauf si vous avez coché l' option...appliquer la protection contre les rétrodiffusions aux domaines de la passerelle ci-dessus.

> Lorsque vous activez la protection contre les rétrodiffusions, attendez environ une semaine avant de la configurer pour rejeter les messages de réponse automatique non valides. En effet, pendant cette période, il se peut que vous receviez encore des DSN ou des réponses automatiques à des messages qui ont été envoyés avant l'activation de la protection contre les rétrodiffusions. Si BP était configuré pour rejeter les

messages non valides pendant cette période, ces messages de réponse légitimes seraient rejetés par erreur. Au bout d'une semaine, il devrait être valide de commencer à rejeter les messages non valides. Le même avertissement s'applique lorsque vous créez une nouvelle clé BP et que vous choisissez de supprimer immédiatement l'ancienne clé au lieu de la laisser fonctionner pendant sept jours supplémentaires. (voir l'option *Créer nouvelle clé protection retours de courrier* ci-dessous).

Liste des Exceptions

Cliquez sur ce bouton pour ouvrir la liste des exemptions de la protection contre la rétrodiffusion Exceptions. Utilisez cette liste pour désigner les adresses IP ou les domaines que vous souhaitez exempter de la protection contre la rétrodiffusion.

Créer une nouvelle clé de protection contre les retours de courrier

Cliquez sur ce bouton pour générer une nouvelle clé de protection contre la rétrodiffusion. Cette clé est utilisée par MDaemon pour créer puis vérifier les codes BP spéciaux qui sont insérés dans les messages. La clé est située dans un fichier appelé rsa.private dans le dossier PEM_batv\ de MDaemon . Lorsque la nouvelle clé est générée, une fenêtre s'ouvre pour vous informer que l'ancienne clé continuera à fonctionner pendant sept jours supplémentaires, à moins que vous ne souhaitiez la supprimer immédiatement. Dans la plupart des cas, vous devez cliquer sur "Non", afin de permettre à la clé de fonctionner pendant sept jours supplémentaires. Si vous choisissez de supprimer la clé immédiatement, certains messages entrants risquent d'échouer à la vérification BP, puisqu'il s'agit de réponses à des messages contenant le code spécial généré par l'ancienne clé.

Si votre trafic de messagerie est réparti sur plusieurs serveurs, il se peut que vous deviez partager le fichier de clé avec tous vos autres serveurs ou agents de transfert de courrier (MTA).

Voir :

Protection contre la rétrodiffusion - Vue d'ensemble

4.2.5.2 Régulation de la bande passante - Présentation

La fonctionnalité Régulation de la bande passante vous permet de contrôler la consommation de bande passante utilisée par MDaemon. Vous pouvezcontrôler la vitesse à laquelle les sessions ou les services progressent - vous pouvez définir des taux différents pour chacun desprincipaux services de MDaemonpar domaine, y compris les domaines et les passerelles de domaine. Vous pouvez également fixer des limites sur les connexions locales en sélectionnant "Trafic local" dans une liste déroulante. Cela vous permettra de créer des paramètres de largeur de bande spéciaux qui prendront effet si la connexion se fait à partir ou à destination d'une adresse IP ou d'un nom de domaine local.

La Régulation de la bande passante peut être appliquée par session ou par service. Lorsque vous utilisez le mode par session, chaque session sera indépendamment limitée au taux associé. Ainsi, plusieurs sessions du même type de service se déroulant simultanément peuvent dépasser lavaleur configuréed'un service.Lorsque MDaemon est configuré pour réguler la bande passante par service, il surveille l'utilisation combinée de toutes les sessions d'un même type de service et leur alloue des fractions égales de la bande passante totale. Les sessions multiples se partageront alors la bande passante maximale configurée de manière égale. Cela vous permet de fixer une limite pour l'ensemble d'un service.

Lorsque la Régulation de la bande passante est étendue à une passerelle de domaine, elle doit être gérée un peu différemment d'un domaine normal car une passerelle de domaine n'a pas d'adresse IP spécifique qui lui est associée. MDaemon doit utiliser la valeur passée dans la commande RCPT pour déterminer si une session SMTP entrante est liée à la passerelle. Si c'est le cas, la Régulation de la bande passante SMTP entrante sera appliquée. En raison des limitations du SMTP, si un seul destinataire d'un message à destinataires multiples est destiné à une passerelle de domaine, la session entière sera limitée.

Le système de Régulation de la bande passante est calibré en kilo-octets par seconde (KB/s). Une valeur de "0" signifie qu'aucune limite ne sera appliquée à la vitesse à laquelle une session (ou un service) progresse, et qu'elle utilisera donc la quantité maximale de bande passante disponible. Une valeur de "10", par exemple, obligera MDaemon à réduire délibérément la vitesse de transmission pour qu'elle reste égale ou légèrement supérieure à 10 Ko/s.

Les rafales d'activité au début d'une session peuvent et vont dépasser les limites fixées. L'étranglement se met en place et se précise au fur et à mesure de la progression de la session.

Voir :

<u>Régulation de la bande passante</u> छि । <u>IP locales</u> बिग

🧐 Paramètres de sécurité - Régulateur de bande passante × 🔲 Activer la régulation de la bande passante - Paramètres de sécurité Configurer les paramètres pour le domaine company.test 🛓 Authentification de l'expéditeur 🛓 Analyse Limiter la bande passante POP3 - 0 Ko/s 🗄 - SSL & TLS 0 0-100 KB/s 🛓 Autres Retours de courrier Limiter la bande passante IMAP - 0 Ko/s---o ()-100 KB/s - Répulsion Limiter la bande passante Inbound SMTP - 0 Ko/s ____ Liste grise 0 0-100 KB/s Domaines LAN IP LAN Limiter la bande passante Outbound SMTP - 0 Politique du site o 🕛 100 KB/s Limiter la bande passante DomainPOP - 0 Ko/s____ o ()-100 KB/s Limiter la bande passante MultiPOP - 0 Ko/s____ o ()-100 KB/s Vitesse maximale de la ligne (Ko/s) Unknown -Appliquer la régulation 'par service' ('par session' par défaut) 0K Annuler Appliquer Aide

4.2.5.2.1 Régulateur de bande passante

Activer la régulation de la bande passante

Cochez cette case si vous souhaitez activer la fonction de Régulation de la bande passante.

Configurez ce paramètre pour le domaine

Sélectionnez un domaine dans la liste déroulante, puis ajustez les options correspondant aux différents services pour configurer la régulation de la bande passante pour le domaine sélectionné. Un paramètre "0" dans un contrôle particulier signifie qu'aucune limite de bande passante n'est définie pour ce type de service. Dans la liste déroulante, l'entrée la plus basse est *Trafic local*. La configuration de la régulation de la bande passante pour cette option déterminera les limites imposées au trafic local (c.-à-d. les sessions et les services se déroulant sur votre réseau local plutôt qu'à l'extérieur). L' Écran<u>IP locales</u> of peut être utilisé pour dresser la liste des adresses IP qui doivent être considérées comme locales.

Services

[Régulation de la bande passante - [xx] KB/s

Après avoir sélectionné un domaine dans la liste déroulante, réglez ces commandes pour définir les limitations de la bande passante pour le domaine sélectionné. Un réglage de "0" signifie qu'aucune limite de bande passante n'est appliquée à ce type de service particulier. Le réglage d'un curseur sur un nombre différent de "0" limitera la bande passante maximale à ce nombre de kilo-octets par seconde pour le service désigné.

Vitesse maximale de la liaison (Ko/s)

Dans la liste déroulante, choisissez la vitesse maximale de votre connexion en kilooctets par seconde.

Appliquer le régulateur "par service" ("par session" par défaut)

Cochez cette case si vous souhaitez réguler la bande passante par service plutôt que par session, comme c'est le cas par défaut. Lors d'une régulation par service, laquantité de bande passante désignée pourle serviceest divisée de manière égale à toutes les sessions actives du type de service donné. Exemple : la quantité totale de bande passante utilisée par plusieurs clients IMAP se connectant en même temps ne pourra jamais dépasser la quantité désignée, quel que soit le nombre de clients connectés. Si la limitation se fait parsession, aucune session IMAP ne pourra dépasser la limite fixée, mais le total de plusieurs sessions simultanées pourra le faire.

Voir :

Régulation de la bande passante - Vue d'ensemble

4.2.5.3 Répulsion

Paramètres de sécurité - Répulsion	
 Paramètres de sécurité Authentification de l'expéditeur Analyse SSL & TLS Autres Retours de courrier Régulateur de bande passante Répulsion Liste grise Domaines LAN IP LAN Politique du site 	La répulsion ralentit délibérément le traitement SMTP afin de décourager le serveur expéditeur de poursuivre la distribution.
	OK Annuler Appliquer Aide

Le tarpitting se trouve dans le menu Sécurité à l'adresse suivante : Sécurité | Paramètres de sécurité | Autres | Tarpitting.

Le tarpitting vous permet de ralentir délibérément une connexion dès qu'un certain nombre de commandes RCPT ont été reçues de l'expéditeur d'un message. Cela permet de décourager les spammeurs d'essayer d'utiliser votre serveur pour envoyer des courriels en masse non sollicités ("spam"). Vous pouvez spécifier le nombre de commandesRCPT autorisées avant que la répulsion ne commence et le nombre de secondes nécessaires pour retarder la connexion chaque fois qu'une commande ultérieure est reçue de cet hôte au cours de la connexion. Cette technique repose sur l'hypothèse que si les spammeurs mettent un temps anormalement long à envoyer chaque message, cela les dissuadera d'essayer d'utiliser votre serveur pour le faire à nouveau à l'avenir.

Activer la répulsion

Cochez cette case pour activer les fonctionnalités de répulsion de MDaemon.

Délai SMTP EHLO/HELO (en secondes)

Cette option permet de retarder la réponse du serveur aux commandes SMTP EHLO/HELO. Le fait de retarder les réponses, ne serait-ce que de dix secondes, peut permettre d'économiser un temps de traitement considérable en réduisant le nombre de spams reçus. Les spammeurs dépendent souvent d'une livraison rapide de

leurs messages et n'attendent donc pas longtemps une réponse aux commandes EHLO/HELO. Avec un délai, même minime, les outils de spam abandonneront parfois et passeront à autre chose plutôt que d'attendre une réponse. Les connexions sur le port MSA (désigné dans l' écran <u>Ports</u> 106] sous Paramètres du serveur) sont toujours exemptes de ce délai. Le paramètre par défaut de cette option est "0", ce qui signifie que lesEHLO/HELO ne sont pas retardés.

Les IP authentifiées subissent un seul délai EHLO/HELO par jour.

Cochez cette case si vous souhaitez limiter le délai EHLO/HELO à une fois par jour pour les connexions authentifiées à partir d'une adresse IP donnée. Le premier message provenant de cette adresse IP sera retardé, mais les messages suivants envoyés à partir de la même adresse IP ne le seront pas.

SMTP RCPT tarpit threshold

Indiquez le nombre de commandes SMTP RCPT que vous souhaitez autoriser pour un hôte donné au cours d'une session de messagerie avant que MDaemon ne commence à tarpiter cet hôte. Exemple : si ce nombre est fixé à 10 et qu'un hôte tente d'envoyer un message à 20 adresses (c'est-à-dire 20 commandes RCPT), MDaemon autorisera les 10 premières normalement, puis marquera une pause après chaque commande suivante pendant le nombre de secondes spécifié dans le paramètre*Délai de répulsion SMTP* ci-dessous.

Délai de répulsion SMTP RCPT (en secondes)

Lorsque le *seuil SMTP RCPT tarpit* est atteint pour un hôte, MDaemon marque une pause de quelques secondes après chaque commandeRCPT reçue de cet hôte au cours de la session de messagerie.

Facteur d'échelle

Cette valeur est un multiplicateur par lequel le délai de répulsion de base sera augmenté au fil du temps. Dans le cas où le seuil de répulsion est atteint et que le délai de répulsion est appliqué à une session, chaque délai est multiplié par cette valeur pour déterminer la durée du délai suivant dans la session. Exemple : si le délai de répulsion est fixé à 10 et le facteur d'échelle à 1,5, le premier délai sera de 10 secondes, le deuxième de 15 secondes, le troisième de 22,5, puis de 33,75, et ainsi de suite (c'est-à-dire 10 x 1,5 = 15, 15 x 1,5 = 33,75, etc.). Le facteur d'échelle par défaut est 1, ce qui signifie que le délai ne sera pas augmenté.

Les sessions authentifiées sont exemptes de tarpitting

Cochez cette case si vous souhaitez que les expéditeurs qui authentifient leur session authentifiée soient exemptés du tarpitting.

Liste des exceptions

Cliquez sur ce bouton pour ouvrir la <u>Liste d'autorisation dynamique</u>, qui est également utilisée pour le tarpitting. Vous pouvez y désigner les adresses IP que vous souhaitez exempter du tarpitting.

4.2.5.4 Liste grise

 Ne pas inclure les IP dans la liste grise (n'utiliser que les valeurs MAIL & RCPT) Si une connexion est approuvée par SPF, ne pas mettre les suivantes sur liste grise Ne pas mettre en liste grise si l'expéditeur est dans un carnet d'adresse local Ne pas mettre en liste grise les messages de liste de diffusion Ne pas mettre en liste grise le courrier provenant de sessions authentifiées Ne pas mettre en liste grise le courrier provenant d'1P autorisées

Le Greylisting se trouve dans la boîte de dialogue Sécurité : Sécurité | Paramètres de sécurité | Autres | Liste grise. La mise en liste grise est une technique de lutte contre le spam qui exploite le fait que les serveurs SMTP tentent à nouveau de délivrer tout message qui recoit un code d'erreur temporaire (c'est-à-dire "réessayez plus tard"). Grâce à cette technique, lorsqu'un message arrive provenant d' un expéditeur qui ne figure pas sur la liste d'autorisation ou qui est inconnu, l'expéditeur, le destinataire et l'adresse IP du serveur d'envoisont enregistrés, puis le message est refusé par Greylisting au cours de la session SMTP avec un code d'erreur temporaire. En outre, pendant une période déterminée (par exemple, 15 minutes), toute tentative de livraison ultérieure sera également temporairement refusée. Étant donné que les "spammeurs" n'effectuent généralement pas d'autres tentatives de livraison lorsqu'un message est refusé, le greylisting peut contribuer de manière significative à réduire le volume de spam que reçoivent vos utilisateurs. Toutefois, même si les spammeurs tentent à nouveau de distribuer le message ultérieurement, il est possible qu'ils aient déjà été identifiés et que d'autres options de lutte contre le spam (telles que les listes de blocage DNS) aient été mises en œuvre avec succès. Listes de blocage DNS bloqueront avec succès. Il est toutefois important de noter que cette technique peut délibérément retarder les "bons" messages électroniques en même temps que les "mauvais". Cependant, les messages légitimes devraient toujours être livrés un peu plus tard, après l'expiration de la période d'inscription sur la liste grise. Il est également important de noter que vous n'avez aucun moyen de savoir combien de temps les serveurs d'envoi attendront avant d'effectuer d'autres tentatives de livraison. Il est

possible que le refus délibéré d'un message avec un code d'erreur temporaire entraîne un retard de quelques minutes ou d'une journée entière.

Plusieurs problèmes et effets secondaires négatifs sont traditionnellement associés à la liste grise, et l'écran Liste grise contient un certain nombre d'options conçues pour y remédier.

Tout d'abord, certains domaines d'envoi utilisent un pool de serveurs de messagerie pour envoyer le courrier sortant. Étant donné qu'un serveur de messagerie différent peut être utilisé pour chaque tentative de distribution, chaque tentative sera traitée comme une nouvelle connexion au moteur de liste grise. Cela pourrait multiplier le temps nécessaire pour passer la liste grise, car chacune de ces tentatives serait traitée comme s'il s'agissait de messages distincts et non de nouvelles tentatives d'envoi d'un message précédent. En utilisant une option de recherche SPF, ce problème peut être résolu pour les domaines d'envoi qui publient leurs données SPF. En outre, il existe une option permettant d'ignorer complètement l'adresse IP du serveur de messagerie d'envoi. L'utilisation de cette option réduit l'efficacité de la liste grise, mais elle résout complètement le problème du pool de serveurs.

Deuxièmement, l'établissement de listes grises nécessite traditionnellement une base de données importante, car chaque connexion entrante doit être suivie. MDaemon minimise la nécessité de suivre les connexions en plaçant la fonctionnalité de liste grise presque en dernier dans la séquence de traitement SMTP. Cela permet à toutes lesautres options deMDaemonde refuser un message avant qu'il n'atteigne l'étape de l'inscription sur la liste grise. Par conséquent, la taille du fichier de données de liste grise est considérablement réduite, et comme il est en mémoire, l'impact sur les performances est minime.

Enfin, plusieurs options sont disponibles pour minimiser l'impact du greylisting sur les "bons" messages. Tout d'abord, les messages envoyés aux listes de diffusion peuvent être exclus. Ensuite, Greylisting dispose de sa propre liste sur laquelle vous pouvez désigner les adresses IP, les expéditeurs et les destinataires que vous souhaitez exclure de la liste grise. Enfin, Greylisting contient une option permettant d'utiliser lecarnet d'adresses dechaque comptecomme liste d'exclusion. Ainsi, le courrier adressé à un utilisateur par une personne figurant dans lecarnet d'adresses decet utilisateurpeut être exclu de la liste grise.

Pour plus d'informations sur le greylisting en général, visitez le site d'Even Harris à l'adresse suivante :

http://projects.puremagic.com/greylisting/

Greylisting

Activer la liste grise

Cliquez sur cette option pour activer la fonctionnalité Greylisting dans MDaemon.

...mais uniquement pour les domaines de la passerelle

Cochez cette case si vous souhaitez mettre sur liste grise uniquement les messages destinés aux domaines de la passerelle.

Liste d'exceptions

Ce bouton permet d'ouvrir la liste d'exclusion du Greylisting dans laquelle vous pouvez désigner les expéditeurs, les destinataires et les adresses IP qui seront exclus du Greylisting.

Différer la première tentative de distribution avec 451 pendant ce nombre de minutes

Indiquez le nombre de minutes pendant lesquelles une tentative de livraison sera mise sur liste grise après la première tentative. Pendant cette période, toute tentative de livraison ultérieure par la même combinaison

serveur/expéditeur/destinataire (c'est-à-dire un "triplet de listes grises") sera refusée avec un autre code d'erreur temporaire. Une fois la période de greylisting écoulée, aucun délai supplémentaire de greylisting ne sera mis en œuvre sur ce triplet, sauf si son enregistrement dans la base de données Greylisting expire.

Expirer les enregistrements inutilisés de la base de données de greylisting après ce nombre de jours

Une fois la période initiale de greylisting écoulée pour un triplet de greylisting donné, aucun autre message correspondant à ce triplet ne sera retardé par le greylisting. Toutefois, si aucun message correspondant à ce triplet n'est reçu pendant le nombre de jours indiqué dans cette option, son enregistrement dans la base de données Greylisting expirera. Une nouvelle tentative de ce triplet entraînera la création d'un nouvel enregistrement de Greylisting et il devra repasser par la période initiale de Greylisting.

Avancé

Cliquez sur ce bouton pour ouvrir la base de données de Greylisting, que vous pouvez utiliser pour revoir ou modifier vos triplets de Greylisting.

Réponse SMTP (laissez le champ vide pour utiliser le paramètre par défaut)

Si vous indiquez une chaîne de texte personnalisée dans cet espace, MDaemon renverra la réponse SMTP "451 <votre texte personnalisé>" au lieu de la réponse par défaut "451 Greylisting activé, réessayez dans X minutes". Ce texte est utile, par Exemple, si vous souhaitez fournir une chaîne contenant une URL décrivant le greylisting.

Ne pas inclure les adresses IP dans la liste grise (n'utiliser que des valeurs MAIL et RCPT) Cochez cette case si vous ne souhaitez pas utiliser l'adresse IP duserveur d'envoicomme l'un des paramètres du greylisting. Cela résoudra le problème potentiel causé par les pools de serveurs, mais réduira l'efficacité de laliste grise.

Lorsqu'une connexion a été analysée avec SPF, ne pas mettre les suivantes en liste grise Si cette option est utilisée, si un message entrant correspond à l'expéditeur et au destinataired'un triplet, mais pas au serveur d'envoi, mais que le traitement SPF détermine que le serveur d'envoi est une alternative valide à celui qui figure dans le triplet, le message sera traité comme une livraison ultérieure correspondant à ce triplet plutôt que comme une nouvelle connexion nécessitant un nouvel enregistrement dans la liste grise.

Ne pas mettre en liste grise le courrier provenant d'utilisateurs présents dans les carnets d'adresses locaux Cochez cette option si vous souhaitez expédier un message sans liste grise lorsque l'expéditeur figure dans le carnet d'adresses dudestinataire. Ne pas mettre en liste grise les messages de**liste** de diffusion

Cochez cette case si vous souhaitez exempter les messages destinés aux listes de diffusion de l'inscription sur la liste grise.

Ne pas mettre en liste grise le courrier provenant de sessions authentifiées Utilisez cette option si vous souhaitez que tous les messages arrivant par le biais d'une session authentifiée soient exemptés de la mise en liste grise.

Ne pas mettre en liste grise le courrier provenant d'IP connues Utilisez cette option si vous souhaitez que tous les messages provenant d'adresses IP autorisées soient exclus de la liste grise.

4.2.5.5 Domaines LAN

🧐 Paramètres de sécurité - Domaines LAN	
 Paramètres de sécurité Authentification de l'expéditeur Analyse SSL & TLS Autres Retours de courrier Régulateur de bande passante Répulsion Liste grise Ormaines LAN IP LAN Politique du site 	Les domaines listés ici ne requièrent pas de connexion RAS et sont considérés en "trafic local" pour la distribution, la régulation de la bande passante, l'accès au service de messagerie. Les messages pour ces domaines sont enregistrés dans le dossier Localq\LnDomain. Domaines LAN
	OK Annuler Appliquer Aide

Domaines LAN

Les domaines listés ici sont considérés par MDaemon comme faisant partie de votre réseau local (LAN). Par conséquent, il n'est pas nécessaire de disposer d'une connexion Internet pour envoyer un message à l'un d'entre eux.

Domaine

Saisissez un Nom de domaine puis cliquez sur *Ajouter* pour l'ajouter à la liste.

Ajouter

Après avoir indiqué un domaine dans l'option*Domaine* ci-dessus, cliquez sur ce bouton pour l'ajouter à la liste.

Supprimer

Sélectionnez un domaine dans la liste puis cliquez sur ce bouton pour le supprimer.

Relayer courrier pour ces domaines LAN

Si cette case est cochée, MDaemon relaiera le courrier pour ces domaines. Cela permet de contrôler dans une certaine mesure le trafic envoyé vers et depuis ces domaines.

Voir :

IP locales 647

4.2.5.6 IP LAN

IP locales

Comme pour les <u>Domaines LAN</u> [646], cet écran sert à répertorier les adresses IP qui résident sur votre LAN (réseau local). Ces adresses IP n'ont donc pas besoin de RAS ou

d'une connexion Internet pour les atteindre, et elles sont traitées comme du trafic local aux fins de la limitation de la bande passante. En outre, elles peuvent être exemptées de diverses autres restrictions en matière de sécurité et de prévention du spam, étant donné qu'il s'agit d'adresses locales.

Supprimer

Sélectionnez une Adresse IP dans la liste et cliquez sur ce bouton pour la supprimer.

IP LOCALES

Saisissez une adresse IP à ajouter à la liste des Adresses IP locales et cliquez sur *Ajouter*. Les caractères génériques tels que 127.0.*.* sont autorisés.

Ajouter

Après avoir saisi une Adresse IP dans le contrôle des*IP locales*, cliquez sur ce bouton pour l'ajouter à la liste.

Voir :

Domaines LAN 646

4.2.5.7 Politique du site

🧐 Paramètres de sécurité - Politique du site 🛛	
 Paramètres de sécurité - Politique du site Paramètres de sécurité Authentification de l'expéditeur Analyse SSL & TLS Autres Retours de courrier Régulateur de bande passante Répulsion Liste grise Domaines LAN IP LAN Politique du site 	Il s'agit du texte transmis au serveur de messagerie expéditeur au début de chaque session de courrier. Il indique par exemple que « toutes les transactions et les adresses IP sont enregistrées » ou que le « relais est interdit ». Activer la fonction Politique du site
	Veuillez limiter votre politique à 15 lignes de 75 caractères chacune. Conformément à la RFC 2821, les lignes blanches ne sont pas autorisées. Elles seront remplacées par * pendant les sessions SMTP.
Création d'une Politique du site SMTP

Cette boîte de dialogue permet de définir une Politique du site pour votre serveur. Ce texte est stocké dans le fichierpolicy.dat situé dans le sous-dossier Serveur MAILde MDaemon et est transmis aux serveurs d'envoi au début de chaque session de courrier SMTP. Exemple de Politique du site : "Ce serveur ne relaie pas" ou "Utilisation non autorisée interdite" Il n'est pas nécessaire de faire précéder chaque ligne de "220 " ou de "220-". MDaemon traite chaque ligne en conséquence, avec ou sans ces codes.

Une Politique d'utilisation du site avec une déclaration concernant le relais du courrier ressemblerait à ceci pendant la transaction SMTP :

```
220-MDaemon Technologies ESMTP MDaemon
220-Ce site ne relaie pas les courriers électroniques non autorisés.
220-Si vous n'êtes pas un utilisateur autorisé de notre serveur
220, vous ne devez pas relayer le courrier par l'intermédiaire de ce
site.
220
HELO exemple.com...
```

Le fichierPOLICY.DAT doit être composé uniquement de texte ASCII imprimable et ne doit pas comporter plus de 512 caractères par ligne ; il est toutefois fortement recommandé de ne pas utiliser plus de 75 caractères par ligne. La taille maximale de ce fichier est de 5000 octets. MDaemon n'affichera pas les fichiers de plus de 5000 octets.

4.3 Écran dynamique

4.3.1 Options/Personnaliser

Diagnostics	Dynami	c Allow List	Dynamic Blog	ck List Don	nain NAT Exemptions
Options/Custor	nize	Auth Failure T	racking	Protocols	Notifications
Enable the Dyr	namic Screer	ning service			
System Options		-			
✓ Enable Auther	ntication Fa	ilure tracking (1)	🗹 Enable D	ynamic Screening	Allow List (3)
🗹 Enable Dynar	nic Screenin	g Block List (2)	Block log	on policy violations	s (4)
Advanced Loggi	na Options -				
Log Auth Fail	ure Data at	Startup		ock List Data at Sta	rtup
Log Allow List	Data at Sta	rtup		cation data when a	available
	using ISO-	3166 Codes			
	, abiling 100 .				
Log Allow List	hits (Info)		🗹 Log Blo	ock List hits (Info)	
🗸 Log Trusted I	P list hits (Ir	nfo)	🗹 Log Log	cation Screen hits	(Info)
🗸 Log failed aut	thentications	s (Info)	Log su	ccessful authentica	ations (Info)
Log connectio	ons allowed	(Info)	🗹 Log cor	nnections refused	(Info)
Log configura	tion when d	hanges detected	🗹 Log Su	mmary once	Hourly \sim
Screening Data	Reset Optio	ns			
Reset All Aut	h Failure Dai	ta			
Reset All Bloc	k List Data		Reset	All Allow List Data	
Enable Advance	ed User Inte	erface features (Z)		
			·		

Grâce à l'Écran dynamique, MDaemon peut suivre le comportement des connexions entrantes afin d'identifier les activités suspectes et de réagir en conséquence. Vous pouvez <u>bloquer</u> a les connexions d'<u>une adresse IP</u> a (ou d'une plage d'adresses) lorsqu'elle échoue à l'authentification un certain nombre de fois dans un laps de temps donné. Vous pouvez également <u>bloquer les comptes</u> au qui tentent de s'authentifier lorsqu'ils échouent trop souvent et trop rapidement. En outre, lorsqu'une adresse IP ou un compte est bloqué, ce n'est pas permanent. L'adresse IP ou le compte qui se connecte sera bloqué pendant le nombre de minutes, d'heures ou de jours que vous aurez spécifié, et ils peuvent être débloqués manuellement par l'administrateur.

Activer le service d'Écran dynamique

Cochez cette case pour activer le service d'Écran dynamique. Vous pouvez également activer/désactiver ce service dans la section Serveurs du volet de navigation de l'interface utilisateur principale de MDaemon.

Options du système

Activer le suivi des échecs d'authentification

Lorsque cette option est activée, le service Écran dynamique suit les échecs d'authentification pour les protocoles désignés dans l'onglet <u>Protocoles</u> of et effectue les actions déterminées par les options de l'onglet<u>Suivi des échecs</u> <u>d'authentification</u> <u>et et option</u> est activée par défaut.

Activer l'Écran dynamique liste blocage

Cette option active la capacité du service d'Écran dynamique à bloquer des adresses IP et des plages d'adresses IP. Vous pouvez gérer la liste de blocage à partir de l' onglet<u>Liste de blocage dynamique.</u> (667) L'option Liste de blocage est activée par défaut.

Activer la Liste d'autorisation de l'Écran dynamique

Cette option active la fonction <u>Liste d'autorisation dynamique</u> au service d'Écran dynamique, que vous pouvez utiliser pour exempter des adresses IP et des plages, afin de les exclure de l'Écran dynamique. La Liste d'autorisation est activée par défaut.

Bloquer les violations de la politique de connexion

Par défaut, MDaemon exige que les comptes utilisent leur adresse électronique complète lors de la journalisation au lieu de la seule partie boîte aux lettres de leur adresse (par exemple, ils doivent utiliser " user1@example.com " au lieu de "user1 "). Ceci est contrôlé par l'option "Demander l'adresse e-mail complète pour l'authentification sur les serveurs" (Les serveurs demandent l'adresse e-mail complète pour l'authentification) sur lapage Systèmes. Si cette option est activée, vous pouvez également activer l' option*Bloquer les violations de la politique de connexion* si vous souhaitez bloquer toute adresse IP qui tente de se connecter sans utiliser l'adresse e-mail complète. Cette option est désactivée par défaut.

Options de journalisation avancées

Enregistrer les données d'échec d'authentification au démarrage

Cette option active l'écriture de toutes les <u>données d'échec d'authentification</u> actuellement stockées par l'Écran dynamique dans le fichier journal au démarrage. Cette option est désactivée par défaut.

Pas de journalisation de la Liste de blocage au démarrage

Cette optionactive l'écriture de toutes les données de la<u>Liste de blocage</u> <u>dynamique</u> actuellement stockées dans le fichier journal au démarrage. Cette fonction est désactivée par défaut.

Enregistrer les données de la Liste d'autorisation au démarrage

Active l'écriture de toutes les données de la Liste d<u>'autorisation dynamique</u> actuellement stockées dans le fichier journal au démarrage. Cette option est désactivée par défaut.

Enregistrer les données de localisation lorsqu'elles sont disponibles

Cochez cette case si vous souhaitez enregistrer les données de localisation de chaque connexion, si elles sont disponibles.

Enregistrer les localisations à l'aide des codes ISO-3166

Cochez cette case si vous souhaitez utiliser les codes de pays à deux lettres ISO-3166 lors de la journalisation des emplacements, au lieu des noms.

Enregistrer les occurrences de la Liste d'autorisation

Cette option ajoute une entrée au journal de l'Écran dynamique chaque fois qu'une connexion entrante provient d'une adresse figurant sur la <u>Liste d'autorisation</u> <u>dynamique</u>.

Enregistrer les hits de la Liste de blocage

Cette option ajoute une entrée au journal de l'Écran dynamique chaque fois qu'une connexion entrante provient d'une adresse figurant sur la <u>Liste de blocage</u> <u>dynamique</u>

Consigner les hits de la liste des IP autorisées

Cette option ajoute une entrée au journal de l'Écran dynamique chaque fois qu'une connexion entrante provient d'une adresse<u>IP autorisée.</u>

Filtrer les occurrences de l'écran de localisation

Cette option ajoute une entrée au journal de l'Écran dynamique chaque fois qu'une connexion entrante est refusée en raison de l'Écran de localisation 2008.

Consigner les échecs d'authentification

Cette option ajoute une entrée au journal de l'Écran dynamique chaque fois qu'une connexion entrante échoue à l'authentification.

Pas de journalisation des authentifications réussies

Activez cette option si vous souhaitez consigner chaque tentative d'authentification entrante qui aboutit. Cette option est désactivée par défaut.

Consigner les connexions autorisées

Activer cette option si vous souhaitez créer une entrée journal pour chaque connexion qui passe l'Écran dynamique et qui est autorisée à poursuivre. Cette option est désactivée par défaut.

Pas de journalisation des connexions refusées

Cette option ajoute une entrée dans le journal chaque fois qu'une connexion entrante est refusée par l'Écran dynamique.

Pas de journalisation de la configuration lorsque des changements sont détectés

Cette option ajoute des entrées dans le journal pour toutes les configurations de l'Écran dynamique lorsque des modifications sont détectées à partir de sources externes (telles que la modification manuelle du fichier INI). Les modifications normales sont journalisées au niveau "infos".

Pas de journalisation une fois [Quotidien | Horaire | Par minute]

Ajoute au journal de l'Écran dynamique un résumé des statistiques de l'Écran dynamique une fois par jour, par heure ou par minute. Non (par défaut), le résumé est journalisé toutes les heures.

Options de réinitialisation des données

Réinitialiser toutes les données échecs auth.

Cochez cette case si vous souhaitez effacer toutes les données d'authentification de l'Écran dynamique. Vous devez ensuite cliquer sur **Appliquer** ou **OK** pour que la réinitialisation ait lieu.

Réinitialiser les données liste de blocage

Cochez cette case si vous souhaitez effacer toutes les données de la Liste de blocage dynamique de l'Écran. Vous devez ensuite cliquer sur **Appliquer** ou **OK** pour que la réinitialisation ait lieu.

Réinitialiser les données de la Liste d'autorisation

Cochez cette case si vous souhaitez effacer toutes les données de la Liste d'autorisation de l'Écran dynamique. Vous devez ensuite cliquer **sur Appliquer** ou **OK** pour que la réinitialisation ait lieu.

Activer les fonctions de l'interface utilisateur avancée

Cochez cette case puis fermez/ouvrez l'interface de configuration de MDaemon pour ajouter plusieurs fonctionnalités avancées de l'Écran dynamique. Un écran <u>Exceptions NAT du domaine</u> est ajouté à la boîte de dialogue Écran dynamique, à partir duquel vous pouvez désigner des combinaisons d'adresses IP/domaines spécifiques à exempter du blocage de l'Écran dynamique lorsque des utilisateurs valides à cette adresse IP ne parviennent pas à s'authentifier par mot de passe. Plusieurs raccourcis d'Écran dynamique ont également été ajoutés à la section Écran dynamique de la barre d'outils, et une option a été ajoutée au menu de raccourcis d'Écran dynamique dans la section Serveurs de l'interface principale pour vous permettre de mettre en pause le service d'Écran dynamique au lieu de le désactiver, empêchant ainsi les clients d'accéder au service pendant que vous gérez ses paramètres.

Voir :

Suivi des échecs d'authentification Liste d'autorisation dynamique Liste de blocage dynamique Exceptions NAT du domaine Liste des comptes exemptés Protocoles Filtrer par emplacement State des Comptes Bloqués Filtrer par SMTP State Sta

4.3.2 Suivi des échecs d'auth.

Dynamic Screening for I	MDaemon			—		>
Dynamic Allow List	Dynamic I	Block List	E	Blocked Acco	ount List	
Exempt Account List	Domain 1	NAT Exemptions		Truste	d IP List	
Options/Customize A	uth Failure Tracking	Protocols	Notific	ations	Diagnos	stics
 ✓ Ignore attempts using ide IP Address Blocking Option ✓ Block addresses after ✓ Enable IPv4 aggregation ✓ Enable IPv6 aggregation 	entical passwords	Only for val	id account ithin 1 entical bits entical bits	s Days (CIDR) (CIDR)	s V	
Defau Sec	It Expiration timeout [ond offense penalty [1 Day 2 Day	ys ∨ ys ∨	Permar	nent	
T	hird offense penalty	3 Day	ys ∨			
Associate Diadrice Options	and offense penalty	· • •	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
Block accounts that fail	authentication 10	times with	in 30	🔹 Minu	ites 🗸	
Admins may unblock acc	Blocke	d Account timeo otification email v	ut 30 vithin the	Minu Minu timeout peri	ites ∨ od	
	ОК	Cance		Apply	He	lp

Ignorer les tentatives d'authentification utilisant des mots de passe identiques

Cette option s'applique aux Options de blocage des adresses IP et aux Options de blocage des adresses IP ci-dessous. ci-dessous. Non par défaut, lorsqu'une tentative d'authentification échoue, les tentatives d'authentification suivantes sont ignorées si elles utilisent le même mot de passe. Elles ne sont pas prises en compte dans le nombre d'échecs autorisés avant le blocage de l'adresse IP ou du compte. Mon compte. Les tentatives multiples utilisant le même mot de passe incorrect se produisent généralement lorsque, par exemple, le mot de passe de la messagerie de l'utilisateur a changé ou a expiré et que son client tente automatiquement de se connecter en utilisant l'ancien mot de passe.

Uniquement pour les comptes valides

Activez cette option si vous souhaitez ignorer les tentatives d'authentification par mot de passe en double uniquement lorsqu'elles tentent de se connecter à un compte valide. Par nom, si, par Exemple, un utilisateur met à jour son mot de passe dans un client mais qu'un autre client fonctionne toujours avec l'ancien mot de passe, les tentatives de Connexion de cet ancien client seront toujours ignorées, puisqu'il aura le bon nom de connexion. Un robot essayant des noms de connexion aléatoires avec un mot de passe similaire ne bénéficiera pas du même avantage et sera bloqué dès qu'il dépassera le seuil d'échec de l'authentification.

Options de blocage des adresses IP

Bloquer les adresses après [xx] échecs d'authentification dans un délai de [xx] [Minutes | Heures | Jours]

Cochez cette case si vous souhaitez bloquer temporairement une adresse IP qui ne parvient pas à s'authentifier auprès de votre serveur un nombre excessif de fois au cours d'une période limitée. Spécifiez le nombre de minutes, d'heures ou de jours et le nombre d'échecs autorisés dans cette période.

Activer l'agrégation IPv4 jusqu'à x.x.x.x/[xx] bits identiques (CIDR)

Cette option bloque une plage d'adresses IPv4 lorsque les échecs d'authentification proviennent d'adresses IP proches les unes des autres plutôt que d'une seule adresse.

Activer l'agrégation IPv6 jusqu'à x::::x:x/ [xx] bits identiques (CIDR)

Cette option bloque une plage d'adresses IPv6 lorsque les échecs d'authentification proviennent d'adresses IP proches les unes des autres plutôt que d'une seule adresse.

Pénalités en cas d'échec multiple

Il s'agit de la durée pendant laquelle une adresse IP ou une plage d'adresses IP sera bloquée par le système d'Écran dynamique lorsqu'elle échoue au nombre spécifié de tentatives d'authentification. Par défaut, la durée pendant laquelle l'adresse IP est bloquée augmente à chaque infraction suivante. Si une adresse IP ne respecte pas la limite d'échecs d'authentification, elle est bloquée pendant un jour. Si cette même adresse IP enfreint à nouveau la limite, la *pénalité pour la deuxième infraction* sera ajoutée au *délai d'expiration par* défaut , puis la *pénalité pour la troisième infraction* sera ajoutée au délai d'expiration par défaut , et ainsi de suite. La durée de la pénalité atteint son maximum avec l'ajout de la *pénalité de quatrième infraction*.

Non (par défaut)

Il s'agit de la durée pendant laquelle une adresse IP ou une plage d'adresses IP ne pourra plus se connecter à MDaemon si elle ne respecte pas la limite d'échec d'authentification spécifiée ci-dessus. Le délai par défaut est de 1 jour.

Pénalités en cas d'échec

Il s'agit du temps ajouté au *délai d'expiration par défaut* lorsqu'une adresse IP ou une plage d'adresses IP est bloquée par l'Écran IP dynamique une deuxième fois.

Pénalités en cas d'échec

Il s'agit du temps qui sera ajouté au *délai d'expiration par défaut* lorsqu'une adresse IP ou une plage d'adresses IP est bloquée une troisième fois par l'Écran dynamique.

Pénalités en cas d'échec

Il s'agit du temps qui sera ajouté au *délai d'expiration par défaut* lorsqu'une adresse IP ou une plage d'adresses IP est bloquée par l'Écran dynamique pour la quatrième fois ou les fois suivantes.

Permanent

Cochez cette case si vous souhaitez bloquer définitivement les adresses IP qui ne respectent pas la limite d'échec d'authentification, plutôt que de les bloquer temporairement à l'aide des pénalités en cas d'infraction spécifiées ci-dessus.

Options blocage de compte

Bloquer les comptes dont l'authentification échoue [xx] fois en l'espace de [xx] [Minutes | Heures | Jours]

Cochez cette case si vous souhaitez ajouter temporairement un compte à la <u>Liste</u> <u>des Comptes Bloqués</u> [674] chaque fois qu'il échoue au nombre spécifié de tentatives d'authentification dans le laps de temps indiqué. Les comptes bloqués ne peuvent se connecter qu'à partir d'<u>IP autorisées</u> [554] et d'IP figurant sur la <u>Liste d'autorisation</u> <u>dynamique</u> [665]. Les comptes figurant dans la <u>Liste des comptes exemptés</u> [671] ne seront jamais ajoutés automatiquement à la Liste des comptes bloqués. Cette option est désactivée par défaut.

Délai d'attente pour les comptes bloqués

Il s'agit de la durée pendant laquelle le compte restera bloqué.

Les Mon comptes peuvent être débloqués en répondant à l'E-mail pour les notifications dans le délai imparti.

Lorsqu'un compte est automatiquement ajouté à la <u>Liste des Comptes Bloqués</u> [674], un administrateur reçoit par défaut un courriel de notification à ce sujet (voir l'option "*Notifier lorsqu'un compte est bloqué*" sur la page Notifications). L'administrateur peut débloquer le compte en répondant simplement à l'e-mail. Cette option est activée par défaut.

Voir :

 Options/Personnaliser

 Liste d'autorisation dynamique

 Liste de blocage dynamique

 Liste des comptes exemptés

 Liste des Comptes Bloqués

 Notifications

4.3.3 Protocoles

Dynamic Screen	ning for N	IDaemon			– 🗆 🗙
Diagnostics	Dyna	mic Allow List	Dynamic	Block List	Domain NAT Exemptions
Options/Custor	mize	Auth Failu	ure Tracking	Protocols	Notifications
SMTP	: 🗹 Use	Allow List	Block List	Auth Failures	Location Screen
POP	: 🗹 Use	Allow List	Block List	Auth Failures	Location Screen
IMAP	: 🗹 Use	Allow List	Block List	Auth Failures	Location Screen
Webmai	l: 🗹 Use	Allow List	Block List	Auth Failures	Location Screen
ActiveSync	:: 🔽 Use	Allow List	Block List	Auth Failures	Location Screen
AutoDiscovery	/: ☑ Use	Allow List	Block List	✓ Auth Failures	 Location Screen
XML API	I: 🗹 Use	Allow List	Block List	Auth Failures	Location Screen
Remote Admin	n: 🗹 Use	Allow List	Block List	Auth Failures	Location Screen
DAV	/: ☑ Use	Allow List	Block List	Auth Failures	Location Screen
XMPP	P: ☑ Use	Allow List	Block List	Auth Failures	Location Screen
Minger	r: 🔳 Use	Allow List	Block List	Auth Failures	Location Screen
MDDP	?: 🗹 Use	Allow List	✓ Block List	✓ Auth Failures	Location Screen
			ОК	Cancel	Apply Help

Non par défaut, le service d'Écran dynamique est appliqué aux protocoles suivants : SMTP, POP, IMAP, Webmail, ActiveSync, <u>AutoDiscovery</u> 75¹, l'API de gestion, MDaemon Remote Admin. WebDAV et CalDAV, XMPP et Minger. Utilisez les options de l'onglet Protocoles pour déterminer quels protocoles verront leurs sessions entrantes vérifiées par rapport à la <u>Liste d'autorisation dynamique</u> 1000 et <u>Liste de blocage dynamique</u> 1007, ceux dont les <u>échecs d'authentification seront suivis</u> 1001 et ceux auxquels s'appliquera le<u>filtrage des emplacements</u> Par défaut, toutes les options de cette boîte de dialogue sont activées, à l'exception de Minger Auth Failures.

Voir :

Suivi des échecs d'authentification Liste d'autorisation dynamique Liste de blocage dynamique

4.3.4 Notifications

Dynamic Screening	for MDaemon			—	
Dynamic Allow List	:	Dynamic Blo	ock List	Blocked Ac	count List
Exempt Account Li	st	Domain NA	T Exemptions	Trus	ted IP List
Options/Customize	Auth Failure 1	Tracking	Protocols	Notifications	Diagnostics
Authentication Failure Notify when an acc Send report to glob Send report to use Send report to use	Reports count's Auth failu val postmaster r's domain postm	are count rea	ches 10 🔹 Send report Send report	occurrences to global admins to user's domain ad	mins
Notify when an acc Send report to glob Send report to use Send report to use	rus count is blocked oal postmaster r's domain postm r	aster (☑ Send report ☑ Send report	to global admins to user's domain ad	mins
IP Address Blocking Re	eports address is blocke	d	Include conr	nection history	
Send report to glob	al postmaster	[Send report	to global admins	
Expiration Reports Send reports on blo Send reports on ex Send reports on blo Send reports on blo Send report to glob	ocked IP address empt/allowed IP ocked accounts t oal postmaster	es as their re addresses a hat are auto	ecords expire s their records matically unbloo Send report	expire :ked to global admins	
Default Notification	Address:	expirations			
		OK	Cancel	Apply	Help

Rapports d'échec d'authentification

Notifier lorsque le nombre d'échecs d'authentification d'un compte atteint [xx] occurrences

Cette option permet à MDaemon d'envoyer un message de notification à un postmaster ou à un autre destinataire sélectionné lorsqu'un compte ne parvient pas à s'authentifier un certain nombre de fois d'affilée. Si aucune des adresses sélectionnées ne peut être résolue, MDaemon enverra le message à l'*Adresse de notification par défaut* indiquée ci-dessous. Si aucune adresse n'a été spécifiée, le message ne sera pas envoyé. L'option est activée par défaut et fixée à 10 occurrences.

Envoyer le rapport au postmaster mondial

Cochez cette case si vous souhaitez envoyer les rapports au postmaster global a. Cette option est activée par défaut.

Envoyer le rapport aux administrateurs globaux

Cochez cette case si vous souhaitez envoyer les rapports aux <u>administrateurs</u> <u>globaux</u> [812].

Envoyer le rapport au postmaster du domaine de l'utilisateur

Cochez cette case si vous souhaitez envoyer les rapports au <u>postmaster</u> ad domaine pour le compte dont les tentatives échouées.

Envoyer le rapport aux administrateurs du domaine de l'utilisateur

Cochez cette case si vous souhaitez envoyer les rapports aux <u>administrateurs du</u> <u>domaine</u> [812] pour le compte qui a échoué les tentatives d'authentification.

Envoyer le rapport à l'utilisateur

Cochez cette case si vous souhaitez envoyer un rapport d'échec à l'utilisateur dont le compte n'a pas réussi à s'authentifier.

Rapports de comptes bloqués

Notifier lorsqu'un compte est bloqué

Cette option permet à MDaemon d'envoyer un message de notification à un postmaster ou à un autre destinataire sélectionné lorsqu'un compte est bloqué en raison d'un <u>trop grand nombre d'échecs d'authentification</u> (164). Si aucune des adresses sélectionnées ne peut être résolue, MDaemon enverra le message à l'Adresse de notification par défaut désignée ci-dessous. Si aucune adresse n'a été spécifiée, le message ne sera pas envoyé. L'option est activée par défaut.

Envoyer le rapport au postmaster mondial

Cochez cette case si vous souhaitez envoyer les rapports au postmaster global al. Cette option est activée par défaut.

Envoyer le rapport aux administrateurs globaux

Cochez cette case si vous souhaitez envoyer les rapports aux <u>administrateurs</u> <u>globaux</u> [812].

Envoyer le rapport au postmaster du domaine de l'utilisateur

Cochez cette case si vous souhaitez envoyer les rapports au <u>postmaster</u> ad domaine pour le compte qui est bloqué.

Envoyer le rapport aux administrateurs du domaine de l'utilisateur

Cochez cette case si vous souhaitez envoyer les rapports aux <u>administrateurs du</u> <u>domaine</u> [812] pour le compte qui est bloqué. bloqué.

Envoyer le rapport à l'utilisateur

Cochez cette case si vous souhaitez envoyer un rapport au compte qui a été bloqué.

Rapports de blocage d'adresses IP

Notifier lorsqu'une adresse IP est bloquée

Cette option permet à MDaemon d'envoyer un message de notification à un maître de poste ou à un autre destinataire sélectionné chaque fois qu'un compte est bloqué par le système d'Écran dynamique. Si aucune des adresses sélectionnées ne peut être résolue, MDaemon enverra le message à l'Adresse de notification par défaut désignée ci-dessous. Si aucune adresse n'a été spécifiée, le message ne sera pas envoyé. L'option est désactivée par défaut.

Inclure l'historique des connexions

Cochez cette case si vous souhaitez que le rapport inclue l'Historique des connexions de l'Adresse IP bloquée.

Envoyer le rapport au postmaster mondial

Cochez cette case si vous souhaitez envoyer les rapports au postmaster global

Envoyer le rapport aux administrateurs globaux

Cochez cette case si vous souhaitez envoyer les rapports aux <u>administrateurs</u> <u>globaux</u> [812].

Rapports d'expiration

Envoyer des rapports sur les adresses Adresses IP bloquées au fur et à mesure de l'expiration de leurs enregistrements

Cette option permet d'envoyer un rapport aux destinataires désignés ci-dessous lorsqu'une adresse IP bloquée arrive à expiration dans la <u>Liste de blocage</u> <u>dynamique</u> [667]. Elle est activée par défaut.

Envoyer des rapports sur les adresses IP exemptées/autorisées Adresses IP exemptées/autorisées au fur et à mesure de l'expiration de leurs enregistrements Cette option permet d'envoyer un rapport aux destinataires autorisés désignés cidessous chaque fois qu'une adresse IP autorisée expire dans la <u>Liste d'autorisation</u> <u>dynamique</u>. Elle est activée par défaut.

Envoyez des rapports sur les comptes bloqués qui sont automatiquement débloqués.

Cette option envoie un rapport aux destinataires désignés ci-dessous lorsqu'un compte bloqué est automatiquement débloqué a l'issue de la période detemporisation du compte bloqué. Elle est activée par défaut.

Envoyer le rapport au postmaster global

Cochez cette case si vous souhaitez envoyer les rapports au postmaster global al. Cette option est activée par défaut.

Envoyer le rapport aux administrateurs globaux

Cochez cette case si vous souhaitez envoyer les rapports aux <u>administrateurs</u> <u>globaux</u> [812].

Adresse de notification par défaut

Il s'agit de l'adresse à laquelle les rapports de notification seront envoyés si aucune autre adresse n'est spécifiée ou si aucune des adresses spécifiées ne peut être résolue. Si aucune adresse ne peut être résolue et qu'aucune *Adresse (par défaut) de notification* n'est désignée, aucun rapport ne sera envoyé.

Ajouter l'heure GMT aux notifications avec expiration

Par défaut, lorsque des Rapports d'expiration sont envoyés, l'heure indiquée est l'heure locale du serveur. Activez cette option si vous souhaitez également inclure l'heure GMT. Cette option est utile lorsque vos administrateurs de messagerie se trouvent dans d'autres fuseaux horaires.

Voir :

<u>Options/Personnaliser</u> िड्छो <u>Suivi des échecs d'authentification</u> िड्ये <u>Liste d'autorisation dynamique</u> िड्डो <u>Liste de blocage dynamique</u> िड्डो <u>Liste des Comptes Bloqués</u> ि7ये

4.3.5 Diagnostics

No Kon	omize	Auth Failur	e Tracking	Proto		INC	tifications
Jiagnostics	Dynamic	: Allow List	Dynamic Blo	ock List	Doma	ain NAT	Exemption
ogging							
Log leve	el None	~			View /	Analyze	e Log
Advanced On	tions						
navancea op	0010		Minimum debugg	er log level	Debug		\sim
	ss Memory Co	unters	No mor	e than eve	rv 30		econds
					(30-3	600)	econus
L DO EVetor	m Wide Dertor	na an co intorna			(00 0	0007	
	in white Perior	mance inform	auon				
		mance inform	2001				
rocess Dumps	in white Perior	mance inform			•	•	
rocess Dumps	based proces	ss dumps	4001	Ir	ndude he	ap inforr	nation
rocess Dumps	based proces	ss dumps	Prefix dum	⊡ Ir	ndude he	ap inforr n	nation
rocess Dumps Enable error	based proces	ss dumps e dumps on	Prefix dum	∑ Ir np files with	ndude he DynScr	ap inforr n	nation
rocess Dumps Enable error	based proces gs to generati DumpCount	ss dumps e dumps on LogEntry	Prefix dum	∑ Ir np files with	nclude he DynScr	ap inforr n	nation
rocess Dumps Enable error rrors / Warning Value 0xC135FE00	based proces gs to generati DumpCount 3	ss dumps e dumps on LogEntry The API insta	Prefix dum alled does not ma	∑ Ir np files with	DynScr	ap inforr n ng called	nation
Process Dumps Enable error Process Dumps Enable error Value 0xC135FE00 0xC135FE01	based proces gs to generati DumpCount 3 3	ss dumps e dumps on LogEntry The API insta The procedu	Prefix dum alled does not ma re called has bee	In files with atch the API	DynScr Level bei ed.	ap inform n	nation
Process Dumps Enable error Process Dumps Enable error Value 0xC135FE00 0xC135FE01 0xC135FE01	based proces gs to generati DumpCount 3 3 3	ss dumps e dumps on LogEntry The API insta The procedu An attempt t	Prefix dum alled does not ma re called has bee to read or write to	☐ Ir np files with atch the API n deprecate o the specif	DynScr Level bei ed.	ap inform n ng callec	nation
Process Dumps Enable error Value 0xC135FE00 0xC135FE01 0xC135FE04 0xC135FE04	based proces gs to generati DumpCount 3 3 3 3	e dumps on LogEntry The API insta The procedu An attempt t Access Denie	Prefix dum alled does not ma re called has bee to read or write to ed (MD_ACCESSD	In files with atch the API on deprecate o the specif DENIED)	I level bei ed. ied memo	ap inform n ng callec	nation
Process Dumps Enable error Value 0xC135FE00 0xC135FE01 0xC135FE04 0xC135FE08 0xC135FE08	based proces gs to generati DumpCount 3 3 3 3 3 3	e dumps on LogEntry The API insta The procedu An attempt t Access Denie This function	Prefix dum alled does not ma re called has bee to read or write to ed (MD_ACCESSD has been discon	✓ Ir np files with atch the API n deprecate o the specif DENIED) tinued for f	I level bei ed. ied memo	ap inform n ng callec ry would	nation
Process Dumps Enable error Value 0xC135FE00 0xC135FE01 0xC135FE04 0xC135FE08 0xC135FE08	based proces gs to generati DumpCount 3 3 3 3 3	e dumps on LogEntry The API insta The procedu An attempt t Access Denie This function	Prefix dum alled does not ma re called has bee to read or write to d (MD_ACCESSD has been discon	✓ Ir np files with atch the API n deprecate o the specif DENIED) tinued for f	I level bei ed. ied memo	ap inform n ng callec vry would velopmen	nation I for. (N I result nt
Process Dumps Enable error Value 0xC135FE00 0xC135FE01 0xC135FE04 0xC135FE08 0xC135FE08 0xC135FE0D ClassFE0D	based proces gs to generati DumpCount 3 3 3 3 3 3	ss dumps on LogEntry The API insta The procedu An attempt t Access Denie This function	Prefix dum alled does not ma re called has bee to read or write to ed (MD_ACCESSD has been discon	In the API atch the API n deprecate of the specif DENIED) tinued for f	level bei ed. ied memo	ap inform n ng called ory would velopmen	nation

Cet écran contient des options avancées qui, dans la plupart des cas, n'auront pas besoin d'être utilisées, sauf si vous essayez de diagnostiquer un problème avec l'Écran dynamique ou si vous êtes en contact avec le support technique.

Pas de journalisation

Niveau de journalisation

Six niveaux de journalisation sont pris en charge, de la plus grande à la plus petite quantité de données enregistrées :

Déboga Il s'agit du niveau de journalisation le plus complet. Il enregistre toutes les entrées disponibles et n'est généralement utilisé que pour diagnostiquer un problème ou lorsque l'administrateur souhaite obtenir des informations détaillées.

- **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.
- AvertisLes avertissements, les erreurs, les erreurs critiques et lessementévénements de démarrage/arrêt sont consignés dans le journal.
- **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Critiqu Les erreurs critiques et les événements de démarrage/arrêt sont e journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.

Visualiser/Analyser le journal

Cliquez sur ce bouton pour ouvrir la fenêtre de visualisation du journal du système MDaemon Advanced. Non (par défaut) Pas de journalisation dans :".. \NMDaemon\Logs\"

Options avancées

Niveau minimal du journal de débogage

Il s'agit du niveau minimal de la journalisation à envoyer au débogage. Les niveaux de journalisation disponibles sont les mêmes que ceux décrits ci-dessus.

Enregistrer les compteurs de mémoire du processus

Cochez cette case pour consigner dans le fichier journal les informations relatives à la mémoire, aux gestionnaires et aux threads spécifiques au processus. Ceci est utile pour trouver des pistes potentielles et des problèmes d'allocation de ressources. Les entrées du journal ne seront émises que si les données ont changé depuis la dernière fois qu'elles ont été journalisées.

Pas de journalisation des informations sur les performances de l'ensemble du système

Cochez cette case si vous souhaitez consigner dans le fichier journal des informations sur les performances de l'ensemble du système. Ceci est utile pour trouver des pistes potentielles et des problèmes d'allocation de ressources. Les entrées journal ne seront émises que si les données ont changé depuis la dernière fois qu'elles ont été journalisées.

Pas plus de toutes les [xx] secondes

Cette option permet de définir la fréquence à laquelle les informations relatives aux processus et aux performances seront journalisées.

Fichiers dumpers

Créer un dump du processus en cas d'erreur

Activez cette option si vous souhaitez générer des Fichiers dumps à chaque fois que survient un avertissement ou une erreur spécifique que vous avez désigné cidessous.

Inclure les informations du tas dans les dumps

Non (par défaut), les informations du tas sont incluses dans les Fichiers dumps. Décochez cette case si vous ne souhaitez pas les inclure.

Préfixe des fichiers dump

Les noms des fichiers dumpiers commenceront par ce texte.

Erreurs/avertissements à partir desquels générer des fichiers dumps

Cliquez avec le bouton droit de la souris sur cette zone et utilisez les options*Ajouter/Modifier/Supprimer une entrée...* pour gérer la liste des erreurs ou des avertissements qui déclencheront des vidages de processus. Pour chaque entrée, vous pouvez spécifier le nombre de Fichiers dumps autorisés avant qu'elle ne soit désactivée.

Voir :

Écran dynamique | Options/Personnaliser

4.3.6 Liste d'autorisation dynamique

Options/Customiz	e Au	th Failure	Tracking	Proto	cols	Notifications
Diagnostics	Dynamic Allow	List	Dynamic Blo	ock List	Domair	n NAT Exemption
IP Address/Range	Comment	Expires	Object ID			
::1	Default Entry	Never	{ccf9d806-20)a6-4761-8	54c-65b5ad	ld11dbe}
127.0.0.0/24	Default Entry	Never	{cd572a1a-9	610-4b8e-a	6d3-f2b0d	fb8d6f8}
10.0.0/8	Default Entry	Never	{625d023b-7	a56-4d0c-a	4e4-451c0	019f995}
fd00::/8	Default Entry	Never	{89568642-7	066-4ce4-8	d97-bbeaf	4af11ef}
fe80::/64	Default Entry	Never	{354ba643-9	3b8-4036-b	1e2-da240	945edfa}
172.16.0.0/12	Default Entry	Never	{c459b77f-bb	00a-4f8f-8e	dc-c74209	b2d29c}
fec0::/10	Default Entry	Never	{d93a2bbf-c	263-4113-8	3ea-3be15	05e6eab}
192.168.0.0/16	Default Entry	Never	{89d12dc0-f	54d-408e-b	e1c-3b8a00)647ab4}
c						
		Add	Remo	IVe		

La Liste d'autorisation dynamique Bloque les connexions des adresses IP/Plage d'adresses qui ne seront pas bloquées par le service d'Écran dynamique lorsqu'elles tenteront de se connecter à MDaemon. Des adresses peuvent être ajoutées à la Liste d'autorisation dynamique en cliquant sur le bouton **Ajouter.** Chaque entrée contient l'adresse IP ou la plage de dates, la date et l'heure d'expiration de l'entrée (ou " Jamais " si elle n'expire pas), tout commentaire que vous souhaitez faire sur l'entrée, et un Object ID. La Liste d'autorisation dynamique est également utilisée par l'Écran SMTP [603], le <u>Filtrer les emplacements</u> [604].

Ajout d'une Adresse IP ou d'une plage d'adresses à la Liste d'autorisation dynamique

Pour ajouter une entrée à la liste :

1. Cliquez sur **Add (Ajouter)**. La boîte de dialogue Add IP List Entry (Ajouter une entrée à la liste IP) s'ouvre.

Add IP List Entry	\times
IP Address / Mask	
wildcards accepted (ie. 192.168.0.0/16, 192.168.0.*)	
Expires 1/21/2023 V 1:21:14 PM Vever	_
Comment	
OK Cancel	

- 2. Saisissez l'adresse IP ou la plage d'adresses IP.
- 3. Choisissez la date et l'heure d'expiration de l'entrée ou cliquez sur Jamais.
- 4. Saisissez un commentaire pour l'entrée (facultatif).
- 5. Cliquez sur **OK**.

Supprimer une entrée de la liste

Pour supprimer une ou plusieurs entrées de la liste :

- 1. Sélectionnez la ou les entrées que vous souhaitez supprimer de la liste (Ctrl+clic pour sélectionner plusieurs entrées).
- 2. Cliquez sur **Supprimer**.

Voir :

<u>Options/Personnaliser</u> िड्छो <u>Suivi des échecs d'authentification</u> िड्यो <u>Liste de blocage dynamique</u> िढिरो <u>Protocoles</u> िडरो

4.3.7 Liste dynamique des blocs

Options/Customiz	e Auth Fail	ure Trackir	ng Prot	ocols	Notifications
Diagnostics	Dynamic Allow List	Dyr	namic Block List	Doma	ain NAT Exemptions
IP Address/Range	Comment	Expires	Object ID		
111.222.111.222	persistent spammer	Never	{16d45229-bf55	-413a-b6f9	-3e5c00db56e5}
	Add	d	Remove		

La liste de blocage dynamique contient la liste des adresses IP ou des plages d'adresses qui seront bloquées par le service d'Écran dynamique lorsqu'elles tenteront de se connecter à MDaemon. Les adresses peuvent être ajoutées automatiquement par les options <u>Auth Failure Tracking</u> at <u>SMTP Screen</u> at ajoutées manuellement en cliquant sur le bouton**Add.** Chaque entrée contient l'adresse IP ou la plage, la date et l'heure d'expiration de l'entrée (ou " Jamais ", si elle n'expire pas), tout commentaire que vous souhaitez faire sur l'entrée, et un Object ID.

1. Cliquez sur **Add (Ajouter)**. La boîte de dialogue Ajouter une entrée de liste IP s'ouvre.

Add IP List Entry	×
IP Address / Mask IPv4 Address must contain a full 4 octets. CIDR notation and asterisks as wildcards accepted (ie. 192.168.0.0/16, 192.168.0.*) Evpires 1/21/2023	
Comment OK Cancel	

- 2. Saisissez l'adresse IP ou la plage d'adresses IP.
- 3. Choisissez la date et l'heure d'expiration de l'entrée ou cliquez sur Jamais.
- 4. Saisissez un commentaire pour l'entrée (facultatif).
- 5. Cliquez sur **OK**.

Supprimer une entrée de la liste

Pour supprimer une ou plusieurs entrées de la liste :

- 1. Sélectionnez la ou les entrées que vous souhaitez supprimer de la liste (Ctrl+clic pour sélectionner plusieurs entrées).
- 2. Cliquez sur **Supprimer**.

Voir :

<u>Options/Personnaliser</u> िक्को <u>Suivi des échecs d'authentification</u> िक्को <u>Liste d'autorisation dynamique</u> िक्की <u>Protocoles</u> िक्री

4.3.8 Exceptions NAT

Options/Customize		Auth Failure	Tracking	Protocols	Notifications
Diagnostics	Dynamic Al	low List	Dynamic Blo	ck List Do	main NAT Exemptions
Router Public IP Ado	dress Dom	ain Object I	ID		
		Add	Remov	/e	

Cet écran est disponible lorsque vous avez activé l'option *Activer les options Actifs de l'interface utilisateur avancée* dans l'écran<u>Options/Personnaliser</u> de l'Écran dynamique.

Utilisez cette fonctionnalité pour accommoder un groupe d'utilisateurs de MDaemon qui résident sur le même réseau local externe (LAN), qui utilise la traduction d'adresse réseau (NAT) pour fournir une seule adresse IP publique partagée pour tous. En ajoutant l'adresse IP publique de leur réseau local et le domaine MDaemon auquel les comptes appartiennent, vous pouvez éviter que l'adresse IP soit bloquée par l'Écran dynamique lorsqu'un ou plusieurs des utilisateurs échouent à l'authentification en raison d'un mot de passe incorrect. Sans cette fonctionnalité, un utilisateur valide dont le client de messagerie est mal configuré pourrait entraîner le blocage de l'adresse IP du réseau local et empêcher ainsi tous les utilisateurs d'accéder à leur messagerie. Cela peut se produire, par Exemple, lorsque le mot de passe d'un utilisateur est modifié mais que l'utilisateur oublie de mettre à jour son client de messagerie avec le nouveau mot de passe.

Les adresses IP répertoriées ici peuvent encore être bloquées pour d'autres raisons, comme des robots qui tentent de se connecter à des comptes non valides, des clients mal configurés qui tentent de se connecter à un domaine MDaemon différent de celui associé à l'adresse IP, etc. Si vous souhaitez exclure complètement une adresse IP de l'Écran dynamique, utilisez la Liste d'autorisation dynamique

Ajout d'une Exceptions NAT du domaine

Cliquez sur **Ajouter**, entrez l'*Adresse IP publique* du *routeur* du LAN externe, et sélectionnez le *Domaine* MDaemon dont les utilisateurs se connecteront à partir de cette adresse IP. Cliquez ensuite sur **OK**.

Voir aussi

Options/Personnaliser 650

4.3.9 Liste des Comptes Exceptions

Dynamic Screening for	MDaemon		—	
Dynamic Allow List	Dynamic Blo	ock List	Blocked Acc	ount List
Options/Customize A	uth Failure Tracking	Protocols	Notifications	Diagnostics
Exempt Account List	Domain NA	T Exemptions	Truste	ed IP List
Account ID frank.thomas@company.t	Object ID est {944f25f9-bc3f-46e	1-a120-12577f0	080439}	
A <u>d</u> d Item(s)	<u>R</u> efresh	List	Remove Ite	m(s)
	ОК	Cancel	Apply	Help

Utilisez cette page pour dresser la liste des comptes que vous souhaitez exempter des Options de blocage de comptes de l'Écran dynamique.

> Vous devez faire preuve de prudence lorsque vous ajoutez un compte à cette liste, car cela pourrait, par exemple, permettre à un réseau de robots attaquants de continuer à envoyer des sondes de mot de passe sur le compte, limité uniquement par la gamme d'adresses IP du réseau de robots. L'Écran dynamique bloquerait toujours l'adresse IP de l'attaquant, mais ce dernier pourrait continuer à sonder le compte ciblé tant qu'il utilise plusieurs adresses IP.

Ajouter des comptes à la liste

Cliquez sur **Ajouter élément(s)** pour ouvrir la boîte de dialogue Sélection des utilisateurs afin de sélectionner et d'ajouter des comptes à la liste.

Select Users, Groups	or Bui	ilt-In Objects	
Select these object	Users		Object Types
From these domains:	comp	any.test	Locations
Common Queries			
Name contains	s:		Find Now
Email contains	s:		
Description contains	s:		
Include Disabled Acco	ounts		
Search Results		Help OK	Cancel
Search Results	Туре	Help OK Email	Cancel
Search Results	Type User	Help OK Email randy.peterman@company.test	Cancel
Search Results Name Arandy Peterman Sir Smith	Type User User	Help OK Email randy.peterman@company.test sir.smith@company.test	Cancel
Search Results Name Anndy Peterman Sir Smith	Type User User	Help OK Email randy.peterman@company.test sir.smith@company.test	Cancel
Search Results Name Anndy Peterman Sir Smith	Type User User	Help OK Email randy.peterman@company.test sir.smith@company.test	Cancel
Search Results Name Anndy Peterman Sir Smith	Type User User	Help OK Email randy.peterman@company.test sir.smith@company.test	Cancel
Search Results Name Bandy Peterman Sir Smith	Type User User	Help OK Email randy.peterman@company.test sir.smith@company.test	Cancel
Search Results Name Arandy Peterman Sir Smith	Type User User	Help OK Email randy.peterman@company.test sir.smith@company.test	Cancel
Search Results Name Arandy Peterman Sir Smith	Type User User	Help OK Email randy.peterman@company.test sir.smith@company.test	Cancel
Search Results Name Arandy Peterman Sir Smith	Type User User	Help OK Email randy.peterman@company.test sir.smith@company.test	Cancel

A partir de ces domaines

Si vous souhaitez afficher les comptes de certains domaines seulement, cliquez sur **Emplacements...**, choisissez les domaines et cliquez sur **OK**.

Requêtes courantes

Utilisez les options de cette section pour affiner votre recherche en spécifiant tout ou partie du nom de l'utilisateur, son adresse électronique ou le contenu de la Description du compte. Laissez ces champs vides si vous souhaitez que les résultats de la recherche contiennent tous les utilisateurs du domaine sélectionné.

Inclure les comptes désactivés

Cochez cette case si vous souhaitez inclure les <u>comptes désactivés</u> dans votre recherche.

Rechercher maintenant

Une fois que vous avez spécifié tous vos critères de recherche, cliquez sur **Rechercher maintenant** pour effectuer la recherche.

Résultats de la recherche

Après avoir effectué la recherche, sélectionnez les utilisateurs souhaités dans les Aucun résultats et cliquez sur **OK** pour les ajouter à la liste des comptes.

Suppression de comptes de la liste

Pour supprimer un compte dans la liste, sélectionnez le compte et cliquez sur **Supprimer élément(s)**.

Voir :

Options/PersonnaliserSuivi des échecs d'authentificationListe d'autorisation dynamiqueProtocoles

4.3.10 Liste des comptes bloqués

Evenet Account List				True	Trusted ID List		
Options/Customize	Auth E	ailure Trackies	Brotocolo	Notifications	Disposition		
Dupamic Allow List	AUUTE		pic Plock List	Blocked Ac	count List		
Dynamic Allow List		Dynai	HIC DIOCK LIST	Dioched Ac			
Account ID	Exp	pires	Object ID				
harry.mudd@example.	com 202	24-09-10 20:2	2 {7c398f95-9937	-4063-b0d4-9f3fdb4	e7aa5}		
A <u>d</u> d Item(s)		<u>R</u> e	fresh List	R <u>e</u> move It	em(s)		

Cette page affiche tous les comptes qui ont été automatiquement bloqués par l'Écran dynamique parce qu'ils n'ont pas satisfait aux conditions de <u>suivi des échecs</u> <u>d'authentification.</u> Les comptes bloqués ne peuvent se connecter qu'à partir d'<u>IP</u> autorisées at d'IP figurant sur la <u>Liste d'autorisation dynamique</u> at d'IP figurant sur la <u>Liste d'autorisation dynamique</u> contra restera sur cette liste jusqu'à ce que son délai d'expiration soit écoulé, comme déterminé par le paramètre <u>Délai d'expiration du compte bloqué</u> contra pouvez également ajouter manuellement des comptes à la liste et définir le délai d'expiration de chaque entrée.

■ Ajout de comptes à la liste

Cliquez sur **Ajouter élément(s)** pour ouvrir la boîte de dialogue Sélection des utilisateurs afin de sélectionner et d'ajouter des comptes à la liste.

Select Users, Groups	or Bui	ilt-In Objects	×
Select these object	Users		Object Types
From these domains:	Locations		
Common Queries Name contain:	s:		Find Now
Email contains	s:		
Description contains	s:		
Include Disabled Acco	ounts		
Search Results		Help OK	Cancel
Name Name	Туре	Email	
🗌 🚨 Randy Peterman	User	randy.peterman@company.test	
Sir Smith	User	sir.smith@company.test	

A partir de ces domaines

Si vous souhaitez afficher les comptes de certains domaines seulement, cliquez sur **Emplacements...**, choisissez les domaines et cliquez sur **OK**.

Requêtes courantes

Utilisez les options de cette section pour affiner votre recherche en spécifiant tout ou partie du nom de l'utilisateur, de son adresse électronique ou du contenu de la Description du compte. Laissez ces champs vides si vous souhaitez que les résultats de la recherche contiennent tous les utilisateurs du domaine sélectionné.

Inclure les comptes désactivés

Cochez cette case si vous souhaitez inclure les <u>comptes désactivés</u> dans votre recherche.

Rechercher maintenant

Une fois que vous avez spécifié tous vos critères de recherche, cliquez sur **Rechercher maintenant** pour effectuer la recherche.

Résultats de la recherche

Après avoir effectué la recherche, sélectionnez les utilisateurs souhaités dans les Aucun résultats et cliquez sur **OK** pour les ajouter à la liste des comptes.

Modifier la Date d'expiration d'un compte bloqué

Pour modifier la date et l'heure d'expiration d'une entrée de compte, cliquez avec le bouton droit de la souris sur l'entrée, puis cliquez sur **Définir la date d'expiration pour les comptes sélectionnés**. Choisissez la date et l'heure d'expiration ou cochez la case **Jamais** si vous ne souhaitez pas qu'elle expire. Cliquez sur **OK**.

Suppression de comptes de la liste

Pour supprimer un compte dans la liste, sélectionnez le compte et cliquez sur **Supprimer élément(s)**.

Voir :

<u>Options/Personnaliser</u> ब्लो <u>Suivi des échecs d'authentification</u> ब्ली <u>Liste d'autorisation dynamique</u> ब्ली <u>Protocoles</u> ब्लिगे

4.4 MDPGP

Enable MDPGP	Setting	;				
Enable encryption & signing services	🗹 Er	Encrypt mail automatically if recipient's public-key is known				
Enable decryption & verification services	🗔 Sig	Sign mail automatically if sender's private-key is known				
Collect public-keys from DNS (pka1) and cache for T2 Trade public-keys using HTTP (Webmail) Trade public-keys during SMTP mail sessions (MDaemon)	hours E	☐ Encrypt/Sign m ☐ Encrypt/Sign m ☐ Encrypt/Sign m	ail sent betwee ail sent betwee ail sent to self	n users of the sarr n users of local M	ne domain Daemon domains	
Authorize all local MDaemon users for all services	⊡ Er	nail details of encry	ption failures to	sender (pgpe ci	ommand)	
	ices 🛛 🗹 Er	Email public-keys when mail sent to self (-pgpk command) Auto-import public-keys sent from authenticated users				
Configure exactly who can and can not use MDPGP served	vices 🗸 🖂 Au					
Encrypt outbound mail based on receiving IP Setu	up Cr	eate keys automat	ically	Key size 2048	3 ~	
Filter Show: 🗹 Local	☑ Remote Cr	eate keys for a spe	ecific user	Expires in 365	days (0 = never	
Key Owner	Key ID	Кеу Туре	Key Status	Key Created	Key Expires	
Frank Thomas <postmaster@company.test></postmaster@company.test>	24E4A737B96239BF	pub/prv	enabled	4/4/2020	4/4/2021	
Harcourt Fenton Mudd <harry.mudd@example.com></harry.mudd@example.com>	62EAE4162EFC32B0	pub/prv	enabled	4/4/2020	4/4/2021	
Michael Mason <michael.mason@company.test></michael.mason@company.test>	CD7AC71CC2502643	3 pub/prv	enabled	4/4/2020	4/4/2021	
Frank Thomas <frank.thomas@company.test></frank.thomas@company.test>	5AA71D544C69635E	pub/prv	enabled	4/4/2020	4/4/2021	
Domain Key (company.test) <anybody@company.test></anybody@company.test>	57EBU/188D1E8D6	o pub/prv	enabled	4/4/2020	4/4/2021	
obilă recursi robilăbilari intăăluaricour	5230000100012E	, bapic	Shabiba	n n 2020	10701	

OpenPGP est un protocole standard pour l'échange de données cryptées, et il existe une variété de plugins OpenPGP pour les clients de messagerie qui permettent aux utilisateurs d'envoyer et de recevoir des messages cryptés. MDPGP est le composant OpenPGP intégré de MDaemon qui peut fournir des services de cryptage, de décryptage et de gestion des clés de base à vos utilisateurs sans qu'ils aient besoin d'utiliser un plugin pour client de messagerie.

MDPGP chiffre et déchiffre les messages électroniques en utilisant un système de clés publiques/privées. Pour ce faire, lorsque vous souhaitez utiliser MDPGP pour envoyer un message privé et sécurisé à quelqu'un, MDPGP crypte ce message à l'aide d'une "clé" que vous avez préalablement obtenue de cette personne (c'est-à-dire sa "clé publique") et importée dans MDPGP. Inversement, si l'expéditeur souhaite vous envoyer un message privé, il doit le crypter à l'aide de votre clé publique, qu'il a obtenue auprès de vous. Il est absolument nécessaire de donner votre clé publique à l'expéditeur, car sans elle, il ne peut pas vous envoyer un message crypté OpenPGP. Votre clé publique unique doit être utilisée pour crypter le message, car c'est votre clé privée unique que MDPGP utilisera pour décrypter le message lorsqu'il arrivera.

Pour que MDPGP puisse gérer la Connexion, le cryptage et le décryptage des messages, il conserve deux stocks de clés (c'est-à-dire des trousseaux de clés), l'un pour les clés publiques et l'autre pour les clés privées. MDPGP peut générer automatiquement les clés de vos utilisateurs en fonction des besoins, ou vous pouvez les créer manuellement pour des utilisateurs spécifiques. Vous pouvez également importer des clés créées ailleurs. De plus, MDaemon peut rechercher les clés publiques jointes aux messages authentifiés des utilisateurs locaux, puis les importer automatiquement. Ainsi, un utilisateur peut demander une clé publique à quelqu'un, puis se l'envoyer par courrier électronique afin que MDPGP la détecte et l'importe dans le trousseau de clés publiques. MDPGP ne stockera jamais plusieurs copies de la même clé, mais il peut y avoir plusieurs clés différentes pour une même adresse. Enfin, lorsqu'un message arrive pour une adresse dont la clé se trouve dans un trousseau, MDPGP signe, crypte ou décrypte le message selon vos paramètres. Si une adresse possède plusieurs clés, MDPGP utilisera celle que vous avez désignée comme clé préférée pour crypter le message. Si aucune clé préférentielle n'a été désignée, MDPGP utilisera la première. Lors du déchiffrement d'un message, MDaemon essaiera chaque clé.

Vous pouvez configurer les services de Connexion et de chiffrement de MDPGP pour qu'ils fonctionnent automatiquement ou manuellement. En mode automatique, MDPGP signe et crypte automatiquement les messages dans la mesure du possible. Si le fonctionnement est manuel, MDPGP ne signera ou ne cryptera un message que si l'utilisateur qui l'envoie insère une commande spéciale dans l'Objet du message. Dans tous les cas, les messages ne seront signés ou cryptés (ou décryptés) que lorsque le compte aura reçu l'autorisation d'utiliser ces services.



La spécification OpenPGP est décrite dans les RFC *** et ***.

Activation de MDPGP

Activer MDPGP

MDPGP est activé par défaut, mais il ne signera, ne chiffrera ni ne déchiffrera aucun message tant que vous n'aurez pas créé ou importé des clés dans ses paramètres par défaut, ou tant que vous n'aurez pas utilisé l'option ci-dessous pour configurer MDPGP de manière à ce qu'il *crée des clés automatiquement*.

Activer les services de chiffrement et de Connexion

Dans le défaut, les messages peuvent être signés et cryptés lorsque les clés requises se trouvent dans le trousseau. Désactivez cette option si vous ne souhaitez pas autoriser MDPGP à signer ou à crypter des messages.



Les messages peuvent être signés sans être cryptés, mais tout message crypté par MDPGP sera toujours signé également.

Activer les services de décryptage et de vérification

Non (par défaut), les messages entrants chiffrés seront déchiffrés si la clé privée du destinataire est connue. En outre, MDPGP vérifiera également les signatures intégrées dans les messages non chiffrés. Non (par défaut), le destinateur et le destinataire doivent être autorisés à utiliser les services de déchiffrement et de vérification, soit par l'option "Autoriser tout le monde...", soit parl'option"Configurer exactement qui..." ci-dessous (tout le monde est autorisé

par défaut). Désactivez cette option si vous ne souhaitez pas vérifier les signatures intégrées ou autoriser MDPGP à déchiffrer les messages, Exemple : si vous souhaitez que tous vos utilisateurs gèrent leur propre déchiffrement via un plugin de client de messagerie. Dans ce cas, tout message entrants chiffré sera traité comme un message normal et placé dans la boîte aux lettres du destinataire.

Collecter les clés publiques du DNS (pka1) et les mettre en cache pendant [xx] heures Activez cette option si vous souhaitez que MDPGP active les requêtes pour les clés publiques des destinataires de messages via DNS à l'aide de PKA1. Cette option est utile car elle automatise le processus d'obtention des clés publiques de certains destinataires, ce qui vous évite, à vous ou à vos utilisateurs, d'avoir à les obtenir et à les importer manuellement pour envoyer des messages cryptés. Lorsque des requêtes PKA1 sont effectuées, tout URI de clé trouvé est immédiatement collecté, validé et ajouté au trousseau. Les clés collectées et importées dans le trousseau à l'aide de cette méthode sont enregistrées dans un fichier appelé fetchedkeys.txt. Ces clés expirent automatiquement après le nombre d'heures spécifié dans cette option ou en fonction de la valeur TTL de l'enregistrement PKA1 qui les a référencées, la valeur la plus élevée étant retenue. Par conséquent, la valeur spécifiée ici est la durée minimale pendant laquelle une clé sera mise en cache. La valeur par défaut est de 12 AM et la valeur la plus basse autorisée est de 1 heure.

> Si vous souhaitez publier vos propres clés publiques dans le DNS, vous devez alors créer des enregistrements TXT **spéciaux.** Exemple, pour l'utilisateur frank@example.com avec le key-id : 0A2B3C4D5E6F7G8H, dans le DNS du domaine "example.com", vous créeriez un enregistrement TXT à "frank. pka.example.com" (en remplaçant le @ de l'adresse électronique par la chaîne". pka."). Les données de l' enregistrementTXT ressembleraient à ceci : "v=pka1 ; fpr=<empreinte digitale complète de la clé> ; uri=<Webmail-URL>/WorldClient.dll ? view=mdpqp&k=0A2B3C4D5E6F7G8H" **où** <empreinte digitale complète de la clé> est l'empreinte digitale complète de la clé (40 caractères représentant la valeur complète de l'empreinte digitale sur 20 octets). Vous pouvez voir l'empreinte complète d'une clé en double-cliquant sur la clé dans l'interface graphique de MDPGP.

Échanger des clés publiques par HTTP (Webmail)

Activez cette option si vous souhaitez utiliser Webmail comme serveur de clés publiques de base ; Webmail honorera les demandes de clés publiques de vos utilisateurs. Le format de l'URL pour effectuer la demande est le suivant: "http://<Webmail-URL>/WorldClient.dll?View=MDPGP&k=<Key-ID>". Où <Webmail-URL> est le chemin d'accès à votre serveur Webmail (par exemple, "http://wc.example.com") et <Key-ID> est l'identifiant de clé à seize caractères de la clé que vous voulez (par exemple, "0A1B3C4D5E6F7G8H"). L'identifiant de la clé est construit à partir des 8 derniers octets de l'empreinte de la clé, soit 16 caractères au total. **Échanger des clés publiques pendant les sessions de messagerie SMTP (MDaemon)** Cochez cette case si vous souhaitez activer la transmission automatique des clés publiques dans le cadre du processus de distribution des messages SMTP. Pour ce faire, le serveur SMTP de MDaemon honorera une commande SMTP appelée RKEY. Lors de l'envoi d'un e-mail à un serveur prenant en charge RKEY, MDaemon propose à l'expéditeur de transmettre sa clé publique préférée à l'autre hôte. Ce dernier répondra en indiquant qu'il possède déjà cette clé (" 250 2.7.0 Clé déjà connue ") ou qu'il en a besoin, auquel cas la clé est immédiatement transférée sous forme ASCII blindée (" 354 Entrez la clé, terminez par CRLF.CRLF "), tout comme un message électronique. Les clés expirées ou révoquées ne sont jamais transmises. Si MDaemon dispose de plusieurs clés pour l'expéditeur, il envoie toujours la clé qui est actuellement considérée comme préférée. Si aucune clé n'est préférée, la première trouvée est envoyée. Si aucune clé valide n'est disponible, rien n'est fait. Seules les clés publiques appartenant à des utilisateurs locaux sont proposées.

Les transferts de clés publiques s'effectuent dans le cadre de la session de courrier distribué en SMTP' qui délivre le message de l'utilisateur. Pour que les clés publiques transmises de cette manière soient acceptées, la clé publique doit être envoyée avec un message qui a été <u>signé par</u> al le domaine du propriétaire de la clé avec le i= réglé sur l'adresse du propriétaire de la clé, qui doit également correspondre exactement à l'adresse de l'en-tête From : dont il ne peut y avoir qu'une seule. Le "propriétaire de la clé" est indiqué dans la clé elle-même. Dans ce cas, le message doit provenir d'un hôte situé dans le <u>chemin SPF de</u> los l'expéditeur . Enfin, le propriétaire de la clé (ou son Domaine entier via l'utilisation de caractères génériques) doit être autorisé pour RKEY en ajoutant une entrée appropriée au fichier de règles MDPGP (les instructions se trouvent dans le fichier de règles) indiquant que le Domaine peut être autorisé pour l'échange de clés. Toutes ces vérifications sont effectuées automatiquement, mais les <u>vérifications</u> <u>bKIM</u> sesi et <u>SPF</u> doivent être activées, faute de quoi aucun travail ne peut être effectué.

Le journal MDPGP enregistre les résultats et les détails de toutes les clés importées ou supprimées, et le journal de la session SMTP suit également cette activité. Ce processus suit la suppression des clés existantes et la sélection de nouvelles clés préférées et met à jour tous les serveurs participants auxquels il envoie du courrier lorsque ces éléments changent.

Autoriser tous les utilisateurs locaux de MDaemon pour tous les services

Par défaut, tous les comptes utilisateurs locaux de MDaemon sont autorisés à utiliser les services MDPGP que vous avez activés : la connexion, le cryptage, le décryptage et la vérification. Si vous ne souhaitez pas autoriser certains utilisateurs à utiliser un ou plusieurs de ces services, vous pouvez utiliser l'option"*Configurer exactement qui peut ou ne peut pas utiliser les services MDPGP*" ci-dessous pour les exclure. Désactivez cette option si vous souhaitez uniquement autoriser des utilisateurs locaux spécifiques. Dans ce cas, utilisez l'option "*Configurer exactement qui peut et ne peut pas utiliser les services MDPGP*" ci-dessous pour accorder l'accès à qui vous voulez.

Autoriser tous les utilisateurs non locaux (étrangers) pour les services de déchiffrement/vérification

Par défaut, tout message entrant chiffré destiné à un destinataire local et provenant d'un expéditeur non local peut être déchiffré si MDPGP connaît la clé privée du destinataire local. De même, MDPGP vérifiera les signatures intégrées dans les messages entrants provenant d'utilisateurs non locaux. Si vous ne souhaitez pas déchiffrer ou vérifier les messages de certains expéditeurs non locaux, vous pouvez utiliser l'option"*Configurer exactement qui peut ou ne peut pas utiliser les services MDPGP*" ci-dessous pour restreindre l'accès de ces expéditeurs à ces services. Désactivez cette option si vous ne souhaitez pas déchiffrer les messages ou vérifier les signatures intégrées lorsque l'expéditeur est une adresse non locale. Dans ce cas, vous pouvez toujours utiliser l'option"*Configurer exactement qui peut et ne peut pas utiliser les services MDPGP*" ci-dessous pour spécifier des exceptions à cette restriction.

Configurer exactement qui peut et ne peut pas utiliser les services MDPGP

Cliquez sur ce bouton pour ouvrir le fichierrules.txt permettant de configurer les autorisations des utilisateurs pour MDPGP. Ce fichier vous permet de spécifier qui est autorisé à signer des messages, à les crypter et à les faire décrypter. Vous pouvez également restreindre spécifiquement l'accès des utilisateurs à ces options. Exemple : vous pouvez utiliser la règle "+*@example.com" pour permettre à tous les utilisateurs d'example.com de crypter les messages, mais ajouter ensuite"-frank@example.com pour empêcher spécifiquement frank@example.com de le faire. Ce texte en tête du fichierrules.txt contient des exemples et des instructions.

Notes et syntaxe du fichier rules.txt

- Seuls les messages authentifiés par SMTP provenant des utilisateurs de ce serveur MDaemon peuvent bénéficier du service de cryptage. Vous pouvez cependant spécifier des adresses non locales que vous souhaitez exclure du service de chiffrement, ce qui signifie que MDPGP ne chiffrerapas les messages qui leur sont destinés, même si la clé publique est connue.
- Si un conflit survient entre les paramètres du fichier rules.txt et l'option globale "Autoriser tous les utilisateurs locaux de MDaemon pour tous les services", les paramètres dufichier rules.txt sont pris en compte.
- Si les paramètres du fichier rules.txt sontincompatibles avec l'option globale "Autoriser tous les utilisateurs non locaux (étrangers) pour les services de décryptage/vérification", c'est le fichier rules.txt qui est utilisé.
- Le texte après # sur une ligne est ignoré.
- Séparez plusieurs adresses électroniques sur la même ligne par un espace.
- Les caractères génériques (* et ?) sont autorisés dans les adresses électroniques.
- Même si les messages chiffrés de MDPGP sont **toujours** signés, le fait d'accorder une autorisation de chiffrement à un utilisateur ne lui permet pas de signer des messages non chiffrés. Dans le but de signer un message non crypté, le compte doit recevoir une autorisation de signature.
- Cette adresse électronique doit être précédée de l'une des balises suivantes :
- + (plus) l'adresse peut utiliser le service de cryptage MDPGP.
- (moins) l'adresse **ne peut pas** utiliser le service de cryptage MDPGP.
- ! (exclamation) l'adresse peut utiliser le service de décryptage MDPGP.

- ~ (tilde) l'adresse **ne peut pas** utiliser le service de décryptage MDPGP.
- ^ (caret) l'adresse peut utiliser le service de Connexion MDPGP.
- = (equal) l'adresse **ne peut pas** utiliser le service de connexion MDPGP.
- \$ (dollar) l'adresse peut utiliser le service de vérification MDPGP.
- & (esperluette) l'adresse **ne peut pas** utiliser le service de vérification MDPGP.

Exemples :

- +*@* tous les utilisateurs de tous les domaines peuvent crypter.
- !*@* tous les utilisateurs de tous les domaines peuvent décrypter.
- ^*@* tous les utilisateurs de tous les domaines peuvent signer.
- ^*@example.com tous les utilisateurs d'exemple.com peuvent signer.
- +frank@example.com ~frank@example.com l'utilisateur peut crypter mais pas décrypter.
- +GROUP:EncryptingUsers les membres du groupeEncryptingUsers de MDaemon peuvent crypter.
- ^GROUP:Signers les membres du groupeSigners de MDaemon peuvent signer.

Modes de chiffrement/signature

Mode automatique

Les options Paramètres permettent de configurer MDPGP pour qu'il signe et chiffre automatiquement les messages pour les comptes autorisés à le faire. Lorsqu'un compte envoie un message authentifié et que MDPGP connaît la clé requise, le message est signé ou crypté selon les paramètres ci-dessous.

> Dans la section Mode manuel ci-dessous, les codes Objet spéciaux ont toujours la priorité sur les options du mode automatique. Par conséquent, si l'une de ces options est désactivée, un compte autorisé à signer ou à crypter des messages peut toujours faire en sorte qu'un message soit signé ou crypté manuellement à l'aide de l'un de ces codes.

Paramètres

Chiffrer automatiquement le courrier si la clé publique du destinataire est connue Par défaut, si un compte est autorisé à crypter des messages, MDPGP les crypte automatiquement si la clé publique du destinataire est connue. Si vous ne souhaitez pas que les messages soient automatiquement cryptés, vous pouvez toujours les crypter manuellement à l'aide des codes spéciaux décrits dans la section Mode manuel ci-dessous.

Signer automatiquement le courrier si la clé privée de l'expéditeur est connue

Cliquez sur cette option si vous souhaitez que MDPGP signe automatiquement les messages lorsque la clé privée du compte de l'expéditeur est connue, si le compte est autorisé à signer des messages. Dans le cas où cette option est désactivée, les messages peuvent toujours être signés manuellement à l'aide des codes spéciaux décrits dans la section Mode manuel ci-dessous.

Cryptage/signature de la messagerie entre utilisateurs d'un même domaine

Lorsque MDPGP est configuré pour crypter ou signer automatiquement les messages, cette option fait en sorte que MDPGP le fasse même lorsque les messages sont envoyés entre des utilisateurs du même domaine, à condition que les clés requises soient connues. Cette option est activée par défaut.

Chiffrer/signer le courrier entre les utilisateurs des domaines locaux de MDaemon

Lorsque MDPGP est configuré pour crypter ou signer automatiquement les messages, cette option fait en sorte que MDPGP le fasse même lorsque les messages sont envoyés entre des utilisateurs de domaines MDaemon locaux, à condition que les clés requises soient connues. Exemple : si vos domaines MDaemon incluent " example.com " et " example.net ", les messages envoyés entre les utilisateurs de ces domaines seront automatiquement cryptés ou signés. Cette option est activée par défaut.

Cryptage/signature du courrier envoyé à soi-même

Lorsque MDPGP est configuré pour crypter ou signer automatiquement les messages, cela se fait même lorsque l'utilisateur de MDaemon s'envoie un message à lui-même (par exemple, frank@example.com qui s'envoie à frank@example.com). Dans ce cas, si le compte est autorisé à utiliser à la fois le cryptage et le décryptage (paramètres par défaut), MDPGP acceptera le message de l'utilisateur, le cryptera, puis le décryptera immédiatement et le placera dans la boîte aux lettres de ce même utilisateur. Si, en revanche, le compte n'est pas configuré pour le déchiffrement, le message sera chiffré, puis placé dans la boîte aux lettres de l'utilisateur, toujours chiffré. Cette option est activée par défaut.

Mode manuel

Dans le cas où vous avez désactivé les options*Signer le courrier automatiquement...* et *Chiffrer le courrier automatiquement...* décrites ci-dessus, vous utilisez MDPGP en mode manuel. MDPGP ne signe ou ne chiffre aucun message, sauf ceux qui sont authentifiés et qui comportent l'un des codes suivants dans l'en-tête Subject du message :

- --pgps Signer ce message si possible. Le code peut être placé au début ou à la fin de l'objet.
- --pgpe Crypter ce message si possible. Le code peut être placé au début ou à la fin du sujet.
- --pgpx Le message **DOIT** être crypté. Si ce n'est pas possible (par exemple, parce que la clé du destinataire n'est pas connue), il ne faut pas le transmettre ; le message sera renvoyé à

l'expéditeur. Le code peut être placé au début ou à la fin du sujet.

- --pgpk Envoyez-moi ma clé publique. L'utilisateur place ce code au début de l'Objet du message et s'envoie le message à lui-même. MDPGP lui enverra alors sa clé publique par courrier électronique.
- -- Envoyez-moi la clé publique de cette adresse. L'utilisateur place ce code au début de l'Objet du message et s'envoie le message à lui-même. MDPGP enverra alors la clé publique de l'adresse électronique à l'utilisateur.

Exemple :

Objet : --pgpk<frank@example.com>

Gestion des clés

Les clés publiques et privées sont gérées à l'aide des options situées dans la partie inférieure de la boîte de dialogue de MDPGP. Il existe une entrée pour chaque clé, et vous pouvez cliquer avec le bouton droit de la souris sur n'importe quelle entrée pour exporter la clé, la supprimer, l'activer ou la désactiver, la définir comme clé préférée (voir "*Échanger des clés publiques pendant les sessions de courrier SMTP*" ci-dessus) ou la définir comme clé de domaine (voir ci-dessous). Lorsque vous cliquez sur **Exporter la clé**, elle est enregistrée dans le dossier\MDaemon\Pem_mdpgp\exports\ et vous pouvez éventuellement envoyer la clé publique par courriel à une adresse électronique. Les options "Afficher local/à distance" et "Filtrer" sont fournies pour vous aider à localiser certaines adresses ou certains groupes.

Utilisation d'une clé de domaine

En option, vous pouvez utiliser une clé unique pour crypter tous les messages destinés à un domaine spécifique, quel qu'en soit l'expéditeur. Ceci est utile si, par exemple, l'un de vos domaines et un domaine hébergé ailleurs souhaitent crypter tous les courriels envoyés entre eux, mais ne souhaitent pas configurer et gérer des clés de cryptage individuelles pour chaque compte d'utilisateur au sein du domaine. Il y a plusieurs façons d'y parvenir :

- Si vous disposez déjà d'une clé publique pour un autre domaine et que vous souhaitez utiliser cette clé pour crypter tous les messages sortants qui lui sont destinés, cliquez avec le bouton droit de la souris sur la clé et cliquez sur Définir comme clé du domaine. Par nom. then, entrez le Nom de domaine et cliquez sur OK. Cela créera une règle Filtre du contenu pour que tous les messages "À :" ce domaine soient cryptés à l'aide de la clé désignée.
- Si la clé publique du domaine vous a été fournie mais ne figure pas encore dans la liste, cliquez sur Importer la clé du domaine, entrez le nom du domaine et cliquez sur OK, puis naviguez jusqu'au fichier public.asc du domaine et cliquez sur Ouvrir. Cela créera également la règle Filtre du contenu pour le cryptage des messages vers le domaine.
- Personnalisez vos Règles du Filtre de contenu si nécessaire pour modifier exactement les messages qui sont cryptés avant d'être envoyés aux domaines.
- Pour créer une nouvelle clé pour l'un de vos domaines, à remettre à un autre domaine pour crypter les messages qui vous sont envoyés, suivez les instructions de l'option"*Créer des clés pour un utilisateur spécifique*" cidessous, en sélectionnant "_Domain Key (domain.tld)_ <anybody@domain.tld>" dans la liste.

N'utilisez pas de clé pour crypter des messages sortants pour lesquels vous possédez également la clé privée correspondante. Si vous le faites, MDPGP cryptera un message, puis constatera immédiatement que la clé de décryptage est connue et décryptera aussitôt ce même message.

E-mail de l'expéditeur en cas d'échec du chiffrement (commande --pgpe)

Lorsque quelqu'un utilise la commande --pgpe pour envoyer du courrier chiffré et que le chiffrement échoue (par exemple, parce qu'aucune clé de chiffrement n'a été trouvée), cette option entraîne l'envoi d'un E-mail de notification à l'expéditeur pour l'informer de l'échec. Cette option est désactivée par défaut, ce qui signifie qu'aucun message de notification d'échec ne sera envoyé.

Email public-keys lorsqu'un courriel est envoyé à soi-même (commande --pgpk)

Lorsqu'un utilisateur s'envoie un e-mail à lui-même avec "--pgpk<adresse électronique>" comme objet (par exemple, --pgpk<frank@example.com>). Si une clé publique existe pour <adresse électronique>, elle sera renvoyée par courrier électronique au demandeur.

Importer automatiquement les clés publiques envoyées par les utilisateurs authentifiés

Par défaut, lorsqu'un utilisateur authentifié envoie un e-mail contenant une clé publique au format ASCII joint, MDPGP importe cette clé publique dans le trousseau. Il s'agit d'un moyen simple pour un utilisateur d'obtenir la clé publique d'un contact dans MDPGP, en s'envoyant la clé publique par courriel en pièce jointe. Désactivez cette option si vous ne souhaitez pas importer automatiquement les clés publiques.

Créer des clés automatiquement

Activez cette option si vous souhaitez que MDPGP crée automatiquement une paire de clés publique/privée pour chaque utilisateur de MDaemon. Plutôt que de les créer toutes en même temps, MDPGP les créera au fur et à mesure, en créant la paire de clés de chaque utilisateur la prochaine fois qu'un message est traité pour cet utilisateur. Cette option est désactivée par défaut afin de préserver les ressources et d'éviter de générer inutilement des clés pour des comptes qui n'utiliseront peutêtre jamais MDPGP.

Par taille

Cette option permet d'indiquer la taille des clés générées par MDPGP. Vous pouvez définir la taille de la clé sur 1024, 2048 ou 4096. Le paramètre par défaut est une clé de 2048 bits.

Expire dans [xx] jours (0 = jamais)

Utilisez cette option pour spécifier le nombre de jours à compter de la date de début de validité d'une clé générée par MDPGP avant qu'elle n'expire. Définissez l'option sur "0" si vous ne souhaitez pas que les clés expirent. Le paramètre par défaut est 0.

Créer des clés pour un utilisateur spécifique

Pour générer manuellement une paire de clés pour un compte :

- 1. Cliquez sur **Créer des clés pour un utilisateur spécifique**.
- 2. Sélectionnez le compte dans la liste déroulante. Si vous souhaitez créer une clé unique applicable à tous les comptes d'un domaine, choisissez l'option "_Domain Key (domain.tld)_ <anybody@domain.tld>" dans la liste.
- Facultatif : Cochez la case Envoyer la clé publique au propriétaire de la clé... si vous souhaitez envoyer la clé à l'utilisateur sous forme de pièce jointe à un courriel.

4.	Cliquez	sur	Ok.
4.	Cliquez	sur	Оκ.

OpenPGP for MDaemon	×
Please enter the email address that you wish to create and bind keys to. Note: this only works if the email address is a local account that MDaemon knows about.	
☑ (Optional) Email public-key to key owner after creation?	
This is the text that will appear in the email message body:	
Attached is a public-key exported from OpenPGP for MDaemon v22.0.0rc1	^
This key was automatically created for use by you. Others must import this key into their encryption software in order to send you encrypted mail.	
It's a good idea to keep a copy of this email somewhere safe in case your key is ever lost and a backup is needed.	
	-
OK Cancel	

Chiffrer le courrier sortant en fonction de l'IP de réception

Si vous souhaitez utiliser une clé de cryptage spécifique pour crypter tous les messages destinés à une certaine adresse IP, activez cette option et cliquez sur **Configuration** pour ouvrir le fichier MDaemon Message Transport Encryption, dans lequel vous pouvez répertorier l'adresse IP et l'ID de la clé associée. Toute session SMTP sortante délivrant un message à l'une des IP répertoriées cryptera le message à l'aide de la clé associée juste avant la transmission. Si le message est déjà crypté à l'aide d'une autre clé, cette étape est ignorée.

Importer des clés

Si vous souhaitez importer manuellement un fichier de clés dans MDPGP, cliquez sur ce bouton, localisez le fichier de clés et cliquez sur **Ouvrir**. Dans l'importation d'un fichier de clé privée, il n'est pas nécessaire d'importer la clé publique correspondante, car elle est incluse dans la clé privée. Si vous importez une clé privée protégée par une phrase de passe, MDPGP vous demandera d'entrer cette phrase. Sans cette phrase, vous ne pouvez pas importer la clé privée. Après avoir importé une clé privée, MDaemon modifie la phrase de passe de cette clé en fonction de la phrase de passe utilisée par MDPGP.

Importer la clé du domaine

Si une clé de chiffrement publique vous a été fournie pour chiffrer tous les messages envoyés à un certain domaine, cliquez sur ce bouton, entrez le nom du domaine, cliquez sur **OK**, puis naviguez dans le fichier <code>public.asc</code> du domaine et cliquez sur **Ouvrir**. Cela ajoutera la clé publique du domaine à la liste et créera une règle Filtre du contenu pour crypter tous les messages sortants pour ce domaine, quel que soit l'expéditeur.

Modifier la phrase de passe

Les clés privées sont protégées à tout moment par une phrase de passe. Lorsque vous tentez d'importer une clé privée, vous devez saisir sa phrase de passe. Lors de l'exportation d'une clé privée, cette clé exportée sera toujours protégée par la phrase de passe, et elle ne pourra pas être utilisée ou importée ailleurs sans elle. La phrase de passe par défaut de MDPGP est **MDaemon**. Pour des raisons de sécurité, vous devez modifier cette phrase de passe après avoir commencé à utiliser MDPGP, car jusqu'à ce que vous le fassiez, chaque clé créée ou importée avec succès dans MDPGP aura sa phrase de passe définie (ou modifiée) en **MDaemon**. Vous pouvez modifier la phrase de passe à tout moment en cliquant sur **Modifier la phrase de passe** dans l'écran MDPGP. Lorsque vous modifiez la phrase de passe, toutes les clés privées du trousseau sont mises à jour avec la nouvelle phrase de passe.

Fichiers à sauvegarder

Cliquez sur ce bouton pour sauvegarder les fichiers des trousseauxKeyring.private et Keyring.public. Par défaut, les fichiers de sauvegarde seront copiés dans :"\MDaemon\Pem_mdpgp\backups" et auront une date et une extension.bak ajoutées aux noms de fichiers.

- Les messages Transférer ne sont pas cryptés.
- Les messages de répondeur automatique ne sont pas cryptés.
- Les serveurs de clés et la révocation des clés ne sont pas pris en charge, sauf dans les cas décrits dans les options"*Collecter les clés publiques à partir du DNS (pka1) et les mettre en cache pendant [xx] heures*" et "*Envoyer les clés publiques par HTTP (Webmail)*" ci-dessus.

- L'action de chiffrement du Filtre de contenu n'agit pas sur les messages déjà chiffrés, et les actions de chiffrement et de déchiffrement sont soumises à toutes les exigences de configuration de MDPGP.
- Les listes déroulantes qui affichent les comptes MDaemon affichent les 500 premiers comptes par défaut. Vous pouvez définir MaxUsersShown=0 dans plugins.dat pour afficher tous les comptes. Le chargement peut être plus long pour les listes d'utilisateurs très volumineuses.
- MDPGPUtil.exe est un outil qui peut crypter et décrypter via des options de ligne de commande. Exécutez MDPGPUtil sans arguments à partir d'une ligne de commande pour obtenir de l'aide.

4.5 Protection instantanée

La Protection instantanée fait partie de la fonctionnalitéoptionnelle <u>MDaemon AntiVirus</u> [718]. Activer MDaemon Antivirus pour la première fois démarre un essai de 30 jours. Si vous souhaitez acheter cette fonctionnalité, contactez votre revendeur MDaemon agréé ou visitez : <u>mdaemon.com</u>.

La Protection instantanée (OP) est accessible à partir du menuSécuritéde MDaemon (Sécurité | Protection instantanée..., ou Ctrl+Shift+1). Il s'agit d'une technologie révolutionnaire d'anti-spam, d'anti-virus et d'anti-phishing en temps réel, capable de protéger de manière proactive une infrastructure de messagerie MDaemon, automatiquement et dans les minutes qui suivent l'apparition d'une épidémie.

La Protection instantanée est totalement agnostique en termes de contenu, ce qui signifie qu'elle ne repose pas sur une analyse lexicale stricte du contenu des messages. Il ne nécessite donc pas de règles heuristiques, de filtrage du contenu ou de mise à jour des signatures. Dans ce cas, il ne se laisse pas tromper par l'ajout d'un texte de départ, par des changements orthographiques astucieux, par des tactiques d'ingénierie sociale, par des barrières linguistiques ou par des différences dans les techniques d'encodage. Au contraire, l'OP est basé sur la détection de motifs récurrents et les technologies "zéro heure". Dans ce cas, il analyse les "schémas" associés à la transmission d'un message électronique et les compare à des schémas similaires collectés à partir de millions de messages électroniques dans le monde entier, qui sont échantillonnés et comparés en temps réel. **Remarque :** OP ne transmet jamais le contenu réel des messages, et le contenu des messages ne peut pas être déduit des modèles extraits.

Les messages étant analysés en temps réel dans le monde entier, la protection est assurée dans les minutes, voire les secondes, qui suivent l'apparition d'un nouveau foyer. Pour les virus, ce niveau de protection est essentiel car il faut souvent des heures après une épidémie avant qu'un fournisseur d'antivirus traditionnel puisse vérifier et soumettre une mise à jour de la signature du virus, et il peut ensuite s'écouler encore plus de temps avant que cette mise à jour ne soit utilisée en production. Pendant cet intervalle, les serveurs dépourvus de Protection Instantanée sont vulnérables à l'épidémie en question. De même, pour les messages de spam, il faut souvent du temps et des efforts pour analyser le spam et créer une règle de filtrage sûre avant qu'il ne soit reconnu par les systèmes heuristiques traditionnels et les systèmes basés sur le contenu.

Il est toutefois important de noter que la fonction de Protection instantanée ne remplace pas les techniques traditionnelles d'antivirus, d'antispam et d'antiphishing. Dans les faits, OP fournit une autre couche de protection spécialisée en plus des outils heuristiques, des signatures et des outils basés sur le contenu que l'on trouve dans MDaemon. Plus précisément, OP est conçu pour traiter les épidémies à grande échelle plutôt que les messages anciens, uniques ou spécifiquement ciblés qui peuvent être plus facilement détectés par les outils traditionnels.

Outbreak Protection	×
Outbreak Protection is a real-time detection system that can detect and block viruses, spam, and certain offensive and illegal content within the first few minutes of an outbreak.	
Enable Outbreak Protection	
Viruses should be Image: blocked in real time Quarantined Quarantined messages are placed in the MD aemon quarantine folder. Spam should be Image: blocked in real time Image: compare the distribution of the distredistres and distribution of the distributicon of the	
 When blocking spam, block messages which classify as "bulk" spam also ✓ Close mail sessions after blocking any virus, spam, or IWF message ✓ Log processing activity to MDaemon's plugin log file ✓ Use HTTPS connections 	
Exceptions	
Authenticated SMTP sessions are exempt from OP processing	
SMTP sessions from trusted IPs are exempt from OP processing	
SPF/DKIM approved mail is exempt from OP processing	
Spam Honeypot and Spam Filter allow listed addresses are exempt from OP processing OP allow listing uses envelope values - not message header values.	
False positives & false negatives	
We are continually refining the detection and classification process.	
Spam false positives may be emailed to spamfp@mdaemon.com spam false negatives to spamfn@mdaemon.com. Virus false positives may be emailed to virusfp@mdaemon.com virus false negatives to virusfn@mdaemon.com.	
Please send the original emails as MIME attachments. Do not forward the emails or important header information will be lost.	
OK Cancel	

Protection instantanée

Activer la protection instantanée

Cochez cette case pour activer la Protection instantanée sur votre serveur. Les messages entrants seront analysés pour déterminer s'ils font partie d'une épidémie de virus, de spam ou de phishing. Les options restantes de cette boîte de dialogue permettent de déterminer ce qui sera fait des messages faisant partie d'une épidémie et de désigner les expéditeurs qui seront exemptés du traitement OP.

Lorsqu'un virus est détecté...

bloquer en temps réel

Sélectionnez cette option si vous souhaitez bloquer les messages pendant le processus SMTP lorsqu'il est établi qu'ils font partie d'une épidémie de virus. Ces messages ne seront pas mis en quarantaine ni remis à leurs destinataires, ils seront rejetés par le serveur.

en quarantaine

Sélectionnez cette option si vous souhaitez accepter les messages qui, selon OP, font partie d'une épidémie de virus. Bien que ces messages ne soient pas rejetés par le serveur, ils seront mis en quarantaine au lieu d'être livrés à leurs destinataires. Les messages mis en quarantaine sont placés dans le dossier de quarantaine.

Lorsqu'il est détecté, le spam est...

bloquer en temps réel

Sélectionnez cette option si vous souhaitez bloquer les messages au cours du processus SMTP lorsqu'OP confirme qu'ils font partie d'une épidémie de spam. Ces messages ne seront pas marqués comme étant du spam et ne seront pas remis à leurs destinataires, ils seront rejetés par le serveur. Les messages classés par OP comme "en masse" ne seront pas bloqués par cette option, sauf si vous activez l' option*Lorsque les spams sont bloqués, bloquer également les messages classés comme "en masse".* Les messages classés comme "en vrac" par le PO pourraient simplement faire partie de certaines très grandes listes de diffusion ou d'autres contenus similaires largement diffusés, de sorte que vous pouvez ou non considérer ces types de messages comme du spam. C'est pourquoi ces types de messages ne doivent généralement pas être évalués négativement ou bloqués par le PO.

accepté pour le filtrage

Sélectionnez cette option si vous souhaitez accepter les messages dont l'OP confirme qu'ils font partie d'une épidémie de spam, afin qu'ils puissent ensuite être soumis au filtrage anti-spam et au traitement du filtre de contenu. Ces messages ne seront pas bloqués par OP, mais leur score au Filtre anti-spam sera ajusté en fonction de l' option*Score* ci-dessous.



Si vous utilisez l'option Accepté pour le filtrage, OP ne bloquera pas directement un message de spam confirmé, mais un message peut toujours être bloqué par MDaemon pendant le processus SMTP si vous avez configuré le Filtre anti-spam pour utiliser l'option *SMTP rejette les messages dont le score est supérieur ou égal à [xx]*, située dans l'écran<u>Filtre anti-spam</u>

Exemple : si l'option de notation ci-dessous fait que le score du Filtre anti-spam est de 15.0, le message sera quand même rejeté comme spam si vous avez également configurél'option"*SMTP rejette...*"du Filtre anti-spampour rejeter les messages dont le score est supérieur ou égal à 15.0.

Score

Lorsque vous utilisez l'option*acceptée pour filtrage* ci-dessus, ce montant sera ajouté au score du Filtre anti-spam lorsque OP confirmera que le message fait partie d'une épidémie de spam.

Contenu IWF

L'option suivante s'applique au contenu identifié par l'Internet Watch Foundation (IWF) comme renvoyant à des sites d'images d'abus d'enfants (c'est-à-dire des sites de pornographie enfantine). Elle permet au PO d'utiliser une liste intégrée d'URL fournie par l'IWF pour détecter et marquer les messages qui renvoient à ce contenu. Dans le cadre de l'IWF, un service d'assistance téléphonique indépendant permet de signaler les contenus en ligne potentiellement illégaux, y compris les contenus pédopornographiques hébergés n'importe où dans le monde. Elle travaille en partenariat avec la police, les gouvernements, l'industrie en ligne au sens large et le public pour lutter contre la disponibilité de contenus illégaux en ligne. La liste d'URL de la Fondation est mise à jour quotidiennement avec de nouveaux sites hébergeant des images d'abus d'enfants.

De nombreuses organisations disposent de règles de conformité internes régissant le contenu des courriels envoyés ou reçus par leurs employés, notamment en ce qui concerne les contenus obscènes ou illégaux. Dans de nombreux pays, l'envoi ou la réception de tels contenus sont interdits. Cette fonction peut vous aider dans vos efforts de mise en conformité.

Pour en savoir plus sur l'IWF, voir :

http://www.iwf.org.uk/

Lorsqu'un contenu de l'IWF est détecté...

bloquer en temps réel

Choisissez cette option si vous souhaitez rejeter les messages entrants pendant le processus SMTP lorsqu'ils ont un contenu limité par l'IWF.

acceptés pour le filtrage

Choisissez cette option si vous souhaitez augmenter le score du Filtre anti-spam d'un message au lieu de le rejeter lorsqu'il a un contenu restreint par l'IWF. Le score du Filtre anti-spam sera augmenté du montant spécifié dans l'option*Score* ci-dessous.

Score

Lorsque l'option*acceptée pour le filtrage* ci-dessus est sélectionnée, il s'agit du montant qui sera ajouté au score du Filtre anti-spam d'un message lorsqu'il contient des restrictions IWF.

Lorsque les spams sont bloqués, refusez également les provenant d'envois d'en masse.

Il arrive qu'OP identifie certains messages qui pourraient être considérés comme du spam mais qui ne sont pas envoyés par un spammeur connu ou un réseau de zombies, comme c'est parfois le cas pour les envois en nombre et les lettres d'information légitimes. OP classe ces types de messages dans la catégorie "Spam (en vrac)" plutôt que dans la catégorie "Spam (confirmé)". Cochez cette case si vous souhaitez appliquer les fonctions de blocage du spam d'OP aux courriers"Spam (en vrac)" également. Si cette option est désactivée, seuls les messages classés comme "Spam (confirmé)" seront affectés par les fonctions de blocage du spam d'OP ci-dessus. Accepter ce type de messages en vue d'un traitement ultérieur peut s'avérer nécessaire pour les sites qui souhaitent recevoir des envois en masse mais qui, pour une raison ou une autre, ne peuvent pas exempter la source ou le destinataire.

Enregistrer l'activité dans ficher journal des modules de MDaemon

Cochez cette case si vous souhaitez enregistrer toutes les activités de traitement des OP dans le fichier journal du plugin de MDaemon.

Exceptions

Ne pas appliquer la Protection Instantanée aux sessions SMTP authentifiées

Lorsque cette option est activée, les sessions SMTP authentifiées sont exemptées du traitement OP. Cela signifie que les messages envoyés au cours de cette session ne seront pas soumis aux contrôles de la Protection instantanée.

Ne pas appliquer la Protection instantanée aux sessions SMTP provenant d'IP autorisées Activez cette option si vous souhaitez exempter les adresses IP autorisées de la Protection Activer instantanée : les messages arrivant d'un serveur situé à une adresse IP autorisée ne seront pas soumis aux contrôles de protection contre les épidémies.

Le courrier approuvé par SPF/DKIM n'est pas traité par la protection instantanée

Cochez cette case si vous souhaitez exempter un message du traitement OP lorsque le domaine d'envoi figure sur la Domaines <u>approuvés</u> et qu'il est validé par SPF ou DKIM.

Les adresses autorisées par le Filtrage anti-spam et les adresses autorisées par le Filtre anti-spam sont exemptées du traitement OP

Cliquez sur cette option si vous souhaitez exempter les listes d'autorisation du Filtre<u>anti-spam</u> [758] et des<u>Honeypots</u> [758] de la Protection instantanée. La Liste d'autorisation s'applique au destinataire ou à la valeur RCPT indiquée lors de la session SMTP. La Liste d'autorisation (expéditeurs) s'applique à l'expéditeur, ou à la valeur MAIL indiquée au cours de la session SMTP. Ces opérations ne sont pas basées sur les valeurs de l'en-tête du message.

Faux positifs et faux négatifs

Les faux positifs, c'est-à-dire le fait de classer à tort un message légitime comme faisant partie d'un foyer, ne devraient que rarement, voire jamais, se produire. Lorsqu'un Faux positif est détecté, vous pouvez nous envoyer ce message à l'adresse **spamfp@mdaemon.com** pour les faux positifs de spam/phishing ou à l'**adresse virusfp@mdaemon.com** pour les faux positifs de virus, afin que nous puissions l'utiliser pour affiner et améliorer nos processus de détection et de classification.

Les Faux positifs et les faux négatifs, c'est-à-dire le fait de classer un message comme ne faisant pas partie d'une épidémie alors qu'il s'agit toujours de spam ou d'une attaque, se produiront plus souvent que les faux positifs. Toutefois, il convient de noter que l'OP n'est pas conçu pour attraper tous les spams, attaques virales et autres ; il s'agit simplement d'une couche de protection qui cible spécifiquement les épidémies. Les anciens messages, les messages spécifiquement ciblés et autres, qui ne font pas partie d'une épidémie en cours, peuvent passer le contrôle OP. Ces types de messages devraient alors être détectés par les autres fonctions d'AntiVirus et de MDaemon en aval de la chaîne de traitement. Lorsqu'un Faux négatifs est détecté, vous pouvez nous envoyer ce message à **spamfn@mdaemon.com** pour les faux négatifs de spam/phishing ou à **virusfn@mdaemon.com** pour les faux négatifs de virus, afin que nous puissions l'utiliser pour affiner et améliorer nos processus de détection et de classification.

Lorsque vous nous envoyez des messages mal classés, l'e-mail original doit être envoyé en tant que pièce jointe MIME plutôt que d'être Transféré. Dans le cas contraire, les en-têtes et autres informations essentielles au processus de classification seront perdus.

4.6 Filtre de contenu et antivirus

Filtre de contenu

Le Filtre de contenu (Sécurité | Filtre de contenu) peut être utilisé pour un grand nombre de raisons telles que : la prévention du spam, l'interception des messages contenant des virus avant qu'ils n'atteignent leur destination finale, la copie de certains messages à un ou plusieurs utilisateurs supplémentaires, l'ajout d'une note ou d'une clause de non-responsabilité au bas des messages, l'ajout et la suppression d'en-têtes, le retrait des pièces jointes aux messages, la suppression des messages, et bien plus encore. Dans la mesure où les règles du Filtre contenu sont créées par l'administrateur, et en raison de leur diversité, elles peuvent être utilisées dans de nombreuses situations et ne sont limitées, pour la plupart, que par la créativité de la personne qui les crée. Avec un peu de réflexion et d'expérimentation, cette fonction peut s'avérer très utile.

MDaemon AntiVirus (MDAV)

Lorsque vous utilisez le contenu AntiVirus de MDaemon, vous avez accès à deux écrans supplémentaires dans la boîte de dialogue Filtre de contenu : <u>Analyse des virus</u> [718] et <u>Mises à jour antivirus</u> [723]. Ces écrans permettent de contrôler directement les

fonctionnalités de l'AntiVirus et de déterminer les actions à entreprendre par MDaemon lorsqu'un virus est détecté. MDAV est équipé de deux moteurs antivirus : IKARUS Anti-Virus et ClamAV. Vous pouvez analyser les messages avec l'un ou l'autre de ces moteurs, ou avec les deux, pour une sécurité accrue. MDAV comprend également la <u>Protection instantanée</u>, qui n'est pas basée sur l'heuristique ou sur les signatures comme les outils de protection traditionnels, mais qui est conçue pour détecter les spams, le phishing et les attaques de virus qui font partie d'une épidémie en cours, et qui peuvent parfois être manqués par les outils traditionnels.



Activer MDaemon AntiVirus 718 pour la première fois démarre un essai de 30 jours. Si vous souhaitez acheter cette fonctionnalité, contactez votre revendeur MDaemon agréé ou visitez : mdaemon.com.

Voir :

Editeur de filtre de contenu <u>Création d'une nouvelle règle du Filtre de contenu</u> <u>Modifier une règle du Filtre de contenu existante</u> <u>Utilisation d'expressions régulières dans vos règles de filtrage</u> <u>Tos</u>

Analyse des virus Mises à jour AntiVirus Protection instantanée

4.6.1 Éditeur du Filtre de contenu

4.6.1.1 Règles



Tous les messages traités par MDaemon résideront temporairement dans l'une des files d'attente. Lorsque le Filtre de contenu est activé, avant qu'un message ne soit autorisé à quitter la file d'attente, il est d'abord traité par les règles du Filtre de contenu. Le résultat de cette procédure déterminera le sort du message.

Les messages dont le nom de fichier commence par la lettre "P" sont ignorés par le processus de filtrage du contenu. Tous les autres messages seront traités par le système de Filtre de contenu. Une fois traité, MDaemon remplace le premier caractère du nom de fichier par un "P". Dans ce cas, un message ne sera traité qu'une seule fois par le système de filtrage du contenu.

Règles du Filtre de contenu

Activer le moteur de traitement des règles

Cochez cette case pour activer le filtrage de contenu. Tous les messages traités par MDaemon seront filtrés par les règles de filtrage du contenu avant d'être délivrés.

Règles du Filtre de contenu existantes

Cette boîte répertorie toutes vos Règles du Filtre de contenu, avec une case à cocher à côté de chacune d'entre elles pour que vous puissiez les activer/désactiver à votre guise. Dans la description d'une règle donnée dans son format de script interne, cliquez sur cette règle et placez le curseur de votre souris dessus (si vous déplacez votre souris, la description disparaîtra). Dans le cadre du traitement d'un message par le Filtre to contenu, ces règles seront appliquées dans l'ordre de leur énumération. Cela vous permet d'organiser vos règles de manière à obtenir une plus grande polyvalence.

Exemple : Si vous disposez d'une règle qui supprime tous les messages contenant les mots "Ceci est un spam !" et d'une règle similaire qui envoie ces messages au Postmaster, le fait de les placer dans le bon ordre permettra d'appliquer les deux règles au message. Cela suppose qu'iln' existepas de règle "Arrêter processing rules" qui s'applique au message plus haut dans la liste. Si c'est le cas, vous devez utiliser les boutons*Monter/Descendre* pour déplacer la règle "Arrêter" en dessous des deux autres. Alors, tout message contenant "This is Spam !" sera copié dans le Postmaster et supprimé.

MDaemon a la capacité de créer des règles qui effectueront des tâches multiples et utiliseront et/ou la logique. Dans l'Exemple ci-dessus, au lieu d'utiliser plusieurs règles, vous pourriez en créer une seule qui accomplirait toutes ces tâches et plus encore.

Nouvelle règle

Cliquez sur ce bouton pour créer une nouvelle règle du Filtre de contenu. La boîte de dialogue<u>Créer une règle san</u> l'ouvre alors.

Modifier la règle

Cliquez sur ce bouton pour ouvrir la règle sélectionnée dans l'éditeur<u>Modifier la</u> <u>règle.</u>

Copier la règle

Cliquez sur ce bouton pour cloner la Règles du Filtre de contenu sélectionnée. Une règle identique sera créée et ajoutée à la liste. La nouvelle règle portera le nom par défaut de "Copie de [Nom de la règle d'origine]". Cette fonction est utile si vous souhaitez créer plusieurs règles similaires. Vous pouvez créer une seule règle, la cloner plusieurs fois, puis modifier les copies selon vos besoins.

Supprimer la règle

Cliquez sur ce bouton pour supprimer la Règles du Filtre de contenu sélectionnée. Il vous sera demandé de confirmer votre décision de supprimer la règle avant que MDaemon ne le fasse.

Monter

Cliquez sur ce bouton pour Monter la règle sélectionnée.

Descendre

Cliquez sur ce bouton pour faire descendre la règle sélectionnée.

Voir :

<u>Créer une nouvelle règle du Filtre de contenu</u> <u>Modifier une Règles du Filtre de contenu existante</u> <u>Utilisation d'expressions régulières dans vos règles de filtrage</u> <u>Tublication d'expressions régulières dans vos règles de filtrage</u>

4.6.1.1.1 Création d'une règle de filtrage de contenu

Modify Rule Message/Partial vulnerability [Move to bad message queue]	×
Create rule Name this rule Message/Partial vulnerability [Move to bad message queue]]
Conditions Actions	
☐ If the FROM HEADER contains ☐ If the TO HEADER contains ☐ If the SUBJECT HEADER contains ☐ If the SUBJECT HEADER contains ☐ If the CHEADER contains ☐ If the SUBJECT HEADER contains ☐ If the SUBJECT HEADER contains ☐ If the SUBJECT HEADER contains ☐ If the USH defined 1 HEADER contains ☐ If the user defined 1 HEADER contains ☐ If the user defined 2 HEADER contains ☐ If the user defined 3 HEADER contains ☐ If the user defined 5 HEADER contains ☐ If the SAGE BODY contains words from file ☐ If MESSAGE BODY contains words from file ☐ If the MESSAGE BODY contains words from file ☐ If the MESSAGE BODY doesn't contain words from file ☐ If the MESSAGE BAS A FILE called ☐ If the MESSAGE SIZE is greater than ☐ If the MESSAGE SIZE is greater than ☐ If the MESSAGE SIZE is greater than	isage e queue #(s) ge ge ge ge ge ge ge
If the message has an attachment with a CONTENT-TYPE of <u>'message/partial'</u>	
then send note 1 <u>"to <postmaster@\$primarydomain\$>","from <md aemon@\$primarydom<="" u=""> and move message to bad message directory</md></postmaster@\$primarydomain\$></u>	<u></u>
	K Cancel

Cette boîte de dialogue est utilisée pour créer des Règles du Filtre de contenu. On y accède en cliquant sur le bouton*Nouvelle règle* dans la boîte de dialogue Filtre de contenu.

Créer une règle

Nom de la règle

Nommez ici un nom descriptif pour votre nouvelle règle. Non (par défaut), elle sera appelée "Nouvelle règle #n".

Conditions...

Cette boîte répertorie les conditions qui peuvent être appliquées à votre Nouvelle règle. Cochez la case correspondant à la condition que vous souhaitez appliquer à la Nouvelle règle. Dans la case Description de la règle ci-dessous, chaque condition activée apparaîtra. La plupart des conditions requièrent des informations supplémentaires que vous pouvez spécifier en cliquant sur lelien hypertexte de laconditiondans la boîte de description de la règle.

Si l'[En-tête] contient-Cliquez sur l'une de ces options pour baser votre règle sur le contenu de ces en-têtes de message particuliers. Vous devez spécifier le texte à rechercher. Cette condition prend désormais en charge les expressions régulières. Voir <u>Utilisation d'expressions régulières dans vos règles de</u> <u>filtrage</u> 708¹.

If the user defined [# HEADER] contains-Cliquez surune ou plusieurs de ces options pour baser la règle sur les en-têtes de message que vous définirez. Vous devez spécifier le Nouvel En-tête From et le texte à rechercher. Ce texte prend désormais en charge les expressions régulières. Cette condition prend désormais en charge les expressions régulières. Voir <u>Utilisation d'expressions régulières dans vos</u> règles de filtrage ⁷⁰³.

Si le CORPS DU MESSAGE BODY contient : cetteoption fait du contenu du corps du message l'une des conditions. Cette condition vous oblige à spécifier une chaîne de texte à rechercher. Cette condition prend désormais en charge les expressions régulières. Voir <u>Utilisation d'expressions régulières dans vos règles de</u> filtrage 703.

Si le MESSAGE comporte une ou des piècesjointes : lorsque cette option est sélectionnée, la règle est subordonnée à la présence d'une ou de plusieurs pièces jointes au message. Aucune information supplémentaire n'est requise.

Si la TAILLE DU MESSAGE est supérieure à : cliquez surcette option si vous souhaitez que la règle soit basée sur la taille du message. La taille doit être spécifiée en *Ko*. Non (par défaut).

Si le MESSAGE A UN FILE appelé-Cetteoption recherche un fichier joint portant un nom particulier. Le nom du fichier doit être spécifié. Les caractères génériques tels que *.exe et file *.* sont autorisés. **Si le message est INFECTED**...- Cette condition est VRAIE lorsque MDaemon détermine qu'un message est infecté par un virus.

Si le code de sortie d'un processus exécuté précédemment est égal
 à - Siune règle précédente de votre liste utilise l'action *Exécuter le processus*, vous pouvez utiliser cette condition pour rechercher un code de sortie spécifique de ce processus.

Si le MESSAGE EST DIGITALLY SIGNED – Cettecondition s'applique aux messages qui ont été signés numériquement. Aucune autre information n'est requise par cette condition.

Si SENDER est member of GROUP...- Cette condition s'applique à un message lorsqu'il est envoyé par un compte qui est membre du groupe de comptes désigné dans la règle.

Si RECIPIENT est membre de GROUP...- Cette condition s'applique à un message lorsque son destinataire est membre du groupe de comptes désigné dans la règle.

Si le message contient un QR CODE...- Cette condition s'applique à un message qui contient un QR Code.

Appliquercette règle à tous les messages- **Cliquez sur**cette option si vous souhaitez que cette règle soit appliquée à tous les messages. Aucune autre information n'est requise ; cette règle s'appliquera à tous les messages, à l'exception de ceux auxquels une action "Arrêter processing rules" ou "Delete message" a été appliquée dans une règle précédente.

Actions...

MDaemon peut effectuer ces actions si un message répond auxconditions de larègle.Dans certains cas, l'action nécessite des informations supplémentaires que vous pouvez spécifier en cliquant sur lelien hypertexte de l'actiondans la boîte de description de la règle.

Supprimer MESSAGE ! ! SUPPRIMERLE MESSAGE!

Strip all attachments from message (Supprimer toutes les pièces jointes du message) : cetteaction permet de supprimer toutes les pièces jointes du message.

Move Message To Bad Message Queue (Déplacer le message dans la file d'attente des messages erronés) : cliquez surcette action pour déplacer un message dans la file d'attente des messages erronés. Un en-têtex-MDBadQueue-Reason est ajouté au message.

Ignorer n règles : cette action permet d'ignorer un certain nombre de règles. Cette action est utile lorsque vous souhaitez qu'une règle soit appliquée dans certaines circonstances, mais pas dans d'autres. Exemple : vous souhaitez supprimer les messages contenant le mot "Spam", mais pas ceux contenant le mot "Good Spam". Pour ce faire, vous pouvez créer une règle qui supprime les messages contenant le mot "Spam", puis placer au-dessus une autre règle qui stipule "si le message contient le mot "Good Spam", alors Ignorer 1 règle".

Arrêter processing rules : cetteaction permet d'ignorer toutes les règles restantes.

Copier le message à l'utilisateur(s) spécifié(s) : une copie du message est envoyée à un ou plusieurs destinataires. Vous devez spécifier les destinataires qui doivent recevoir le message.

Ajouter une signature d'entreprise : cetteaction vous permet de créer un petit texte qui sera ajouté en pied de page au message. Il est également possible d'ajouter le contenu d'un fichier texte. Une case à cocher *Rédiger en HTML* est disponible si vous souhaitez inclure du code HTML dans le texte de votre signature. Cette action prend en charge les <u>macros de signature</u> 134] \$ CONTACT...\$.

Exemple : vous pouvez utiliser cette règle pour inclure une déclaration disant "Ce courriel provient de mon entreprise, veuillez adresser toute plainte ou question à user01@example.com".

Ajouter un élément d'en-tête supplémentaire au message : cetteaction permet d'ajouter un add-tête supplémentaire dans le message. Vous devez spécifier le nom du nouvel en-tête et sa valeur.

Delete A Header Item From Message – Cetteaction permet de supprimer un en-tête dans un message. Vous devez spécifier l'en-tête que vous souhaitez supprimer.

Envoyer la note à... - Cette action permet d'envoyer un e-mail à une adresse [...]. Vous pourrez spécifier le destinataire, l'expéditeur, le sujet et un peu de texte. Vous pouvez également configurer cette action de manière à ce que le message original soit joint à la note. **Remarque :** cette action ignore tous les messages qui n'ont pas de chemin de retour. Elle ne peut donc pas être déclenchée, par exemple, par des messages de type Delivery Status Notification (DSN).

Exemple : vous pouvez créer une règle qui déplacera tous les messages contenant "Ceci est un spam !" dans le bad message directory et créer une autre règle qui enverra une note à quelqu'un pour l'informer que cela a été fait.

Supprimer la signature numérique : cliquez surcette action pour supprimer la signature numérique du message.

Exécuterun programme suivant : cette action permet d'exécuter un programme particulier lorsqu'un message remplit lesconditions de la règle.Vous devez indiquer le chemin d'accès au programme que vous souhaitez exécuter. Vous pouvezutiliser la macro\$MESSAGEFILENAME\$ pour transmettre le nom du message au Traiter, et vous pouvez spécifier si MDaemon doit ou non suspendre ses opérations temporairement ou indéfiniment en attendant que le Traiter se termine. De plus, vous pouvez forcer le processus à terminer et/ou l'exécuter dans une fenêtre masquée.

Send message Through SMS Gateway Server...- Cliquez sur cette option pour envoyer le message par l'intermédiaire d'un serveur de passerelle SMS. Vous devez fournir l'Adresse hôte ou IP et le numéro de téléphone du SMS.

Copy message to Folder...-Utilisez cette option pour placer une copie du message dans un dossier spécifique.

MOVE the messages to custom QUEUE...-Utilisez cette action pour déplacer le message dans une ou plusieurs files d'attente personnalisées créées précédemment. Lorsque vous déplacez des messages vers des files d'attente distantes personnalisées, vous pouvez utiliser les options de programmation personnalisées du planificateur d'événements pour contrôler le moment où ces messages seront traités.

Ajouter une ligne à un fichier texte : cetteoption permet d'ajouter une ligne de texte à un fichier texte spécifique. Lorsque vous choisissez cette action, vous devez spécifier le Chemin du fichier et le texte que vous souhaitez y ajouter. Vous pouvez utiliser certaines macros de MDaemon dans votre texte pour que le Filtre de contenu inclue dynamiquement des informations sur le message telles que l'expéditeur, le destinataire, l'ID du message, etc. Cliquez sur le bouton Macros dans la boîte de dialogue " Ajouter une ligne à un fichier texte " pour afficher une liste des macros autorisées.

[Copy|Move] Message to public Folders...-Utilisez cette action pour que le message soit copié (ou déplacé) dans un ou plusieurs Dossiers publics.

Rechercher et remplacer des mots dans un en-tête :

utilisezcette option pour rechercher certains mots dans un en-tête spécifié, puis les supprimer ou les remplacer. Lors de la création de cette règle, cliquez sur le lien "spécifier les informations" dans la description de la règle pour ouvrir la boîte de dialogue "En-tête - Rechercher et remplacer dans l'en-tête" dans laquelle vous désignerez l'en-tête et les mots à remplacer ou à supprimer. Cette action prend désormais en charge les expressions régulières. Voir <u>Utilisation d'expressions</u> <u>régulières dans vos règles de filtrage</u> [703].

Chercher et remplacer des mots dans le Corps du message – Utilisezcette option pour rechercher le corps du message et remplacer tout texte souhaité. Cette action prend désormais en charge les expressions régulières. Voir <u>Utilisation d'expressions régulières dans vos règles de filtrage</u> 703¹.

Passage à la règle...-Utilisez cette action pour passer immédiatement à une règle située plus bas dans la liste, en ignorant toutes les règles entre les deux.

Send an instant message... - Cette action permet d'envoyer un message instantané à une personne dont le message correspond aux critères de la règle. Vous spécifierez l'adresse e-mail **À :**, l'adresse**De :** et le contenu du message.

Add to Journal des événements Windows...-Utilise cette action pour enregistrer une chaîne de texte dans le Journal des événements Windows. Vous pouvez utiliser des macros dans la chaîne, et un bouton permet d'afficher les macros autorisées. **Extraire les pièces jointes to folder...**-Utilise cette action pour extraire les pièces jointes d'un message. Vous indiquerez le dossier dans lequel les pièces jointes seront copiées et vous pourrez choisir de supprimer les attachments du message après l'extraction. Vous pouvez également définir des conditions pour déterminer quelles pièces jointes seront extraites, en fonction du Nom du fichier, du type de contenu et de la taille des pièces jointes.

Modifier la priorité de traitement du message... - Cette action permet de définir la priorité de traitement du message, de "10 (Urgent)" à "90 (Renvoi)". Les paramètres par défaut sont "50 (normal)".

Signer avec sélecteur DKIM... - Utilisez cette action si vous souhaitez que la règle fasse en sorte qu'un message contienne <u>une signature DKIM</u> [566]. Vous pouvez également l'utiliser si vous souhaitez signer certains messages à l'aide d'un sélecteur autre que celui désigné dans la boîte de dialogue DKIM. R**EMARQUE :** L'authentification SMTP [568] de Connexion est toujours requise lors de la signature de messages DKIM.

Marquer message pour REQUIRETLS...-Indique que le message doit utiliser <u>REQUIRETLS</u> [628].

[Sign|Encrypt|Decrypt] message with the user's [Private|Public] key...-Use this actions to sign, encrypt, or decrypt a message using a private or public key of user's....Pour plus d'informations, voir : MDPGP or plus d'informations. Remarque : ces actions seront exécutées même si MDPGP est désactivé.

Ajouter un avertissement au début du message...- Utilisez cette action si vous souhaitez ajouter une sorte d'avertissement au début d'un message. Vous entrez une chaîne de caractères ou un code HTML et vous cochez la case "Rédiger en HTML". Vous pouvez également charger le texte à partir d'un fichier.

Ajouter une pièce jointe... - Utilisez cette action si vous souhaitez joindre un fichier à un message qui répond aux critères de la règle. Le fichier doit être contenu dans le dossier./MDaemon/CFilter/Attachments/.

Extraire pièce jointe et ajouter lien..-Utilisez cette action si vous souhaitez extraire les pièces jointes des messages répondant aux critères de la règle, et ajouter un lien vers ces pièces. Voir : <u>Liens vers les pièces jointes</u>.

Description de la règle

Cette zone affiche leformat de script interne de lanouvelle règle.Cliquez sur l'une desconditions ou actions de larègle(listées sous forme d'hyperliens) et l'éditeur approprié s'ouvrira pour spécifier les informations nécessaires.

Voir :

Editeur de filtre de contenuModifier une Règles du Filtre de contenu existanteUtilisation d'expressions régulières dans vos règles de filtrage

4.6.1.1.2 Modification d'une règle de filtrage de contenu

Pour modifier une règle du Filtre de contenu existante, sélectionnez-la et cliquez sur le bouton *Modifier la règle* dans la boîte de dialogue Filtre de contenu. La règle sera ouverte pour être éditée dans l'éditeur Modifier la règle. Les contrôles de cet éditeur sont identiques à ceux de la <u>boîte de dialogue Créer une règle</u> [997].

Voir :

<u>Editeur de filtre de contenu</u> ଭଣ୍ଟି <u>Création d'une Nouvelle règle du Filtre de contenu</u> ଭମ <u>Utilisation d'expressions régulières dans vos règles de filtrage</u> 703

4.6.1.1.3 Utilisation d'expressions régulières dans les règles de filtrage de contenu

Le système de filtrage de contenu prend en charge les recherches *par expressions régulières*. Il s'agit d'un système polyvalent qui vous permet de chercher non seulement des chaînes de texte spécifiques, mais aussi des *motifs de* texte . Les expressions régulières contiennent un mélange de texte brut et de caractères spéciaux qui indiquent le type de correspondance à effectuer, et peuvent ainsi rendre vos règles de Filtre de contenu plus puissantes et mieux ciblées.

Qu'est-ce qu'une expression régulière ?

Une expression régulière (regexp) est un modèle de texte composé d'une combinaison de caractères spéciaux appelés *métacaractères* et de caractères alphanumériques, ou "*littéraux*" (abc, 123, etc.). Ce motif est utilisé pour établir une correspondance avec des chaînes de texte, le résultat de la correspondance étant soit positif, soit négatif. Les Remplacer sont principalement utilisés pour les correspondances de textes réguliers et pour la recherche et le remplacement.

Les métacaractères sont des caractères spéciaux qui ont des fonctions et des utilisations spécifiques dans les expressions régulières. L'implémentation des expressions rationnelles dans le système de filtrage de contenu MDaemon autorise les métacaractères suivants :

\ | () [] ^ \$ * + ? . <>

Métacaractère Description du métacaractère

Lorsqu'elle est utilisée avant un métacaractère, la barre oblique inverse ("\") fait en sorte que le métacaractère soit traité comme un caractère littéral. Cela est nécessaire si

١

Т

vous souhaitez que l'expression régulière cherche l'un des caractères spéciaux utilisés comme métacaractères. Exemple : pour Chercher "+", votre expression doit inclure "\ +".

Le caractère d'alternance (également appelé "ou" ou "barre") est utilisé lorsque vous souhaitez que l'une des expressions situées du côté du caractère corresponde à la chaîne cible. L'expression rationnelle "abc|xyz" correspondra à toute occurrence de "abc" ou de "xyz" lors d'une recherche dans une chaîne de texte.

- [...] Un ensemble de caractères entre crochets ("[" et "]") signifie que n'importe quel caractère de l'ensemble peut correspondre à la chaîne de texte recherchée. Un tiret ("-") entre les caractères entre crochets indique une "range of". Exemple : Chercher la chaîne "abc" avec l'expression rationnelle "[a-z]" donnera trois résultats : "a", "b" et "c". L'expression "[az]" ne donnera qu'un seul résultat : "a".
- Indique le début de la ligne. Dans la chaîne cible, "abc ab a", l'expression "^a" ne donnera qu'une seule correspondance : le premier caractère de la chaîne cible. Dans la regexp "^ab", il y aura également une correspondance, à savoir les *deux*premiers caractères de la chaîne cible.
- [^...] La caret ("^") qui suit immédiatement le crochet gauche ("[") a une signification différente. Elle est utilisée pour exclure les caractères restants entre crochets de la correspondance avec la chaîne cible. L'expression "[^0-9]" indique que le caractère cible ne doit pas être un chiffre.
- (...) La parenthèse affecte l'ordre d'évaluation du motif et sert également d'expression *balisée* pouvant être utilisée dans les expressions de*recherche et de remplacement.*

Les résultats d'une recherche avec une expression régulière sont conservés temporairement et peuvent être utilisés dans l' expression de *remplacement* pour construire une nouvelle expression. Dans l' expression de *remplacement*, vous pouvez inclure un caractère "0", qui sera remplacé par la sous-chaîne trouvée par l'expression régulière au cours de la recherche. Ainsi, si l' expression de *recherche* "a(bcd)e" trouve une sous-chaîne correspondante, l' expression de*remplacement* "123-\$0-123" remplacera le texte correspondant par "123-abcde-123".

De même, vous pouvez utiliser les caractères spéciaux "\$1", "\$2", "\$3", etc. dans l'expression de *remplacement*. Ces caractères ne seront remplacés que par les résultats de l' expression *balisée* au lieu de la correspondance de la souschaîne entière. Le nombre qui suit la barre oblique inverse indique l'expression balisée à laquelle vous souhaitez faire référence (dans le cas d'une expression balisée contenant plusieurs expressions balisées). Exemple : si votre expression de *recherche* est "(123)(456)" et votre expression de *remplacement* "a-\$2-b-\$1", la sous-chaîne correspondante sera remplacée par "a-456-b-123", tandis que l' expression de*remplacement* "a-\$0-b" sera remplacée par "a-123456-b".

- Le signe du dollar ("\$") indique la fin de la ligne. Dans la chaîne de texte "13 321 123", l'expression "3\$" ne donnera qu'une seule correspondance, le dernier caractère de la chaîne. Dans l'expression rationnelle "123\$", il y aura également une correspondance, à savoir les *trois*derniers caractères de la chaîne cible.
 - Le quantificateur astérisque ("*") indique que le caractère situé à sa gauche doit correspondre à zéro ou plusieurs occurrences du caractère dans une ligne. Ainsi, "1*abc" correspondra aux textes "111abc" et "abc".
 - + Dans la même veine que le quantificateur astérisque, le quantificateur "+" indique que le caractère situé à sa gauche doit correspondre à *une ou plusieurs* occurrences du caractère dans une ligne. Ainsi, "1+abc" ne contiendra pas le texte "111abc" mais pas "abc".
 - Le point d'interrogation (" ?") indique que le caractère à sa gauche doit correspondre à zéro ou une fois.
 Ainsi, "1?abc" correspondra au texte "abc", et il correspondra à la partie "1abc" de "111abc".

Le métacaractère point ou point (".") correspond à n'importe quel autre caractère. Ainsi, ".+abc" correspondra à "123456abc", et "a.c" à "aac", "abc", "acc", etc.

Conditions et actions admissibles

Les expressions régulières peuvent être utilisées dans n'importe quelle *condition de* règle d'*En-tête From:*. Exemple : toute règle utilisant la condition "If the FROM HEADER contains". Les expressions régulières peuvent également être utilisées dans la condition "If the MESSAGE BODY contains".

Les expressions régulières peuvent être utilisées dans deux *actions de*règles du Filtre de contenu : "Rechercher et remplacer des mots dans un En-tête" et "Rechercher et remplacer des mots dans le Corps du message".



Les expressions régulières utilisées dans les *conditions des*règles du Filtre de contenu ne tiennent pas compte de la casse. La

casse n'est pas prise en compte.

La sensibilité à la casse dans les expressions régulières utilisées dans les *actions des*règles du Filtre de contenu est facultative. Lors de la création de l'expression régulière dans l'action de la règle, vous aurez la possibilité d'activer/désactiver la sensibilité à la casse.

Configuration d'une expression rationnelle dans une condition de règle

Pour configurer une condition d'en-tête ou de corps de message afin d'utiliser une expression régulière :

- Dans la boîte de dialogue Créer une règle, cliquez sur la case à cocher correspondant à la condition d'en-tête ou de corps de message que vous souhaitez insérer dans votre règle.
- Dans la zone de résumé située en bas de la boîte de dialogue Créer une règle, cliquez sur le lien"contient des chaînes spécifiques" qui correspond à la condition que vous avez sélectionnée à l'étape 1. Ce texte ouvre la boîte de dialogue Texte à rechercher.
- 3. Dans la zone "Chaînes pour caractères spécifiées", cliquez sur le lien "contient".
- 4. Choisissez "Matches Regular Expression" dans la liste déroulante et cliquez sur OK.
- 5. Si vous n'avez pas besoin d'utiliser la boîte de dialogue Tester l'expression régulière, saisissez votre expression régulière dans la zone de texte prévue à cet effet, cliquez sur **Ajouter**, puis passez à l'étape 8.
- 6. Tapez votre expression régulière dans la zone de texte "Rechercher expression". Pour simplifier le processus, nous avons prévu un menu de raccourcis qui peut être utilisé pour insérer facilement les métacaractères souhaités dans votre expression rationnelle. Cliquez sur le bouton ">" pour accéder à ce menu. Lorsque vous choisissez une option dans ce menu, le métacaractère correspondant est inséré dans l'expression et le point d'insertion du texte est déplacé à l'endroit approprié requis par le caractère.
- 7. Dans la zone de texte prévue à cet effet, utilisez le Type ou le texte que vous souhaitez utiliser pour tester votre expression, puis cliquez sur **Test**. Lorsque vous avez terminé de tester votre expression, cliquez sur **OK**.
- 8. Cliquez sur **OK**.
- 9. Poursuivez la création de votre règle normalement.

Configuration d'une Regexp dans l'action d'une règle

Pour configurer une action "Chercher et remplacer des mots dans..." afin d'utiliser une expression régulière :

- 1. Dans la boîte de dialogue Créer une règle, cliquez sur la case à cocher correspondant à l'action"*Chercher et remplacer des mots dans…*" que vous souhaitez insérer dans votre règle.
- Dans la zone de résumé au bas de la boîte de dialogue Créer une règle, cliquez sur le lien"specify information" qui correspond à l'action que vous avez sélectionnée à l'étape 1. La boîte de dialogue Chercher et remplacer s'ouvre alors.
- 3. Dans le cas où vous avez choisi l'action"Chercher...en-tête" à l'étape 1, utilisez la liste déroulante fournie pour choisir l'en-tête que vous souhaitez rechercher, ou tapez un en-tête dans la boîte si l'en-tête souhaité n'est pas répertorié. Si vous n'avez pas choisi l'action "Chercher dans l'en-tête" à l'étape 1, ignorez cette étape.
- 4. Cherchez l' expression derecherche que vous souhaitez utiliser dans cette action. Pour simplifier le processus, nous avons fourni un menu de raccourcis qui peut être utilisé pour insérer facilement les métacaractères souhaités dans votre expression de recherche. Cliquez sur le bouton ">" pour accéder à ce menu. Lorsque vous choisissez une option dans ce menu, le métacaractère correspondant est inséré dans l'expression et le point d'insertion du texte est déplacé à l'endroit approprié requis par le caractère.
- 5. Dans cette action, utilisez le Type d'expression de *remplacement* que vous souhaitez utiliser. Comme pour la *Rechercher* expression, nous avons prévu un menu de raccourcis pour les métacaractères pour cette option également. Laissez cette zone de texte vide si vous souhaitez supprimer une sous-chaîne correspondante au lieu de la Remplacer par un autre texte.
- 6. Cliquez sur "**Respecter la casse**" si vous souhaitez que l'expression soit sensible à la casse.
- 7. Cliquez sur Expression régulière si vous souhaitez que les chaînes de recherche et de remplacement soient traitées comme des expressions régulières. Dans le cas contraire, chaque chaîne sera traitée comme une simple recherche et un remplacement de sous-chaîne, c'est-à-dire qu'elle cherchera une correspondance littérale exacte du texte au lieu de le traiter comme une expression régulière.
- 8. Si vous n'avez pas besoin de tester votre expression, passez cette étape. Si vous devez tester votre expression, cliquez sur "Exécuter le test". Dans la boîte de dialogue Testeur de recherche et de remplacement, saisissez vos expressions de recherche et de remplacement et le texte que vous souhaitez tester, puis cliquez sur Test. Lorsque vous avez terminé de tester vos expressions rationnelles, cliquez sur OK.
- 9. Cliquez sur OK.
- 10. Poursuivez la création de votre règle normalement.

4.6.1.2 Pièces jointes

Content Filter	×
Content Filter Cules Cultachments Cultac	Attachment Handling ALLOW only these attachments (ex: *.txt) RESTRICT these attachments (ex: *.vbs) Remove *.ace *.ace *.ade *.adp *.apk *.appx *.appxuntle *.arj *.asf Add Add
	Click here to configure exceptions to attachment handling Check for restricted files within ZIP and RAR attachments When restricted attachments are detected
	OK Cancel

Utilisez cet onglet pour spécifier les pièces jointes que vous souhaitez classer comme autorisées ou interdites. Les pièces jointes non autorisées seront automatiquement supprimées des messages.

Gestion des pièces jointes

Les noms de fichiers spécifiés dans la liste *RESTRICTER ces pièces jointes* seront automatiquement supprimés des messages lorsque MDaemon les rencontrera. Si vous indiquez des fichiers dans la liste*Autoriser uniquement ces pièces jointes*, seuls ces fichiers seront autorisés - toutes les autres pièces jointes seront supprimées des messages. Une fois la pièce jointe supprimée, MDaemon continue normalement et délivre le message sans la pièce jointe. Vous pouvez utiliser les options de l'onglet Notifications pour qu'un message de notification soit envoyé à différentes adresses lorsque l'une de ces pièces jointes interdites est rencontrée.

Les caractères joker sont autorisés dans les entrées de la liste. Une entrée "*.exe", par exemple, entraînerait l'autorisation ou la suppression de toutes les pièces jointes se terminant par l'extension de fichierEXE. Pour ajouter une entrée à l'une ou l'autre des listes, tapez le nom du fichier dans l'espace prévu à cet effet, puis cliquez surAjouter.

Cliquez ici pour configurer les exceptions à la Gestion des pièces jointes

Cliquez sur ce bouton pour spécifier les adresses que vous souhaitez exclure de la surveillance des pièces jointes interdites. Si un message est adressé à l'une de ces adresses, MDaemon le laissera passer même s'il contient une pièce jointe interdite.

Rechercher les fichiers refusés dans les pièces jointes interdites ZIP et RAR

Cliquez sur cette option si vous souhaitez analyser le contenu des fichiers compressés Zip, 7-Zip et RAR à la recherche de pièces jointes interdites. En outre, toute règle du Filtre du contenu définie pour rechercher un nom de fichier particulier sera déclenchée si un fichier correspondant est trouvé dans une pièce jointe compressée.

Lorsque des pièces jointes interdites sont détectées...

Cliquez sur l'action à entreprendre lorsqu'un message contient une pièce jointe interdite.

...ne rien faire (utiliser le filtre de contenu)

Choisissez cette option si vous ne souhaitez pas entreprendre une action spécifique en fonction des Paramètres des pièces jointes, mais plutôt baser les actions sur les règles du Filtre de contenu [196].

... Supprimez tout le message !

Cette option permet de supprimer tout le message lorsqu'il contient une pièce jointe interdite.

...mettre en quarantaine l'ensemble du message pour...

Cette option met en quarantaine les messages contenant des pièces jointes interdites dans l'emplacement spécifié.

... supprimer la pièce jointe interdite

Choisissez cette option si vous souhaitez supprimer toutes les pièces jointes interdites plutôt que de supprimer le message entier.

...mettre les pièces jointes interdites en quarantaine vers...

Cliquez sur cette option et indiquez un emplacement si vous souhaitez mettre les pièces jointes interdites en quarantaine dans un emplacement spécifique plutôt que de les supprimer purement et simplement. Non (par défaut).

Ajouter un avertissement en haut du corps du message si la pièce jointe est supprimée

Lorsque MDaemon supprime une pièce jointe d'un message, par exemple parce qu'un virus a été détecté, il ajoute un message d'alerte en haut du corps du message. Cliquez sur le bouton**Messages d'avertissement** si vous souhaitez revoir ou modifier le modèle de ce message. Cette option est activée par défaut.

4.6.1.3 Notifications

Content Filter		\times
 Content Filter Rules Attachments Notifications Recipients Compression Antivirus Virus Scanning AV Updater 	Notification Messages All messages sent From: Postmaster@\$PRIMARYDOMAIN\$ Send restricted attachment notification message to Administrator Send restricted attachment notification message to Sender Send restricted attachment notification message to Sender Send restricted attachment notification message to Recipient Send virus notification message to Administrator Send virus notification message to Sender Send virus notification message to Sender Send virus notification message to Recipient Send virus notification message to Recipient Send Spam Filter update notification to Administrators	
	Message Subject: MDaemon Notification - Restricted Attachment Found	
	OK	

Cet écran permet de désigner les personnes qui doivent recevoir des messages de notification lorsqu'un virus ou une pièce jointe interdite est détecté, ou lorsque les fichiers de l'anti-spam ou du Filtre anti-spam sont mis à jour.

Messages de notification

Tous les messages envoyés de :

Utilisez cette case pour spécifier l'adresse à partir de laquelle vous souhaitez que les messages de notification soient envoyés.

Envoyer le message de notification de virus à...

Dans le cas d'un message dont la pièce jointe contient un virus, un message d'alerte est envoyé aux personnes désignées dans cette section. Un message d'alerte personnalisé peut être envoyé à l'expéditeur, au destinataire et aux administrateurs que vous avez désignés dans l' écran<u>Destinataires</u> 714. Pour personnaliser le message pour l'une des trois entrées, sélectionnez-en une dans la liste, puis modifiez le message qui apparaît dans la partie inférieure de cet écran. Chaque entrée a son propre message, bien que cela ne soit pas évident par défaut puisque certains sont identiques.

Envoyer un message de notification de pièce jointe interdite à...

Dans le cas d'un message contenant une pièce jointe correspondant à une entrée de pièce jointe interdite (listée dans l'onglet Pièces jointes), un message d'alerte est envoyé aux personnes désignées dans cette section. Un message d'alerte personnalisé peut être envoyé à l'expéditeur, au destinataire et aux administrateurs que vous avez désignés dans l'onglet Destinataires. Pour personnaliser le message pour l'une des trois entrées, sélectionnez-en une dans la liste, puis modifiez le message qui apparaît dans la partie inférieure de cet onglet. Chaque entrée a son propre message, bien que cela nesoitpas évident pardéfautpuisque les trois entrées sont identiques.

Envoyer une notification de mise à jour du Filtre anti-spam aux administrateurs

Utilisez cette option si vous souhaitez envoyer un e-mail aux administrateurs à chaque fois que le Filtre anti-spam est mis à jour, contenant les résultats de la mise à jour. Cette option est la même que l'option "*Envoyer un e-mail de notification avec les résultats de la mise à jour*" située à : Filtre anti-spam | Mises à jour.

Objet du message :

Ce texte sera affiché dans l'en-tête "Subject :" du message de notification envoyé.

Message

Il s'agit du message qui sera envoyé à l'entrée sélectionnée dans la liste ci-dessus lorsque la case à cocher correspondant à cette entrée est activée. Vous pouvez modifier directement ce message à partir de la boîte dans laquelle il est affiché.

```
Les fichiers contenant ce texte se trouvent dans le
répertoireMDaemonapp\. Il s'agit des fichiers suivants :
cfattrem[adm].dat - Message jointe interdite - Admins
cfattrem[rec].dat - Message jointe interdite - Recipient
cfattrem[snd].dat - Message jointe interdite - Sender
cfvirfnd[adm].dat - Message jointe interdite - Admins
cfvirfnd[rec].dat - Message contenant un virus -
Destinataire
cfvirfnd[snd].dat - Message contenant un virus -
ExpéditeurLorsque vous souhaitez rétablir l'apparence originale de l'un de
ces messages, il vous suffit de supprimer le fichier
correspondant et MDaemon le recréera dans son état par
défaut.
```

4.6.1.3.1 Macros de messages

Pour votre commodité, certaines macros peuvent être utilisées dans les messages de notification et autres messages que les Filtres de contenu génèrent. Vous pouvez utiliser l'une des macros suivantes :

\$ACTUALTO\$	Certains messages peuvent contenir un champ "ActualTo" qui représente généralement la boîte aux lettres et l'hôte de destination tels qu'ils ont été saisis par l'utilisateur d'origine avant tout reformatage ou conversion d'alias. Cette macro est remplacée par cette valeur.
\$AV_VERSION	Indique la version de l'antivirus que vous utilisez.
\$CURRENTTIME	Cette macro est remplacée par l'heure à laquelle le message est traité.
\$ACTUALFROM\$ (DATE D'ENVOI)	Certains messages peuvent contenir un champ "ActualFrom" qui représente généralement la boîte aux lettres et l'hôte d'origine avant tout reformatage ou conversion d'alias. Cette macro est remplacée par cette valeur.
\$FILTERRULENAME\$ (NOM DU FILTRE)	Cette macro est remplacée par le Nom de la règle dont les critères correspondent au message.
\$FROM\$	Cette macro est remplacée par l'adresse complète contenue dans l'en-tête "From :" du message.
\$FROMDOMAIN	Cette macro insère le nom de domaine contenu dans l'adresse figurant dans l'en-tête "From :" du message (la valeur à droite de "@" dans l'adresse électronique).
\$FROMMAILBOX	Liste la partie boîte aux lettres de l'adresse trouvée dans l'en-tête "From :" du message (la valeur à gauche de "@" dans l'adresse électronique).
\$GEN_GUID	Génère un identifiant unique composé de 11 caractères alphanumériques. Exemple : 0XVBASADTZC
En-tête From : \$HEADER:xx\$	Cette macro entraîne le développement de la valeur de l'en-tête spécifié à la place du "xx" dans le message reformaté. Exemple : Si le message original contient "TO : user01@example.com", la macro \$HEADER:TO\$ le remplacera par "user01@example.com". Si le message original contient "Objet du message : Ceci est le sujet", la macro\$HEADER:SUBJECT\$ sera Remplacée par le texte "Ceci est le sujet".
\$HEADER:MESSAGE-ID\$ (EN- TÊTE)	Comme pour <i>\$HEADER</i> : [xx] <i>\$</i> ci-dessus, cette macro s'étendra à la valeur de l' en-tête Message-ID.

\$LIST_ATTACHMENTS_REMOVED\$\$ (LISTE DES PIÈCES JOINTES SUPPRIMÉES)	Lorsqu'une ou plusieurs pièces jointes sont supprimées du message, cette macro en dresse la liste.
\$LIST_VIRUSES_FOUND\$\$ (LISTE DES VIRUS TROUVÉS)	Lorsqu'un ou plusieurs virus sont trouvés dans un message, cette macro en dresse la liste.
\$MESSAGEFILENAME	Cette macro s'étend auNom du fichier du message en cours de traitement.
\$MESSAGEID\$\$ CETTE MACRO SE DÉVELOPPE EN NOM DE FICHIER DU MESSAGE EN COURS DE TRAITEMENT.	Identique à <code>\$HEADER:MESSAGE-ID\$ ci-dessus, sauf que cette macro supprime "<>" de la valeur de l'ID du message.</code>
\$PRIMARYDOMAIN\$ (DOMAINE PRIMAIRE)	S'étend auDomaine par défaut de MDaemon, qui est désigné dans le <u>Gestionnaire de</u> <u>domaines 184</u> 1.
\$PRIMARYIP	Cette macro se développe jusqu'à l' <u>adresse</u> <u>IPv4</u> 1871 de votre <u>Domaine par défaut</u> 1841.
\$PRIMARYIP6\$ CETTE MACRO SE DÉVELOPPE EN ADRESSE IPV4 DE VOTRE DOMAINE PAR DÉFAUT.	Cette macro se développe jusqu'à l' <u>adresse</u> <u>IPv6</u> ाक्षी de votre <u>Domaine par défaut</u> ाक्षी.
\$RECIPIENT\$ (RÉCIPIENDAIRE)	Cette macro se résout en l'adresse complète du destinataire du message.
\$RECIPIENTDOMAIN\$ (DOMAINE DU DESTINATAIRE)	Cette macro insère le Nom de domaine du destinataire du message.
BOÎTE AUX LETTRES DU DESTINATAIRE	Liste laboîte aux lettres dudestinataire(la valeur à gauche de "@" dans l'adresse e-mail).
\$REPLYTO	Cette macro se développe en fonction de la valeur de l'en-tête "Reply-to" dumessage.
\$SENDER\$ (EXPÉDITEUR)	Se développe jusqu'à l'adresse complète à partir de laquelle le message a été envoyé.
\$SENDERDOMAIN\$ (NOM DE DOMAINE DE L'EXPÉDITEUR)	Cette macro insère le nom de domaine de l'expéditeur dumessage(la valeur à droite de "@" dans l'adresse électronique).
BOÎTE AUX LETTRES DE L'EXPÉDITEUR	Liste laboîte aux lettres de l'expéditeur(la valeur à gauche de "@" dans l'adresse électronique).
\$SUBJECT	Affiche le texte contenu dans l'objet dumessage.

4.6.1.4 Destinataires

Content Filter		\times
Content Filter Hules Attachments Compression Antivirus Virus Scanning W Updater	Recipients This is a list of email addresses which will receive Content Filter notification messages. Use the 'Notifications' tab to configure which messages are sent. postmaster@company.test Remove	
	OK Cancel	

Destinataires

Cette liste de destinataires correspond aux différentes options "*envoyer…à l'administrateur*" situées dans l'onglet Notifications. Ces adresses recevront des messages de notification lorsque l'une des options "Administrateur" est sélectionnée dans cet onglet. Pour ajouter une adresse à cette section, tapez-la dans l'espace prévu à cet effet, puis cliquez sur *Ajouter*. Pour supprimer une adresse, sélectionnez-la dans la liste, puis cliquez sur *Supprimer*.

Ne pas envoyer de notifications aux domaines étrangers

Cochez cette case si vous souhaitez limiter les messages de notification du Filtre de contenu aux destinataires du domaine local. Cette option est désactivée par défaut.

4.6.1.5 Compression

Content Filter				×
Content Filter Attachments Attachments Recipients Compression Antivirus Virus Scanning	Outbound Compression Enable compression of attachments for outbo Compress outbound local domain attachment Inbound Decompression Enable decompression of attachments for inb Decompress inbound local domain attachment	ound messa s ound mess	ges ages	
- AV Updater	Compression Options Create self-extracting zips Compress only if compression % is greater than Compress if total attachment size is greater than Compression level Medium (Default) Use fixed archive name: Archive Compression Exclusions Exclude these files Winmail dat attachments Extract file attachments from winmail dat (Out	25 50 Exclu	% KB .ZIP or .EXE ide these domains	
			OK Cancel	

Avec les contrôles de cet onglet, vous pouvez faire en sorte que les pièces jointes soient automatiquement compressées ou décompressées avant que le message ne soit délivré. Le niveau de compression peut être contrôlé ainsi que plusieurs autres paramètres et exclusions. Cette fonction peut réduire de manière significative la bande passante et le débit nécessaires à la distribution de vos messages sortants.

Compression en sortie

Activer la compression des pièces jointes en sortie

Cochez cette case si vous souhaitez activer la compression automatique des pièces jointes pour les courriers distants sortants. L'activation de cette commande n'entraîne pas la compression de toutes les pièces jointes des messages ; elle active simplement la fonction.La compression ou non des fichiers d'un message sortantest déterminée par les autres paramètres de cet onglet.

Compression des pièces jointes sortantes du domaine local

En activant cette commande, les paramètres de compression des fichiers seront appliqués à tout le courrier en sortie - même aux messages dont la destination est une autre adresse locale.

Décompression en entrée

Activer la décompression des pièces jointes des messages entrants

Cochez cette case si vous souhaitez activer la décompression automatique des pièces jointes des messages de courrier distant entrants. Lorsqu'un message arrive avec une pièce jointe zippée, MDaemon la décompresse avant de la distribuer dans la boîte aux lettres de l'utilisateur local.

Décompression des messages entrants des pièces jointes du domaine local

Activez cette commande si vous souhaitez que la décompression automatique s'applique également au courrier local.

Options de compression

Créer des zips auto-extractibles

Cochez cette case si vous souhaitez que les fichiers de compression créés par MDaemon soient des fichiers zip auto-extractibles portant l'extensionEXE. Si vous craignez que les destinataires du message n'aient pas accès à un utilitaire de décompression, cette option est utile. Les fichiers zip auto-extractibles peuvent être décompressés simplement en double-cliquant dessus.

Ne compressez que si le pourcentage de compression est supérieur à [xx] %.

MDaemon ne compressera pas les pièces jointes d'un messageavant de l'envoyer, sauf si elles peuvent être compressées avec un pourcentage supérieur à la valeur spécifiée dans cette commande. Exemple : si vous indiquez une valeur de 20 et qu'une pièce jointe ne peutpas être compressée d'au moins 21 %, MDaemon ne la compressera pas avant d'envoyer le message.

> MDaemon doit d'abord compresser un fichier pour déterminer de quel pourcentage il peut être compressé. Dans ce cas, cette fonctionnalité n'empêche pas les fichiers d'être compressés - elle empêche simplement les pièces jointes d'être envoyées dans un format compressé lorsqu'elles ne peuvent pas être compressées au-delà de la valeur désignée. Dans ce cas, si MDaemon constate, après avoir compressé le fichier, qu'il ne peut pas être compressé au-delà de cette valeur, la compression ne sera pas prise en compte et le message sera envoyé avec ses pièces jointes inchangées.

Compression des pièces jointes jointes si leur taille est supérieure à [xx] KB

Lorsque la compression automatique des pièces jointes est activée, MDaemon ne tente de compresserles pièces jointes d'un message quesi leur taille totale dépasse la valeur indiquée ici. Les messages dont la taille totale des pièces jointes est inférieure à ce seuil seront distribués normalement, sans modification des pièces jointes.

Niveau de compression

Utilisez la liste déroulante pour choisir le degré de compression que vous souhaitez que MDaemon applique aux pièces jointes compressées automatiquement. Vous pouvez choisir trois niveaux de compression : minimum (processus de compression le plus rapide avec le moins de compression), moyen (valeur par défaut), ou maximum (processus de compression le plus lent mais degré de compression le plus élevé).

Utiliser un nom d'archive fixe : [nom de l'archive]

Cochez cette case et choisissez un nom si vous souhaitez que les pièces jointes compressées automatiquement aient un nom de fichier spécifique.

Exclusions de la compression

Exclure ces pièces jointes...

Cliquez sur ce bouton pour spécifier les fichiers que vous souhaitez exclure des fonctions de compression automatique. Lorsqu'une pièce jointe à un message correspond à l'un de ces noms de fichier, elle n'est pas compressée, quels que soient les paramètres de compression. Les caractères joker sont autorisés dans ces entrées. Vous pouvez donc spécifier "*.exe", par exemple, et tous les fichiers se terminant par ".exe" ne seront pas compressés.

Exclure des domaines...

Cliquez sur ce bouton pour spécifier les domaines de destinataires dont vous souhaitez exclure les messages de la compression automatique. Les messages destinés à ces domaines ne verront pas leurs pièces jointes compressées, quels que soient vos paramètres de compression.

Pièces jointes Winmail.dat

Extraire les pièces jointes jointes de winmail.dat (messages RTF d'Outlook)

Activez cette option si vous souhaitez extraire les fichiers les pièces jointes de winmail.dat et les transformer en pièces jointes MIME standard.

4.6.2 Antivirus

4.6.2.1 Analyse antivirus



Les options de cet écran ne sont disponibles que si vous utilisez la fonctionoptionnelle <u>MDaemon AntiVirus</u> [718]. Activer MDaemon AntiVirus pour la première fois démarre un essai de 30 jours. Si vous souhaitez acheter cette fonctionnalité, contactez votre revendeur MDaemon agréé ou visitez : <u>mdaemon.com</u>.

Activer l'antivirus

Cochez cette case pour activer l'analyse antivirus des messages. Lorsque MDaemon reçoit un message avec des pièces jointes, il les analyse pour détecter les virus avant d'envoyer le message à sa destination finale.

Exclure les passerelles de l'analyse antivirus

Cochez cette case si vous souhaitez que les messages destinés à l'une despasserelles du domaine deMDaemonsoient exclus de l'analyse antivirus. Cela peut être souhaitable pour ceux qui souhaitent laisser l'analyse de ces messages auserveur de messagerie du domaine.Pour plus d'informations sur les passerelles de domaines, voir <u>Gestionnaire de passerelles</u> ²⁶¹.

Configurer les Exclusions

Cliquez sur le bouton Configurer les Exclusions pour spécifier les adresses de destinataires à exclure de l'analyse antivirus. Les messages destinés à ces adresses ne seront pas analysés. Les caractères génériques sont autorisés dans ces adresses. Vous pouvez donc utiliser cette fonction pour exclure des domaines entiers ou des Boîtes aux Lettres spécifiques dans tous les domaines. Exemple : "*@exemple.com ou "VirusArchive@*".

Exclure les IP autorisées de l'analyse antivirus

Cochez cette case si vous souhaitez exempter les messages de l'analyse antivirus lorsqu'ils proviennent de l'une de vos <u>adresses IP autorisées</u> [54].

Refuser les messages infectés par des virus

Cochez cette option si vous souhaitez analyser les messages entrants à la recherche de virus pendant la session SMTP plutôt qu'après la fin de la session, puis rejeter les messages contenant des virus. Comme chaque message entrant est analysé avant que MDaemon ne l'accepte officiellement et ne termine la session, le serveur d'envoi en est toujours responsable : le message n'a pas encore été livré. Le message peut donc être rejeté d'emblée lorsqu'un virus est détecté. De plus, comme le message a été rejeté, aucune autre action liée à l'antivirus et répertoriée dans cette boîte de dialogue ne sera effectuée. Aucune procédure de quarantaine ou de nettoyage ne sera entreprise et aucun message de notification ne sera envoyé. Cela peut réduire considérablement le nombre de messages infectés et de messages de notification de virus que vous et vos utilisateurs recevez.

Le journal SMTP-(dans) indiquera le résultat du traitement AV. Les résultats possibles sont les suivants :

- le message a été analysé et s'est avéré infecté par un virus.
- le message a été analysé et aucun virus n'a été trouvé
- le message n'a pas pu être analysé (généralement parce qu'un fichier ZIP ou un autre type de pièce jointe n'a pas pu être ouvert/accédé)
- le message n'a pas pu être analysé (il dépasse la taille maximale autorisée)
- une erreur s'est produite pendant l'analyse

Lorsque des virus sont détectés...

Cliquez sur l'une des options de cette section pour désigner l'action que MDaemon va entreprendre lorsque l'AntiVirus détecte un virus.

...ne rien faire (utiliser le filtre de contenu)

Choisissez cette option si vous ne souhaitez prendre aucune des mesures cidessus et si vous avez configuré les règles du Filtre de contenu pour qu'elles prennent d'autres mesures à la place.

...Supprimez tout le message !

Cette option permet de supprimer l'intégralité du message, et non la seule pièce jointe, lorsqu'un virus est détecté. Suppression tout message. Comme elle supprime le message entier, l'option"*Ajouter un avertissement*..." ne s'applique pas. Cependant, vous pouvez toujours envoyer un message de notification au destinataire en utilisant les commandes de l'onglet Notifications.

...mettre en quarantaine l'ensemble du message pour...

Cette option est similaire à l'option"*Supprimer tout le message*" ci-dessus, mais le message sera mis en quarantaine à l'emplacement spécifié au lieu d'être supprimé.

... supprimer la pièce jointe infectée

Cette option supprime la pièce jointe infectée. Le message sera toujours remis au destinataire, mais sans la pièce jointe infectée. Vous pouvez utiliser la commande"*Ajouter un avertissement…*" au bas de cette boîte de dialogue pour ajouter un texte au message informant l'utilisateur qu'une pièce jointe infectée a été supprimée.

...mettre les pièces jointes en quarantaine dans...

Choisissez cette option et indiquez un emplacement dans l'espace prévu à cet effet si vous souhaitez que les pièces jointes infectées soient mises en quarantaine dans cet emplacement plutôt que d'être supprimées ou nettoyées. Comme pour l'option"*Supprimer la pièce jointe infectée*", le message sera toujours remis au destinataire, mais sans la pièce jointe infectée.

...nettoyer la pièce jointe infectée

Lorsque cette option est sélectionnée, AntiVirus tente de nettoyer (c'est-à-dire de désactiver) la pièce jointe infectée. Si la pièce jointe ne peut pas être nettoyée, elle sera supprimée.

Mettre en quarantaine les messages qui ne peuvent pas être analysés

Lorsque cette option est activée, MDaemon met en quarantaine les messages qu'il ne peut pas analyser, par exemple ceux qui contiennent des fichiers protégés par un mot de passe.

Autoriser les fichiers protégés par un mot de passe dans la liste d'exclusion...

Utilisez cette option si vous souhaitez autoriser un message contenant un fichier non analysable et protégé par un mot de passe à passer par l'analyseur antivirus si le nom ou le type de fichier figure dans la liste d'exclusion.

Configurer les Exclusions

Cliquez sur ce bouton pour ouvrir et gérer la liste d'exclusion des fichiers. Les Nom et type de fichiers figurant dans cette liste ne seront pas analysés.
Ajouter un avertissement au début du message si le message est INFECTED. Si le message estESSAGE BODY.

Si l'une des options"...pièce jointe" est sélectionnée ci-dessus, cliquez sur cette option si vous souhaitez ajouter un texte d'avertissement en haut du message INFECTED avant qu'il ne soit envoyé au destinataire. Vous pouvez ainsi informer le destinataire que la pièce jointe a été supprimée et pourquoi.

Message d'avertissement...

Cliquez sur ce texte pour afficher le texte d'avertissement qui sera ajouté aux avertissements lorsque la fonction "*Ajouter un message d'avertissement*..." est utilisée. Après avoir apporté les modifications souhaitées à ce texte, cliquez sur **OK** pour fermer la boîte de dialogue et enregistrer les modifications.

Ajouter un avertissement au début du corps du message s'il n'est pas scanné

Lorsque cette option est activée, MDaemon ajoute un texte d'avertissement au début du message s'il n'a pas pu l'analyser.

Message d'avertissement...

Cliquez sur ce texte pour afficher le texte d'avertissement qui sera ajouté aux messages qui ne peuvent pas être analysés. Après avoir apporté les modifications souhaitées à ce texte, cliquez sur **OK** pour fermer la boîte de dialogue et enregistrer les modifications.

Analyser toutes les Boîtes aux Lettres tous les n jours

Cochez cette case si vous souhaitez analyser périodiquement tous les messages stockés, afin de détecter tout message infecté qui aurait pu passer par le système avant qu'une mise à jour de la définition du virus ne soit disponible pour l'attraper. Les messages infectés seront déplacés dans le dossier de quarantaine et l' en-tête X-MDBadQueue-Reason sera ajouté, afin que vous puissiez obtenir une explication lors de l'affichage dans MDaemon. Les messages qui ne peuvent pas être analysés ne sont pas mis en quarantaine.

Configurer l'analyse des boîtes aux lettres.

Cliquez sur ce bouton pour indiquer la fréquence à laquelle vous souhaitez analyser les Boîtes aux Lettres et si vous souhaitez analyser tous les messages ou seulement ceux qui sont inférieurs à un certain nombre de jours. Vous pouvez également exécuter manuellement une analyse de boîte aux lettres immédiatement.

Moteurs antivirus

MDaemon AntiVirus est équipé de deux moteurs antivirus : ClamAV et IKARUS Anti-Virus. Lorsque les deux moteurs sont activés, les messages sont analysés par les deux moteurs ; d'abord par d'abord par IKARUS Anti-Virus, puis par ClamAV. Ceci fournit une couche supplémentaire de protection, puisqu'un virus pourrait potentiellement être identifié par un moteur avant que les définitions de virus de l'autre moteur n'aient été mises à jour.

Utiliser le moteur ClamAV pour analyser les messages

Cochez cette case si vous souhaitez utiliser le moteur ClamAV pour analyser les messages à la recherche de virus.

Configurer

Cliquez sur ce bouton pour accéder à une option permettant d'activer la journalisation débogage pour ClamAV. Le fichier journal sera enregistré dans le dossier journal de MDaemon.

Utiliser le moteur Moteurs antivirus d'IKARUS pour analyser les messages

Cochez cette case si vous souhaitez utiliser le moteur antivirus d'IKARUS pour analyser les messages à la recherche de virus.

Configurer

Utilisez cette option si vous souhaitez marquer comme virus les pièces jointes contenant des documents qui contiennent des macros. Vous pouvez définir un niveau heuristique de -1 à 5. "-1" est automatique, "0" est désactivé et 1-5 est le niveau heuristique le plus bas au plus haut.

Voir :

<u>Mises à jour antivirus</u> त्यो <u>Filtre de contenu - Antivirus</u> ब्झो

4.6.2.2 Mises à jour antivirus

Content Filter		×
Content Filter Rules Attachments Recipients Compression Antivirus Virus Scanning Artivirus Virus Scanning	AntiVirus Scanner Info MD aemon AntiVirus detected. MD aemon AntiVirus version: 24.5.0a IKARUS AV definition version: Signature date: ClamAV signature version: 27337 Signature date: Mon Jul 15 03:35:59 2024 For more information, please visit <u>https://www.mdaemon.com/SecurityPlus</u> ClamAV Updater Update AV signatures now View update report Log settings Scheduler Scheduler Send notification if virus definitions have not updated for 7 day(s) AntiVirus Test Send EICAR Test Virus in Email to Postmaster	
	OK Cancel Hel;	

Certaines des options de cet écran ne seront disponibles que si vous utilisez la fonctionoptionnelle <u>MDaemon AntiVirus</u> 7181. Activer MDaemon Antivirus pour la première fois démarre un essai de 30 jours. Si vous souhaitez acheter cette fonctionnalité, contactez votre revendeur MDaemon agréé ou visitez : <u>mdaemon.com</u>.

Utilisez les commandes de cet écran pour mettre à jour manuellement ou automatiquement vos définitions de virus. Vous disposez d'un planificateur pour la mise à jour automatique, d'une visionneuse de rapports vous permettant de vérifier quand et quelles mises à jour ont été téléchargées, et d'une fonction de test utilisée pour confirmer que l'analyse antivirus fonctionne correctement.

Informations de l'analyse antivirus

Cette section vous indique si l'antivirus est disponible et quelle version vous utilisez. Elle indique également la date de la Dernière mise à jour à jour des définitions de virus.

Utilitaire de mise à jour à ClamAV

Mettre à jour les signatures antivirus maintenant

Cliquez sur ce bouton pour mettre à jour les définitions de virus manuellement. L'outil de mise à jour se connectera immédiatement après avoir appuyé sur le bouton.

Pas de Paramètres de journalisation

Cliquez sur ce bouton pour ouvrir les Pasètres de journalisation de l'Updater. Dans cette boîte de dialogue, vous pouvez choisir d'inclure ou non les actions de l'Updater dans un fichier journal. Vous pouvez également choisir de définir une taille maximale d'un fichier journal.

Afficher le rapport de mise à jour

Le bouton*Afficher le rapport de mise à jour*permet d'ouvrir la visionneuse du journal AntiVirus . La visionneuse répertorie les heures, les actions effectuées et d'autres informations relatives à chaque mise à jour.

Planificateur

Cliquez sur ce bouton pour ouvrir l' écran de<u>planification de l'AntiVirus</u> [403], utilisé pour planifier les vérifications des mises à jour des signatures de virus à des heures précises, des jours précis ou à intervalles réguliers.

Envoyer une notification si les signatures de virus n'ont pas été mises à jour depuis [xx] jour(s)

Non (par défaut) l'administrateur sera notifié si les définitions de virus ClamAV n'ont pas été mises à jour pendant le nombre de jours spécifié.

Test antivirus

Envoyer test au postmaster un e-mail avec un virus EICAR

Cliquez sur ce bouton pour envoyer un message test au postmaster, avec le fichier du virus EICAR joint. Cette pièce jointe est inoffensive - elle est simplement utilisée pour un test antivirus. En observantla fenêtre de journal duFiltre de contenu dans l'interface principale de MDaemon, vous pouvez voir ce que MDaemon fait de ce message lorsqu'il le reçoit. Exemple, en fonction de vos paramètres, vous pouvez voir un extrait de journalisation qui ressemble à ce qui suit :

```
Mon 2008-02-25 18:14:49 : Processing C:
\MDAEMON\LOCALQ\md75000001128.msg
Mon 2008-02-25 18:14:49 : > eicar.com (C:
\MDaemon\CFilter\TEMP\cf1772420862.att)
Mon 2008-02-25 18:14:49 : > Message de : postmaster@example.com
Mon 2008-02-25 18:14:49 : > Message à : postmaster@example.com
Mon 2008-02-25 18:14:49 : > Objet du message : Message de test EICAR
Mon 2008-02-25 18:14:49 : > Message ID :
<MDAEMON10001200202251814.AA1447619@example.com>
Mon 2008-02-25 18:14:49 : Exécution d'une analyse virale...
Mon 2008-02-25 18:14:50 : > eicar.com est infecté par EICAR-Test-File
Mon 2008-02-25 18:14:50 : > eicar.com a été supprimé du message
Mon 2008-02-25 18:14:50 : > eicar.com a été placé en quarantaine dans
C:\MDAEMON\CFILTER\QUARANT\
```

Mon 2008-02-25 18:14:50 : > Total des pièces jointes analysées : 1 (y compris les multipart/alternatives) Mon 2008-02-25 18:14:50 : > Nombre total de pièces jointes infectées : 1 Mon 2008-02-25 18:14:50 : > Total des pièces jointes désinfectées : 0 Mon 2008-02-25 18:14:50 : > Total des pièces jointes jointes supprimées : 1 Mon 2008-02-25 18:14:50 : > Nombre total d'erreurs lors de l'analyse : Ω Mon 2008-02-25 18:14:50 : > Notification de virus envoyée à postmaster@example.com (expéditeur) Mon 2008-02-25 18:14:50 : > Notification de virus envoyée à postmaster@example.com (destinataire) Mon 2008-02-25 18:14:50 : > Notification de virus envoyée à postmaster@example.com (admin) Mon 2008-02-25 18:14:50 : > Notification de virus envoyée à postmaster@example.com (admin) Mon 2002-02-25 18:14:50 : Traitement terminé (correspondance avec 0 des 12 règles actives)

Voir :

AntiVirus 718 Filtre de contenu - Antivirus 📾

4.7 Filtre anti-spam

4.7.1 Filtre anti-spam

Le Filtre anti-spam est l'une des principales fonctionnalités de lasuite complète d'outils de prévention du spam deMDaemon. Il utilise des méthodes heuristiques pour examiner les messages entrants afin de calculer un "score" basé sur un système complexe de règles. Ce score est ensuite utilisé pour déterminer la probabilité qu'un message soit du spam, et certaines actions peuvent être entreprises en fonction de ce score : vous pouvez refuser le message, le marquer comme pouvant être du spam, etc.

Les adresses peuvent être autorisées ou bloquées, ou désignées comme totalement exemptes d'examen par le Filtre anti-spam. Vous pouvez insérer un rapport de spam dans les messages, indiquant leurs scores de spam et la manière dont ces scores ont été obtenus, ou vous pouvez générer le rapport sous la forme d'un courrier électronique séparé et y joindre le message de spam d'origine en tant que pièce jointe. En outre, vous pouvez même utiliser l' apprentissage<u>bayésien</u> mour aider le Filtre anti-spam à apprendre à identifier les spams avec plus de précision au fil du temps, augmentant ainsi sa fiabilité.

Enfin, en examinant plusieurs milliers de messages de spam connus, les règles ont été optimisées au fil du temps et sont très fiables dans la détection de l'empreinte digitale d'un message de spam. Vous pouvez cependant personnaliser le Filtre anti-spam ou ajouter de nouvelles règles en modifiant lesfichiers de configuration duFiltre anti-spampour répondre à vos besoins spécifiques.

Le Filtre anti-spam deMDaemonutilise une technologie heuristique intégrée, populaire et open-source. La page d'accueil du projet open-source est la suivante

```
http://www.spamassassin.org
```

Voir :

Filtre anti-spamTistes de blocage DNS751

4.7.1.1 Filtre anti-spam

🧐 Filtre anti-spam - Filtre anti-spam	
 Filtre anti-spam Classification bayésienne Apprentissage bayésien Daemon anti-spam (MDSpamD) Liste blanche (automatique) Liste blanche (pas de filtrage) Liste blanche (destinataires) Liste blanche (expéditeurs) Liste noire (expéditeurs) Liste noire (expéditeurs) Paramètres DNS-BL Pièges à spam 	Le Filtre anti-spam de MD aemon associe des analyses heuristiques et bayésiennes pour détecter le spam.
	OK Annuler Appliquer Aide

Activer le Filtre anti-spam

Cochez cette case pour activer le système heuristique de filtrage des messages et des spams. Aucune des autres options du Filtre anti-spam de cet écran ne sera disponible tant que cette option n'aura pas été activée.

Un message est considéré comme du spam si son score est supérieur ou égal à [xx] (0.0 - 500.0)

La valeur que vous indiquez ici est le Seuils des spams que MDaemon comparera auscore de spam dechaque message.Tout message dont le score de spam est supérieur ou égal à cette valeur sera considéré comme du spam, et les actions appropriées seront prises en fonction des autres paramètres du Filtre anti-spam. **SMTP rejette les messages dont le score est supérieur ou égal à [xx] (0 = jamais)** Cette option permet de définir un seuil de rejet des scores de spam. Lorsquele score de spam d'un messageest supérieur ou égal à ce score, le message est complètement rejeté au lieu de passer par les autres options et d'être éventuellement distribué. La valeur de cette option doit toujours être supérieure à la valeur de l'option"*Un message est détecté comme spam si son score…*" ci-dessus. Dans le cas contraire, un message ne serait jamais considéré comme du spam et ne se verraitpas appliquer le reste desoptions du Filtre anti-spam;ilserait simplement rejeté lors de la distribution. Utilisez "0" dans cette option si vous souhaitez désactiver l'analyse au cours du processus SMTP, et si vous ne voulez pas que MDaemon rejette les messages, quel que soit leur score. Si l'analyse SMTP est désactivée, une analyse basée sur la file d'attente sera tout de même effectuée sur les messages après leur acceptation. Le paramètre par défaut de cette option est "12.0".

Exemple,

Si le seuil du score de spam est fixé à 5.0 et le seuil de rejet à 10.0, tout message dont le score de spam est supérieur ou égal à 5.0 mais inférieur à 10.0 sera considéré comme du spam et traité conformément aux autres paramètres du Filtre anti-spam. Tout message dont le score de spam est supérieur ou égal à 10.0 sera rejeté par MDaemon au cours du processus de distribution.

> Lorsqu'un Filtre anti-spam est détecté, vous devez surveillerses performances au fil du temps et affiner les seuils de spam et de rejet en fonction de vos besoins. Cependant, pour la plupart des gens, un Seuils des scores de spam de 5.0 permet d'attraper la plupart des spams, avec relativement peu de Faux positifs et de faux négatifs (les spams qui passent inaperçus) et rarement de Faux positifs (les messages marqués comme spams qui ne le sont pas). Un seuil de rejet de 10-15 n'entraînera le rejet que des messages qui sont presque certainement des spams. Il est extrêmement rare qu'un message légitime ait un score aussi élevé. Le seuil de rejet par défaut est de 12.

Enregistrer les résultats de l'heuristique dans les pas de journalisation de la session SMTP

Cliquez sur cette option pour enregistrer les résultats du traitement heuristique au cours des sessions SMTP dans les journaux de session SMTP [177].

Envoyer les résultats heuristiques aux clients SMTP

Cliquez sur cette option pour afficher les résultats du traitement heuristique en ligne avec les transcriptions des sessions SMTP. Cette option n'est pas disponible lorsque le seuil de rejet du score de spam est fixé à "0", ce qui signifie que le spam ne sera jamais rejeté en raison de son score. Pour plus d'informations, voir, "SMTP rejette les messages dont le score est supérieur ou égal à [xx] (0=jamais)" ci-dessus.

Ignorer l'analyse basée sur la file d'attente pour les messages traités pendant les sessions SMTP

Non (par défaut), MDaemon analyse les messages pendant la session SMTP afin de déterminer s'ils doivent être rejetés lorsque le score de spam est supérieur au seuil de rejet. Pour les messages acceptés, MDaemon effectue une autre analyse basée sur la file d'attente et traite les messages en conséquence, en fonction de leur score et de la configuration de votre filtre anti-spam. Cliquez sur cette option si vous souhaitez que MDaemon ne procède pas à l'analyse basée sur la file d'attente et traite les résultats de l'analyse initiale du Filtre anti-spam comme définitifs. Cela peut réduire considérablement l'utilisation du processeur et augmenter l'efficacité du système anti-spam. Non (par défaut), seuls les en-têtes SpamAssassin par défaut seront ajoutés aux messages lorsque l'analyse basée sur la file d'attente est omise. Si vous avez apporté des modifications aux en-têtes par défaut de SpamAssassin ou spécifié des en-têtes personnalisés dans votre fichierlocal.cf, ces modifications et ajouts seront ignorés.

Refususées en cas d'erreur lors de l'analyse SMTP

Cliquez sur cette option si vous souhaitez qu'un message soit refusé lorsqu'une erreur est rencontrée lors de son analyse au cours du processus SMTP.

Balise sujet

Cette balise sera insérée au début de l'en-tête Subject de tous les messages qui atteignent ou dépassent le seuil de score de spam requis. Elle peut contenir des informations sur le score de spam, et vous pouvez utiliser vos filtres de messages IMAP pour les rechercher et filtrer le message en conséquence (en supposant que vous ayez configuré le Filtre anti-spam pour qu'il continue à délivrer des messages de spam). Il s'agit d'une méthode simple pour le routage automatique des messages de spam vers un dossier "spam" désigné. Si vous souhaitez insérer dynamiquementle score de spam dumessageet la valeur du seuil de spam requis, utilisez la balise "_HITS_" pour lescore du messaget "_REQD_" pour le seuil requis. Vous pouvez également utiliser "_SCORE (0) _" au lieu de "_HITS_" - cela insérera un zéro initial dans les scores inférieurs, ce qui peut aider à assurer un ordre de tri correct lorsque les messages sont triés par sujet dans certains clients de messagerie.

Exemple,

Une balise d'objet définie comme suit : ***SPAM*** Score/Req : HITS / REQD -

fera ensorte qu'un message de spam avec un score de 6.2 et le sujet : "Hey, here'ssome spam !" soit modifié en "***SPAM*** Score/Req : 6.2/5.0 - Hey, here's some spam !"

Si "_SCORE (0)_" est substitué à "_HITS_", il sera remplacé par "***SPAM*** Score/Req : 06.2/5.0 - Hey, here'ssome spam !".

Si vous ne souhaitez pas modifier l'en-tête From, laissez cette option vide. Aucune balise d'objet ne sera insérée.



Cette option n'est pas disponible si vous avez configuré MDaemon pour qu'il utilise leMDaemon anti-spam (MDSpamD) d'unautre serveurpour le traitement du Filtre anti-spam. La configuration de la balise Sujet sera déterminée par lesparamètres de l'autre serveur.Voir : <u>Spam Daemon</u> [736], pour plus d'informations.

Sort du spam

Le Filtre anti-spam effectuera l'action choisie ci-dessous sile score de spam d'un messageest supérieur ou égal au score de spam spécifié ci-dessus.

... supprimer le spam immédiatement

Choisissez cette option si vous souhaitez simplement supprimer tout message entrant dont le score de spam est égal ou supérieur à la limite désignée.

...mettre le spam dans le Dossier Dossiers publics spam

Choisissez cette option si vous souhaitez marquer les messages comme étant du spam et les déplacer alors dans le Dossier public spam plutôt que de les autoriser à être distribués.

Envoyer le rapport sur le contenu du piège à spam au postmaster tous les jours Si vous utilisez l'option...placer le spam dans le Dossier public du piège à

spam ci-dessus, cochez cette case si vous souhaitez que le postmaster reçoive chaque jour un message contenant un résumé du contenu du dossier.

...signaler le spam mais le laisser poursuivre sa route

Filtrez par cette option si vous souhaitez que chaque message de spam soit livré à son destinataire, mais qu'il soit marqué comme spam par l'insertion de divers en-têtes et/ou balises de spam désignés ci-dessus et sur l'écran de<u>rapport</u>. Il s'agit de l'option par défaut, qui permet aux utilisateurs de profiter d'options telles que le filtrage du courrier dans un dossier de spams à des fins d'examen et d'éviter ainsi de perdre des messages susceptibles d'être étiquetés à tort comme des spams (c'est-à-dire des faux positifs).

Redémarrer le Filtre anti-spam

Cliquez sur ce bouton pour redémarrer le moteur du Filtre anti-spam.

4.7.1.2 Classification bayésienne

🧐 Filtre anti-spam - Classification bayésienne	
 Filtre anti-spam Filtre anti-spam Classification bayésienne Apprentissage bayésien Daemon anti-spam (MDSpamD) Liste blanche (automatique) Liste blanche (pas de filtrage) Liste blanche (destinataires) Liste blanche (expéditeurs) Liste noire (expéditeurs) Mises à jour Rapports Paramètres DNS-BL Pièges à spam 	ification bayésienne est un processus statistique permettant à une machine ndre". En analysant des centaines d'e-mails reconnus comme spams et non-spams, elle à détecter ces deux types de messages de façon plus précise au fil du temps. stiver la classification bayésienne ogrammer l'apprentissage bayésien tous les soirs à minuit Apprentissage ammer l'apprentissage bayésien toutes les O heures (0=jamais) as inclure les messages de plus de 50000 octets (0=pas de limite) stiver les adresses de transfert des spams et non-spams in du dossier des spams connus (faux négatifs) : in du dossier des non-spams connus (faux négatifs) : in du dossier des non-spams connus (faux négatifs) : in du dossier des non-spams connus (faux positifs) : in une fois traités, les messages sont supprimés des dossiers
	OK Annuler Appliquer Aide

La classification bayésienne n'est pas disponible lorsque vous avez configuré MDaemon pour qu'il utilise le MDaemon antispam (MDSpamD) d'un autre serveur pour le traitement du Filtre anti-spam. Tout l'apprentissage bayésien sera effectué sur l'autre serveur. Filtrer par l'écran<u>Spam Daemon</u> [736] pour plus d'informations.

Le Filtre anti-spam prend en charge l'apprentissage bayésien, qui est un processus statistique pouvant éventuellement être utilisé pour analyser les messages spam et non-spam afin d'augmenter la fiabilité de la reconnaissance du spam au fil du temps. Vous pouvez désigner un dossier pour les messages de spam et les messages non spam qui seront analysés manuellement ou automatiquement à intervalles réguliers. Tous les messages contenus dans ces dossiers seront analysés et indexés afin que les nouveaux messages puissent y être comparés statistiquement pour déterminer la probabilité qu'il s'agisse de spam. Le Filtre anti-spam peut alors augmenter ou diminuer lescore de spam d'un messageen fonction des résultats de sa comparaison bayésienne.

730

Le Filtre anti-spam n'appliquera pas de classification bayésienne aux messages tant qu'une analyse bayésienne n'aura pas été effectuée sur le nombre de messages spam et non-spam désignés sur l' écran d'<u>Apprentissage bayésien</u> <u>automatique</u>. 1734 Dans ce cas, le Filtre anti-spam dispose d'un ensemble de statistiques suffisant pour effectuer la comparaison bayésienne. Une fois que vous aurez donné au système ces messages à analyser, il sera suffisamment équipé pour commencer à appliquer les résultats d'une comparaison bayésienne auscore de spam de chaque message entrants. En continuant à analyser davantage de messages, les classifications bayésiennes deviendront de plus en plus précises au fil du temps.

Classification bayésienne

Activer la classification bayésienne

Cochez cette case si vous souhaitez que lescore de spam dechaque messagesoit ajusté sur la base d'une comparaison avec les statistiques bayésiennes actuellement connues.

Programmer l'apprentissage bayésien tous les soirs à minuit

Dans cette option, une fois par jour à minuit, le Filtre anti-spam analysera puis supprimera tous les messages contenus dans les dossiers spam et non-spam spécifiés ci-dessous. Si vous souhaitez programmer l'apprentissage bayésien pour un autre intervalle de temps, effacez cette option et utilisez l'option *Programmer l'apprentissage bayésien toutes les [xx] heures*. Si vous ne souhaitez pas que l'apprentissage bayésien se produise automatiquement, décochez cette option et indiquez "0" heure dans l'option ci-dessous.

Programmer l'apprentissage bayésien une fois toutes les [xx] heures (0 = jamais)

Si vous souhaitez que l'apprentissage bayésien se produise à un intervalle de temps autre qu'une fois chaque nuit à minuit, décochez l'option ci-dessus et indiquez un nombre d'heures dans cette option. Chaque fois que ce nombre d'heures sera écoulé, le Filtre anti-spam analysera et supprimera tous les messages contenus dans les dossiers spam et non-spam spécifiés ci-dessous. Si vous ne souhaitez pas que l'apprentissage bayésien se fasse automatiquement, décochez l'option ci-dessus et indiquez "0" heure dans cette option.

> Si, pour une raison quelconque, vous ne souhaitez pas que les messages soient supprimés après leur analyse, vous pouvez empêcher cela en copiant LEARN.BAT dans MYLEARN.BAT dans le sous-dossier SUPPRIMER LEESSAGE !, puis en supprimant les deux lignes commençant par "if exist" vers le bas de ce fichier. Dans ce dossier, lorsque le fichier MYLEARN.BAT est présent, MDaemon l'utilise à la place de LEARN.BAT. Voir SA-Learn.txt dans le sous-dossier MDaemon SpamAssassin pour plus d'informations.

Pour des informations plus détaillées sur la technologie de filtrage anti-spam heuristique et l'apprentissage bayésien, consultez :

http://www.spamassassin.org/doc/sa-learn.html.

Ne pas inclure les messages de plusde [xx] octets (0 = pas de limite)

Cette option permet de désigner une taille maximale de message pour l'analyse bayésienne. Les messages dont la taille est supérieure à cette valeur ne seront pas analysés. Par taille "0" dans cette option si vous ne souhaitez pas mettre en œuvre de restriction de taille.

Apprendre

Cliquez sur ce bouton pour lancer une analyse bayésienne manuelle des dossiers désignés plutôt que d'attendre l'analyse automatique.

Activer les adresses de transfert de spam et de courrier indésirable

Cochez cette case si vous souhaitez autoriser les utilisateurs à Transférer les messages spam et non-spam (ham) à des adresses désignées afin que le système bayésien puisse en tirer des enseignements. Les paramètres par défaut utilisés par MDaemon sont "SpamLearn@<domain>" et "HamLearn@<domain>". Les messages envoyés à ces adresses doivent être reçus via SMTP à partir d'une session authentifiée à l'aide de SMTP AUTH. De plus, MDaemon s'attend à ce que les messages soient transférés aux adresses ci-dessus sous forme de pièces jointes de type "message/rfc822". Tout message d'un autre type envoyé à ces adresses électroniques ne sera pas traité.

Vous pouvez modifier les adresses utilisées par MDaemon en ajoutant la clé suivante au fichierCFilter.INI:

```
[SpamFilter]
SpamLearnAddress@
HamLearnAddress=MyNonSpamLearnAddress@ (adresse d'apprentissage du
spam)
```

Remarque : le dernier caractère de ces valeurs doit être "@".

Créer

Cliquez sur ce bouton pour créer automatiquementdes <u>Dossiers publics IMAP</u> [116]spam et non-spam , et pour configurer MDaemon afin qu'il les utilise. Les dossiers suivants seront créés :

\Apprentissage bayésien.IMAP	Dossier IMAP racine
\Apprentissage bayésien.IMAP Apprendre comme spam.IMAP	Ce dossier est destiné aux Faux négatifs dans le filtrage de spams (les spams qui n'obtiennent pas un score suffisamment élevé pour être signalés comme tels).

élevé pour être marqués comme

\Apprentissage bavésien IMAP\NNon-Spam IMAP\N	Ce dossier est destiné aux Faux positifs dans le filtrage de spams
	(messages non spam qui obtiennent
	par erreur un score suffisamment

spam).

Par défaut, l'accès à ces dossiers n'est accordé qu'aux utilisateurs locaux des domaines locaux et est limité à la Recherche et à l'Insertion.Les autorisations par défaut dupostmastersont Lookup, Read, Insert et Delete.

Chemin d'accès au dossier spam connu (faux négatifs) :

Il s'agit du chemin d'accès au dossier qui sera utilisé pour l'analyse bayésienne des messages de spam connus. Ne copiez dans ce dossier que les messages que vous considérez comme du spam. Vous ne devez pas automatiser le processus de copie des messages dans ce dossier, à moins de le faire via les options<u>Apprentissage</u> bayésien automatique 734 ou Pièges à spam. 758 L'automatisation de ce processus par d'autres moyens pourrait potentiellement entraîner l'analyse de messages non spam en tant que spam, ce qui diminuerait la fiabilité des statistiques bayésiennes.

Chemin d'accès au dossier non-spam connu (faux positifs) :

Il s'agit du chemin d'accès au dossier qui sera utilisé pour l'analyse bayésienne des messages qui **ne**sont certainement **pas** des spams. Seuls les messages que vous ne considérez **pas** comme du spam doivent être copiés dans ce dossier. Vous ne devez pas automatiser le processus de copie des messages dans ce dossier, à moins de le faire via les options d'<u>Apprentissage bayésien</u> ⁷³⁴. L'automatisation de ce processus par d'autres moyens pourrait potentiellement entraîner l'analyse de messages de spam en tant que non-spam, ce qui diminuerait la fiabilité des statistiques bayésiennes.

Dossier public

Cliquez sur l'un de ces boutons pour désigner l'un de vos Dossiers publics existants comme Dossier public Bayesian. C'est un moyen facile pour vos utilisateurs de placer leurs messages incorrectement catégorisés comme spam ou non-spam dans vos répertoires bayésiens pour analyse. Notez toutefois qu'en donnant l'accès à un plus grand nombre de personnes, vous augmentez la probabilité que certains messages soient placés dans les mauvais dossiers, ce qui fausse les statistiques et diminue la fiabilité.

> Si vous renommez un dossier public via un client de messagerie, l'explorateur Windows ou tout autre moyen, vous devez réinitialiser manuellement ce chemin d'accès au nouveau nom de dossier approprié. Si vous renommez un dossier sans modifier son chemin d'accès, le Filtre anti-spam continuera à utiliser ce chemin d'accès pour le dossier Bayesian au lieu du nouveau.

Voir :

Apprentissage bayésien automatique

4.7.1.3 Apprentissage bayésien

🧐 Filtre anti-spam - Apprentissage bayésien	×
 Filtre anti-spam Filtre anti-spam Classification bayésienne Apprentissage bayésien Daemon anti-spam (MDSpamD) Liste blanche (automatique) Liste blanche (pas de filtrage) Liste blanche (destinataires) Liste blanche (expéditeurs) Liste noire (expéditeurs) Liste noire (expéditeurs) Mises à jour Rapports Paramètres DNS-BL Pièges à spam 	Apprentissage Automatique Activer l'apprentissage automatique bayésien Seuil de score des non-spams 0.1 Les messages dont le score est inférieur à ce seuil seront assimilés comme des non-spams. Seuil de score des spams 12.0 Les messages dont le score est supérieur à ce seuil seront assimilés comme des spams. Échantillons de non-spams nécessaires pour la classification bayésienne 200 Échantillons de spams nécessaires pour la classification bayésienne 200 Gestion de la base de données 200 Ø Activer l'expiration automatique des références du système bayésien 150000 À chaque expiration, MD aemon conserve 75 % des références ou 100 000 références. Un fichier de base de données de 8 Mo correspond approximativement à 150 000 références. Restaurer les paramètres par défaut du serveur
	OK Annuler Appliquer Aide

L'Apprentissage bayésien n'est pas disponible lorsque vous avez configuré MDaemon pour qu'il utilise leDaemon anti-spam (MDSpamD) d'un autre serveurpour le traitement du Filtre antispam. Tout l'apprentissage bayésien sera effectué sur l'autre serveur. Voir l'écran<u>Spam Daemon</u> 736 pour plus d'informations.

Apprentissage automatique

Activer l'apprentissage automatique bayésien

Dans le cadre de l'apprentissage bayésien automatique, vous pouvez définir des seuils de score pour le spam et le non-spam, ce qui permet au système

d'apprentissage bayésien d'apprendre automatiquement à partir des messages plutôt que de vous demander de placer manuellement ces messages dans les dossiers spam et non-spam. Tout message dont le score est inférieur au seuil de non-spam sera traité par l'apprentissage automatique comme non-spam, et tout message dont le score est supérieur au seuil de spam sera traité comme spam. Avec l'apprentissage automatique, les anciens jetons expirés qui sont supprimés de la base de données (voir *Gestion de la base de données* ci-dessous) peuvent être remplacés automatiquement. Il n'est donc pas nécessaire de procéder à un réapprentissage manuel pour récupérer les jetons périmés. L'Apprentissage automatique peut être utile et bénéfique si vous êtes prudent dans la définition de vos seuils, afin d'éviter de placer des messages mal classés dans les dossiers.

Seuils des scores de spam

Les messages dont le score de spam est inférieur à cette valeur seront traités comme des messages non spam par le système de classification bayésienne.

Seuils des scores de spam

Les messages dont le score de spam est supérieur à cette valeur seront traités comme des messages de spam par le système de classification bayésienne.

Échantillons de non-spam nécessaires pour que la classification bayésienne soit possible

Le Filtre anti-spam n'appliquera pas de classification bayésienne aux messages tant que ce nombre de messages non-spam (et de messages spam spécifiés dans l'option suivante) n'aura pas été analysé par le système bayésien. Dans ce cas, le Filtre anti-spam dispose d'un ensemble suffisant de Statistiques pour effectuer la comparaison bayésienne. Une fois que vous aurez donné au système ces messages à analyser, il sera suffisamment équipé pour commencer à appliquer les résultats d'une comparaison bayésienne auscore de spam dechaque message entrants. En continuant à analyser davantage de messages, les classifications bayésiennes deviendront de plus en plus précises au fil du temps.

Échantillons de spam nécessaires avant de pouvoir procéder à une classification bayésienne

Tout comme l'option précédente s'applique aux messages non spam, cette option permet de désigner le nombre de messages*spam* qui doivent être analysés avant que le Filtre anti-spam ne commence à appliquer une classification bayésienne aux messages.

Gestion de la base données

Activer l'expiration automatique des jetons bayésiens

Cliquez sur cette option si vous souhaitez que le système bayésien expire automatiquement les jetons de la base de données lorsque le nombre de jetons spécifié ci-dessous est atteint. La définition d'une limite de jetons permet d'éviter que la base de données bayésienne ne devienne trop volumineuse.

Nombre maximal de jetons de la base de données bayésienne

Il s'agit du nombre maximal de jetons de la base de données bayésienne autorisé. Lorsque ce nombre de jetons est atteint, le système bayésien supprime les plus anciens, réduisant ainsi le nombre de jetons à 75 % de cette valeur ou à 100 000 jetons, la valeur la plus élevée étant retenue. Le nombre de jetons ne tombera jamais en dessous de la plus grande de ces deux valeurs, quel que soit le nombre de jetons expirés. Remarque : 150 000 jetons de base de données représentent environ 8 Mo.

Restaurer les paramètres par défaut du serveur

Cliquez sur ce bouton pour restaurer les paramètres par défaut de toutes les options avancées de la méthode bayésienne.

Voir :

Classification bayésienne 730

4.7.1.4 Daemon anti-spam (MDSpamD)

 Filtre anti-spam Filtre anti-spam Classification bayésienne Apprentissage bayésien Daemon anti-spam (MDSpamD) Liste blanche (pas de filtrage) Liste blanche (pas de filtrage) 	Configuration de MDSpamD Hôte ou IP 127.0.0.1 Si MDSpamD est externe, envoyer "ping" toutes les 30 secondes (0=jamais) Options disponibles uniquement lorsque MDSpamD est exécuté en local Afficher MDSpamD dans une fenêtre de processus externe
 Liste blanche (destinataires) Liste blanche (expéditeurs) Liste noire (expéditeurs) Mises à jour Rapports Paramètres DNS-BL Pièges à spam 	Enregistrer l'activité locale de MDSpamD (débogage - ralentit les performances) Nombre maximal de threads de traitement des messages 4 (1 - 6) Nombre maximal de connexions TCP par thread 10 (10 - 200) I Écouter et accepter uniquement les connexions provenant de 127.0.0.1 Écouter les connexions sur cette IP (<alb ip):<="" les="" p="" signifie="" toutes=""> <alb< p=""> Autoriser les connexions provenant de ces IP : 127 10</alb<></alb>
	La notation CIDR et les adresses séparées par plusieurs espaces sont autorisées Options supplémentaires en ligne de commande

Le système de filtrage anti-spam de MDaemon fonctionne sous la forme d'un démon distinct, le Daemon anti-spam (MDSpamD), qui est alimenté en messages via TCP/IP pour l'analyse. Cela augmente considérablement lesperformances duFiltre anti-spamet vous permet d'exécuter MDSpamD localement, sur un ordinateur séparé, ou de demander à MDaemon d'utiliser un autre MDSpamD (ou tout autre produit compatible avec le Spam Daemon) s'exécutant à un autre endroit. Par défaut, MDSpamD s'exécute localement et reçoit les messages sur le port 783 à 127.0.0.1, mais vous pouvez configurer un port et une adresse IP différents si vous souhaitez envoyer les messages à un autre daemon anti-spam fonctionnant à un autre endroit ou sur un autre port.

Configuration de MDSpamD

Hôte ou IP

Il s'agit de l'adresse IP ou de l'hôte auquel MDaemon enverra les messages à analyser par MDSpamD. Utilisez 127.0.0.1 si MDSpamD est exécuté localement.

Port

Il s'agit du port sur lequel les messages seront envoyés. Le port par défaut de MDSpamD est 783.

Ping de MDSpamD distant une fois toutes les [xx] secondes (0 = jamais).

Si vous utilisez un Spam Daemon qui s'exécute à distance, vous pouvez utiliser cette option pour effectuer périodiquement un ping vers son emplacement. Utilisez "0" si vous ne souhaitez pas envoyer de ping à cet emplacement.

Ces options sont disponibles lors de l'exécution locale de MDSpamD

Afficher la fenêtre du processus externe de MDSpamD

Si MDSpamD est exécuté localement, activez cette option si vous souhaitez qu'il s'exécute dans une fenêtre de processus externe. La sortie de MDSpamD est alors dirigée vers la fenêtre du processus externe plutôt que vers l'interface utilisateur interne ou le système de journalisation de MDaemon.L'utilisation de cette option permet d'améliorer les performances carles données de MDSpamDn'ont pas besoin d'être acheminées et journalisées par MDaemon. Dans ce cas, aucun fichier journal n'est créé et cette fonctionnalité ne peut pas être utilisée avec l'option de journalisation ci-dessous. Les données de MDSpamD n'apparaissent pas non plus dans l' onglet *Sécurité* "*MDSpamD* de l'interface graphique principale de MDaemon.

Enregistrer toute l'activité locale de MDSpamD (Pas de journalisation de débogage)

Cliquez sur cette option si vous souhaitez journaliser toute l'activité de MDSpamD. Cette option n'est pas disponible si vous utilisez l'option*Afficher la fenêtre du processus externe de MDSpamD* ci-dessus. En outre, si vous utilisez les informations d'identification de l'utilisateur dans la boîte de dialogue <u>Service Windows</u> [537] plutôt que d'exécuter MDaemon sous le compte SYSTEM, aucune activité de MDSpamD ne sera journalisée.

> Dans le cas où vous utilisez cette option de journalisation, il se peut que les performances de votre système de messagerie diminuent, en fonction de votre système et du niveau d'activité. En règle générale, vous ne devez utiliser cette option qu'à des fins de débogage.

Nombre maximal de threads de traitement des messages (1-6)

Il s'agit du nombre maximum de threads que MDaemon utilisera pour le traitement interne. Cette valeur peut être comprise entre 1 et 6.

Nombre maximum de connexions TCP par thread (10-200)

Il s'agit du nombre maximum de connexions TCP acceptées par un thread MDSpamD avant qu'il ne passe à un autre thread. Cette valeur peut être comprise entre 10 et 200.

Écouter et accepter les connexions uniquement à partir de 127.0.0.1

Cliquez sur cette option si vous ne souhaitez pas autoriser votre MDSpamD local à accepter des connexions en provenance de n'importe quelle source externe. Seules les connexions provenant de la même machine que celle sur laquelle il est exécuté seront autorisées.

Écouter les connexions sur cette IP

Si l'option précédente est désactivée, vous pouvez utiliser cette option pour lier ou limiter les connexions à cette adresse IP spécifique. Seules les connexions à l'adresse IP désignée seront autorisées. Utilisez"<all>" si vous ne souhaitez pas restreindre MDSpamD à une adresse IP particulière.

Connexions autorisées à partir de ces adresses IP

Il s'agit des adresses IP à partir desquelles MDSpamD acceptera les connexions provenant de cette IP. Les connexions provenant d'autres adresses IP seront rejetées. Ceci est utile si vous souhaitez autoriser les connexions à partir d'un autre serveur afin de partager le traitement du Filtre anti-spam.

Options supplémentaires en ligne de commande :

MDSpamD peut accepter de nombreuses options de ligne de commande, documentées à l'adresse suivante :

http://spamassassin.apache.org/

Si vous souhaitez utiliser l'une de ces options, construisez une chaîne contenant les options souhaitées et placez-la ici.



Certaines de ces options peuvent être configurées via les paramètres de cette boîte de dialogue et n'ont donc pas besoin d'être configurées manuellement à l'aide des options de la ligne de commande.

4.7.1.5 Liste d'autorisation (automatique)

🧐 Filtre anti-spam - Liste blanche (automatiq	que)
 Filtre anti-spam Filtre anti-spam Classification bayésienne Apprentissage bayésien Daemon anti-spam (MDSpamD) Liste blanche (automatique) Liste blanche (pas de filtrage) Liste blanche (destinataires) Liste blanche (expéditeurs) Liste noire (expéditeurs) Mises à jour Rapports Paramètres DNS-BL Pièges à spam 	Inscription automatique sur liste blanche Remarque : certains de ces paramètres sont globaux. Les comptes doivent être configurés individuellement pour utiliser certaines options (voir l'Éditeur de compte). Utiliser les contacts, liste blanche et liste noire personnels Seules les adresses authentifiées via DKIM sont enregistrées sur liste blanche Mettre les contacts de la liste blanche à jour automatiquement Avec cette option, les adresses auxquelles un utilisateur envoie du courrier sont ajoutées à sa liste blanche Supprimer les contacts sans nom ni numéro de téléphone Mettre à jour la liste blanche lorsqu'un message est transféré à blacklist@ Mettre à jour la liste noire lorsqu'un message est transféré à blacklist@ Lorsqu'un message est transféré à ces adresses, l'expéditeur est ajouté à la liste blanche ou noire du compte. Mettre le moteur bayésien à jour avec les copies des messages inscrits sur liste blanche MD aemon analyse les messages en liste blanche afin de s'assurer qu'ils ne seront plus considérés comme du spam.
	OK Annuler Appliquer Aide

Automatique Liste d'autorisation

Utiliser les contacts personnels, les expéditeurs autorisés et les expéditeurs bloqués Cliquez sur cette option pour utiliser les contacts personnels de chaque utilisateur, ainsi que les expéditeurs autorisés et bloqués pour le filtrage anti-spam de cet utilisateur. Pour chaque message entrant, MDaemon recherche l'expéditeur du message dans les contacts ducompte destinataire et dans les listes d'expéditeurs autorisés et bloqués. Si l'expéditeur est trouvé, le message est automatiquement autorisé ou bloqué. Si vous ne souhaitez pas appliquer la liste automatique d'autorisation et de blocage à chaque utilisateur de MDaemon, vous pouvez la désactiver pour les utilisateurs individuels en décochant l' option *Le Filtre anti-spam utilise les contacts personnels, les expéditeurs autorisés et les expéditeurs bloqués* dans l' écran Liste expéditeurs de l'Éditeur de compte.

...n'autoriser que les adresses de la liste qui s'authentifient à l'aide de DKIM Lorsque cette option est activée, MDaemon ne met pas le message sur liste d'autorisation si l'expéditeur n'a pas été authentifié via <u>DomainKeys Identified</u> <u>Mail</u> (DKIM). Cette option permet d'éviter d'inscrire dans la liste les messages dont l'adresse a été usurpée. Cette option est désactivée par défaut.

Ajouter automatiquement les destinataires des e-mails aux expéditeurs autorisés Lorsque cette option est activée, MDaemon ajoute automatiquement les destinataires à la liste des expéditeurs autorisés dès qu'un utilisateur envoie du

courrier à une adresse électronique non locale. Dans le cadre de l'option"*Utiliser les contacts personnels, les expéditeurs autorisés et les expéditeurs bloqués*" cidessus, le nombre de faux positifs du Filtre anti-spam peut être considérablement réduit.

Si vous ne souhaitez pas appliquer cette option à tous les utilisateurs de MDaemon, vous pouvez la désactiver pour chaque utilisateur en décochant la case "Ajouter automatiquement les destinataires du courrier aux expéditeurs autorisés" dans l 'écranListe expéditeurs [813] de l'Éditeur de compte.



Cette option est désactivée pour les comptes utilisant des autorépondeurs.

Supprimer les contacts dont le nom ou le numéro de téléphone est manquant

Cliquez sur ce bouton si vous souhaitez supprimer tous les contacts qui ne contiennent qu'une adresse électronique du dossier Contacts par défaut de chaque utilisateur. Si un contact n'a pas au moins un nom ou des données téléphoniques, il sera supprimé. Cette option a pour but d'aider les utilisateurs de la Liste d'autorisation automatique de MDaemon antérieure à la version 11 à supprimer les contacts qui ont été ajoutés uniquement dans le cadre de la Liste d'autorisation. Dans les versions précédentes de MDaemon, les adresses étaient ajoutées aux contacts principaux au lieu d'être placées dans un dossier Expéditeurs autorisés dédié. Les utilisateurs peuvent donc se retrouver avec de nombreuses entrées dans leurs contacts qu'ils préfèreraient ne pas voir figurer.



Redirection vers les mises à jour d'Expéditeurs autorisés de allowlist@

Lorsque cette option est activée, les comptes utilisant l'option "*Le Filtre anti-spam utilise les contacts personnels, les expéditeurs autorisés et les expéditeurs bloqués*" dans l'écran Paramètres de l'Éditeur de comptepeuvent Transférer les messages à allowlist@<domain> et faire en sorte que MDaemon ajoute l'expéditeur du message d'origine à ce domaine. L'adresse autorisée est extraite de l'en-tête From du message transféré.

Les messages transférés à allowlist@<domain> doivent être transmis sous forme de pièces jointes de type message/rfc822, et MDaemon doit les recevoir via SMTP à partir d'une session authentifiée. Les messages transférés qui ne remplissent pas ces conditions ne seront pas traités.

Vous pouvez modifier l'adresse utilisée par MDaemon en modifiant la clé suivante dans le fichierCFILTER.INI:

```
[SpamFilter]
WhiteListAddress=MyAllowListAddress@
```

Remarque : le dernier caractère doit être "@".

La redirection vers blocklist@ met à jour les expéditeurs bloqués

Lorsque cette option est activée, les comptes utilisant l'option "*Le Filtre anti-spam utilise les contacts personnels, les expéditeurs autorisés et les expéditeurs* bloqués " dans l'écran Paramètres de l'Éditeur de comptepeuvent Transférer les messages à blocklist@<domaine> et demander à MDaemon d'ajouter l'expéditeur du message d'origine aux expéditeurs bloqués. L'adresse bloquée est extraite de l'En-tête From du message Transféré.

Les messages transférés à blocklist@<domaine> doivent être transmis sous forme de pièces jointes de type message/rfc822, et MDaemon doit les recevoir via SMTP à partir d'une session authentifiée. Les messages transférés qui ne répondent pas à ces exigences ne seront pas traités.

Mettre à jour le moteur bayésien avec les copies des Liste d'autorisation des messages Cochez cette case pour que les messages qualifiés soient copiés automatiquement dans le dossier Apprentissage automatique comme non-spam de Bayesian (désigné dans l'écran<u>Bayesian</u>⁷³⁰). Cela permet d'automatiser le processus consistant à fournir au moteur bayésien des échantillons de messages non spam. Le fait de fournir régulièrement au moteur bayésien de nouveaux exemples de messages non spams à partir desquels il peut apprendre augmentera sa fiabilité au fil du temps et contribuera à réduire le nombre de faux positifs (c'est-à-dire de messages classés par erreur comme spams).

Pour bénéficier de cette fonctionnalité, un message entrants doit être adressé à un utilisateur local et l'expéditeur doit figurer dans son carnet d'adresses ou dans son dossier Expéditeurs autorisés. Si le message est sortant, il doit alors s'agir d'un destinataire figurant dans le carnet d'adresses ou des Expéditeurs autorisés. Si vous ne souhaitez pas que les messages sortants soient qualifiés, utilisez le Bloc-notes pour modifier le paramètre suivant dans le fichierCFILTER.INI:

```
[SpamFilter]
UpdateHamFolderOutbound=No (par défaut = Oui)
```

Si un message est qualifié, il est copié dans le dossier d'apprentissage comme nonspam de Bayesian, même si l'apprentissage programmé de Bayesian est désactivé dans l'écran Bayesian. Ainsi, lorsque l'apprentissage programmé est activé ultérieurement, ou lorsque l'apprentissage est activé manuellement, un ensemble de messages non-spam est prêt à être analysé. Cependant, tous les messages admissibles ne sont pas copiés dans le dossier d'apprentissage. Lorsque la fonction est activée, MDaemon copie les messages qualifiés jusqu'à ce qu'un certain nombre soit atteint. Par la suite, il copiera des messages individuels à des intervalles déterminés. Non (par défaut), les 200 premiers messages qualifiés sont copiés, puis tous les dix messages qualifiés. Le nombre initial de messages copiés est égal au nombre indiqué dans l'option "Échantillons de non-spam nécessaires avant que l'apprentissage bayésien ne soit possible" située dans l'écran Apprentissage bayésien automatique. 734 Si vous modifiez ce paramètre, cette valeur sera également modifiée. Si vous souhaitez modifier l'intervalle selon leguel les messages suivants sont copiés, vous pouvez le faire en modifiant le paramètre suivant dans le fichierMDaemon.ini:

```
[SpamFilter]
HamSkipCount=10 (Non (par défaut))
```

Enfin, une fois qu'un certain nombre de messages a été copié, le processus recommence : 200 messages sont copiés, puis tous les 10 (ou une autre valeur si vous avez modifié ces paramètres). Non (par défaut), le processus sera relancé après la copie de 500 messages de qualification. Vous pouvez modifier cette valeur en éditant le paramètre suivant dans le fichierMDaemon.ini :

[SpamFilter] HamMaxCount=500 (par défaut, 500)

> Cette option n'est pas disponible si vous avez configuré MDaemon pour qu'il utilise leMDaemon anti-spam (MDSpamD) d'unautre serveurpour le traitement du Filtre anti-spam. Toutes les fonctions d'apprentissage bayésien sont déterminées par lesparamètres de l'autre serveur et sont exécutées sur ce dernier. Voir <u>Spam Daemon</u> [736] pour plus d'informations.

4.7.1.6 Liste d'autorisation (pas de filtrage)

🧐 Filtre anti-spam - Liste blanche (pas de filtra	ge)
 Filtre anti-spam Filtre anti-spam Classification bayésienne Apprentissage bayésien Daemon anti-spam (MDSpamD) Liste blanche (automatique) Liste blanche (qast de filtrage) Liste blanche (destinataires) Liste blanche (expéditeurs) Liste noire (expéditeurs) Liste noire (expéditeurs) Mises à jour Rapports Paramètres DNS-BL Pièges à spam 	# Liste des exceptions du Filtre anti-spam. # Ce fichier est utilisé pour définir les critères des messages qui ne sont pas an # filtre anti-spam. Les messages doivent contenir un en-tête/une valeur corres # de ce fichier pour être exempts du filtrage. # si vous n'indiquez pas d'en-tête (juste une valeur), alors cette valeur # est comparée à celle de l'enveloppe SMTP RCPT. Si vous indiquez 'From'' # en-tête, alors cette valeur est comparée à la fois avec celle de l'en-tête 'Fror # et celle de l'enveloppe SMTP MAIL. # Les caractères jokers ? et * sont acceptés - Une entrée par ligne. # "vuser01@exemple.com" # From "user02@exemple.com # Reply-To "@domaine123.exemple.com # Subject Ceci est un exemple de sujet
	Les messages envoyés à ces adresses ne sont pas traités par le Filtre Avancé
	OK Annuler Appliquer Aide

Les messages envoyés à ces adresses ne sont pas du tout filtrés.

Cliquez sur **Avancé** dans cet écran pour désigner les adresses des destinataires que vous souhaitez voir Exclure du Filtre anti-spam. Les messages destinés à ces adresses ne seront pas traités par le filtre anti-spam.

Cet écran n'est pas disponible si vous avez configuré MDaemon pour qu'il utilise leMDaemon anti-spam (MDSpamD) d'un autre serveurpour le traitement du Filtre anti-spam. Cette liste de Filtre anti-spam sera maintenue sur l'autre serveur. Voir <u>Spam</u> <u>Daemon</u> pour plus d'informations.

4.7.1.7 Liste d'autorisation (destinataires)



Les messages envoyés à ces adresses reçoivent un score avantageux

Cliquez sur **Avancé** pour ajouter des adresses à cette liste. Cette liste est similaire à <u>Liste d'autorisation (pas de filtrage)</u> [742], sauf qu'au lieu d'exempter les messages destinés au destinataire du traitement par le Filtre anti-spam, ils seront traités mais verront leur <u>score au Filtre anti-spam</u> [726] réduit du montant spécifié dans l'écran<u>Paramètres du Filtre anti-spam</u>. [749] Par conséquent, l'ajout d'une adresse à cette liste d'autorisation ne garantit pas automatiquement qu'un message adressé à cette adresse ne sera pas considéré comme du spam. Exemple : si le seuil du score de spam est fixé à 5,0 et la valeur de la liste d'autorisation à 100, et qu'un message de spam particulièrement excessif arrive et obtient un score de 105,0 ou plus avant la soustraction de la valeur de la liste d'autorisation, le score de spam final du message sera d'au moins 5,0, ce qui le désignera comme du spam. C'est toutefois très peu probable, car le spam a rarement une valeur aussi élevée, à moins qu'il ne contienne un autre élément dont le score est exceptionnellement élevé, tel qu'une une adresse bloquée.

> Cet écran n'est pas disponible si vous avez configuré MDaemon pour qu'il utilise le MDaemon anti-spam (MDSpamD) d'un autre serveur pour le traitement du Filtre anti-spam. Cette liste de Filtre anti-spam sera maintenue sur l'autre serveur. Voir <u>Spam</u> <u>Daemon</u> 738 pour plus d'informations.

4.7.1.8 Liste d'autorisation (expéditeurs)



Les messages envoyés à partir de ces adresses reçoivent un score avantageux

Cliquez sur **Avancé** pour ajouter des adresses à cette liste. Cette liste d'autorisation est similaire à la liste d'autorisation (par destinataire). Liste d'autorisation est similaire à la *Liste d'autorisation (par destinataires*) [743], sauf que la réduction du score du filtre anti-spam est basée sur l'*expéditeur du* message plutôt que sur le destinataire. Les messages provenant de ces expéditeurs verront leur <u>score au</u> Filtrage [726] anti-spam [749] réduit du montant spécifié dans l'écran <u>Paramètres du Filtre anti-spam</u>. [749] Par conséquent, l'inclusion d'une adresse dans cette liste d'autorisations ne garantit pas automatiquement qu'un message adressé à cette adresse ne sera pas considéré comme du spam. Exemple : si le seuil du score de spam est fixé à 5,0 et la valeur de la liste d'autorisation à 100, et qu'un message de spam particulièrement excessif arrive et obtient un score de 105,0 ou plus avant la soustraction de la valeur de la liste d'autorisation, le score de spam final du message sera d'au moins 5,0, ce qui le désignera comme du spam. C'est toutefois très peu probable, car le spam a rarement une valeur aussi élevée, à moins qu'il ne contienne un autre élément dont le score est exceptionnellement élevé, tel qu'une une adresse bloquée.

Cet écran n'est pas disponible si vous avez configuré MDaemon pour qu'il utilise leMDaemon anti-spam (MDSpamD) d'un autre serveurpour le traitement du Filtre anti-spam. Cette liste de Filtre anti-spam sera maintenue sur l'autre serveur. Voir <u>Spam</u> <u>Daemon</u> [736] pour plus d'informations.

4.7.1.9 Liste de blocage (expéditeurs)

🧐 Filtre anti-spam - Liste noire (expéditeurs)	
 Filtre anti-spam Filtre anti-spam Classification bayésienne Apprentissage bayésien Daemon anti-spam (MDSpamD) Liste blanche (automatique) Liste blanche (pas de filtrage) Liste blanche (destinataires) Liste blanche (expéditeurs) Liste blanche (expéditeurs) Mises à jour Rapports Paramètres DNS-BL Pièges à spam 	####################################
	OK Annuler Appliquer Aide

Les messages envoyés à partir de ces adresses reçoivent une note négative.

Cliquez sur **Avancé** pour ajouter des adresses à cette liste. Les messages provenant d'adresses figurant sur cette Liste de blocage verront leur <u>score au Filtre anti-</u> <u>spam</u> [726] augmenté du montant spécifié dans l'écran<u>Paramètres du Filtre anti-</u> <u>spam</u> [749], ce qui entraîne généralement leur marquage en tant que spam. Toutefois, l'ajout d'une adresse à cette liste ne garantit pas automatiquement qu'un message provenant de cette adresse sera toujours considéré comme du spam. Exemple : si un message provient d'un expéditeur bloqué mais qu'il est adressé à l'adresse suivante Expéditeurs bloqués, mais qu'il est adressé à un destinataire autorisé, les modificateurs de score peuvent se compenser et faire en sorte que le score final du message soit inférieur au seuil du score de spam. Cela peut également se produire si le modificateur de score de la liste de blocage est réglé à un niveau particulièrement bas. liste de blocage est particulièrement bas.

> Cet écran n'est pas disponible si vous avez configuré MDaemon pour qu'il utilise le MDaemon anti-spam (MDSpamD) d'un autre serveurpour le traitement du Filtre anti-spam. Cette liste de Filtre anti-spam sera maintenue sur l'autre serveur. Voir <u>Spam</u> <u>Daemon</u> [736] pour plus d'informations.

4.7.1.10 Mises à jour

🦻 Filtre anti-spam - Mises à jour	
 Filtre anti-spam Filtre anti-spam Classification bayésienne Apprentissage bayésien Daemon anti-spam (MDSpamD) Liste blanche (automatique) Liste blanche (pas de filtrage) Liste blanche (destinataires) Liste blanche (expéditeurs) Liste noire (expéditeurs) Mises à jour Rapports Paramètres DNS-BL Pièges à spam 	Mises à jour du Filtre anti-spam ✓ Activer les mises à jour du Filtre anti-spam MD aemon peut vérifier automatiquement les mises à jour du moteur heuristique afin d'éviter que les fichiers de détection du spam ne deviennent obsolètes. Les vérifications s'effectuent une fois par jour. ✓ Envoyer une notification par e-mail avec les résultats de la mise à jour Options supplémentaires en ligne de commande pour SA-UPDATE : Vérifier les mises à jour maintenant
	OK Annuler Appliquer Aide

Mises à jour du Filtre anti-spam

Activer les mises à jour du Filtre anti-spam

Cochez cette case si vous souhaitez que le Filtre anti-spam soit mis à jour automatiquement. Une fois par jour, MDaemon vérifiera si des mises à jour sont disponibles pour le moteur anti-spam. Si c'est le cas, il les téléchargera et les installera automatiquement.

Envoyer un e-mail de notification avec les résultats de la mise à jour

Utilisez cette option si vous souhaitez envoyer un e-mail aux administrateurs à chaque fois que le Filtre anti-spam est mis à jour, contenant les résultats de la mise à jour. Cette option est la même que l'option "*Envoyer une notification de mise à jour du Filtre anti-spam aux administrateurs*" située à : Filtre de contenu | Notifications.

Options supplémentaires en ligne de commande pour SA-UPDATE

Utilisez cette option avancée si vous souhaitez transmettre des options de ligne de commande à SA-UPDATE.

Rechercher les mises à jour maintenant

Cliquez sur ce bouton pour vérifier immédiatement la mise à jour des règles du Filtre anti-spam.

4.7.1.11 Rapports

🧐 Filtre anti-spam - Rapports	
 Filtre anti-spam Filtre anti-spam Classification bayésienne Apprentissage bayésien Daemon anti-spam (MDSpamD) Liste blanche (automatique) Liste blanche (qas de filtrage) Liste blanche (destinataires) Liste blanche (expéditeurs) Liste noire (expéditeurs) Liste noire (expéditeurs) Paramètres DNS-BL Pièges à spam 	 Rapports Insérer un rapport du filtre anti-spam dans l'en-tête du message d'origine Cochez cette case pour ajouter un en-tête au spam entrant. Aucune modification ne sera faite sur le corps du message ni sur le message d'origine Créer un message et y joindre le message d'origine Cochez cette case pour créer un message contenant un rapport sur le spam. Le message d'origine sera joint au format MIME (RFC 822). Créer un message et y joindre le message d'origine au format text/plain Cochez cette case pour créer un message contenant un rapport sur le spam. Le message d'origine sera joint au format MIME (RFC 822). Créer un message et y joindre le message contenant un rapport sur le spam. Le message d'origine sera joint au format MIME (text/plain)
	OK Annuler Appliquer Aide

Les options du Filtre anti-spam ne sont pas disponibles si vous avez configuré MDaemon pour qu'il utilise leMDSpamD (MDaemon anti-spam) d'unautre serveurpour le traitement du Filtre anti-spam. Les Paramètres duFiltre anti-spam seront contrôlés par les paramètres de l'autre serveur.Filtrer par l'écran<u>Spam Daemon</u>

Rapport

Insérer le rapport de spam dans l'en-tête du message d'origine

Il s'agit de l'option de rapport par défaut. Utilisez cette option si vous souhaitez que le Filtre anti-spam insère un rapport de spam dans les en-têtes dechaque message de spam.Voici un exemple de rapport de spam simple :

```
X-Spam-Report : ---- De Filtre anti-spam résultats
5,30 points, 5 requis ;
* -5.7 -- Message ID indique que le message a été envoyé depuis MS
Exchange
* 2.0 -- Le sujet contient beaucoup d'espaces blancs
* -3.3 -- Dans l'en-tête TO : * 3.0 -- Le message contient beaucoup
d'espace blanc
* 3.0 -- Le message a été marqué par le DNS-BL de AMaemon
* 2.9 -- BODY : Remède contre l'impuissance
* 2.2 -- BODY : Parle de l'exercice avec une exclamation !
* 0.5 -- BODY : Le message est 80% à 90% HTML
* 0.1 -- BODY : HTML inclus dans le message
* 1.6 -- BODY : Le message HTML est une page web sauvegardée
* 2.0 -- Date : est 96 heures ou plus avant la date de réception.
```

---- À la fin des résultats du Filtre anti-spam

Créer un nouveau message et y joindre le message original

Choisissez cette option de rapport si vous souhaitez que le spam entraîne la création d'un nouveau message électronique contenant le rapport de spam. Le message d'origine du spam y sera inclus en tant que pièce jointe.

Identique à l'option précédente, mais en joignant le message en tant que texte/plain

Comme l'option de rapport précédente, cette option génère le rapport de spam sous la forme d'un nouveau message qui inclut le message de spam original en tant que pièce jointe. La différence est que le message original sera joint en utilisant le type MIME text/plain. Étant donné que le spam contient parfois un code HTML unique pour chaque message et qu'il peut potentiellement révéler au spammeur l'adresse électronique et l'adresse IP qui l'ont ouvert, cette méthode permet d'éviter que cela ne se produise en convertissant le code HTML en texte brut.

4.7.1.12 Paramètres

🧐 Spam Filter - Settings	×		
 Spam Filter Spam Filter Bayesian Classification Bayesian Auto-learning Spam Daemon (MDSpamD) Allow List (automatic) Allow List (no filtering) Allow List (by recipient) Allow List (by sender) Block List (by sender) Updates Reporting Settings DNS-BL Spam Honeypots 	Settings Is DNS service available? Yes No ● Test Do not filter mail from local sources I trusted or authenticated sources Do not filter messages larger than 20 MB (1-39, 0 = no limit) Image: Close SMTP sessions when spam is detected Image: MAP spam folder automatically Image: Do not forward spam Image: Sort allow and block list entries An allow list match subtracts this many points from the spam score 100.0 A block list match adds this many points to the spam score 100.0		
Ok Cancel Apply Help			

Paramètres

Le service DNS est-il disponible ?

Ces options vous permettent de choisir si le service DNS est disponible ou non pour le Filtre anti-spam lors du traitement des messages. Vous pouvez choisir l'une des options suivantes :

- **Oui** Le service DNS est disponible. SURBL/RBL et les autres règles qui nécessitent une connectivité DNS seront donc utilisées.
- Non Le DNS n'est pas disponible. Les règles de filtrage anti-spam qui nécessitent une connexion DNS ne seront pas utilisées.
- **Test** La disponibilité du DNS sera testée et s'il est présent, il sera utilisé. Non (par défaut).

Ne pas filtrer les messages provenant de

sources locales

Cochez cette case si vous souhaitez que les messages provenant d'utilisateurs et de domaines locaux soient exemptés de filtrage.

sources fiables ou authentifiées

Activez cette option si vous souhaitez que les messages provenant de domaines de confiance ou d'expéditeurs authentifiés soient exemptés du filtrage anti-spam.

Ne pas filtrer les messages supérieursà [xx] MB MB (1-99, 0 = aucune limite) Dans la plupart des cas, les messages de spam sont relativement petits, car l'objectif des spammeurs est d'envoyer le plus grand nombre de messages possible en un minimum de temps. Si vous souhaitez que les messages dépassant une certaine taille ne soient pas soumis au filtrage anti-spam, indiquez ici la taille (en Mo). (en Mo). Utilisez "0" si vous ne souhaitez pas fixer de limite de taille de message pour le filtrage anti-spam.

Fermer les sessions SMTP en cas de détection de spam

Cette option est activée par défaut et ferme une session SMTP si une analyse en ligne détecte un message de spam.

Déplacerautomatiquement les spamsdans le dossier IMAP de l'utilisateur

Cliquez sur cette option pour que MDaemon place automatiquement chaque message que le Filtre anti-spam considère comme du spam dans le dossier IMAP"spam" dechaque utilisateur(si un tel dossier existe). Il créera également automatiquement ce dossier pour chaque Nouveau compte utilisateur ajouté.

Lorsque vous cliquez sur cette option, un message vous demande si vous souhaitez que MDaemon crée ce dossier pour chacun de vos Dossiers utilisateurs existants. Si vous choisissez " Oui ", un dossier sera créé pour tous les utilisateurs. Si vous choisissez " Non ", un dossier ne sera créé que lors de l'ajout d'un nouvel utilisateur. Les Dossiers existants pour certains ou tous vos utilisateurs ne seront pas modifiés ou affectés de quelque manière que ce soit.

Ne pas transférer les spams

Cochez cette case si vous ne souhaitez pas que les messages de spam soient transférés.

Trier les entrées de la liste d'autorisation/de blocage

Utilisez cette option si vous souhaitez que les entrées de la liste anti-spam - liste anti-spam - soient triées dans l'ordre. **Remarque :** si vous avez ajouté vos propres commentaires au fichier (lignes commençant par #), l'activation de cette option triera ces lignes en tête du fichier. Cette fonctionnalité est désactivée par défaut. Si vous activez l'option, le tri sera effectué lors de la prochaine modification du fichier d'autorisation/de liste blocage.

> Les autres options de cet écran ne sont pas disponibles si vous avez configuré MDaemon pour qu'il utilise le MDaemon anti-spam (MDSpamD) d'un autre serveurpour le traitement du Filtre antispam. Voir l' écran <u>Spam Daemon</u> [736] pour plus d'informations.

Une correspondance avec la liste d'autorisation soustrait autant de points au score de spam.

Le fait de placer une adresse sur les écrans <u>Liste d'autorisation (par destinataire)</u> [743] ou <u>Liste d'autorisation (par expéditeur)</u> [744] du Filtre anti-spam ne garantit pas automatiquement qu'un message à destination ou en provenance de cette adresse ne sera pas considéré comme du spam. Au lieu de cela, ces adresses Au lieu de cela,

ces adresses verront simplement le montant spécifié dans cette commande soustrait de leur score de spam. Exemple : si le Seuils des scores de spam est fixé à 5.0 et cette valeur à 100, et qu'un message de spam particulièrement excessif arrive et obtient un score de 105.0 ou plus avant que la valeur de la liste d'autorisation ne soit soustraite, le Seuils des scores de spam de la liste d'autorisation sera automatiquement soustrait de son score de spam. soit soustraite, le score de spam final du message sera d'au moins 5,0, ce qui signifie qu'il s'agit d'un spam. Toutefois, cela se produit rarement, car le spam a rarement une valeur aussi élevée, à moins qu'il ne contienne un autre élément dont le score est exceptionnellement élevé, tel que une adresse figurant sur la liste de blocage. Bien entendu, si vous fixez la valeur de soustraction de la liste la valeur de soustraction de la liste de blocage à un niveau beaucoup plus bas, le spam se produirait alors beaucoup plus fréquemment.

> Si vous souhaitez que les messages adressés à certains destinataires contournent complètement le Filtre anti-spam plutôt que de simplement ajuster leurs scores, incluez ces adresses de destinataires dans la <u>Liste d'autorisation (pas de</u> <u>filtrage)</u> (742). Vous pouvez également exclure les messages de l'évaluation du Filtre anti-spam en fonction de l'expéditeur en utilisant les options de l' écran Liste d<u>'autorisation</u> <u>(automatique)</u>, (739)

Une correspondance avec la Liste de blocage ajoute ce nombre de points au score de spam

Cette valeur est ajoutée au score de spam des messages provenant d'adresses figurant sur l' écran<u>Liste de blocage (expéditeurs)</u> 745). Comme pour l'option liste anti-spam ci-dessus, l'inclusion d'une adresse dans laliste anti-spam du Filtre anti-spamne garantit pas qu'un message provenant de cette adresse sera considéré comme du spam. Dansce cas, la valeur spécifiée dans cette option sera ajoutée auscore de spam dumessage, qui sera alors utilisé pour déterminer si le message est un spam ou non.

4.7.2 DNS-BL

Les listes de blocage DNS (DNS-BL) peuvent être utilisées pour empêcher les courriers électroniques non sollicités d'atteindre vos utilisateurs. Cette fonction de sécurité vous permet de spécifier plusieurs services de liste de blocage DNS (qui tiennent à jour des listes de serveurs connus pour relayer les spams) qui seront vérifiés chaque fois que quelqu'un tentera d'envoyer un message à votre serveur. Si l'IP de connexion a été répertoriée par l'un de ces services, le serveur sera bloqué. répertoriée par l'un de ces services, le serveur sera bloqué. répertoriée par l'un de ces services, le serveur sera bloqué. répertoriée par l'un de ces services, le serveur sera bloqué. Repertoriée par l'un de ces services, le serveur sera bloqué. Repertoriée par l'un de ces services de services de serveur sera bloqué. Repertoriée par l'un de ces services de serveur sera bloqué.

DNS Les listes de blocage comprennent une Liste d'autorisation pour désigner les adresses IP que vous souhaitez exempter des requêtes DNS-BL. Avant d'activer la liste de blocage DNS, vous devez vous assurer que votre plage d'adresses IP locales figure sur la liste d'autorisation afin d'empêcher les recherches sur ces adresses. L'adresse "127.0.0.1" est exclue et n'a donc pas besoin d'être ajoutée à la liste.

Voir :

Hôtes DNS-BL 752 Paramètres DNS-BL 754 Liste d'autorisation DNS-BL 753

4.7.2.1 Hôtes

🧐 Filtre anti-spam - Hôtes	
Filtre anti-spam DNS-BL Liste des exceptions Paramètres Pièges à spam	Certains hôtes DNS-BL possèdent des prérequis pour l'utilisation de leurs services (voir le fichier http://www.spamhaus.org). Si vous ne respectez pas les prérequis d'un hôte DNS-BL spécifique, il est conseillé de ne pas utiliser cet hôte et de le supprimer de la liste configurée ci-dessous. Activer les requêtes DNS-BL Hôtes DNS-BL - Le contenu du champ "Message" est envoyé en tant que réponse SMTP [zen.spamhaus.org, \$IP\$ listed at spamhaus, see http://www.spamhaus.org Supprimer Hôte DNS-BL Le contenu du champ "Message" est envoyé en tant que réponse SMTP [zen.spamhaus.org, \$IP\$ listed at spamhaus, see http://www.spamhaus.org Supprimer Hôte DNS-BL
	OK Annuler Appliquer Aide

Hôtes DNS-BL

Activer les requêtes DNS-BL

Activez cette option si vous souhaitez vérifier le courrier entrant par rapport aux DNS Listes de blocage. MDaemon interrogera chaque hôte répertorié lorsqu'il effectuera une recherche DNS-BL sur l'Adresse IP d'envoi. Si un hôte répond à la requête avec un résultat positif, MDaemon peut marquer le message ou le refuser, en fonction des options que vous avez activées dans l' écran<u>Paramètres DNS-BL</u> 1754].

Supprimer

Sélectionnez une entrée dans la liste des services DNS-BL et cliquez sur ce bouton pour la supprimer de la liste.

Hôtes DNS-BL

Si vous souhaitez ajouter un nouvel hôte à interroger pour les adresses IP de la liste de blocage, saisissez-le ici. les adresses IP bloquées, saisissez-le ici.

Test

Saisissez un hôte dans l'option*Hôtes DNS-BL* et cliquez sur ce bouton pour le tester en recherchant 127.0.0.2.

Message

Il s'agit du message qui peut être envoyé au cours de la session SMTP lorsqu'une adresse IP a été répertoriée par l'hôte DNS-BL correspondant listé ci-dessus. Ce message correspond à l' option ...et répondre par 'Message' plutôt que 'utilisateur inconnu' située dans l' écranOptions DNS-BL 754.

Ajouter

Après avoir saisi un hôte et un message renvoyer, cliquez sur ce bouton pour l'ajouter à la liste des hôtes DNS-BL.

4.7.2.2 Liste d'autorisation

Siltre anti-spam - Liste des exceptions	×			
Filtre anti-spam DNS-BL Hötes Hötes Hötes Paramètres Pièges à spam Pièges à spam # Liste blanche DNS-BL # Liste blanche DNS-BL # Ce fichier regroupe les adresses IP des sites exclus des vérifications DNSBL. # Il est conseillé dy inclure toutes les IP locales ainsi que l'adresse 127.0.0.1. Vous # pouvez également y ajouter les adresses IP inscrites par erreur sur liste noire, ou que # vous souhaitez toujours exclure du processus de vérification DNS-BL. # Use conseillé dy inclure toutes les IP locales ainsi que l'adresses 127.0.0.1. Vous # pouvez également y ajouter les adresses Prinscrites par erreur sur liste noire, ou que # vous souhaitez toujours exclure du processus de vérification DNS-BL. # The injuitant des adresses d'expéditeurs précédées du # ten ajoutant des adresses d'expéditeurs précédées du # to "from" (sans les guillemets), les messages envoyés contenant ces adresses dans la seront enregistrés sur liste blanche. Celte fonctionnalité pred en compte # la valeur MALL FROM de la session SMTP, et non cellé de len-tête From: du message. # Uses caractères jokers sont pris en charge. Une entrée par ligne. # 127.0.0.1 # arve@alin.com # from "@alin.com <td></td>				
OK Annuler Appliquer Aide				

Cet écran permet de désigner les adresses IP qui seront exemptées des requêtes DNS Liste de blocage. Vous devriez toujours inclure votre plage d'adresses IP locales afin d'empêcher la liste de blocage DNS de rechercher des messages provenant d'utilisateurs et de domaines locaux (c'est-à-dire 127.0.0.*, 192.168.*.*, etc.). Vous pouvez également inclure des adresses électroniques dans la liste. Lorsqu'un message est adressé à l'une d'entre elles, il est accepté quels que soient les résultats des recherches DNS-BL. Enfin, vous pouvez également exempter des expéditeurs spécifiques des résultats de la recherche DNS-BL en inscrivant "from *sender@example.com" dans la liste.* Cette adresse doit correspondre à la valeur "MAIL FROM" de la session SMTP, et non à l'en-tête "From :" du message.

Ne placez qu'une seule entrée sur chaque ligne. Les caractères génériques sont autorisés.

4.7.2.3 Paramètres

🧐 Spam Filter - Settings		—
Spam Filter DNS-BL Hosts Allow List Settings Spam Honeypots	Check IPs within 'Received' headers on SMTP delivered mail Check only this many 'Received' headers (0 = all) Skip this many of the most recent 'Received' headers (0 = none) Skip this many of the oldest 'Received' headers (0 = none)	0
	Check IPs within 'Received' headers on POP3 collected mail Check only this many 'Received' headers (0 = all) Skip this many of the most recent 'Received' headers (0 = none) Skip this many of the oldest 'Received' headers (0 = none)	0 1 1
	Settings DNS-BL match adds this many points to the spam score Don't check DNS-BLs if session is authenticated Don't check DNS-BLs if session is from a trusted IP Don't check DNS-BLs if session is an ATRN dequeue Skip 'Received' headers within messages from IPs on allow list Stop further DNS-BL queries on first DNS-BL match SMTP server should refuse mail from block-listed IPs and respond with 'Message' rather than 'user unknown' Auto-filter block-listed mail into user's spam folder	3.0
	Ok Cancel Apply	Help

Vérifier les IP dans les en-têtes "Received" pour le Courrier distribué en SMTP

Cliquez sur ce bouton si vous souhaitez que les Listes de blocage DNS vérifient l'adresse IP indiquée dans les en-têtes"Received" des messages reçus via SMTP.

Vérifier uniquement ce nombre d' en-têtes "Received" (0 = tout)

Indiquez le nombre d'en-têtes "Received" que vous souhaitez que DNS-BL vérifie, en commençant par le plus récent. La valeur "O" signifie que tous les entêtes "Received" seront vérifiés.

Skip this many of the most recent 'Received' en-têtes (0 = aucune)

Utilisez cette option si vous voulez que DNS-BL saute un ou plusieurs des entêtes "Received" les plus récents lors de la vérification des messages SMTP.

Sauter ce nombre d'en-têtes 'Received' les plus anciens (0 = aucune)

Utilisez cette option si vous voulez que DNS-BL saute un ou plusieurs des entêtes 'Received' les plus anciens lors de la vérification des messages SMTP.

Vérifier les IP dans les en-têtes 'Received' pour le courrier collecté en POP3 Lorsque ce commutateur est activé, DNS-BL vérifiera l'adresse IP estampillée dans les en-têtes "Received" des messages collectés via DomainPOP et MultiPOP.

Vérifier seulement ce nombre d' en-têtes 'Received' (0 = tout)

Indiquez le nombre d'en-têtes "Received " que vous souhaitez que DNS-BL vérifie, en commençant par le plus récent. Une valeur de "0" signifie que tous les en-têtes "Received " seront vérifiés.

Skip this many of the most recent 'Received' en-têtes (0 = aucune)

Utilisez cette option si vous voulez que DNS-BL saute un ou plusieurs des entêtes "Received" les plus récents lors de la vérification des messages DomainPOP et MultiPOP. Comme il est souvent nécessaire d'ignorer l'entêteReceived le plus récent dans le courrier collecté en POP3 tel que DomainPOP, cette option a un paramètre par défaut de "1".

Skip this many of the oldest 'Received' en-têtes (0 = aucune)

Utilisez cette option si vous voulez que DNS-BL saute un ou plusieurs des entêtes "Received" les plus anciens lors de la vérification des messages DomainPOP et MultiPOP.

Paramètres

Le match DNS-BL ajoute ce nombre de points au score de spam

Utilisez cette option pour spécifier une valeur qui sera ajoutée au<u>score de spam</u> d'un message lorsqu'une correspondance DNS-BL est trouvée. Il arrive que l'examen heuristique d'un message par le Filtre anti-spamne lui attribue pas un score suffisamment élevé pour qu'il soit considéré comme du spam, mais qu'une recherche DNS-BL indique qu'il l'est. L'ajout de cette valeur au score de spam peut donc permettre d'attraper certains messages de spam qui pourraient autrement passer inaperçus. Non (par défaut), une correspondance DNS-BL ajoute 3,0 points au score de spam.

Ne pas vérifier les DNS-BL si la session est...

authentifiée

Cochez cette case si vous souhaitez que les sessions authentifiées à l'aide de la commande AUTH soient exemptées des requêtes DNS-BL.

à partir d'une IP autorisées

Cochez cette case si vous voulez que les adresses "<u>Hôtes autorisés</u>" soient exclues des requêtes DNS-BL.

d'une file d'attente ATRN

Activez cette option si vous ne souhaitez pas effectuer de recherches DNS-BL sur le courrier collecté via des sessions de retrait de file d'attente ATRN. Ce paramètre est désactivé par défaut, mais vous pouvez l'activer si, par exemple, votre Hôte relais par défaut effectue déjà des vérifications DNS-BL sur votre courrier stocké.

Ignorer les en-têtes "Received" dans les messages provenant d'adresses IP figurant dans la liste d'autorisation

Lorsque cette option est activée, la liste DNS-BL ne vérifiera pas les en-têtes "Received" dans les messages provenant d'adresses IP que vous avez listées dans la Liste Exceptions DNS-BL

Arrêter d'autres requêtes DNS-BL lors de la première correspondance DNS-BL

Souvent, il y a plusieurs hôtes contenus dans les en-têtes de chaque message que la DNS-BL traite, et plusieurs services DNS-BL qui sont interrogés. Par défaut, la base de données DNS-BL continuera à interroger ces services pour tous les hôtes dans le message, quel que soit le nombre de correspondances trouvées. Cliquez sur cette option si vous voulez que DNS-BL arrête d'interroger les services pour un message donné dès qu'une correspondance est trouvée.

Le serveur SMTP doit refuser le courrier provenant d'IP bloquées.

Par défaut, cette case n'est pas cochée, ce qui signifie que les messages provenant d'adresses IP bloquées ne seront pas refusés pendant la session SMTP, mais qu'un en-têteX-MDDNSBL-Result sera inséré. Vous pouvez alors utiliser le Filtre de contenu pour Chercher les messages dans cet en-tête et en faire ce que vous voulez. Vous pouvez également utiliser l'option "*Filtrer automatiquement les messages de la liste de blocage dans le dossier anti-spam* de l'utilisateur " ci-dessous pour filtrer les messages automatiquement dans le dossier anti-spam de chaque utilisateur. Cochez cette case si vous souhaitez que MDaemon refuse les messages provenant d'adresses IP bloquées plutôt que de les marquer.

> Certaines adresses IP pouvant être bloquées par erreur, il convient d'être prudent avant de choisir de refuser des messages plutôt que de simplement les marquer d'un drapeau. Il convient également de noter qu'en plus de marquer un message, vous pouvez ajuster son score de spam en fonction des résultats du DNS-BL via l' option *La correspondance DNS-BL ajoute ce nombre de points au score de spam* situé dans le Filtre anti-spam

...et répondre par 'Message' plutôt que par 'utilisateur inconnu'

Cliquez sur cette option si vous souhaitez que le message spécifique que vous avez attribué à l'<u>Hôtes DNS-BL</u>⁷⁵² soit transmis au cours de la session SMTP chaque fois qu'une adresse IP est trouvée dans la liste. Dans le cas contraire, un message "utilisateur inconnu" sera transmis à la place. Cette option n'est disponible que si vous avez choisi d'utiliser l'option "*Le serveur SMTP doit refuser le courrier provenant d'IP bloquées*" ci-dessus.

Filtrer automatiquement le courrier inscrit sur la liste de blocage dans le dossier spam de l'utilisateur

Cliquez sur cette option et un dossier IMAP "Dossiers courrier "sera créé pour tous les futurs comptes utilisateurs que vous ajouterez à MDaemon. MDaemon créera également un Filtrage du courrier pour chacun de ces utilisateurs, qui recherchera l'
en-têteX-MDDNSBL-Result et placera les messages contenant cet en-tête dans le dossier spam de l'utilisateur.Lorsque vous cliquez sur cette option, il vous sera également demandé si vous souhaitez ou non que MDaemon crée ce dossier et ce filtre pour chacun de vos comptes utilisateurs déjà existants. Voir *Génération automatique d'un dossier et d'un filtre anti-spam pour chaque compte* ci-dessous.

Création automatique d'un dossier et d'un filtre anti-spam pour chaque compte

MDaemon peut créer automatiquement un dossier IMAP " Courrier indésirable " pour chaque compte et générer un filtre de courrier qui déplacera les messages dans ce dossier chaque fois qu'il trouvera un X-MDDNSBLBL. chaque fois qu'il trouve l'en-tête X-MDDNSBL-Result. Lorsque vous cliquez sur l' option Filtre automatique des courriers bloqués dans le dossier anti-spam de l'utilisateur, vous avez la possibilité de créer le dossier et le filtre qui l'accompagne pour tous les comptes. Il vous suffit de choisir "oui" dans la boîte de dialogue pour créer les dossiers et les filtres. Bien gu'elle ne soit pas infaillible, cette méthode est facile et généralement fiable pour aider vos utilisateurs à identifier rapidement les messages électroniques non sollicités ; elle peut empêcher efficacement les messages non sollicités d'être mélangés à tous les messages légitimes. Ils n'auront qu'occasionnellement besoin de vérifier le contenu de leur dossier spam pour s'assurer qu'un message important ne s'y trouve pas accidentellement (ce qui peut parfois se produire). Lors de la création des dossiers et des filtres pour vos comptes, si MDaemon constate qu'un compte possède déjà un filtre qui vérifie l'existence de l'en-tête X-MDDNSBL-Result, aucune action ne sera entreprise et aucun filtre ne sera créé pour ce compte. Si vous souhaitez que le nom du dossier IMAP soit autre chose que " Courrier indésirable ", vous pouvez modifier le paramètre par défaut en modifiant l' option *Dossier spam par défaut* située dans l' écran <u>Système</u> sous Configuration " Préférences".

4.7.3 Pièges à spam

🧐 Filtre anti-spam - Pièges à spam	X
Filtre anti-spam - Pièges à spam Filtre anti-spam DNS-BL Pièges à spam	Les pièges à spam sont des adresses locales destinées à recevoir le spam. Elles ne doivent jamais être attribuées à des utilisateurs. Ajoutez ces adresses dans les destinataires de messages de forums ou de listes de diffusion publiques. Elles recevront rapidement de nombreux spams. Le filtre anti-spam ainsi que d'autres mesures de sécurité ne s'appliquent pas aux messages envoyés à un piège à spam. Ils sont directement envoyés dans le dossier d'apprentissage bayésien. Activer les pièges à spam Activer les pièges à spam Activer les pièges à spam Activer les pièges à spam
	OK Annuler Appliquer Aide

L'option Pièges à spam (située dans Sécurité | Filtre anti-spam | Pièges à spam) permet de désigner des adresses électroniques locales conçues spécialement pour collecter des spams. Ces pots de miel ne sont pas des comptes MDaemon ou des alias d'adresses valides et ne doivent jamais être utilisés pour envoyer ou recevoir des emails légitimes. Cependant, en publiant une adresse de pot de miel dans un groupe de discussion, une liste de diffusion publique ou toute autre source à partir de laquelle les spammeurs obtiennent souvent des adresses, vous devriez commencer à voir des messages entrants adressés aux pots de miel de spam - vous pourriez également obtenir des adresses à partir d'autres spams que vous avez reçus et qui sont adressés à d'autres adresses locales invalides. Les pots de miel ne recevant jamais d'adresses électroniques légitimes, tous les messages entrants qui leur sont adressés seront toujours routés directement vers votre dossier d'apprentissage bayésien du spam pour être traités. dossier d'apprentissage bayésien du spam 🖚 pour y être traités. En outre, les adresses IP des serveurs expéditeurs peuvent, en option, être ajoutées au système de filtrage dynamique de l Écran dynamique (m), ce qui permet de filtrer les connexions futures à partir de ces adresses pendant une période déterminée. Tout cela contribue à augmenter la probabilité d'identifier et de bloquer les spams à l'avenir.

Points d'intérêt pour le spam

Cette liste contient toutes les adresses que vous avez désignées comme étant des pots de miel pour le spam.

Activer les pots de miel de spam

Cette option est activée par défaut. Décochez cette case si vous souhaitez désactiver la fonctionnalité des pots de miel pour spam.

Nouveau pot de miel de spam

Pour ajouter un pot de miel de spam, entrez l'adresse ici et cliquez sur Ajouter.

Supprimer

Pour supprimer un pot de miel de spam, sélectionnez l'adresse souhaitée et cliquez sur Supprimer.

Soumettre les IP d'envoi au système d'Écran dynamique

Cochez cette case si vous souhaitez soumettre au système d'<u>Écran</u> <u>dynamique</u> [603] toutes les adresses IP à partir desquelles un message Pièges à spam arrive. L'Écran dynamique (situé dans Sécurité | Paramètres de sécurité | Écran | Écran dynamique) doit être activé sur votre serveur pour que cette fonction soit disponible.

Envoyer une notification lorsqu'une IP est bloquée

Par défaut, lorsqu'une adresse IP soumise est bloquée par le système d'Écran dynamique, les options *Rapports du blocage des adresses IP de l* ⁽¹⁾Écran dynamique seront utilisées pour vous notifier cette action. Décochez cette case si vous ne souhaitez pas être averti lorsqu'une adresse IP est bloquée en raison de la fonction de soumission de Pièges à spam.

4.7.4 Data Query Service

760

🧐 Spam Filter - Data Query Service (DQS)	
 Spam Filter Spam Filter Bayesian Classification Bayesian Auto-learning Spam Daemon (MDSpamD) Allow List (automatic) Allow List (by recipient) Allow List (by recipient) Allow List (by sender) Block List (by sender) Updates Reporting Settings DNS-BL Spam Honeypots Data Query Service (DQS) 	Data Query Service (DQS) is a set of DNSBLs, updated in real-time, operated by Spamhaus Technology. Click here to learn about Spamhaus DQS. DQS key must be valid in order for this option to work. Click here for Spamhaus DQS registration.
	Ok Cancel Apply Help

Data Query Service (DQS) est un ensemble de DNSBL 751, mis à jour en temps réel et géré par Spamhaus Technology afin de bloquer plus de 99% des menaces véhiculées par le courrier électronique. Le service Clé DQS nécessite un abonnement valide et une clé d'utilisation fournie par Spamhaus Technology. Pour utiliser le service DQS :

- 1. Activez votre essai gratuit du Data Query Service.
- 2. Cliquez sur Activer DQS.
- 3. Saisissez votre Clé DQS de Spamhaus.
- 4. Cliquez sur **Ok**.



5 Menu Comptes

5.1 Gestionnaire de comptes

Pour mieux gérer la sélection, l'ajout, la suppression ou la modification de vos comptes, MDaemon contient le Gestionnaire de comptes. Cette boîte de dialogue permet d'accéder aux informations du compte et peut être utilisée pour trier les comptes par boîte aux lettres, domaine, nom réel ou dossier courrier. Le Gestionnaire des comptes se trouve dans le menu Comptes, à l'adresse suivante : Comptes | Gestionnaire des comptes...

Arricher les comptes	contenant			dans le	e champ BAL 🔻 🔻	OK
iste des comptes - 7	au total, 6 affichés	s (6 compte(s) utilisateur(s), 1	compte(s) système	e)		
Boîte aux lettres	Domaine	Nom réel	Groupes	Nbre de messages	Disque utilisé	Dernier
🤣 Bill.Farmer	company.test	Bill Farmer	N/A	1	0.0 (MB)	<unkno< td=""></unkno<>
🦿 Frank. Thomas	company.test	Frank Thomas	N/A	1	0.0 (MB)	Kunkno
🧼 harry.mudd	example.com	Harcourt Fenton Mudd	N/A	1	0.0 (MB)	Kunkno
🕖 michael.mason	company.test	Michael Mason	N/A	39	0.6 (MB)	Kunkho
🥜 Randy.Peter	company.test	Randy Peterman	N/A	1	0.0 (MB)	<unkno< td=""></unkno<>
🎺 Sir.Smith	company.test	Sir Smith	N/A	1	0.0 (MB)	<unkno< td=""></unkno<>
•						•
<i>«</i> 1 1 .	le ce domaine	Tous los domainos		- Nouv	eau Modifier	Supprime

Gestion des comptes

Au-dessus de la liste des comptes, vous verrez deux statistiques concernant la liste. Le premier chiffre est le nombre total de comptes utilisateurs MDaemon qui existent actuellement sur votre système. Le deuxième chiffre est le nombre de ces comptes actuellement affichés dans la liste. Les comptes qui seront affichés dépendent de ce que vous avez choisi dans l' option*Afficher uniquement les comptes de ce domaine* sous la liste. Si vous avez sélectionné "Tous les domaines", tous vos comptes MDaemon seront affichés dans la liste. Il existe une option de recherche en haut de cette boîte de dialogue que vous pouvez utiliser pour définir exactement quels comptes seront affichés au-delà du simple domaine auquel ils appartiennent.

Chaque entrée de la liste contient une icône Statut du compte (voir ci-dessous), la boîte aux lettres, le domaine auquel elle appartient, le "vrai nom" du titulaire du compte, les groupes auxquels le compte appartient, le nombre de messages, l'espace disque utilisé (en Mo), la dernière fois que le compte a été consulté et le dossier courrier dans lequel les messages sont stockés. Cette liste peut être triée par ordre croissant ou décroissant selon la colonne de votre choix. Dans n'importe quel titre de colonne,

cliquez sur cette colonne pour trier la liste par ordre croissant. Cliquez à nouveau sur la colonne pour la trier par ordre décroissant.

Non (par défaut), 500 comptes seulement sont affichés à la fois dans cette liste. Si vous voulez voir plus de comptes du domaine actuellement sélectionné (ou de Tous les domaines, si vous avez sélectionné cette option), vous devez cliquer sur le bouton *Afficher plus de comptes* pour afficher les 500 suivants. Si vous souhaitez afficher plus de 500 comptes à la fois, ouvrez le fichier MDaemon.ini et modifiez la cléMaxAccountManagerEntries=500 pour la valeur de votre choix.

Icônes de statut du compte

- Ce compte est administrateur global ou de domaine.
- Compte à accès total. Les accès POP et IMAP sont activés.
- Compte à accès limité. L'accès POP, IMAP ou les deux sont désactivés.
- Le compte est figé. MDaemon accepte toujours le courrier pour ce compte, mais l'utilisateur ne peut ni envoyer ni consulter du courrier.
- Con
 - Compte désactivé. Tous les accès au compte sont désactivés.

Nouveau

Cliquez sur ce bouton pour ouvrir l'<u>Éditeur de comptes</u> afin de créer un nouveau compte.

Modifier vos

Sélectionnez un compte dans la liste, puis cliquez sur ce bouton pour l'ouvrir dans l'<u>Éditeur de compte</u> [765]. Vous pouvez également double-cliquer sur le compte pour l'ouvrir.

Supprimer

Sélectionnez un compte dans la liste et cliquez sur ce bouton pour le supprimer. Il vous sera demandé de confirmer votre décision de supprimer le compte avant que MDaemon ne procède.

Afficher uniquement les comptes de ce domaine

Sélectionnez "Tous les domaines " dans cette liste déroulante pour afficher tous les comptes MDaemon. Sélectionnez un domaine spécifique pour n'afficher que les comptes dece domaine.

Afficher plus de comptes

La liste des comptes n'affiche que 500 comptes à la fois. Si le domaine que vous avez choisi contient plus de 500 comptes, cliquez sur ce bouton pour afficher les 500 suivants. Voir la note ci-dessus pour savoir comment augmenter le nombre maximum de comptes pouvant être affichés.

Haut de page

Cliquez sur ce bouton pour vous déplacer rapidement vers le haut de la liste des comptes.

Importer

Cliquez sur ce bouton si vous souhaitez importer des comptes à partir d'un fichier texte délimité par des virgules. Ce bouton est identique à la sélection de menu Comptes | Importer | Importer des comptes à partir d'un fichier texte délimité par des virgules .

Modèles

Cliquez sur ce bouton pour ouvrir la boîte de dialogue <u>Groupes et modèles</u>, à partir de laquelle vous pouvez gérer les paramètres par défaut des <u>Nouveaux</u> <u>comptes</u> will et contrôler l'appartenance aux groupes de comptes.

Supprimer de la liste

Sélectionnez un ou plusieurs comptes, puis cliquez sur ce bouton si vous souhaitez les désinscrire de toutes les Listes de diffusion [287] hébergées sur le serveur. Une boîte s'ouvrira pour vous demander de confirmer la décision de supprimer les adresses des listes.

Voir :

<u>Mon compte</u> ୮୫ଟି <u>Nouveau Modèles de comptes</u> ୟୋ

Menu Comptes	765
--------------	-----

5.1.1 Éditeur de compte

5.1.1.1 Informations générales

👶 Account Editor - Frank Thomas	
 Account Editor - Frank Thomas Account Settings Account Details Mail Services Web Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases Shared Folders App Passwords Signature Administrative Roles Allow List Settings ActiveSync 	Account Status Account is ENABLED (can check, send, and receive email) Account is DISABLED (can not check, send, or receive email) Account is FRDZEN (can receive but can not send or check email) Account Details First and last name Frank Thomas Mailbox domain company.test Mailbox name frank.thomas New password (twice) AD authentication: disabled AD name (optional) Account must change mailbox password before it can connect Password never expires for this account Description (visible in account's public address book data)
	Created on : Tue Oct 4 2016 8:13PM Last access: Wed Oct 20 2021 01:31 PM Ok Cancel Apply Help

Statut du compte

Ce compte est ACTIVÉ (peut consulter, envoyer et recevoir des e-mails) Non (par défaut), le compte peut consulter, envoyer et recevoir des e-mails.

Le compte est DÉSACTIVÉ (ne peut pas consulter, envoyer et recevoir des e-mails) Sélectionnez cette option si vous souhaitez désactiver tout accès au compte. L'utilisateur ne pourra plus accéder au compte par aucun moyen, ou MDaemon n'acceptera plus de courrier pour ce compte. Il ne sera pas supprimé et comptera toujours dans le nombre de comptes utilisés dans lalimite de votre licence, mais MDaemon fonctionnera comme si le compte n'existait pas, à une exception près : les dossiers qui ont été partagés avec d'autres utilisateurs pourront toujours être accédés par ces derniers, conformément aux permissions de l'ACL du dossier.

Le compte est FIGÉ (peut recevoir mais ne peut pas envoyer ou consulter des e-mails) Sélectionnez cette option si vous souhaitez autoriser le compte à recevoir des messages entrants, mais l'empêcher de vérifier ou d'envoyer des messages. Cette option est utile lorsque, par exemple, vous soupçonnez que le compte a été piraté. Figer les comptes empêcherait l'utilisateur malveillant d'accéder à ses messages ou d'utiliser le compte pour envoyer des messages, mais il serait toujours en mesure de recevoir ses messages entrants.

Informations générales du compte

Prénom et nom

Saisissez ici le prénom et le nom de l'utilisateur. Lors de la création d'un nouveau compte, certains champs des différents écrans de l'Éditeur de compte (par exemple, *Nom Boîte aux lettres* et *Dossier courrier*) seront automatiquement remplis lors de la saisie du Prénom et du Nom et du choix du *Domaine de courrier*. Vous pouvez toutefois modifier ces valeurs par défaut. Le champ Prénom et Les nom ne peut pas contenir " ! " ou " | ".

Domaine de la BAL

Utilisez cette liste déroulante pour spécifier le domaine auquel ce compte appartiendra et qui sera utilisé dans son adresse électronique. Le <u>Domaine par</u> <u>défaut de</u> 184 MDaemon apparaît par défaut dans la liste déroulante.

Nom de la BAL

Il s'agit de la partie de l'adresse électronique du compte qui le différencie des autres comptes du domaine. L'adresse électronique complète (c'est-à-dire [*Nom de la boîte aux lettres*]@[*Domaine de la boîte aux lettres*]) est utilisée comme identifiant unique pour le compte et comme login pour POP3 & IMAP, Webmail, etc. Les adresses électroniques ne peuvent pas contenir d'espaces ni de caractères " ! "ou " | ". N'utilisez pas "@" dans cette option. Exemple : utilisez "frank.thomas" et non "frank.thomas@".

Nouveau mot de passe (deux fois)

Dans le cas où vous souhaiteriez modifier le mot de passe du compte, tapez-en un nouveau ici, une fois dans chaque case. Il s'agit du mot de passe que le compte utilisera lorsqu'il se connectera à MDaemon pour envoyer ou recevoir des e-mails via POP3 ou IMAP, lorsqu'il s'authentifiera au cours du processus SMTP, ou lorsqu'il utilisera Webmail, Remote Admin, ou MDaemon Connector. Si les mots de passe ne correspondent pas ou s'ils ne respectent pas les restrictions de mot de passe [915], ces deux cases seront surlignées en rouge. Dans le cas contraire, elles seront en vert.

Si vous utilisez l'<u>authentification Active Directory</u> pour ce compte, vous devez alors saisir deux barres obliques inverses suivies du domaine Windows auquel l'utilisateur appartient, au lieu de saisir un mot de passe (par exemple, \\NALTN au lieu de 123Password). Sous les champs de mot de passe, une courte déclaration indique si l'authentification AD est activée ou désactivée pour le compte.

> Le compte doit avoir un mot de passe même si vous ne souhaitez pas autoriser l'accès POP3 & IMAP au compte de messagerie. Si vous souhaitez empêcher l'accès POP/IMAP, utilisez les options situées dans l' écran <u>Services de</u> <u>messagerie.</u> Tool Si vous souhaitez empêcher tout accès, utilisez les options*Compte est DÉSACTIVÉ* ou *Compte est FIGÉ* cidessus.

Nom AD (facultatif)

Utilisez ce paramètre si vous souhaitez spécifier un nom de compte Active Directory facultatif pour accéder au compte.

Le compte doit changer de mot de passe avant de se connecter

Cochez cette case si vous souhaitez demander au compte de modifier le *mot passe desa boîte aux lettres* avant de pouvoir accéder à POP, IMAP, SMTP, Webmail ou MDaemon Remote Admin. L'utilisateur peut se connecter au Webmail ou au MDaemon Remote Admin, mais il lui sera demandé de changer son mot passe avant de continuer. Filtrer les mots de passe dans le Webmail et le MDaemon Remote Admin est une tâche difficile pour les utilisateurs. Filtrer les mots de passe dans le Webmail et le MDaemon Remote Admin est une tâche difficile pour les utilisateurs, qui doivent d'abord obtenir l'autorisation d'accès au Web "...modifier le mot de passe" dans l'écran des Services *Web.* Une fois le mot de passe modifié, cette option sera désactivée.



Comme il peut être difficile ou impossible pour certains utilisateurs de modifier le mot de passe, il convient de faire preuve de prudence avant d'activer cette option.

Le mot de passe n'expire jamais pour ce compte

Cochez cette case si vous souhaitez exempter le compte de l'option d'expiration du mot de passe située dans la boîte de dialogue<u>Mots de passe.</u>

Description

Utilisez cette zone de texte si vous souhaitez ajouter une description publique du compte.

Cette description est incluse dans la fiche de contact public du compte et peut être consultée par d'autres personnes. N'incluez pas d'informations privées ou sensibles dans ce champ. Pour les notes privées ou les commentaires concernant ce compte, utilisez l'espace prévu à cet effet dans l' écran<u>Rôles d'administration.</u>

Sécurité du Compte (Cette section n'est disponible que dans MDRA)

E-mail Récupération de Mot de Passe

Il s'agit d'une adresse électronique alternative que vous pouvez utiliser pour accéder à votre compte via le Webmail si vous oubliez le *mot de passe de*votre *boîte aux lettres*. Si vous essayez de vous connecter au Webmail avec un mot de passe incorrect, un lien "Mot de passe oublié ?" apparaîtra. Ce lien vous conduit à une page qui vous demande de confirmer votre adresse e-mail de Récupération de Mot de Passe. Si vous saisissez l'adresse électronique correcte, un message électronique sera envoyé avec un lien vers une page où vous pourrez modifier votre mot de passe.

Identifiants WebAuthn d'Administration à Distance WebAuthn et Messagerie Web Ces deux sections listent les identifiants WebAuthn que vous avez configurés pour l'ouverture de session sans mot de passe ou l'Authentification à deux étapes pour MDRA ou Webmail. Si vous le souhaitez, vous pouvez retirer tout identifiant listé en le sélectionnant et en cliquant sur le bouton**X Retirer**correspondant.

Voir :

 Authentification AD
 D

 Mots de passe
 915

 Mon compte
 Services web

5.1.1.2 Dossier de courrier et groupes

	Mail Folder
Account Settings	
Account Details	C:\MDaemon\Users\company.test\frank.thomas\ Browse
Mail Services	
Web Services	All mail messages which arrive for this account will be stored in View
Autoresponder	
- Forwarding	Group membership
Restrictions	Groups
Quotas	Dent A: Users in Denartment A
Attachments	Dept R, Users in Department R
MAP Filters	
MultiPOP	
Aliases	
Shared Folders	
Ann Passwords	
Signature	
Administrative Boles	
Allow List	
Settings	
ActiveSunc	
Activesync	

Dossier de courrier :

Saisissez le dossier dans lequel vous souhaitez stocker les messages électroniques de ce compte. Lors de la création d'un nouveau compte, l'emplacement par défaut de ce dossier est basé sur le paramètre de dossier de messagerie désigné dans le modèle Nouveaux comptes. *Dossier courrier* désigné dans le <u>modèle Nouveaux</u> <u>comptes</u>

Afficher

Cliquez sur ce bouton pour ouvrir le <u>Gestionnaire de files d'attente/stats</u> dans le Dossier courrier de l'utilisateur.

Ce compte appartient au(x) groupe(s)

Utilisez cette case pour ajouter le compte à un ou plusieurs groupes accesses. Cochez la case en regard de chaque groupe auquel vous souhaitez que le compte adhère.

Voir :

<u>Modèle Nouveaux comptes</u> ଌ୶୭ <u>Groupes</u> ଛେଚି

5.1.1.3 Services de messagerie

👶 Account Editor - Frank Thomas	
Account Settings Account Details Mail Services Web Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP	Mail Services Enable POP access (Post Office Protocol) but only from LAN IPs Enable MultiPOP mail collection Enable IMAP access (Internet Message Access Protocol) but only from LAN IPs but only from LAN IPs enable MDaemon Connector access (requires IMAP) Restrict SMTP access to LAN IPs only
Aliases Shared Folders App Passwords Signature Administrative Roles Allow List Settings ⊋- ActiveSync	Smart Host Access Smart host login Smart host password
	Ok Cancel Apply Help

Les options de cet écran filtrent les services de messagerie que le compte est autorisé à utiliser : POP, IMAP, MultiPOP et MDaemon Connector. L'accès au courrier électronique via Webmail est contrôlé à partir de l' écran<u>Services Web.</u> (77) Cet écran contient également des options permettant de spécifier les informations d'identification de l'Accès Hôte de relais pour le compte.

Services de messagerie

Activer l'accès POP (Post Office Protocol)

Lorsque cette case est cochée, il est possible d'accéder au courrier du compte via Post Office Protocol (POP). Pratiquement tous les logiciels de messagerie prennent en charge ce protocole.

... mais seulement à partir d'IP du réseau local

Cochez cette case si vous souhaitez autoriser l'accès au compte via POP uniquement lorsque l'utilisateur se connecte à partir d'une <u>adresse IP locale</u> [47].

Activer la collecte de courrier MultiPOP

Cochez cette case si vous souhaitez autoriser le compte à utiliser <u>MultiPOP</u> (792). Collecte MultiPOP permet à l'utilisateur de collecter du courrier à partir d'autres comptes de messagerie, maintenus sur d'autres serveurs de messagerie.

Activer l'accès IMAP (Internet Message Access Protocol)

Lorsque cette case est cochée, il est possible d'accéder au courrier du compte via le protocole IMAP (Internet Message Access Protocol). IMAP est plus polyvalent que POP3, car il permet de gérer le courrier électronique sur le serveur et d'y accéder à l'aide de plusieurs clients. La plupart des logiciels de messagerie prennent en charge ce protocole.

... mais seulement à partir d'IP du réseau local

Cochez cette case si vous souhaitez autoriser l'accès au compte via IMAP uniquement lorsque l'utilisateur se connecte à partir d'une <u>adresse IP locale</u> [47].

...activer l'accès MDaemon Connector (requiert IMAP)

Cochez cette option si vous souhaitez autoriser le compte à se connecter via <u>MDaemon Connector</u> [409]. **Remarque :** cette option ne sera disponible que si la prise en charge de MDaemon Connector est activée sur votre serveur.

Limiter l'accès SMTP aux IP LAN uniquement

Cochez cette case si vous souhaitez limiter l'accès SMTP aux IP locales uniquement. Cela empêchera les comptes d'envoyer du courrier s'ils ne sont pas connectés à votre réseau. Si le compte tente d'envoyer du courrier à partir d'une adresse IP extérieure, la connexion sera refusée et abandonnée.

Accès Hôte de relais

Mot de passe Identifiant de l'hôte de relais

Si l'option Autoriser l'authentification par compte est activée sur l'écran de distribution dans Configuration | Paramètres du serveur, et que vous souhaitez utiliser l'authentification par compte avec ce compte au lieu d'utiliser les informations d'identification spécifiées sur cet écran, indiquez ici les informations d'identification de l'hôte intelligent facultatif du compte. Si vous ne souhaitez pas utiliser l'authentification par compte pour ce compte, laissez ces options vides.

5.1.1.4 Services web

🚨 Account Editor - Frank Thomas		×
 Account Settings Account Details Mail Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases Shared Folders App Passwords Signature Administrative Roles Allow List Settings ActiveSync 	Web Services & Two-Factor Authentication Image: Provide the services in the service of the	
	Remote Administration Allows User to edit real name edit private flag edit mailbox edit mail restrictions edit password edit quota settings edit forwarding address edit MultiPDP settings edit advanced forwarding edit autoresponder settings edit IMAP filters edit attachment handling edit aisaes manage mobile devices edit app passwords manage mobile devices	
	Load "New Accounts" template settings	
	Ok Cancel Apply Help	>

Services Web

Activer l'accès au webmail

Activez cette case à cocher si vous souhaitez que le compte puisse accéder à <u>Webmail</u> [33], qui permet aux utilisateurs d'accéder à leur courrier électronique, à leurs calendriers et à d'autres fonctionnalités à l'aide d'un navigateur web.

... mais seulement à partir d'IP du réseau local

Cochez cette case si vous souhaitez que le compte ne puisse accéder à Webmail que lorsqu'il se connecte à partir d'une <u>adresse IP locale</u> [47].

Autoriser l'accès au MDaemon Remote Admin

Cochez cette case si vous souhaitez autoriser l'utilisateur à modifier les paramètres de son compte via le <u>MDaemon Remote Admin</u> [376]. L'utilisateur ne pourra modifier que les paramètres que vous aurez désignés ci-dessous.

Dans le cas où cette fonction est activée et que le serveur Remote Admin est actif, l'utilisateur pourra se connecter à Remote Admin en pointant un navigateur vers le domaine MDaemon désigné et le <u>port assigné à Remote Admin</u> (par exemple http://example.com:1000). Un écran de connexion lui sera d'abord présenté, puis un écran contenant les paramètres qu'il a été autorisé à modifier. Il lui suffit de modifier les paramètres de son choix, puis de cliquer sur le bouton *Enregistrer les modifications*. Il peut ensuite se déconnecter et fermer le navigateur. Si l'utilisateur a accès à Webmail, il peut également accéder à MDaemon Remote Admin à partir du menu Options avancées de Webmail.

Si l'utilisateur est un compte administrateur global ou de domaine (désigné dans l' écran<u>Rôles administratifs</u> and l'éditeur de compte), il verra un écran différent après s'être connecté à l'administration à distance.

... mais seulement à partir d'IP du réseau local

Cochez cette case si vous souhaitez autoriser le compte à accéder à l'administration à distance uniquement lorsqu'il se connecte à partir d'une <u>adresse</u> <u>IP locale [647]</u>.

Activer MDaemon Instant Messenger

Cochez cette case si vous souhaitez activer la prise en charge de<u>MDIM</u> pour ce compte est activé.

Activer la messagerie instantanée

Lorsque la prise en charge de MDIM est activée pour le compte, cliquez sur cette option si vous souhaitez également activer la prise en charge du système de messagerie instantanée de MDIM. Si cette case n'est pas cochée, vous pourrez accéder aux autres fonctions du MDIM, mais pas à la messagerie instantanée.

L'utilisateur peut modifier les catégories

Cochez cette case si vous souhaitez autoriser cet utilisateur du Webmail à modifier les catégories. Cette option est activée par défaut. **Note :** Cette option n'est disponible que dans l' interface web de<u>MDaemon Remote Admin (MDRA).</u>

Ignorer la vérification de la persistance d'IP pour les sessions Webmail

Si l' option <u>Serveur Web</u> [339] "Exiger la persistance IP pendant la session Webmail" est activée, vous pouvez cocher cette case si vous souhaitez exempter cet utilisateur de l'exigence de persistance IP. **Note :** Cette option n'est disponible que dans l' interface web de<u>MDaemon Remote Admin (MDRA)</u> [376].

Activer l'assistant IA pour les e-mails

Si l' option Activer les options IA pour les e-mails est activée dans la boîte de dialogue Webmail [197] de ce compte , cochez cette case si vous souhaitez permettre à ce compte d'utiliser ces options dans MDaemon Webmail ; les options ne seront disponibles pour l'utilisateur que lorsque l'option au niveau du domaine sera activée. **Remarque :** Vous pouvez utiliser les fonctions Modèles de comptes [347] et Groupes [366] pour assigner des utilisateurs à un groupe qui a accès aux fonctions de messages AI. Voir : "Fonctionnalités des messages AI du webmail [775]" ci-dessous pour des informations importantes et des mises en garde concernant l'utilisation de ces fonctionnalités.

Authentification à deux facteurs

MDaemon supporte l'Authentification à deux facteurs (2FA) pour les utilisateurs qui se connectent à Webmail ou à l'interface web de MDaemon Remote Admin. Les comptes qui se connectent au Webmail via HTTPS peuvent activer l'Authentification à deux facteurs pour ce compte dans l'écran **Options | Sécurité du** Webmail. Dès lors, l'utilisateur doit entrer un code de vérification lorsqu'il se connecte au Webmail ou à MDaemon Remote Admin. Le code est obtenu lors de la Connexion à partir d'une Application d'authentification installée sur l'appareil mobile ou la tablette de l'utilisateur. Cette fonctionnalité est conçue pour tout client qui prend en charge Google Authenticator. Voir le fichier d'aide du Webmail pour plus d'informations sur la configuration de 2FA pour un compte.

Autoriser l'Authentification à deux facteurs

Par défaut, les<u>Nouveaux comptes</u> sont autorisés à configurer et à utiliser la fonction d'authentification à deux facteurs (2FA) du Webmail. Décochez cette case si vous ne souhaitez pas autoriser ce compte à utiliser l'authentification à deux facteurs.

Requérir Authentification à deux facteurs

Activez cette option si vous souhaitez forcer le compte à utiliser l'Authentification à deux facteurs (2FA) lors de la connexion au Webmail. Dans le cas où l'authentification à deux facteurs n'a pas encore été configurée pour le compte, la prochaine fois que le compte se connectera à Webmail, l'utilisateur sera redirigé vers une page pour configurer l'authentification à deux facteurs. Consultez le fichier d'aide du Webmail pour plus d'informations sur la configuration de l'authentification à deux facteurs pour un compte.

Désactiver l'Authentification à deux facteurs étapes

Cliquez sur ce bouton si vous devez désactiver l'Authentification à deux facteurs pour le compte. Cela peut s'avérer nécessaire si, par exemple, l'utilisateur perd son appareil et ne peut pas accéder à ses données d'authentification.

MDaemon Remote Admin permet aux utilisateurs de modifier...

...Modifier votre nom réel

L'activation de cette fonction permettra à l'utilisateur de modifier le paramètre Prénom et nom du compte.

...Modifier la boîte aux lettres

L'activation de cette fonction permet à l'utilisateur de modifier le Nom de la BAL du compte.

Comme le *Nom de la Boîte aux lettres* fait partie de l'adresse email du compte, qui est l'identifiant unique et la valeur de connexion pour le compte, le fait de le modifier signifie que l'utilisateur changera son adresse e-mail actuelle. Dans ce cas, tout message adressé à l'ancienne adresse risque d'être rejeté, supprimé ou autre.

...Modifier le mot passe

Cochez cette case si vous souhaitez autoriser l'utilisateur à modifier le mot de passe de la Boîte aux lettres du compte . Pour en savoir plus sur les demandes de mot passe, voir : <u>Mots de passe</u>

...Modifier l'adresse de transfert

Lorsque cette fonction est activée, l'utilisateur pourra modifier les adresses de<u>transfert.</u>

... Modifier le transfert avancé

Lorsque cette fonctionnalité est activée, l'utilisateur pourra modifier <u>les Paramètres de</u> <u>transfert avancés</u>

...Modifier les filtres IMAP

Utilisez cette commande pour permettre à l'utilisateur de créer et de gérer ses propres <u>Filtres IMAP</u> [789].

...Modifier des alias

Activez cette option si vous souhaitez permettre au titulaire du compte d'utiliser l'administration à distance pour modifier les <u>alias</u> associés à son compte.

...les mots passe d'application

Par défaut, les utilisateurs peuvent modifier leurs <u>Mots passe d'application</u> autri-Désactivez cette case à cocher si vous ne souhaitez pas autoriser l'utilisateur à les modifier.

...Modifier le compte est privé

Cette option détermine si l'utilisateur sera autorisé ou non à utiliser le MDaemon Remote pour modifier l'option "*Compte masqué des listes "Tout le monde", des calendriers partagés et de VRFY*" située dans l'écran Paramètres de l'éditeur de compte.

...Modifier les restrictions de courrier

Cette case à cocher détermine si le compte pourra ou non modifier la restriction Courrier entrant et sortant, située sur l'écran<u>Restrictions</u>

...modifier les paramètres des quotas

Cochez cette case si vous souhaitez autoriser le compte à modifier les paramètres de<u>quotas.</u>

...modifier les paramètres MultiPOP

Cochez cette case si vous souhaitez autoriser le compte à ajouter de nouvelles entrées <u>MultiPOP</u> [792] et à activer/désactiver la Collecte MultiPOP pour ces entrées dans <u>MDRA</u> [376]. Lorsque cette option et l' option <u>Activer MultiPOP</u> [792] du compte sont toutes deux activées, une page Boîtes aux lettres sera disponible dans le <u>Webmail</u> [333] pour que l'utilisateur puisse gérer ses Paramètres MultiPOP. Enfin, l'option globale permettant d'activer/désactiver le serveur MultiPOP se trouve à l'adresse suivante : <u>Configuration | Paramètres de serveur | MultiPOP</u> [144].

...les paramètres de l'autorépondeur

Cochez cette case si vous souhaitez donner à l'utilisateur la permission d'ajouter, de modifier ou de supprimer des <u>autorépondeurs</u> mi pour son compte.

...modifier la gestion des pièces jointes

Cochez cette case si vous souhaitez autoriser l'utilisateur à modifier les options de gestion des pièces jointes de son compte, situées dans l'écran Autoriser pièces jointes.

...gestion terminaux mobiles

Cochez cette option si vous souhaitez autoriser le titulaire du compte à utiliser l'administration à distance pour gérer les paramètres spécifiques à son appareil, par exemple pour les appareils ActiveSync.

Charger les paramètres du modèle Nouveaux comptes

Cliquez sur ce bouton pour ramener les paramètres de cet écran aux valeurs par défaut désignées dans l' écran <u>Services Web</u> au modèle*Nouveaux comptes.*

Fonctionnalités des messages IA du Webmail

Dans la version 23.5.0 de MDaemon, le thème Pro du client Webmail de MDaemon inclut diverses fonctionnalités d'intelligence artificielle (IA) pour aider vos utilisateurs à gérer leur courrier électronique et à augmenter leur productivité. Ces fonctionnalités sont facultatives et désactivées par défaut, mais peuvent être activées pour tout utilisateur de votre choix.

Grâce à ces fonctionnalités, dans le MDaemon Webmail, vous pouvez utiliser l IA pour :

- Vous donner un résumé du contenu d'un message électronique.
- Suggérer une réponse au message, selon plusieurs directives que vous pouvez demander à l'IA d'utiliser. Vous pouvez définir le *ton de* la réponse (professionnel, respectueux ou décontracté). La position à adopter dans la réponse peut être intéressée ou non, d'accord ou non, ou sceptique. L'attitude à adopter dans la réponse peut être confiante, enthousiaste, calme ou apologétique. Les derniers peuvent indiquer la *longueur de* la réponse, qui peut être très brève ou détaillée.
- Vous aider à composer un nouveau message électronique, sur la base d'un texte que vous avez déjà inclus. Comme pour l'option *Suggérer* ci-dessus, vous pouvez également définir le ton, la position, l'attitude et la longueur que l'IA utilisera pour rédiger le message.

L' option Activer les fonctions IA pour les messages de la boîte de dialogue principale Paramètres du Webmail (365) permet de déterminer si la prise en charge des fonctions IA est activée par défaut pour vos domaines. Une option du même nom située dans la boîte de dialogue du (197) Gestionnaire de domaines peut être utilisée pour remplacer ce paramètre principal pour des domaines spécifiques. **Remarque :** Activer assistant IA pour les e-mails pour un domaine ne permet pas à tous les utilisateurs de ce domaine d'accéder à ces fonctions. Vous devez activer l' option Activer les options IA pour les *e-mails dans* l'écran Services Web (771) de l'éditeur de compte pour tout utilisateur que vous souhaitez autoriser à les utiliser. Vous pouvez également utiliser les fonctionsModèles de comptes (847) et Groupes (836) pour affecter des utilisateurs à un groupe ayant accès aux fonctions de messages AI. Activer les assistants IA pour les e-mails de MDaemon permet aux comptes d'envoyer et de recevoir des informations en provenance et à destination de services d'IA générative tiers, en particulier ChatGPT d'OpenAI. Les administrateurs et les utilisateurs doivent donc être conscients que cela introduit plusieurs problèmes potentiels de confidentialité en raison de la capacité de la fonctionnalité à traiter des données personnelles et à générer des informations potentiellement sensibles. Pour répondre à ces préoccupations, il est essentiel que les organisations forment leurs employés à une utilisation responsable de l'IA. **Remarque :** Les données soumises à/depuis I OpenAI ne sont pas stockées sur le serveur local ou sur notre réseau.

Vous trouverez la politique d'utilisation de l'IA de MDaemon Technologies sur notre <u>page d'information sur l'intelligence</u> <u>artificielle (IA)-la MDaemon</u>. Sur cette même page, il y a également un lien vers les Conditions d'utilisation d'OpenAI.

Voir :

<u>Webmail</u> <u>MDaemon Remote Admin</u> <u>Gestionnaire de modèles | Services web</u> क्ष्डी

5.1.1.5 Autorépondeurs

👶 Account Editor - Frank Thomas	×
 Account Settings Account Details Mail Services Web Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases Shared Folders App Passwords Signature Administrative Roles Allow List Settings ActiveSync 	Autoresponder Enable autoresponder Edit autoresponder file Schedule Publish Do not send auto response if message is from one of these addresses Remove New excluded address - wildcards ok Run this program Browse Pass message to process Add sender to this mailing list Remove sender from this list
	Ok Cancel Apply Help

Les répondeurs automatiques sont des outils utiles pour faire en sorte que les messages entrants déclenchent automatiquement certains événements, tels que l'exécution d'un programme, l'ajout de l'expéditeur à une liste de diffusion, l'envoi d'un message généré automatiquement, etc. L'utilisation la plus courante des répondeurs automatiques consiste à répondre automatiquement aux messages entrants par un message défini par l'utilisateur indiquant que le destinataire est en vacances, qu'il n'est pas disponible, qu'il répondra dès que possible, etc. Les utilisateurs de MDaemon disposant d'un <u>accès</u> <u>Web</u>[774] au <u>Webmail</u>[333] ou à l'<u>Administration à distance</u>[376] peuvent utiliser les options fournies pour composer eux-mêmes des messages de réponse automatique et programmer les dates auxquelles ils seront utilisés. Enfin, les messages de réponse automatique sont basés sur le contenu du fichier OOF.mrk, qui se trouve dans le dossier racine de chaque utilisateur . Ce fichier prend en charge un grand nombre de macros, qui peuvent être utilisées pour générer dynamiquement une grande partie du contenu du message, ce qui rend les répondeurs automatiques très polyvalents.

> Les Autorépondeurs sont toujours honorés lorsque le message déclencheur provient d'une source distante. Toutefois, pour les messages provenant provenant du même domaine d'un utilisateur, les autorépondeurs ne seront déclenchés que si vous activez l'option *Les autorépondeurs sont déclenchés par le courrier intra-domaine*, située dans l' écran<u>" Paramètres |</u> <u>des autorépondeurs</u> 2021. Vous pouvez également utiliser une

option de cet écran pour limiter les messages de réponse automatique à une réponse par expéditeur et par jour.

Répondeur automatique

Activer l'autorépondeur

Activer ce compte est ACTIVÉ pour activer un autorépondeur pour ce compte. Pour plus d'informations sur les répondeurs automatiques, voir : <u>Répondeurs</u> <u>automatiques</u>

Modifier le fichier de réponse automatique

Cliquez sur ce bouton pour modifier le fichier de réponse automatique du compte. Ce fichier est le fichier oof.mrk, situé dans le dossier Mon compte.

Planification

Cliquez sur ce bouton pour ouvrir la boîte de dialogue Schedule dans laquelle vous pouvez définir une date et une heure de début et de fin pour l'autorépondeur, ainsi que les jours de la semaine où il doit être actif. Laissez la case Schedule vide si vous souhaitez que l'autorépondeur soit actif en permanence.

Schedule	
Schedule Action	
Erase the 'Start date/time' to deactivate this schedule.	
Start date/time at 12 V 00 V AM	\sim
End date/time at 12 ~ 00 ~ AM	\sim
Select days of the week	
🗹 Monday 🛛 🗹 Saturday	
🗹 Tuesday 🛛 🗹 Sunday	
✓ Wednesday	
🗹 Thursday	
Friday Ok Can	cel

Publier

Cliquez sur ce bouton si vous souhaitez copier le fichier et les paramètres du répondeur automatique de ce compte vers un ou plusieurs autres comptes. Sélectionnez les comptes vers lesquels vous souhaitez copier le répondeur automatique, puis cliquez sur **Ok**.

Ne pas envoyer de réponse automatique si le message provient d'une de ces adresses Vous pouvez ici dresser la liste des adresses que vous souhaitez exclure des réponses initiées par ce répondeur automatique. Il peut arriver que des messages de réponse automatique soient envoyés à une adresse qui renvoie elle-même une réponse automatique. Cela peut créer un effet "ping-pong" qui fait que les messages sont continuellement renvoyés entre les deux serveurs. Si vous rencontrez l'une de ces adresses, indiquez-la ici pour éviter que cela ne se produise. Il existe également une option, située dans l' écran<u>" Paramètres</u> <u>autorépondeurs</u>" [902], qui peut être utilisée pour limiter les messages de réponse automatique à une réponse par expéditeur et par jour.

Supprimer

Cliquez sur ce bouton pour supprimer toutes les entrées sélectionnées de la liste des adresses exclues.

Nouvelle adresse exclue - jokers acceptés

Si vous souhaitez ajouter une adresse à la liste des adresses exclues, saisissez-la ici, puis cliquez sur le bouton*Ajouter*.

Exécuter un programme suivant.

Exécuter un programme suivant.

Utilisez ce champ pour indiquer le chemin d'accès et le nom de fichier d'un programme que vous souhaitez exécuter lorsque du nouveau courrier arrive pour ce compte. Il convient de veiller à ce que ce programme se termine correctement et puisse être exécuté sans surveillance. Des paramètres de ligne de commande facultatifs peuvent être saisis immédiatement après le chemin d'accès à l'exécutable, si vous le souhaitez.

Traiter le message

Sélectionnez cette option et le processus spécifié dans le champ *Exécuter ce programme* se verra transmettre le nom du message de déclenchement en tant que premier paramètre de ligne de commande disponible. Dans le cas où le paramètre autorépondeur est défini pour un compte qui transfère le courrier vers un autre endroit et **ne** conserve **pas** de copie locale dans sa propre boîte aux lettres (voir <u>Transfert</u> 780), cette fonction est désactivée.

Non par défaut, MDaemon place le nom du fichier de messages comme dernier paramètre de la ligne de commande. Vous pouvez modifier ce comportement en utilisant la macro \$MESSAGE\$. Dans ce cas, utilisez cette macro à la place du nom du fichier de messages. Cela permet une plus grande flexibilité dans l'utilisation de cette fonctionnalité puisqu'une ligne de commande complexe telle que celle-ci sera possible : logmail /e /j /message=\$MESSAGE\$ /q.

Liste de diffusion

Ajouter l'expéditeur à la liste de diffusion

Si une liste de diffusion est ajoutée dans ce champ, l'expéditeur du message entrant sera automatiquement ajouté en tant que membre de cette liste de diffusion. Il s'agit d'une fonction pratique pour la constitution automatique de listes.

Supprimer expéditeur de cette liste de diffusion

Si une liste de diffusion est indiquée dans ce champ, l'expéditeur du message entrant sera automatiquement supprimé de la liste de diffusion spécifiée.

Voir :

Autorépondeurs | Comptes Autorépondeurs | Liste des exceptions de l'autorépondeur Autorépondeurs " Paramètres " l'autorépondeur Création de messages de réponse automatique

5.1.1.6 Transfert

👶 Account Editor - Frank Thomas					×
 Account Editor - Frank Inomas Account Details Account Details Mail Services Web Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases Shared Folders App Passwords Signature Administrative Roles Allow List Settings ActiveSync 	Mail Forwarding □ Enable mail forwarding Forwarding address(es) (separate e Domain, (Host), or IP AUTH Logon AUTH Password SMTP 'MAIL' Value Port (default = 25) ☑ Retain a local copy of forwarde	each address with a comr 25 .d mail	ma)		
			Ok	Cancel Ap	pply Help

Transfert de courrier

Activer le transfert de courrier

Cochez cette case si vous souhaitez faire suivre les messages entrants de ce compte à l'adresse ou aux adresses spécifiées dans l'option Adresses de transfert cidessous. Les utilisateurs de MDaemon qui ont un <u>accès Web</u> 771 au <u>Webmail</u> 333 ou à l'<u>Accès Admin</u> 376 peuvent utiliser les options fournies pour définir eux-mêmes les options de transfert, sans avoir à demander à un administrateur de le faire.

Adresses de transfert (séparez chaque adresse par une virgule)

Utilisez ce champ pour désigner les adresses e-mail auxquelles vous souhaitez transférer des copies des messages entrants de ce compte au fur et à mesure de leur arrivée. Une copie de chaque nouveau message arrivant sur le serveur sera automatiquement générée et transférée aux adresses spécifiées dans ce champ, à condition que l'option*Activer le transfert de courrier* ci-dessus soit cochée. Lors de la redirection vers plusieurs adresses, séparez chacune d'elles par une virgule.

Domaine, [Hôte] ou IP

Si vous souhaitez Routage des messages Transférer MESSAGE ! via un autre serveur, tel que lesserveurs MX d' un domaine particulier, indiquez ici le domaine ou l'adresse IP. Si vous souhaitez router les messages vers un hôte spécifique, mettez la valeur entre parenthèses (par exemple [host1.example.com]).

Mot de passe AUTH

Saisissez ici les Exigences relatives aux mots passe du serveur vers lequel vous transférez le courrier de l'utilisateur.

Valeur SMTP 'MAIL' (en anglais)

Si une adresse est spécifiée ici, elle sera utilisée dans l'instruction"MAIL From" envoyée au cours de la session SMTP avec l'hôte acceptant, au lieu d'utiliser l'expéditeur réel du message. Si vous avez besoin d'une instruction SMTP "MAIL From" vide(c'est-à-dire "MAIL FROM<>"), entrez "[poubelle]" dans cette option.

Port (par défaut = 25)

MDaemon enverra les messages transférés en utilisant le port TCP spécifié ici. Le port SMTP par défaut est 25.

Garder une copie locale du courrier transféré

Par défaut, une copie de chaque message transféré est délivrée normalement dans la boîte aux lettres de l'utilisateur local. Si vous décochez cette case, aucune copie locale ne sera conservée.

Planification

Cliquez sur ce bouton pour créer un calendrier de transfert du courrier électronique du compte. Vous pouvez définir une date et une heure de début, une date et une heure de fin, et spécifier les jours de la semaine où le courrier sera transféré.

5.1.1.7 Restrictions

👶 Account Editor - Frank Thomas		×
Account Settings Account Details Mail Services Web Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases Shared Folders And Palese Shared Folders And Palese	Inbound Message Restrictions Restrict messages FROM outside domains except if from one of these addresses Messages from outside domains should be: Refused	New address Add Remove
App Passwords Signature Administrative Roles Allow List Settings ActiveSync	Outbound Message Restrictions Restrict messages TO outside domains except if to one of these addresses Messages to outside domains should be: Refused	New address Add Remove
	Ok	Cancel Apply Help

Les options de cet écran permettent de déterminer si le compte peut ou non envoyer ou recevoir du courrier à destination ou en provenance de domaines non locaux.

Restrictions appliquées aux messages entrants

Refuser les messages PROVENANT DE domaines externes

Cochez cette case pour empêcher ce compte de recevoir des messages électroniques provenant de domaines non locaux.

... sauf si l'expéditeur est l'une de ces adresses

Les adresses spécifiées dans cette zone constituent des exceptions aux Restrictions aux messages entrants. Les caractères génériques sont autorisés. Ainsi, si vous désignez "*@altn.com" comme exception, aucun message entrant provenant d'une adresse de altn.com ne sera restreint.

Nouvelle adresse

Si vous souhaitez ajouter une adresse à la liste des Restrictions aux messages entrants, tapez-la ici et cliquez sur le bouton*Ajouter*.

Ajouter

Après avoir saisi une adresse dans l'option*Nouvelle adresse*, cliquez sur ce bouton pour l'ajouter à la liste des exceptions.

Supprimer

Si vous souhaitez supprimer une adresse de la liste des restrictions, sélectionnez-la, puis cliquez sur ce bouton.

Les messages provenant d'un domaine externe doivent être...

Les options de cette liste déroulante déterminent ce que MDaemon fera des messages destinés à ce compte mais provenant d'un domaine non local. Vous pouvez choisir l'une des options suivantes :

Refusées - Les messages restreints seront refusés par MDaemon.

Renvoyé à l'expéditeur - Les messages provenant de domaines restreints seront renvoyés à l'expéditeur.

Envoyé au postmaster - Les messages restreints seront acceptés mais livrés au postmaster au lieu de ce compte.

Envoyé à... - Les messages restreints seront acceptés mais livrés à l'adresse que vous indiquez dans la zone de texte à droite.

Restrictions appliquées aux messages sortants

Refuser les messages ENVOYÉS À des domaines externes

Cochez cette case pour empêcher ce compte d'envoyer des messages électroniques à des domaines non locaux.

... sauf si expéditeur est l'une de ces adresses

Les adresses spécifiées dans cette zone constituent des exceptions à la restriction sur les messages sortants. Les caractères génériques sont autorisés. Ainsi, si vous désignez "*@altn.com" comme exception, les messages sortants adressés à n'importe quelle adresse de altn.com ne seront pas restreints.

Nouvelle adresse

Si vous souhaitez ajouter une adresse à la liste des Restrictions aux messages sortants, tapez-la ici et cliquez sur le bouton*Ajouter*.

Ajouter

Après avoir saisi une adresse dans l'option*Nouvelle adresse*, cliquez sur ce bouton pour l'ajouter à la liste des exceptions.

Supprimer

Si vous souhaitez supprimer une adresse de la liste des restrictions, sélectionnez-la et cliquez sur ce bouton.

Les messages envoyés à un domaine externe doivent être...

Les options de cette liste déroulante déterminent ce que MDaemon fera des messages provenant de ce compte mais destinés à un domaine non local. Vous pouvez choisir l'une des options suivantes :

Refusées - Les messages restreints seront refusés par MDaemon.

Renvoyé à l'expéditeur - Les messages à destination de domaines restreints seront renvoyés à l'expéditeur.

Envoyé au postmaster - Les messages restreints seront acceptés mais remis au postmaster au lieu du destinataire désigné.

Envoyé à... - Les messages restreints seront acceptés mais remis à l'adresse que vous indiquez dans la zone de texte à droite.

5.1.1.8 Quotas

	 Account Settings Account Details Mail Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Mathematical Poly (Construction) Attachments IMAP Filters MultiPOP Aliases Shared Folders Administrative Roles Allow List Settings ActiveSync 	uota restrictions count exceeds its quota settings, subsequent delivery attempts ad and a warning message will be placed in the account's amber of messages stored at once 0 (0 = no limit) sk space allowed (in megabytes) 0 (0 = no limit) essages sent per day 0 (0 = no limit) essages sent per day 0 (0 = no limit) ecount: 1563 Update counts ned: 5.1 (MB) 0 unt if inactive for this many days 0 (0 = never) sages older than this many days 0 (0 = never) eted IMAP msgs older than this many days 0 (0 = never) old messages from IMAP folders as well 0 (0 = never)
--	---	--

Quotas

Activer les quotas

Cochez cette case si vous souhaitez spécifier un nombre maximum de messages que le compte peut stocker, définir un espace disque maximum que le compte peut utiliser (y compris les pièces jointes dans ledossier Pièces des comptes) ou désigner un nombre maximum de messages que le compte peut envoyer via SMTP par jour. Dans le cas d'une tentative de distribution du courrier qui dépasserait les limites maximales de messages ou d'espace disque, le message sera refusé et un message d'alerte approprié sera placé dans la boîte aux lettres de l'utilisateur. Si une collecte Collecte MultiPOP [792] dépasse lalimite maximale du compte, un avertissement similaire est émis et les entrées MultiPOP ducomptesont automatiquement désactivées (mais pas supprimées de la base de données).

Utilisez l'option *Envoyer un avertissement à l'utilisateur si ce pourcentage de son quota est atteint* sur "<u>Comptes |</u> <u>Paramètres du compte | Quotas</u>" ^{BTO} pour qu'un message d'avertissement soit envoyé lorsqu'un compte s'approche de ses limites de quota. Lorsque le compte dépasse un certain pourcentage du *nombre maximal de messages stockés en une seule fois* ou de l'*espace disque maximal autorisé*, un message d'avertissement est envoyé au compte à minuit. Ce message indiquera le nombre de messages stockés par le compte, la taille de sa boîte aux lettres, ainsi que le pourcentage utilisé et restant. En outre, si un avertissement existant est trouvé dans la boîte aux lettres du compte, il sera remplacé par un message mis à jour.

Nombre maximal de messages stockés à la fois

Cette option permet de désigner le nombre maximum de messages pouvant être stockés pour le compte. L'utilisation de "0" dans l'option signifie qu'il n'y aura pas de limite au nombre de messages autorisés.

Espace disque maximum autorisé (en Mo)

Utilisez cette option pour désigner la quantité maximale d'espace disque que le compte peut utiliser, y compris les pièces jointes éventuellement stockées dans le Dossier Pièces ducompte.L'utilisation de "0" dans l'option signifie qu'il n'y aura pas de limite à la quantité d'espace disque que le compte peut utiliser.

Nombre max. de messages envoyés par jour

Cette option permet de définir le nombre maximum de messages que le compte peut envoyer par jour via SMTP. Si le compte atteint cette limite, les nouveaux messages provenant du compte seront refusés jusqu'à ce que le compteur soit remis à zéro à minuit. Utilisez "0" dans l'option si vous ne souhaitez pas limiter le nombre de messages que le compte peut envoyer.

Actualiser les compteurs

Cliquez sur ce bouton pour actualiser les statistiques relatives au*nombre de messages/fichiers* et au *disque consommé* affichées à gauche.

Élagage

Les options de cette section permettent de déterminer si le compte sera supprimé par MDaemon s'il devient inactif. Vous pouvez également indiquer si les anciens messages appartenant à ce compte seront ou non supprimés après un certain temps. Tous les jours à minuit, MDaemon supprimera tous les messages qui ont dépassé les délais indiqués, ou il supprimera complètement le compte s'il a atteint la limite d'inactivité.

Utiliser les paramètres par défaut du domaine

Les paramètres d'élagage par défaut sont propres à chaque domaine et se trouvent dans l'écran Paramètres du Gestionnaire de domaines. Si vous souhaitez ignorer les paramètres par défaut du domaine pour ce compte, décochez cette case et définissez les valeurs souhaitées dans les options ci-dessous. **Supprimer les comptes s'ils sont inactifs depuis plus plus de jours (0 = jamais)** Indiquez le nombre de jours pendant lesquels le compte doit être inactif avant d'être supprimé. Une valeur de "0" dans ce champ signifie que le compte ne sera jamais supprimé pour cause d'inactivité.

Supprimer les messages plus anciens que ce nombre de jours (0 = jamais)

Il s'agit du nombre de jours pendant lesquels un message donné peut rester dans laboîte aux lettres ducompteavant d'être supprimé automatiquement par MDaemon. La valeur "0" signifie que les messages ne seront jamais supprimés en raison de leur ancienneté. Dans cette option, les messages contenus dans les dossiers IMAP ne sont pas pris en compte, sauf si vous activez l'option "Nettoyer les anciens messages des dossiers IMAP également" ci-dessous.

PURGEZ les messages IMAP supprimés qui datent de plus de ce nombre de jours (0 = jamais)

Utilisez cette commande pour spécifier le nombre de jours pendant lesquels vous souhaitez que les messages IMAP marqués pour suppression restent dans les dossiers decet utilisateur.Les messages marqués pour suppression au-delà de ce nombre de jours seront supprimés. La valeur "0" signifie que les messages marqués pour suppression ne seront jamais supprimés en raison de leur ancienneté.

Nettoyer également les anciens messages des dossiers IMAP

Cochez cette case si vous souhaitez que l'option"*Supprimer les messages effacés depuis plus de ce nombre de jours*" ci-dessus s'applique également aux messages des dossiers IMAP. Lorsque ce contrôle est désactivé, les messages ordinaires contenus dans les dossiers IMAP ne seront pas supprimés en raison de leur ancienneté.

Voir :

<u>Gestionnaire de modèles | Quotas</u> <u>Paramètres des comptes | Quotas</u> 201

5.1.1.9 Pièces jointes



Gestion des pièces jointes

Cet écran permet de contrôler si MDaemon extraira ou non les pièces jointes des messages électroniques de ce compte. Vous pouvez utiliser le <u>Gestionnaire de</u> <u>modèles</u> arg pour désigner les paramètres (par défaut) de ces options.

Ne pas extraire les pièces jointes des messages

Si cette option est sélectionnée, les pièces jointes ne seront pas extraites des messages du compte. Les messages contenant des pièces jointes seront gérés normalement, en laissant les pièces jointes intactes.

Extraire les pièces jointes et les enregistrer dans le dossier Documents du compte

Si cette option est activée, MDaemon extraira automatiquement les pièces jointes MIME Base64 présentes dans les messages entrants de ce compte. Les fichiers extraits sont supprimés du message entrant, décodés et placés dans le dossier Documents du compte. Une note est alors placée dans le corps du message, indiquant les noms des fichiers qui ont été extraits. Cette option ne fournit pas de lien vers les pièces jointes jointes. Webmail as pour accéder à leur dossier Documents.

Utiliser la fonctionnalité Liens vers les pièces jointes jointes

Sélectionnez cette option si vous souhaitez utiliser la fonctionnalité Liens vers les pièces jointes pour les messages entrants ou sortants contenant des pièces jointes.



Si cette option est sélectionnée mais que la fonction Liens jointes est désactivée dans la boîte de dialogue<u>Liens</u> jointes seront pas extraites.

Extraire les pièces jointes des messages entrants

Lorsque cette option est activée, les pièces jointes sont extraites des messages entrants du compte et stockées à l'emplacement désigné dans la boîte de dialogue <u>Liens jointes.</u> (a) Des liens URL sont alors placés dans le Corps du message, sur lesquels l'utilisateur peut cliquer pour télécharger les fichiers. Pour des raisons de sécurité, ces liens URL ne contiennent pas de chemin d'accès direct aux fichiers. Au lieu de cela, ils contiennent un identifiant unique (GUID) que le serveur utilise pour faire correspondre le fichier au chemin d'accès réel. Ce GUID est stocké dans le fichierAttachmentLinking.dat. Cette option est activée par défaut.

Extraire les pièces jointes des messages sortants

Cochez cette case si vous souhaitez utiliser la fonctionnalité Liens vers les pièces jointes pour extraire les pièces jointes des messages sortants du compte. Lorsque le compte envoie un e-mail, Liens les pièces jointes extrait le fichier, le stocke et le remplace par une URL permettant de télécharger le fichier.

Modifier les paramètres des Liens vers les pièces jointes

Cliquez sur ce bouton pour ouvrir la boîte de dialogue<u>Liens vers les pièces jointes</u>

Voir :

Liens vers les pièces jointes 708 Gestionnaire de modèles | Pièces jointes 873

5.1.1.10 Filtres IMAP

👃 Account Editor - Frank Thomas		×
Account Editor - Frank Thomas Account Settings Account Details Account Details Mail Services Web Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases	Existing IMAP Filtering Rules	Remove Clear all Up Down
 Aliases Shared Folders App Passwords Signature Administrative Roles Allow List Settings ActiveSync 	New IMAP Filtering Rule If the <u>HEADER contains 'THIS TEXT'</u> [+] then <u>move message to THIS FOLDER</u>	Add filter Publish
	Ok Cancel Apply	Help

Les filtres permettent aux utilisateurs IMAP et Webmail 333 d'acheminer

automatiquement leur courrier vers des dossiers spécifiques du serveur. Comme pour les <u>filtres de contenu</u>, MDaemon examine les en-têtes de chacun des messages entrants du compte, puis les compare aux filtres du compte. Lorsqu'un message pour le compte correspond à l'un de ses filtres, MDaemon le Déplacera dans le dossier spécifié dans ce filtre, supprimera le message, ou le redirigera ou le transmettra à l'adresse électronique de votre choix. Cette méthode est beaucoup plus efficace (pour le client comme pour le serveur) que d'essayer de filtrer les messages au niveau du client, et comme certains clients de messagerie ne prennent même pas en charge les règles ou le filtrage local des messages, les Filtres IMAP leur offrent cette option.

Les administrateurs peuvent créer des filtres via l'écran Filtres IMAP de l'éditeur de compte, ou par le biais de <u>MDaemon Remote Admin</u> [376]. Cependant, vous pouvez également autoriser vos utilisateurs à créer et gérer eux-mêmes des filtres dans le Webmail ou dans MDaemon Remote Admin. Ces autorisations sont définies dans l'écran<u>Services Web.</u> [771]

Règles de filtrage IMAP existantes

Cette boîte affiche la liste de toutes les règles de filtrage qui ont été créées pour le compte de l'utilisateur. Les filtres sont traités dans l'ordre dans lequel ils sont listés jusqu'à ce qu'une correspondance soit trouvée. Dans ce cas, dès qu'un message correspond à l'un des filtres, il est déplacé dans le dossier spécifié dans ce filtre, puis le traitement de ce message s'arrête. Utilisez les boutons*Monter* et *Descendre* pour déplacer les filtres à différentes positions dans la liste.

Enlever

Cliquez sur un filtre dans la liste, puis sur Supprimer pour le supprimer de la liste.

Effacer tout

Cliquez sur ce bouton pour supprimer tous lesfiltres de l'utilisateur.

Haut de la page

Dans la liste, cliquez sur un filtre, puis sur ce bouton pour le déplacer vers une position plus élevée dans la liste.

Vers le bas

Dans la liste, cliquez sur un filtre, puis sur ce bouton pour le déplacer vers le bas de la liste.

Nouvelle règle de courrier IMAP

Utilisez les liens de cette zone pour élaborer une nouvelle règle de filtrage. Lorsque votre règle est terminée, cliquez sur **Ajouter un filtre** pour l'ajouter aux *Règles de filtrage IMAP existantes*.

Conditions de filtrage

Cliquez sur les liens dans la première section de la règle de filtrage pour définir les paramètres du filtre. Lorsqu'un message répond aux conditions du filtre, l'action de filtrage est exécutée.

EN-TÊTE FROM: : HEADER

Cliquez sur "HEADER" pour choisir**l'en-tête dans l'en-tête**FROM :.ou un autre composant du message que vous souhaitez examiner dans le cadre de la règle de filtrage. Vous pouvez choisir : **TO**, **CC**, **FROM**, **SUBJECT**, **SENDER**, **LIST-ID**, **X-MDMAILING-LIST**, **X-MDRCPT-TO**, **X-MDDNSBL-RESULT**, **X-SPAM-FLAG**, **MESSAGE SIZE**, **MESSAGE BODY**, ou **Autre...** Si vous choisissez "Other...", une boîte de dialogue Filter Condition s'ouvrira pour vous permettre de spécifier un nom d'en-tête qui ne figure pas dans la liste. Si vous cliquez sur MESSAGE SIZE, les liens "contains" et "THIS TEXT" seront remplacés respectivement par "is greater than" et "0 KB".

contient / est plus grand que

Cliquez sur "**contient**" ou " **est plus grand que"** pour choisir le type de condition à appliquer lors de l'examen de l'en-tête. Par exemple, l'en-tête existe-t-il ou non, contient-il ou non un certain texte, commence-t-il ou se termine-t-il par un certain texte, etc. Vous pouvez choisir parmi les conditions suivantes : **commence par, se termine par, est égale à, n'est pas égale à, contient, ne contient pas, existe, n'existe pas, est supérieur à, est inférieur à**. Les options "est supérieur à" et "est inférieur à" ne sont disponibles que lorsque le lien En-tête est défini sur "Taille du message".

CE TEXTE / 0 KB

Saisissez le texte que vous souhaitez que MDaemon recherche lors de l'analyse de l'en-tête que vous avez sélectionné pour le filtre. Dans le cas où l'option ENTÊTE est réglée sur TAILLE DU MESSAGE, le lien indiquera "O KB" et la boîte de

dialogue Condition du Filtre comportera une case permettant d'indiquer la "Taille du message en KB".

[+] [x] et

Cliquez sur [+] si vous souhaitez définir deux conditions ou plus pour la règle de filtrage. Ce texte ajoutera une autre ligne contenant les composants "HEADER", "contains" et "THIS TEXT" pour étendre le filtre. Lorsque vous testez un message par rapport à une règle de filtrage comportant plusieurs conditions, le message doit, par défaut, satisfaire à chacune des conditions pour correspondre à la règle. Cliquez sur "et", puis sélectionnez "ou" si vous souhaitez que le message corresponde à la règle lorsqu'il remplit l'une des conditions. Lorsqu'une règle de filtrage comporte plusieurs lignes, vous pouvez cliquer sur [x] en regard de la ligne que vous souhaitez supprimer.

Actions de filtrage

Dans la section inférieure de la règle de filtrage, cliquez sur les liens pour désigner l'action à entreprendre lorsqu'un message remplit les conditions du filtre.

déplacer le message vers

Cliquez sur **"déplacer le message vers**" pour désigner l'action de filtrage. Vous pouvez choisir : **déplacer le message vers**, **supprimer le message, rediriger le message vers** ou **Transférer le message vers**.

CE DOSSIER / EMAIL

Si vous avez sélectionné l'action "déplacer le message vers", cliquez sur **CE DOSSIER** pour désigner le dossier dans lequel le message doit être déplacé. Si vous avez choisi de rediriger ou de transférer le message, cliquez sur **EMAIL** et entrez l'adresse électronique du destinataire. Pour les messages redirigés, aucune modification n'est apportée aux en-têtes ou au corps du message. Seul le destinataire de l'enveloppe SMTP est modifié. Pour les messages transférés, un nouveau message sera créé et envoyé, avec l'Objet du message et le corps du message repris du message original.

Ajouter un filtre

Lorsque vous avez terminé de créer votre nouveau filtre, cliquez sur ce bouton pour l'ajouter aux *Règles de filtrage IMAP existantes*.

Publier

Après avoir créé une règle, cliquez sur **Publier** si vous souhaitez copier cette règle sur tous les autres comptes utilisateurs appartenant au domaine de ce compte. Il vous sera demandé de confirmer votre décision de copier la règle vers les autres comptes.

5.1.1.11 MultiPOP

Account Settings Account Details Mail Services Web Services	MultiPOP MultiPOP collec single mailbox.	ts mail from any nu POP	mber of POP servers a	nd stores it in	ia
Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments	Server	Name	Password (En	Enabled	Rem
MultiPOP Aliases Shared Folders App Passwords Signature Administrative Roles Allow List Settings	Server Logon Enable this of Leave a cop Use APOP	Pas entry y of message on P	'OP3 server Use OAuth	A Rei En Rei	,dd move able
	Delete message Do not downloa	es older than d messages larger	0 days (0 = 0 KB (0 = r	= never) no limit)	

La fonction MultiPOP vous permet de créer un nombre illimité de combinaisons hôte/utilisateur/mot de passe POP3 pour la Collecte des messages courrier en provenance de plusieurs sources. Cette fonction est utile pour vos utilisateurs qui possèdent des comptes de messagerie sur plusieurs serveurs mais qui préfèrent collecter et regrouper tous leurs messages électroniques en un seul endroit. Avant d'être placé dans laboîte aux lettres de l'utilisateur, le courrier collecté par MultiPOP est d'abord placé dans la File locale afin qu'il puisse être traité comme les autres courriers auxquels sont appliqués des répondeurs automatiques et des filtres de contenu. Les options de planification pour MultiPOP se trouvent à l'adresse suivante : Configuration | Programmation d'événements | Programmation du courrier | Collecte MultiPOP 406.

Activer MultiPOP

Cochez cette case pour activer le traitement MultiPOP pour ce compte. Si vous souhaitez permettre à l'utilisateur de modifier ses propres paramètres MultiPOP dans MDRA [376], activez l'option "...modifier les paramètres MultiPOP" sur la page des Services Web du compte. Dans le cas où cette option et l'option Services web sont toutes deux activées, une page Boîtes aux lettres sera disponible dans le <u>Webmail</u>[333] pour que l'utilisateur puisse gérer ses paramètres MultiPOP. L'option globale permettant d'activer/désactiver le serveur MultiPOP se trouve à l'adresse suivante : <u>Configuration | Paramètres de serveur | MultiPOP</u>[144]. Si cette option est désactivée, MultiPOP ne peut pas être utilisé, même si cette option de compte est activée.
Créer ou Modifier une entrée MultiPOP

Serveur

Saisissez le serveur POP3 à partir duquel vous souhaitez collecter le courrier en POP3. Si ce serveur exige que vous vous connectiez sur un port spécifique autre que les ports POP3 standard, ajoutez ": [port]" au nom du serveur. Exemple : "mail.example.com:1000". Lors de la collecte à partir de Gmail ou de Microsoft (Office) 365, utilisez respectivement "pop.gmail.com:995" ou "outlook.office365.com:995".

Connexion

Saisissez le nom d'utilisateur POP3 ou le nom de connexion qui est associé au compte de messagerie sur le serveur spécifié ci-dessus.

Mot de passe

Entrez le mot de passe POP3 ou APOP utilisé pour accéder au compte de messagerie sur le serveur spécifié.

Utiliser APOP

Cochez cette case si vous souhaitez que l'entrée MultiPOP utilise la méthode d'authentification APOP lors de la récupération du courrier sur l'hôte correspondant.

Utiliser OAuth

Choisissez cette méthode d'authentification lorsque vous collectez du courrier à partir de Gmail ou d'Office365. Voir les <u>instructions OAuth pour MultiPOP 2.0</u> [144] sur la page Paramètres de serveur " MultiPOP pour plus d'informations. **Remarque : l**'option "...modifier les paramètres MultiPOP" sur la page <u>Services Web</u> [771] du compte doit également être activée pour que l'utilisateur puisse utiliser OAuth avec Gmail ou Office 365, car il doit se connecter à Webmail et aller sur la page **Boîtes aux lettres** afin d'authentifier l'entrée de la boîte aux lettres Gmail ou Office 365.

Laisser une copie du message sur le serveur POP3

Cochez cette case si vous souhaitez laisser une copie des messages collectés sur le serveur. Cette option est utile lorsque vous prévoyez de récupérer ces messages ultérieurement à partir d'un autre emplacement. Si vous souhaitez passer outre cette option pour tous les utilisateurs, c'est-à-dire que les messages seront toujours supprimés du serveur POP après avoir été téléchargés sur MDaemon, vous pouvez le faire en activant*l'option*"MultiPOP supprime toujours*le courrier de tous les serveurs après la collecte* | *Paramètres du serveur* | *MultiPOP*.

Ajouter

Après avoir saisi toutes les informations relatives à la nouvelle entrée MultiPOP, cliquez sur ce bouton pour l'ajouter à la liste.

Supprimer

Si vous souhaitez supprimer une de vos entrées MultiPOP, sélectionnez l'entrée souhaitée et cliquez ensuite sur ce bouton.

Activer/désactiver

En cliquant sur ce bouton, vous modifiez l'état des entrées MultiPOP sélectionnées, ce qui vous permet de déterminer si MDaemon collectera le courrier pour cette entrée ou s'il l'ignorera lorsqu'il effectuera son traitement MultiPOP.

Remplacer

Pour modifier une entrée, cliquez sur l'entrée dans la liste, apportez les modifications souhaitées et cliquez sur ce bouton pour enregistrer les modifications dans l'entrée.

Supprimer les messages de plus de [xx] jours (0 = jamais)

Il s'agit du nombre de jours pendant lesquels un message peut rester sur l'hôte MultiPOP avant d'être supprimé. Utilisez "0" si vous ne souhaitez pas supprimer les messages plus anciens.

Ne pas télécharger les messages de plus de (0 = pas de limite) Ko (0 = pas de limite) Saisissez une valeur ici si vous souhaitez limiter la taille des messages qui peuvent être téléchargés.

Voir :

Paramètres de serveur | MultiPOP 144 Planification de la Collecte MultiPOP 406

5.1.1.12 Alias

Account Details Mail Services Web Services Web Services Autoresponder Forwarding Restrictions Quotas Attachments MAP Filters MultiPOP Aliases Shared Folders App Passwords Signature Administrative Roles Allow List Settings B ActiveSync Remove New Alias - Wildcards ? and " are allowed Alias Actual email Frank thomas@company.test	Account Editor - Frank Thomas	Alaces
Settings	 Account Details Mail Services Web Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases Shared Folders App Passwords Signature Administrative Roles Allow List 	Alases postmaster@company.test = frank.thomas@company.test abuse@company.test = frank.thomas@company.test
	⊕ ActiveSync	Remove New Alias - Wrildcards ? and " are allowed Alias Actual email frank.thomas@company.test (Frank TI v) State Add

Cet écran filtre toutes les adresses <u>Alias</u> associées au compte et permet d'en ajouter ou d'en supprimer.

Suppression d'un alias

Pour supprimer un alias du compte, sélectionnez-le dans la Liste d'alias, puis cliquez sur **Supprimer**.

Ajout d'un alias

Pour ajouter un nouvel alias au compte, tapez dans la case *Alias* l'adresse que vous souhaitez associer au compte, puis cliquez sur **Ajouter**. Les caractères génériques "?" et "*" sont autorisés ; ils représentent respectivement des caractères et des mots isolés.

Voir :

Paramètres des comptes | Alias 894

5.1.1.13 Dossiers partagés

👃 Account Editor - Frank Thomas						×
 Account Settings Account Details Mail Services Web Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases Signature Administrative Roles Allow List Settings ActiveSync 	ne ints id Senders id Senders id Senders id Senders id Senders id tems id tems inents imail if tems if tems ade here cannot be undone by ne	pressing Cancel Folder type Mail	Remove			
			Ok C	ancel	Apply	Help

Cet écran n'est disponible que lorsque l'option Activer les dossiers publics est activée dans l'écran <u>Dossiers publics &</u> <u>partagés</u>[118], situé dans Configuration | Paramètres du serveur | Dossiers publics et partagés. Les Dossiers publics peuvent être gérés à partir du <u>Gestionnaire des Dossiers</u> <u>publics</u>[325].

Cette section affiche tous les Dossiers IMAP partagés de l'utilisateur et peut être utilisée pour partager l'accès à ces dossiers avec d'autres utilisateurs ou <u>groupes</u> <u>de</u> MDaemon . Lorsque le compte est créé, cette section ne contient que la boîte de réception jusqu'à ce que vous utilisiez les options *Nom de dossier* et *Création* (ou les options sur les <u>Filtres IMAP</u> [789]) pour y ajouter des dossiers. Dans cette liste, les noms des sous-dossiers et des dossiers sont séparés par une barre oblique.

Supprimer

Pour supprimer un dossier Dossiers IMAP partagés de la liste, sélectionnez le dossier souhaité, puis cliquez sur le bouton*Supprimer*.

Nom de dossier

Pour ajouter un nouveau dossier à la liste, indiquez-lui un nom dans cette option et cliquez sur *Créer*. Si vous souhaitez que le nouveau dossier soit un sous-dossier de l'un des dossiers de la liste, préfixez le nom du nouveau dossier par le nom du dossier parent et une barre oblique. Exemple : si le dossier parent est "Mon dossier", le nom du nouveau dossier sera "Mon dossier/Mon Nouveau dossier". Si vous ne souhaitez pas qu'il s'agisse d'un sous-dossier, nommez le nouveau dossier "Mon Nouveau Dossier" sans le préfixe.

Imbriquer sous

Utilisez la liste déroulante pour choisir le dossier parent sous lequel ce dossier partagé sera imbriqué. **Note :** Cette option n'est disponible que dans l' interface web de<u>MDRA</u> [376].

Type de dossier

Utilisez cette liste déroulante pour choisir le Type de dossier que vous souhaitez créer : Courrier, Calendrier, Contacts, etc.

Créer

Après avoir spécifiéle nom d'un dossier, cliquez sur ce bouton pour ajouter le dossier à la liste.

Remplacer

Si vous souhaitez modifier l'un des Dossiers partagés, cliquez sur l'entrée, apportez la modification souhaitée, puis cliquez sur *Remplacer*.

Modifier la liste de contrôle d'accès

Choisissez un dossier, puis cliquez sur ce bouton pour ouvrir la boîte de dialogue<u>Liste de contrôle d'accès</u> [327] pour ce dossier. Utilisez la Liste de contrôle d'accès pour désigner les utilisateurs ou les groupes qui pourront accéder au dossier et les autorisations pour chaque utilisateur ou groupe.

Voir :

Contrôle d'accès 327

Gestionnaire des dossiers publics 325

5.1.1.13.1 Liste de contrôle d'accès

La Liste de contrôle d'accès (ACL) est utilisée pour définir les droits d'accès des utilisateurs ou des groupes pour vos <u>Dossiers publics et partagés</u> [116]. On y accède à partir du bouton *Modifier les listesde contrôle d'accès* dans le <u>Gestionnaire des</u> <u>dossiers publics</u> [325] ou du bouton *Modifier la liste de contrôle d'accès* dans l'écran Dossiers publics et partagés de l'Éditeur de comptes.

curité Général		
om de robjet: Contacts oms de groupes ou d'utili	sateurs:	
Nom	Туре	E-mail
🥝 anyone	Intégrés	
😹 Bill Farmer	Utilisateur	Bill.Farmer@company.test
📚 company test Membr	es Groupe	anyone@company.test
🚨 Frank Thomas	Utilisateur	Frank.Thomas@company.test
🚨 Michael Mason	Utilisateur	michael.mason@company.test
😹 Randy Peterman	Utilisateur	Randy.Peterman@company.test
our modifier les droits d'a	iccès, cliquez su	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès	ccès, cliquez su ner Autorisa	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration	accès, cliquez su ner Autorisa	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création	ccès, cliquez su ner Autorisa Non Non	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer	ccès, cliquez su ier Autorisa Non Non Non	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu"	accès, cliquez su ner Autorisa Non Non Non Non	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion	eccès, cliquez su ner Autorisa Non Non Non Non Non	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion V Consultation	ccès, cliquez su ier Autorisa Non Non Non Non Non Oui	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion Consultation Envoi	ccès, cliquez su ner Autorisa Non Non Non Non Non Oui Non	ur Modifier Modifi <u>e</u> r
our modifier les droits d'a roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion Consultation Envoi Lecture	ccès, cliquez su ner Autorisa Non Non Non Non Oui Non Oui	ur Modifier Modifi <u>e</u> r

Sécurité	
Chemin du dossier:	C:\MDaemon\Public Folders \company.test.IMAP\Contacts.IMAP
Nom de dossier:	Contacts
Type de dossier:	IPF.Contact
Nombre d'éléments:	2
Taille du dossier:	719
Nombre de sous-dossiers IMAP:	0
Éléments dans les sous-dossiers:	0
Taille des sous-dossiers IMAP:	0
ID ActiveSync:	
ID partagé ActiveSync:	
ID utilisateur ActiveSync:	
<u>O</u> uvrir	Ouvrir le dossier dans l'Explorateur Windows
Commentaires sur le dossier:	

Sécurité

Cet onglet affiche la liste des groupes ou des utilisateurs associés au dossier et les autorisations d'accès spécifiques accordées à chacun. Dans la liste, sélectionnez un groupe ou un utilisateur afin d'afficher ses <u>autorisations</u> dans la fenêtre Permissions ci-dessous. Pour modifier les autorisations, cliquez sur <u>Modifier</u> 2001.

Général

Cet onglet affiche les propriétés du dossier, telles que son chemin d'accès, son Nom, son type, sa taille, etc.

Éditeur ACL

Cliquez sur **Modifier** dans l'onglet Sécurité de la liste de contrôle d'accès pour ouvrir l'éditeur de liste de contrôle d'accès afin de modifier les autorisations d'accès.

Noms de groupes ou d'utilisateurs:				
Nom	Туре	E-mail		
onyone 🕗	Intégrés			
😽 Bill Farmer	Utilisateur	Bill.Farmer@company.test		
📚 company.test Membres	Groupe	anyone@company.test		
😣 Frank Thomas	Utilisateur	Frank.Thomas@company.test		
😞 Michael Mason	Utilisateur	michael.mason@company.test		
🚨 Randy Peterman	Utilisateur	Randy.Peterman@company.test		
'oits d'accès de Bill Farm	her	Ajouter Supprimer		
roits d'accès de Bill Farm Droit d'accès	ner Autorisa	Ajouter Supprimer		
oits d'accès de Bill Farm Droit d'accès Administration	ner Autorisa Non	Ajouter Supprimer		
roits d'accès de Bill Farm Droit d'accès Administration Création	ner Autorisa Non Non	Ajouter Supprimer		
roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer	ner Autorisa Non Non Non	Ajouter Supprimer		
roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu"	ner Autorisa Non Non Non Non	Ajouter Supprimer		
roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion	ner Autorisa Non Non Non Non Oui	Ajouter Supprimer		
roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion Consultation Envoi	ner Autorisa Non Non Non Non Oui Non	Ajouter Supprimer		
roits d'accès de Bill Farm Droit d'accès Administration Création Supprimer Marqueur "lu" Insertion Consultation Envoi Lecture	ner Autorisa Non Non Non Non Oui Non Oui	Ajouter Supprimer		

Par nom

Votre nom est celui de l'objet ou du dossier auquel les autorisations de la liste de contrôle d'accès s'appliqueront.

Nom du groupe ou de l'utilisateur

Il s'agit des groupes ou des utilisateurs auxquels un certain niveau d'accès a été accordé. Sélectionnez un groupe ou un utilisateur pour afficher ses autorisations dans la fenêtre*Autorisations pour <groupe ou utilisateur* > ci-dessous. Cochez la case en regard de toute autorisation d'accès que vous souhaitez accorder au groupe ou à l'utilisateur.

Ajouter

Pour accorder des autorisations d'accès à un groupe ou à un utilisateur qui ne figure pas dans la liste ci-dessus, cliquez sur **Ajouter** 31.

Supprimer

Pour supprimer un groupe ou un utilisateur, sélectionnez son entrée dans la liste cidessus et cliquez sur **Supprimer**.

Autorisations pour <groupe ou utilisateur>

Cochez la case en regard de toute autorisation d'accès que vous souhaitez accorder au groupe ou à l'utilisateur sélectionné ci-dessus.

Vous pouvez accorder les autorisations de contrôle d'accès suivantes :

- Administrer l'utilisateur peut gérer les droits d'accès d'un dossier.
- Créer l'utilisateur peut créer des sous-dossiers dans ce dossier.
- Supprimer l'utilisateur peut supprimer des éléments de ce dossier.
- Marqueur lu l'utilisateur peut modifier l'état lu/non lu des messages de ce dossier.
- Insérer l'utilisateur peut ajouter et copier des éléments dans ce dossier.
- **Liste des dossiers** l'utilisateur peut voir ce dossier dans sa liste personnelle de dossiers IMAP.
- **Dossiersiers -** l'utilisateur peut envoyer du courrier directement à ce dossier (si le dossier le permet).
- **Lire** l'utilisateur peut ouvrir ce dossier et en consulter le contenu.
- **Écrire l'** utilisateur peut modifier les drapeaux sur les messages de ce dossier.

Appliquer à tous les dossiers enfants

Cochez cette case si vous souhaitez appliquer les autorisations de contrôle d'accès de ce dossier à tous les sous-dossiers qu'il contient actuellement. Cela ajoutera les autorisations d'utilisateur et de groupe du dossier aux dossiers enfants, en les remplaçant en cas de conflit. Toutefois, cela ne supprimera pas les autres autorisations d'utilisateur ou de groupe qui ont actuellement accès à ces dossiers.

Exemple,

Le dossier parent accorde certaines autorisations à User_A et User_B. Le dossier enfant accorde des autorisations à User_B et User_C. Cette option ajoutera les autorisations de User_A au dossier enfant, remplacera les autorisations de User_B du dossier enfant par celles du dossier parent et ne modifiera pas les autorisations de User_C. Le dossier enfant disposera donc des autorisationsUser A, User B et User C.

Écraser les dossiers enfants

Cochez cette case si vous souhaitez que toutes les autorisations d'accès des dossiers enfants soient remplacées par les autorisations actuelles du dossier parent. Les autorisations du dossier enfant seront alors identiques à celles du dossier parent.

Ajout d'un groupe ou d'un utilisateur

Cliquez sur **Ajouter** dans l'éditeur ACL si vous souhaitez ajouter un autre groupe ou utilisateur à la liste de contrôle d'accès. L'écran Ajouter un groupe ou un utilisateur s'ouvre et vous permet de le rechercher, puis de l'ajouter.

💷 Sélectio	on d'utilisateur	s, de groupes ou d'objets intégrés	×
Sélecti d'a De c	ionner les types objets suivants: :es domaines : es communes	Intégré, Groupes, Utilisateurs Tous les domaines	Types d' <u>o</u> bjets Emplacements
L	Le <u>n</u> om contient L'e- <u>m</u> ail contient		
La <u>d</u> es	cription contient	isactivés	
<u>R</u> ésultats (de la recherche	Aide	Annuler
Nom Ty	ype E-mail		

Sélectionnez ces types d'objets

Cliquez sur **Types d'objets...** pour sélectionner les types d'objets dans lesquels vous souhaitez rechercher les groupes ou les utilisateurs que vous souhaitez ajouter. Vous pouvez sélectionner : Intégré, Groupes et Utilisateurs.

À partir de ces emplacements

Cliquez sur **Lieux...** pour sélectionner les domaines que vous souhaitez rechercher. Vous pouvez sélectionner Tous les domaines MDaemon ou des domaines spécifiques.

Requêtes courantes

Utilisez les options de cette section pour limiter votre recherche en spécifiant tout ou partie du nom de l'utilisateur, son adresse électronique ou le contenu de la Description du compte. Laissez ces champs vides si vous souhaitez que les résultats de la recherche contiennent tous les groupes et utilisateurs correspondant aux types d'objets et aux emplacements spécifiés ci-dessus.

Inclure les comptes désactivés

Cochez cette case si vous souhaitez inclure les <u>comptes désactivés</u> dans votre recherche.

Rechercher maintenant

Une fois que vous avez spécifié tous vos critères de recherche, cliquez sur **Rechercher maintenant** pour effectuer la recherche.

Chercher les résultats

Dans les résultats de la recherche, sélectionnez les groupes ou utilisateurs souhaités et cliquez sur **OK** pour les ajouter à la liste de contrôle d'accès.

Les droits d'accès sont contrôlés grâce à laprise en charge parMDaemondes listes de contrôle d'accès (ACL). L'ACL est une extension du protocole IMAP4 (Internet Message Access Protocol) qui vous permet de créer une liste d'accès pour chacun de vos Dossiers de courrier IMAP, accordant ainsi des droits d'accès aux dossiers à d'autres utilisateurs qui ont également des comptes sur votre serveur de messagerie. Si votre client de messagerie ne prend pas en charge l'ACL, vous pouvez toujours définir les autorisations à l'aide des commandes de cette boîte de dialogue.

L'ACL est traité en détail dans la RFC 2086, qui peut être consultée à l'adresse <u>suivante</u> : http://www.rfc-editor.org/rfc/rfc2086.txt.

Voir :

Gestionnaire des dossiers publics325Dossiers publics - Vue d'ensemble116Dossiers publics & partagés118Éditeur de compte | Dossiers partagés796Liste des dossiers | Dossiers publics314

5.1.1.14 Mots de passe d'application

👶 Account Editor - Frank Thomas		
Account Settings	App passwords	
 Account Details Mail Services Web Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases Shared Folders Agmature Administrative Roles Allow List Settings ActiveSync 	Name Created Last Used Last IP ID Phone email app 10/13/2021 1 cdef2e87 0ed61710 Tablet mail app 10/13/2021 1 0ed61710 adde82ec Changes made here cannot be undone by pressing Cancel Remove Name Create Rename Rename	
	Ok Cancel Apply Help	

Mots de passe d'application

Les Mots passe d'application sont des mots de passe très forts, générés de manière aléatoire, à utiliser dans les clients de messagerie et les applications, afin de rendre vos applications de messagerie plus sécurisées puisqu'elles ne peuvent pas être protégées par l'<u>Authentification à deux facteurs</u> [77] (2FA). L'authentification à deux facteurs est un moven sûr pour un utilisateur de se connecter au Webmail ou à MDaemon Remote Admin (MDRA), mais une application de messagerie ne peut pas l'utiliser, car l'application doit pouvoir accéder à votre messagerie en arrière-plan sans que vous ayez à saisir un code à partir de votre application d'authentification. La fonctionnalité Mots de passe d'application vous permet de créer des mots de passe forts et sécurisés à utiliser dans vos apps, tout en conservant le mot de passe de votre compte sécurisé par 2FA. Les Mots passe d'application ne peuvent être utilisés que dans les applications de messagerie, ils ne peuvent pas être utilisés pour se connecter à Webmail ou MDRA. Cela signifie que même si un mot de passe d'application était compromis, l'utilisateur non autorisé ne pourrait pas accéder à votre compte pour modifier votre mot de passe ou d'autres paramètres, mais vous, vous seriez toujours en mesure de vous connecter à votre compte avec votre mot de passe de compte et 2FA, pour supprimer le mot de passe compromis et en créer un nouveau si nécessaire.

Si vous ne souhaitez pas autoriser un utilisateur à utiliser les Mots mots passe, vous pouvez le faire en désactivant l'option <u>...modifier les mots passe de l'application</u> $\overline{m_1}$ sur la page des Services Web de l'utilisateur. Si vous souhaitez désactiver la prise en

_____1

804

charge des Mots passe d'application pour tous les utilisateurs, vous pouvez le faire en utilisant l'option<u>Activer les mots passe d'application</u> au la page Mots passe.

Exigences relatives aux mots passe d'application et recommandations

- Dans le but de créer des mots passe d'application, 2FA doit être activé pour le compte (bien que vous puissiez <u>désactiver cette exigence</u> si vous le souhaitez).
- Les Mots passe d'application ne peuvent être utilisés que dans les applications de messagerie - ils ne peuvent pas être utilisés pour se connecter à Webmail ou MDRA.
- Chaque Mot de passe d'application n'est affiché qu'une seule fois, lors de sa création. Il n'y a aucun moyen de le récupérer plus tard, les utilisateurs doivent donc être prêts à le saisir dans leur application lorsqu'il est créé.
- Les utilisateurs doivent utiliser un Mot de passe d'application différent pour chaque application de messagerie, et ils doivent révoquer (supprimer) leur mot de passe chaque fois qu'ils cessent d'utiliser une application ou en cas de perte ou de vol d'un appareil.
- Chaque Mot de passe d'application indique la date de sa création, la date de sa dernière utilisation et l'adresse IP à partir de laquelle il a accédé pour la dernière fois à la messagerie du compte. Si un utilisateur trouve quelque chose de suspect dans les données de Dernière utilisation ou de Dernière IP, il doit révoquer ce Mot de passe d'application et en créer un nouveau pour son application.
- Lorsque le mot de passe d'un compte est modifié, tous les Mots passe d'application sont automatiquement supprimés l'utilisateur ne peut pas continuer à utiliser d'anciens Mots passe d'application.

Création et utilisation des mots de passe d'application

Les utilisateurs créent et gèrent leurs propres mots de passe d'application à partir de Webmail en suivant les étapes décrites ci-dessous (ces informations sont incluses dans le fichier d'aide de Webmail). Avant de commencer, l'utilisateur doit avoir son application ou son client de messagerie prêt à saisir le mot de passe, car le Mot de passe d'application ne sera affiché qu'une seule fois lors de sa création.

- 1. Préparez l'application ou le client de messagerie à saisir le Mot de passe d'application.
- 2. Connexion à MDaemon Webmail et cliquez sur **Options | Sécurité**.
- 3. Dans Mot de passe actuel, entrez le mot de passe du compte .
- 4. Cliquez sur **Nouveau mot de passe d'application**.
- 5. Saisissez le nom de l'application qui utilisera ce mot de passe (par exemple, "Phone email app"), puis cliquez sur **OK**.
- Copiez/collez ou saisissez manuellement le mot de passe affiché dans l'application de messagerie, ou collez-le dans un fichier texte ou notez-le si nécessaire. Si l'on copie le mot de passe pour l'utiliser plus tard, il faut alors

supprimer la copie après l'avoir saisi dans son client de messagerie. Lorsque vous avez terminé, cliquez sur **OK**.

Si, pour une raison quelconque, vous devez créer ou supprimer un Mot passe d'application pour l'un de vos utilisateurs, vous pouvez le faire en utilisant les options de cette page. Tout comme dans le Webmail, le Mot de passe d'application ne sera affiché qu'une seule fois lors de sa création, il doit donc être immédiatement saisi dans l'application ou copié quelque part pour être remis à l'utilisateur ultérieurement.



Il existe une option de compte sur la page<u>Paramètres des</u> <u>comptes de l'éditeur de compte</u> [815] que vous pouvez utiliser pour "*Exiger un mot de passe d'application pour se connecter* à SMTP, IMAP, ActiveSync, etc."

Demander des Mots passe d'application peut aider à protéger le mot de passe d'un compte contre les attaques par dictionnaire et par force brute via SMTP, IMAP, etc. Cette solution est plus sûre car même si une attaque de ce type permettait de deviner le mot de passe réel d'un compte, elle ne fonctionnerait pas et l'attaquant ne le saurait pas, car MDaemon n'accepterait qu'un Mot passe Mon compte correct. De plus, si vos comptes dans MDaemon utilisent l' authentification<u>Active Directory</u> and et que Active Directory verrouille un compte après un certain nombre de tentatives échouées, cette option permet d'éviter le verrouillage des comptes, car MDaemon ne vérifiera que les Mots passe d'application, et n'essaiera pas de s'authentifier auprès d'Active Directory.

Voir aussi

<u>Mots de passe</u> জাচী <u>Mon compte | Paramètres des comptes</u> জাচী

5.1.1.15 Signatures

👵 Account Editor - Frank Thomas -		x
 Account Settings Account Details Mail Services Web Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases Shared Folders App Passwords Signature Allow List Settings ActiveSync 	Append the following text to all emails sent from account.	<
	Ok Cancel Apply H	elp

Signature du compte

Utilisez cet écran pour désigner une signature qui sera ajoutée au bas de chaque email envoyé par le compte. Cette signature est ajoutée en plus de toutes les autres signatures ou pieds de page ajoutés par d'autres options, telles que l'option de signature incluse dans le Webmail et d'autres clients de messagerie, les options Signatures <u>par défaut</u> [32] et <u>Domaine</u> [210], et <u>les pieds de page Liste de diffusion</u> [311]. Les Signatures <Domain par défaut> et les pieds de page des listes de diffusion sont toujours ajoutés sous les Signatures du compte.

Les utilisateurs ayant accès au Webmail ou au <u>MDaemon Remote Admin</u> [376] peuvent modifier leurs propres signatures à partir de là.

Macros de signature

Les signatures MDaemon prennent en charge les macros qui insèrent dans la signature les Informations de contact de l'expéditeur, extraites du contact de l'expéditeur situé dans le Dossier public de son domaine. Cela permet de personnaliser les signatures par défaut et par domaine avec les informations de l'expéditeur. Par exemple, \$CONTACTFULLNAME\$ insère le nom complet de l'expéditeur et \$CONTACTEMAILADDRESS\$ insère l'adresse électronique de l'expéditeur. Utilisez Webmail, MDaemon Connector ou ActiveSync pour modifier les contacts publics. Des valeurs vides sont utilisées si aucun contact n'existe pour l'expéditeur. Les macros disponibles sont listées ci-dessous.

Les utilisateurs peuvent contrôler l'emplacement des signatures MDaemon dans leurs

courriers électroniques en plaçant l'une des macros**du Sélecteur de signature** dans un message, à l'endroit où ils souhaitent que la signature apparaisse.

Sélecteur de signature	
\$SYSTEMSIGNATURE\$	Place la <u>Signature par défaut (132</u>) ou la <u>Signature du</u> <u>domaine (210</u>) dans un message. Si les deux existent, c'est la signature de domaine qui est utilisée.
SIGNATURE DU CLIENT	Place la <u>Signature client par défaut</u> [138] ou la <u>Signature client par domaine dans</u> [216] un message. Si les deux existent, c'est la Signature client du domaine qui est utilisée.
\$ACCOUNTSIGNATURE\$	Place la <u>signature du compte</u> m ¹ dans le message.
Par noms et identifiants	
Votre nom complet	\$CONTACTFULLNAME\$\$ (NOM DE LA PERSONNE À CONTACTER)
Votre nom	\$CONTACTFIRSTNAME\$ (PRÉNOM DU CONTACT)
Deuxième prénom	\$CONTACTMIDDLENAME\$,
Votre nom	NOM DE FAMILLE \$CONTACTLASTNAME\$
Titre	TITRE \$CONTACTTITLE
Suffixe	SUFFIXE \$CONTACTSUFFIX\$
Surnom	NOM DE FAMILLE DU CONTACT
Votre nom	PRÉNOM DE YOMI \$CONTACTYOMIFIRSTNAME
Votre nom\$ \$contactyomifirstname\$ \$contactyomilastname	NOM DE FAMILLE \$CONTACTYOMILASTNAME\$
Nom du compte	NOM DU COMPTE \$CONTACTACCOUNTNAME\$
ID du client	\$CONTACTCUSTOMERID\$ (IDENTIFIANT DU CLIENT)
Identifiant du gouvernement	ID DU GOUVERNEMENT \$CONTACTGOVERNMENTID
Fichier comme	FICHIER EN TANT QUE \$CONTACTFILEAS\$
Adresses électroniques	
Adresse électronique	ADRESSE ÉLECTRONIQUE \$CONTACTEMAILADDRESS
Cette adresse électronique [2	ADRESSE DE COURRIEL 2\$ \$CONTACTEMAILADDRESS2

Cette adresse électronique 3	\$CONTACTEMAILADDRESS3\$ (ADRESSE DE COURRIER ÉLECTRONIQUE)
Numéros de téléphone et de	e fax
Téléphone portable	TÉLÉPHONE PORTABLE \$CONTACTHOMEMOBILE
Téléphone portable 2	\$CONTACTMOBILE2
Téléphone de voiture	\$CONTACTNUMÉRODEVOITURE
Téléphone fixe	\$CONTACT TÉLÉPHONE DOMICILE
Téléphone fixe 2	\$CONTACTHOMEPHONE2\$ \$CONTACTHOMEPHONE3\$ \$CONTACTHOMEPHONE4
Fax à domicile	\$CONTACTHOMEFAX
Autre téléphone	\$CONTACTAUTRETÉLÉPHONE
Messagerie instantanée et V	Neb
Adresse IM	ADRESSE DE MESSAGERIE INSTANTANÉE \$CONTACTTIMADDRESS
Adresse de messagerie instantanée 2	ADRESSE DE MESSAGERIE INSTANTANÉE 2\$ \$CONTACTIMADDRESS2
Adresse IM 3	\$CONTACTIMADDRESS3
Adresse MMS	ADRESSE MMS\$ \$CONTACTMMSADDRESS
Adresse web du domicile	ADRESSE WEB DU DOMICILE \$CONTACTHOMEWEBADDRESS
Adresse de la maison	
Adresse du domicile	\$CONTACTHOMEADDRESS
Ville du domicile	\$CONTACTHOMECITY\$
État du domicile	ÉTAT DU DOMICILE \$CONTACTHOMESTATE
Code postal du domicile	CODE POSTAL DU DOMICILE \$CONTACTHOMEZIPCODE
Pays d'origine	PAYS DU DOMICILE \$CONTACTHOMECOUNTRY
Autre adresse	\$CONTACTAUTREADRESSE
Autre ville	\$CONTACTOTHERCITY\$ (AUTRE VILLE)
Autre état	\$CONTACTAUTREÉTAT\$ AUTRE CODE POSTAL
Autre code postal	\$CONTACTOTHERZIPCODE\$ AUTRE CODE POSTAL

Autre pays	\$CONTACTOTHERCOUNTRY
Entreprise	
Nom de l'entreprise	\$CONTACTBUSINESSCOMPANY\$ (EN ANGLAIS)
Nom de l'entreprise Votre nom	\$CONTACTYOMICOMPANYNAME\$ (NOM DE L'ENTREPRISE)
Titre de l'entreprise	TITRE DE L'ENTREPRISE \$CONTACTBUSINESSTITLE
Bureau de l'entreprise	BUREAU DE L'ENTREPRISE \$CONTACTBUSINESSOFFICE\$
Département de l'entreprise	DÉPARTEMENT DE L'ENTREPRISE \$CONTACTBUSINESSDEPARTMENT
Chef d'entreprise	CONTACT MANAGER D'ENTREPRISE \$CONTACTBUSINESSMANAGER
Assistant(e) commercial(e)	ASSISTANT COMMERCIAL \$CONTACTBUSINESSASSISTANT
Téléphone de l'assistant commercial	TÉLÉPHONE DE L'ASSISTANT D'AFFAIRES \$CONTACTBUSINESSASSISTANT\$
Téléphone principal de l'entreprise	TÉLÉPHONE PRINCIPAL DE L'ENTREPRISE \$CONTACTBUSINESSMAINPHONE\$
Téléphone de l'entreprise	TÉLÉPHONE PRINCIPAL \$CONTACTBUSINESSMAINPHONE\$ TÉLÉPHONE PROFESSIONNEL \$CONTACTBUSINESSMAINPHONE\$ TÉLÉPHONE PROFESSIONNEL \$CONTACTBUSINESSMAINPHONE
Téléphone professionnel 2	TÉLÉPHONE PROFESSIONNEL 2\$ \$CONTACTBUSINESSPHONE2
Téléphone IP professionnel	TÉLÉPHONE IP PROFESSIONNEL \$CONTACTBUSINESSIPPHONE
Fax professionnel	FAX PROFESSIONNEL \$CONTACTBUSINESSFAX
Téléavertisseur professionnel	TÉLÉAVERTISSEUR D'ENTREPRISE \$CONTACTBUSINESSPAGER
Radio professionnelle	RADIO PROFESSIONNELLE \$CONTACTBUSINESSRADIO\$
Adresse professionnelle	ADRESSE DE L'ENTREPRISE \$CONTACTBUSINESSADDRESS
Ville de l'entreprise	VILLE DE L'ENTREPRISE \$CONTACTBUSINESSCITY

État de l'entreprise	ÉTAT DE L'ENTREPRISE \$CONTACTBUSINESSSTATE\$
Code postal de l'entreprise	CODE POSTAL DE L'ENTREPRISE \$CONTACTBUSINESSZIPCODE\$
Pays de l'entreprise	PAYS DE L'ENTREPRISE \$CONTACTBUSINESSCOUNTRY
Adresse web de l'entreprise	ADRESSE WEB DE L'ENTREPRISE \$CONTACTBUSINESSWEBADDRESS
Autre	
Conjoint	\$CONTACTCONJOINT\$
Enfants	\$CONTACTENFANTS\$
Catégories	CATÉGORIES\$ DE CONTACT
Commentaire	COMMENTAIRE\$CONTACT

Voir :

Signatures par défaut 132 Signatures de domaine 210 Pieds de page des listes de diffusion 311

5.1.1.16 Rôles d'administration

👃 Account Editor - Frank Thomas -		×
 Account Editor - Frank Thomas - Account Settings Account Details Mail Services Web Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases Shared Folders App Passwords Signature 	Administrative Roles Adcount is a global administrator Account is a domain administrator Enter any notes you wish to save for your reference.	^
Administrative Roles Allow List Settings ActiveSync	Ok Cancel Apply He	elp

Rôles d'administration

Ce compte est administrateur global

Activez cette case à cocher pour accorder à l'utilisateur un accès administratif au niveau du serveur. Les administrateurs globaux ont :

- Accès complet à la configuration du serveur, à tous les utilisateurs et à tous les domaines via Serveur Remote Admin.
- Un accès à tous les utilisateurs de tous les domaines MDaemon en tant que contacts de messagerie instantanée.
- La possibilité d'envoyer des messages à toutes les listes de diffusion, même si elles sont marquées comme "Lecture seule".
- La possibilité d'envoyer des messages aux listes de diffusion même s'il n'est pas membre.

L'utilisateur aura un accès complet auxfichiers et aux options de MDaemon. Pour plus d'informations sur les options d'administration de l'interface web d'administration à distance, voir Administration à distance

Ce compte est administrateur de domaine

Cochez cette case pour désigner l'utilisateur en tant qu'Administrateur de domaine. Les administrateurs de domaine sont similaires aux administrateurs globaux, sauf que leur accès administrateur est limité à ce domaine et aux autorisations accordées sur la page<u>Services Web.</u>

Si vous souhaitez autoriser ce compte à administrer un autre domaine, vous pouvez le faire à partir de l'interface web de<u>MDaemon Remote Admin</u> (376), sur la page Gestionnaire de domaines | Administrateurs.

Entrez les commentaires que vous souhaitez conserver.

Utilisez cet espace pour toute note ou autre information que vous souhaitez enregistrer pour votre propre référence concernant ce compte. Contrairement au champ <u>Description</u> de l'écran<u>Informations générales du compte</u> sera pas synchronisée avec les contacts publics ni associée à un champ dans Active Directory.

5.1.1.17 Liste d'autorisation

🚨 Account Editor - Frank Thomas -		×
 → Account Settings → Account Details → Mail Services → Web Services → Mail Folder & Groups → Autoresponder → Forwarding → Restrictions → Quotas → Attachments → IMAP Filters → MultiPOP → Aliases → Shared Folders → App Passwords → Signature → Administrative Roles → Allow List → Settings ⊕ ActiveSync 	Allow Listing The following options require global on/off switches on the Spam Filter Allow List (automatic) screen to be enabled in order to function. Spam Filter uses personal contacts, allowed senders, and blocked senders This following option does not function when an autoresponder is operating. Automatically add mail recipients to allowed senders Remove contacts which are missing name or phone data	
	Ok	Cancel Apply Help

Liste d'autorisation

Le Filtre anti-spam utilise les contacts personnels, les expéditeurs autorisés et les expéditeurs bloqués

L'écran<u>Liste d'autorisation (automatique)</u> L'écran<u>Liste d'autorisation (automatique)</u> L'écran<u>Liste d'autorisation (automatique)</u> L'as du Filtre anti-spam contient une option globale qui peut être utilisée pour que le Filtre anti-spam autorise automatiquement un message lorsque l'expéditeur du message est trouvé dans les contacts personnels du destinataire local ou dans le dossier des expéditeurs autorisés. Il bloquera également automatiquement un message lorsque l'expéditeur se trouve dans le

dossier Expéditeurs bloqués de l'utilisateur. Si vous avez activé l'option globale du Filtre anti-spammais que vous ne souhaitez pas l'appliquer à ce compte, décochez cette case pour remplacer le paramètre global. Si l'option globale est désactivée, cette option ne sera pas disponible.

Ajouter automatiquement les destinataires des e-mails aux expéditeurs autorisés Cochez cette option si vous souhaitez mettre à jour ledossier \$SENDER\$ - adresse de l'expéditeur autorisé de ce comptechaque fois qu'il envoie un message sortant à une adresse e-mail non locale. Dans le cas où le *Filtre anti-spam utilise les contacts personnels, les expéditeurs autorisés et les expéditeurs bloqués,* en conjonction avec l'option ci-dessus, le nombre de faux positifs du Filtre anti-spam peut être considérablement réduit. L'option *Ajouter automatiquement les destinataires des e-mails aux expéditeurs autorisés* située sur l' écranListe expéditeur (automatique).



Cette option est désactivée lorsque le compte utilise un autorépondeur.

Supprimer les contacts dont le nom ou le numéro de téléphone est manquant

Cliquez sur ce bouton si vous souhaitez supprimer du dossier Contacts par défaut du compte tous les contacts qui ne contiennent qu'une adresse électronique. Si un contact n'a pas au moins un nom ou des données téléphoniques, il sera supprimé. Cette option est principalement destinée à aider les personnes qui utilisaient l'option d'inscription automatique de MDaemon avant la version 11 à se débarrasser des contacts qui ne contiennent pas d'adresse électronique. MDaemon avant la version 11 de Nettoyer et supprimer les contacts qui ont été ajoutés uniquement dans le cadre de la fonction de liste d'autorisation. Dans les versions précédentes de MDaemon, les adresses étaient ajoutées aux contacts principaux au lieu d'être placées dans un dossier dédié à la liste d'autorisation. Dans ce cas, le compte pouvait contenir de nombreuses entrées dans le dossier des contacts que l'utilisateur aurait préféré ne pas avoir.



Examinez attentivement cette option avant de l'utiliser, car les contacts ne contenant qu'une adresse électronique peuvent toujours être légitimes.

Paramètres des valeurs par défaut pour les Nouveaux comptes et groupes

Les options de cet écran correspondent à celles de l'écran <u>Propriétés du modèle | Liste</u> <u>d'autorisation</u> au permet de définir les valeurs par défaut pour les <u>Nouveaux</u> <u>comptes</u> at les valeurs pour les comptes appartenant à certains <u>groupes</u>.

Voir :

<u>Liste d'autorisation (automatique)</u> 7उडी <u>Gestionnaire de modèles</u> बिगी <u>Propriétés du modèle | Liste d'autorisation</u> छिन्ही

5.1.1.18 Settings



Paramètres

Masquer le compte des listes "Tout le monde" et du Dossier public du domaine

MDaemon peut créer et gérer automatiquement les <u>listes de diffusion "Everyone@"</u> <u>et "MasterEveryone@"</u>, 284] qui peuvent être utilisées pour envoyer un message à tous les utilisateurs d'un domaine et à tous les utilisateurs de MDaemon, respectivement. Par défaut, ces listes incluent tous les comptes de chaque domaine, mais vous pouvez cocher cette case si vous souhaitez masquer ce compte de ces listes : les messages destinés à ces listes ne seront pas envoyés au compte. Les messages destinés à ces listes ne seront pas envoyés au compte. Cela masquera également le compte du dossier Dossiers publics du domaine.

Placer automatiquement les nouvelles demandes de réunion dans le calendrier, marquées comme provisoires

Par défaut, lorsqu'un compte reçoit une nouvelle demande de réunion, celle-ci est placée dans le calendrier de l'utilisateur et marquée comme *provisoire*.

Le compte traite automatiquement les demandes de réunion et les annulations de réunion.

Cochez cette case si vous souhaitez que les demandes, les modifications et les annulations de réunion soient traitées automatiquement pour ce compte. Lorsque le compte reçoit un message contenant une demande de réunion, le calendrier du compte est automatiquement mis à jour. Cette option est désactivée par défaut pour tous les comptes.

Refuser automatiquement les demandes qui entrent en conflit avec un événement existant

Si le traitement automatique des demandes et des annulations de réunion est activé pour ce compte, ces demandes de réunion seront automatiquement refusées par défaut lorsqu'elles entrent en conflit avec un événement existant. Décochez cette case si vous souhaitez autoriser la création de l'événement en conflit.

Refuser automatiquement les demandes récurrentes

Cochez cette case si le traitement automatique des demandes et des annulations de réunion est activé pour ce compte, mais que vous souhaitez refuser ces demandes lorsqu'elles concernent des réunions récurrentes.

Traiter les requêtes uniquement lorsqu'elles proviennent de ces adresses e-mail

Si vous souhaitez traiter automatiquement les demandes provenant uniquement de certaines adresses électroniques, dressez la liste de ces adresses ici. Séparez chaque adresse par une virgule. Les caractères joker sont autorisés dans les adresses (par exemple <u>*@exemple.com</u>). Si vous laissez cette case vide, n'importe quelle adresse est autorisée.

Le compte peut utiliser le sous-adressage pour router le courrier entrant dans des dossiers

Cochez cette case si vous souhaitez autoriser le <u>sous-adressage</u> [817] pour ce compte.

Ajouter la signature de domaine à tous les messages envoyés par ce compte

Lorsqu'il existe une <u>Signature de domaine</u> 200¹ pour le domaine auquel ce compte appartient, cette option fait en sorte qu'elle soit ajoutée à tous les e-mails envoyés par le compte. Elle est activée par défaut.

Le compte est exempté de la requiert "Les identifiants doivent correspondre à ceux de l'expéditeur de l'e-mail".

Utilisez cette option si vous souhaitez exempter le compte de l'option globale "*Les informations d'authentification doivent correspondre à celles de l'expéditeur du courriel*" située dans l'écran<u>Authentification SMTP</u> 558. Cette option est désactivée par défaut.

Exiger un mot de passe d'application pour se connecter à SMTP, IMAP, ActiveSync, etc. Cochez cette case si vous souhaitez que le compte utilise des <u>Mots passe</u> <u>d'application</u> al dans les clients de messagerie, pour se connecter à SMTP, IMAP, ActiveSync, ou à d'autres protocoles de service de messagerie. Le<u>mot de passe</u> habituel du compte doit cependant être utilisé pour se connecter au Webmail ou à MDaemon Remote Admin.

Demander des Mots passe d'application peut aider à protéger le mot de passe d'un compte contre les attaques par dictionnaire et par force brute via SMTP, IMAP, etc. Cette méthode est plus sûre car même si une attaque de ce type permettait de deviner le mot de passe réel d'un compte, elle ne fonctionnerait pas et l'attaquant n'en saurait rien, car MDaemon n'accepterait qu'un mot de passe Mon compte correct. De plus, si vos comptes dans MDaemon utilisent l' authentification<u>Active</u> Directory at que Active Directory est configuré pour verrouiller un compte après un certain nombre de tentatives échouées, cette option permet d'éviter que les

comptes ne soient verrouillés, car MDaemon ne vérifiera que les Mots passe d'application, sans essayer de s'authentifier auprès d'Active Directory.

Activer le dossier Documents de MDaemon Webmail

Cochez cette case pour activer le dossier Documents pour cet utilisateur. Cette option ne peut être utilisée que si l'option correspondante de la page Paramètres de MDaemon Webmail est activée. **Remarque :** Cette option et les options Liens de Documents ci-dessous ne sont disponibles que dans l' interface web de<u>MDaemon Remote Admin (MDRA)</u> [376].

Le compte est autorisé à partager des liens temporaires vers des documents personnels

Dans cette option, l'utilisateur pourra créer des liens dans le Webmail vers des documents personnels, qui pourront être partagés avec importe qui. Les liens de plus de 30 jours sont automatiquement purgés.

Voir les Liens de Documents

Cliquez sur ce bouton pour afficher la pageLiens de Documents, qui contient une liste de tous les liens actifs que l'utilisateur a créés. À partir de cette page, vous pouvez révoquer les Liens de votre choix. Les liens datant de plus de 30 jours seront automatiquement révoqués.

Afficher tous les Dossiers partagés auxquels ce compte a accès

Cliquez sur ce bouton pour afficher tous les Dossierssiers partagés auxquels le compte a eu accès.

Afficher toutes les listes de diffusion dont ce compte est membre

Cliquez sur ce bouton pour ouvrir une liste de toutes les <u>Listes de diffusion</u> ant ce compte est membre.

Sous-adressage

Le sous-adressage est un système permettant d'inclure un nom de dossier dans la partie boîte aux lettres de l'adresse électronique d'un compte. Grâce à ce système, les messages adressés à la combinaison*boîte aux lettres* + nom de*dossier* sont automatiquement routés vers le dossier du compte inclus dans l'adresse (à condition que ce dossier existe réellement), sans qu'il soit nécessaire de créer des règles de filtrage spécifiques pour y parvenir.

Exemple : si bill.farmer@example.com possède un dossier courrier IMAP appelé "stuff", le courrier adressé à "bill.farmer+stuff@example.com" sera automatiquement acheminé vers ce dossier. Les sous-dossiers peuvent être désignés en incluant les noms du dossier et du sous-dossier séparés par un caractère "+" supplémentaire, et les traits de soulignement sont utilisés pour remplacer les espaces dans les noms de dossiers. Ainsi, pour reprendre l'exemple cidessus, si le dossier"stuff" de Bill comportait un sous-dossier intitulé "my older stuff", les messages adressés à

"bill.farmer+stuff+my_older_stuff@example.com" seraient automatiquement acheminés vers le dossier courrier"\stuff\Nmy older stuff" de Bill. Étant donné que le sous-adressage nécessite l'utilisation du caractère"+", les boîtes aux lettres qui contiennent "+" ne peuvent pas être sous-adressées. Dans l'exemple ci-dessus, si l'adresse réelle était "bill+farmer@example.com" au lieu de "bill.farmer@example.com", elle ne pourrait pasêtre sous-adressée. En outre, vous ne pouvez pas utiliser un Alias d'adresse dans une sous-adresse. Vous pouvez toutefois créer un alias qui se réfère à l'ensemble d'un formulaire de sous-adresse. Ainsi, même si "alias+stuff@example.com" n'est pas autorisé, l'utilisation de"alias@example.com" pour pointer vers "bill.farmer+stuff@example.com" ne pose aucun problème.

Dans le but d'éviter les exploits ou les abus, le dossier IMAP inclus dans la sousadresse **doit être** valide. Si un message sous-adressé arrive pour un compte dont le dossier ne correspond pas au nom du dossier défini dans la sous-adresse, cette dernière sera traitée comme une adresse électronique inconnue, en fonction des autres paramètres définis par MDaemon. Par exemple, si bill.farmer@example.com n'a pas de dossier nommé "stuff" et qu'un message arrive pour "bill.farmer+stuff@example.com", ce message sera traité comme s'il était adressé à un utilisateur inconnu et sera très probablement rejeté.

> Non (par défaut), la fonction de sous-adressage est désactivée pour chaque compte. Vous pouvez toutefois la désactiver globalement via l'option *Désactiver le sousadressage pour tous les comptes* située dans l'écran<u>Divers</u> <u>de</u> al boîte de dialogue Préférences. Si le sous-adressage est désactivé via cette option, il ne sera autorisé pour aucun compte, quels que soient les paramètres des comptes individuels.

Voir :

Liste d'autorisation (automatique) 739 MDaemon Admin 376 Gestionnaire de modèles 847 Mots de passe 915



👶 Account Editor - Frank Thomas -		×
 Account Settings Account Details Mail Services Web Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases Shared Folders App Passwords Signature Administrative Roles Allow List Settings 	ActiveSync Management PlugIn	
	Ok Cancel Apply Help	

Les écrans ActiveSync pour MDaemon de l'Éditeur de comptes permettent d'activer ou de désactiver ActiveSync pour le compte, de configurer les <u>paramètres spécifiques au</u> <u>compte</u> [200], d' <u>attribuer une politique par défaut</u> [200] et de gérer les clients ActiveSync du compte.

Activer/Désactiver ActiveSync pour ce compte

Si vous souhaitez autoriser le compte à utiliser un client ActiveSync pour accéder à sa messagerie et à ses données PIM, activez cette option.

Voir :

Editeur d'Accout | ActiveSync | Paramètres client 201 Éditeur Accout | ActiveSync | Politiques attribuées 2021 Editeur d'Accout | ActiveSync | Clients 2021

5.1.1.19.1 Paramètres du client

🚨 Account Editor - Frank Thomas	
Account Settings	General FolderSync Options Content Handling
Account Details	Troubleshooting
Mail Services	Log level Use inherited or default
Web Services	
Mail Folder & Groups	
- Autoresponder	Validate/correct PIM mrk file integrity
- Forwarding	Client Options
Quetes	
Attachments	Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation
IMAP Filters	New clients require administrative approval
	Max diants per user Use inherited or default
Aliases	Max cients per user luse inherited of default
- Shared Folders	Bandwidth reset Day Use inherited or default \checkmark
App Passwords	Convitu
Signature	Event from Location Screen
Administrative Roles	
Allow List	
Settings	
i ActiveSync	Milow clients provisioned/managed by outer servers
Client Settings	
Assigned Policy	Example of Settings
Clients	Off On Inherit from parent Preview Effective Settings
	Settings are inherited in the order Global, Domain, Group, Account, Client Type, then Client, Any non-
	inherit setting in a subsequent level over-rides the previous level. Group based settings are applied in
<u>[]</u>	lowest to highest priority order. Not all options are available at all levels. If a setting is not available to 🗸
	Ok Cancel Apply Help

Les options de cet écran permettent de contrôler les paramètres du client ActiveSync pour les clients associés à ce compte. Par défaut, chacune de ces options est configurée pour hériter de son paramètre du domaine correspondant auquel le compte appartient. Filtrer des paramètres de cet écran remplacera le <u>paramètre du domaine</u> pour ce compte. En outre, vous pouvez utiliser l' option *Paramètres* de l' écran<u>Clients</u> ar si vous souhaitez remplacer ces paramètres au niveau du compte pour des clients spécifiques.

Général

Résolution des problèmes

Niveau de journalisation

ActiveSync for MDaemon prend en charge six niveaux de journalisation, du plus élevé au plus faible :

- Déboga Il s'agit du niveau de journalisation le plus complet. Il consigne
 ge toutes les entrées disponibles et n'est généralement utilisé que pour diagnostiquer un problème.
 - **Info** Pas de journalisation modérée. Pas de journalisation des opérations

820

générales sans détails. Il s'agit du niveau de journalisation par défaut.

- AvertisLes avertissements, les erreurs, les erreurs critiques et lessementévénements de démarrage/arrêt sont consignés dans le journal.
- **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Critiqu Les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.
- HériterNon (par défaut), le niveau journalisation est hérité de la hiérarchie
des Paramètres clients. Ainsi, les clients héritent leurs paramètres
des Types de clients, les Types de clients des Comptes, les
Comptes des Groupes, etc. Le Paramètres globaux du client pour
cette option est déterminé par le paramètre de niveau de
journalisation dans le dialogue
Diagnostics

Archiver les transactions en [XML | WBXML]

Utilisez les options d'archivage*XML...* et *WBXML* si vous souhaitez enregistrer ces données, qui peuvent parfois être utiles à des fins de débogage. Les options globales sont désactivées par défaut.

Valider/corriger l'intégrité du fichier mrk PIM

Cette option exécute un processus de validation et de correction des données PIM du client afin de rechercher les problèmes connus susceptibles d'empêcher une synchronisation correcte, tels que des UID iCal en double ou des champs facultatifs vides. L'option globale est désactivée par défaut.

Options client

Appliquer les restrictions de protocole

Activez cette option si vous souhaitez refuser les connexions de tout client qui tente d'utiliser un protocole autre que les *Versions du protocole autorisées* spécifiées pour le client. Non (par défaut), cette option est désactivée, ce qui signifie que les restrictions de protocole n'empêchent pas un client d'utiliser un protocole différent ; elles indiquent simplement au client quels protocoles utiliser. Si un client tente malgré tout d'utiliser un protocole restreint, MDaemon autorisera quand même la connexion. Pour plus d'informations, voir <u>Restrictions de protocole</u> [459]

Répondre à 'Get/UserInformation' en utilisant l'alias de l'identifiant comme 'adresse SMTP principale'

Dans ce cas, le service peut renvoyer un Alias/une adresse secondaire en tant qu'adresse primaire en réponse à une requête de type Configurer/Gérer/Informations sur l'utilisateur. Cela permet de contourner un problème causé par une mise à jour postérieure à iOS9.x qui faisait que les clients ne pouvaient pas envoyer de courrier à l'aide d'un alias. L'utilisation de cette option résulte en une réponse non conforme aux spécifications à Settings/Get/UserInformation.

Les nouveaux clients doivent recevoir l'autorisation de l'administrateuravant de synchroniser.

Activez cette option si vous souhaitez que les nouveaux clients soient autorisés par un administrateur avant de pouvoir commencer à se synchroniser avec un compte. La liste <u>Clients</u> indique tous les clients en attente d'autorisation, et l'administrateur peut les autoriser à partir du même écran. Ce paramètre est Non (par défaut).

Max. clients par utilisateur

Si vous souhaitez limiter le nombre de clients ActiveSync ou de terminaux qui peuvent être associés à un compte MDaemon, indiquez le nombre souhaité dans cette option. L'option globale est réglée sur "illimité" par défaut. Cette option est disponible sur les écrans Paramètres clients globaux, de domaine et de compte, et non sur les écrans Clients individuels.

Jour de réinitialisation de la bande passante

Utilisez cette option si vous souhaitez réinitialiser les statistiques d'utilisation de la bande passante pour les Terminaux ActiveSync un jour précis de chaque mois. L'événement de réinitialisation a lieu dans le cadre du processus de maintenance nocturne normal et est consigné dans le journal du système comme les autres routines de maintenance. L'option globale est réglée sur "0 (Jamais)" par défaut, ce qui signifie que les statistiques d'utilisation ne seront jamais réinitialisées. Paramétrez les options enfant sur un jour différent si, par exemple, vous souhaitez que le jour de réinitialisation coïncide avec la date de réinitialisation de la facturation de l'opérateur sans fil d'un utilisateur ou d'un client.

Sécurité

Exclure du Filtrage de pays

Activez cette option dans l'écran des paramètres d'un client ActiveSync si vous souhaitez que l'appareil puisse filtrer l' <u>écran de localisation</u> and localisation and localisation and localisation and localisation and localisation and localisation and localisateur valide de continuer à accéder à son compte via ActiveSync lorsque, par exemple, il se rend à un endroit où les tentatives d'authentification sont bloquées. Pour que l'appareil soit exempté, il doit s'être connecté et authentifié via ActiveSync dans le délai configuré dans le paramètre<u>Supprimer les clients inactifs après ce</u> <u>nombre de jours</u> 443 situé dans l'écran Régètres.

Autoriser dynamiquement l'adresse distante

Si vous excluez un pays du Filtrage de l'emplacement, activez cette option si vous souhaitez également autoriser l'adresse IP distante à partir de laquelle il se connecte. Cela peut s'avérer utile pour autoriser d'autres clients susceptibles de se connecter à partir de la même adresse IP.

Autoriser les clients gérés par d'autres serveurs

Par défaut, lorsque le serveur ActiveSync envoie des données de provisionnement/des spécificités de politiques à un client et que celui-ci signale qu'il est également géré par un autre serveur ActiveSync, le client sera toujours autorisé à se connecter à MDaemon. Dans ce cas, il n'y a aucun moyen de s'assurer que les spécificités de votre politique seront appliquées lorsqu'elles entrent en conflit avec la politique de l'autre serveur ActiveSync. En général, les clients utilisent par défaut l'option la plus restrictive en cas de conflit. Désactivez cette option si vous ne souhaitez pas autoriser ces clients à se connecter.

Interdire les réinitialisations aux paramètres d'usine

Si cette option est activée (On/Oui), il ne sera pas possible d'**effacer complètement** un client ActiveSync. Si vous souhaitez pouvoir effectuer un Effacer complètement à distance sur un client, vous devez d'abord désactiver cette option. L'option est désactivée par défaut. Pour plus d'informations, voir : <u>Effacer</u> <u>complètement un client ActiveSync</u> with sur la page Clients.

Options FolderSync

Options de dossier

Exclure

Dossier Expéditeurs bloqués autorisés/ bloqués

Par défaut, les dossiers Expéditeurs autorisés et Dossiers Expéditeurs bloqués de l'utilisateur ne sont pas synchronisés avec les périphériques. Ils ne sont généralement utilisés par MDaemon que dans le cadre de la prévention automatique du spam. C'est pourquoi ils n'ont pas besoin d'être affichés sur les appareils en tant que contacts.

Dossiers de courrier personnalisés (Non par défaut)

Par défaut, tous les Dossiers de courrier créés par l'utilisateur et par défaut peuvent être synchronisés avec le terminal. Activez cette option si vous souhaitez que seuls les dossiers courrier par défaut soient synchronisés, c'est-àdire la Boîte de réception, les Éléments envoyés, les Éléments supprimés, les Brouillons, etc. Aucun dossier créé par l'utilisateur ne sera inclus. Cette option est désactivée par défaut.

Dossiers PIM personnalisés non (par défaut)

Par défaut, tous les dossiers PIM de l'utilisateur (contacts, calendrier, notes, tâches, etc.) sont synchronisés avec l'appareil. Activez cette option si vous souhaitez que seuls les dossiers PIM par défaut soient synchronisés. Exemple : si cette option est activée et qu'un utilisateur possède plusieurs dossiers de calendrier, seul le calendrier par défaut sera synchronisé. Cette option est désactivée par défaut.

Inclure

Arborescence Dossiers publics

Cochez cette case si vous souhaitez que les <u>Dossiers publics</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les Dossiers publics

auxquels il a accès. Cette option est autorisée par défaut.

Navigation dans les dossiers publics (affiche les noms de dossiers)

Non par défaut, pour qu'un client puisse synchroniser un sous-dossier public ou y accéder, le compte doit disposer de l'<u>autorisation de Recherche</u> [327] pour le sousdossier (c'est-à-dire le dossier enfant) et tous les <u>Dossiers publics</u> [325] parents situés au-dessus. Si le compte n'a pas l'autorisation de voir les dossiers parents, il ne peut pas non plus voir le dossier enfant, même s'il en a l'autorisation. Activez cette option si vous souhaitez autoriser le client à accéder à ces dossiers enfants. **Par nom : l** 'activation de cette option doit nécessairement révéler les noms des dossiers parents au client, ce qui pourrait être considéré comme un risque de sécurité. Cette option est désactivée par défaut.

Nombre max de Dossiers publics

Utilisez cette option si vous souhaitez limiter le nombre de Dossiers publics autorisés sur le périphérique. Lorsqu'une limite est définie, le serveur parcourt la liste des dossiers jusqu'à ce que la limite soit atteinte, puis plus aucun dossier n'est envoyé à l'appareil. Il n'existe aucun moyen de garantir l'ordre dans lequel les dossiers seront traités. Non (paramètres par défaut).

Dossiers IMAP partagés

Cochez cette case si vous souhaitez que les <u>dossiers partagés</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers partagés</u> auxquels il a accès. Cette option est autorisée par défaut.

Gestion du contenu

Options de gestion des e-mails

Créer des tâches/rappels pour les e-mails avec indicateurs

Cette option permet à MDaemon de rappeler à l'utilisateur les éléments marqués, en créant un élément de tâche pour chaque courrier électronique marqué. lorsque le client le demande. L'option globale de ce contrôle est activée par défaut.

Toujours envoyer les mises à jour de réunion lorsque l'événement est modifié

Certains clients n'envoient pas correctement les e-mails de mise à jour des réunions lorsqu'ils modifient une réunion. Cette option indique au service ActiveSync d'envoyer une mise à jour de la réunion lorsqu'un élément de la réunion est mis à jour par l'organisateur. Cette option ne doit être définie que pour les <u>clients</u> al et les <u>types de clients</u> al qui n'envoient pas correctement les mises à jour de réunion, sous peine d'envoyer des mises à jour de réunion en double. Par conséquent, cette option n'est disponible que dans les pages de paramètres pour les Clients et les Types de clients.

Demander des confirmations de lecture pour tous les e-mails envoyés

Activez cette option si vous souhaitez que le serveur demande des confirmations de lecture pour tous les courriers envoyés par un client. Cette option est désactivée par défaut.

Envoyer des confirmations de lecture du serveur lorsque le courrier est marqué comme lu et lorsque l'expéditeur le demande.

Activez cette option si vous souhaitez que le serveur prenne en charge les demandes de confirmation de lecture et délivre un accusé de réception de lecture lorsqu'un message est marqué comme lu par un client. Cette option est désactivée par défaut.

Envoyer avec l'alias spécifié dans ReplyTo

Certains clients peuvent ne pas autoriser un expéditeur à envoyer du courrier à l'aide d'un alias. Cette fonctionnalité a été ajoutée au <u>protocole Exchange ActiveSync</u> (EAS) (453) 16.x, mais certains clients ne supportent pas la version 16.x. Par exemple, Outlook pour Windows n'utilise que EAS 14.0, et bien qu'il permette à un utilisateur de spécifier une autre adresse pour l'envoi, le message généré ne reflète pas correctement les choix de l'utilisateur. Cette faculté permet d'utiliser le champ ReplyTo pour envoyer l'e-mail, à condition que l'adresse ReplyTo soit un <u>alias</u> valide (1994) pour cet utilisateur. L'option globale est activée par défaut.

Fusionner virtuellement les contacts publics et les contacts par défaut

Activez cette option si vous souhaitez fusionner les contacts publics avec les contacts par défaut de l'utilisateur sur le terminal. Il s'agit uniquement d'une fusion virtuelle, c'est-à-dire qu'ils ne sont pas réellement copiés dans le dossier des contacts de l'utilisateur. Cela peut être utile sur les clients qui ne prennent pas en charge les recherches dans la liste d'adresses globale (GAL). Non (par défaut).

Dossiers Expéditeurs bloqués lors du déplacement d'un courrier dans le dossier Courriers indésirables

Si cette option est activée, lorsqu'un client déplace un e-mail vers le dossier Courriers indésirables du compte, le service ajoute l'adresse SENDER\$ - adresse de l'expéditeur de cet e-mail au dossier Contacts des expéditeurs bloqués.

Forcer l'envoi des réponses aux réunions lorsqu'une demande de réunion est acceptée/déclinée, etc.

Dans cette option, lorsqu'un client accepte, refuse ou choisit une action en réponse à une demande de réunion, le service envoie une réponse à l'organisateur de la réunion. Cette fonction est destinée aux clients spécifiques qui n'envoient pas correctement ces mises à jour eux-mêmes.

Aperçu des paramètres effectifs

Ce bouton est disponible sur tous les écrans des Paramètres clients enfant (c.-à-d. <u>domaines</u> [422], <u>comptes</u> [479] et <u>clients</u> [488]). Non (par défaut), les options de ces écrans sont définies pour hériter de leurs paramètres d'un écran parent. Utilisez cette fonction pour voir quels paramètres sont actuellement appliqués à l'écran affiché.

Voir :

ActiveSync | Domaines 462 Éditeur Accout | ActiveSync | Clients 827

5.1.1.19.2 Politiques assignées

👶 Account Editor - Frank Thomas -			—
 Account Editor - Frank Thomas - Account Settings Account Details Mail Services Web Services Mail Folder & Groups Autoresponder Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases Shared Folders App Passwords Signature Administrative Roles Allow List Settings ActiveSync Client Settings Clients 	Select Policy for Account Current Effective Policy <no effective="" policy<br="">Policy to Assign <no policy="" set=""></no></no>	frank.thomas@company.test licy y>	
			Curved Araba Ulda
		UK	Салса Арру Пер

Utilisez cet écran pour désigner la <u>Politique ActiveSync</u> [470] par défaut qui sera utilisée pour tout client ActiveSync qui se connecte à l'aide de ce compte. Par défaut, ce paramètre de stratégie est hérité <u>de celui du domaine</u> [242], mais vous pouvez le modifier ici pour remplacer ce paramètre pour ce compte. En outre, vous pouvez également remplacer ce paramètre spécifique au compte et attribuer une politique différente à des <u>clients</u> [327] spécifiques.

Attribuer une Politique ActiveSync attribuée

Pour attribuer une politique au compte, cliquez sur la liste déroulante Politique à appliquer. **Politique à appliquer**, choisissez la politique et cliquez sur **Ok** ou **Appliquer**.



Tous les Terminaux ActiveSync ne reconnaissent pas ou n'appliquent pas les politiques de manière cohérente. Certains peuvent ignorer les politiques ou certains éléments de politique, et d'autres peuvent nécessiter un redémarrage de l'appareil avant que les changements ne prennent effet. De plus, lorsque vous tentez d'attribuer une nouvelle politique, elle ne sera pas appliquée à un terminal avant la prochaine connexion de ce dernier au serveur ActiveSync ; les politiques ne peuvent pas être "poussées" vers les terminaux avant qu'ils ne se connectent.

Voir :

ActiveSync | Gestionnaire des politiques ActiveSync 470 ActiveSync | Domaines ActiveSync 462 Editeur d'Accout | ActiveSync | Clients 827

5.1.1.19.3 Clients

🔒 Account Editor - Frank Thomas -				×
Account Settings Account Details Mail Services Web Services	* Right-Click on or press the Co Email Address	ntext-Menu on an aci Client Type	<u>R</u> efresh count key to make modifications Client ID	Prob
Mail Folder & Groups Autoresponder	frank.thomas@company.test frank.thomas@company.test	iPad SAMSUNGSGHI747	AppIDMRJJX05F182 SEC192C55F9C4C8A	14.1 14.1
Forwarding Restrictions Quotas Attachments IMAP Filters MultiPOP Aliases Shared Folders App Passwords Signature Administrative Roles Allow List Settings	frank.thomas@company.test	WindowsOutlook15	90907568DAE942CFA4F56DFDD279579E	>
- ActiveSync - Client Settings - Assigned Policy Clients	Filter Client Listing to A	l dients	~	
			Ok Cancel	Apply Help

Cet écran affiche des informations sur tous les clients ActiveSync associés au compte de l'utilisateur. A partir de cet écran, vous pouvez attribuer une <u>Politique ActiveSync</u> a chaque client, contrôler les différents paramètres du client, supprimer des clients, les effacer à distance, et réinitialiser les statistiques du client dans MDaemon.

ActiveSync Client		×
Email Address	frank.thomas@company.test	^
Domain	company.test	
Client Type	iPad	
Client ID	14A65AD03AA182FADF712A69	
User Agent	UA_iPad/9.6.9.8	
Client Model	iPad 4.22	
IMEI	528514162102	
Friendly Name	Frank's iPad	
Operating System	Fizzbin Mobile Systems 20.0	
Operating System Language	en-us	
Phone Number	8175559876	
Mobile Operator	Example Wireless Ltd.	
IP Address	192.168.0.100	
Last GMT Logon Time	2023-01-03T16:43:28.000Z (2023-01-03 10:43:28)	
Protocol Version	16.1	
Effective Policy	<no policy="" set=""></no>	
Device Wipe Requested	No	
Account Only Wipe Requested	No	
Authorization Time Stamp	2022-06-10T19:13:58.420Z (2022-06-10 14:13:58)	
Authorization made by	MDAirSync	
192, 168, 0, 100	2023-01-03T16:00:00.000Z (2023-01-03 10:00:00)	~

Détails du client ActiveSync

Double-cliquez sur une entrée, ou cliquez avec le bouton droit de la souris sur l'entrée et cliquez sur **Voir les détails du client**, pour ouvrir la boîte de dialogue Détails du client. Cet écran filtre les informations relatives au client, telles que son Type de client, son ID client, l'heure de sa dernière connexion, etc.

Paramètres clients

Cliquez avec le bouton droit de la souris sur un client et cliquez sur **Personnaliser les paramètres du client** pour gérer ses Paramètres clients. Par défaut, ces paramètres sont hérités des paramètres du Type de client, mais ils peuvent être ajustés comme vous le souhaitez. Voir <u>Gérer les paramètres des clients d'un appareilGérer les</u>

Attribuer une Politique ActiveSync attribuée

Pour Attribuer une <u>Politique</u> 470 du terminal : Cliquez avec le bouton droit de la souris sur le terminal dans la liste:

- 1. Cliquez avec le bouton droit de la souris sur un périphérique dans la liste.
- 2. Cliquez sur **Appliquer politique**. La boîte de dialogue Appliquer une politique s'ouvre.
- 3. Cliquez sur la liste déroulante**Politique à appliquer** et choisissez la politique souhaitée.
- 4. Cliquez sur OK.

Statistiques de

Cliquez avec le bouton droit de la souris sur une entrée, puis cliquez sur **Afficher les statistiques** pour ouvrir la boîte de dialogue Statistiques du client, qui contient diverses statistiques d'utilisation pour le client.
Réinitialiser les statistiques

Si vous souhaitez réinitialiser les statistiques d'un client, cliquez avec le bouton droit de la souris sur le client, cliquez sur **Réinitialiser les statistiques**, puis sur **OK** pour confirmer l'action.

Suppression d'un client ActiveSync

Pour supprimer un client ActiveSync, cliquez avec le bouton droit de la souris sur le client et cliquez sur **Supprimer**, puis sur **Oui**. Cela supprimera le client de la liste et toutes les informations de synchronisation le concernant dans MDaemon. Dans ce cas, si à l'avenir le compte utilise ActiveSync pour synchroniser le même client, MDaemon traitera le client comme s'il n'avait jamais été utilisé sur le serveur ; toutes les données du client devront être resynchronisées avec MDaemon.

Effacer complètement un client ActiveSync

Lorsqu'une politique [470] a été appliquée à un client ActiveSync sélectionné, et que le client l'a appliquée et a répondu, il y aura une option d'Effacement complètement disponible pour ce client. Si c'est le cas, cliquez avec le bouton droit de la souris sur le client (ou sélectionnez-le si vous utilisez MDRA) et cliquez sur **Effacer complètement**. Lors de la prochaine connexion du client, MDaemon lui demandera d'effacer toutes les données ou de restaurer les paramètres par défaut. Selon le client, cela peut supprimer tout ce qu'il contient, y compris les applications téléchargées. En outre, tant que l'entrée ActiveSync du client existe, MDaemon continuera d'envoyer la demande d'effacement chaque fois que ce périphérique se connectera à l'avenir. Si, à un moment donné, vous souhaitez supprimer le client, assurez-vous de l'ajouter d'abord à la liste de blocage. d'abord I 'ajouter à la Liste de blocage [454], afin qu'il ne puisse plus se connecter à l'avenir. Enfin, si un terminal effacé est récupéré et que vous souhaitez l'autoriser à se connecter à nouveau, vous devez le sélectionner et cliquer sur **Annuler les actions "Effacer"**. Vous devez également le supprimer de la Liste de blocage.

Effacement du compte d'un client ActiveSync

Pour effacer les données de messagerie et de PIM du compte du client ou de l'appareil, cliquez avec le bouton droit de la souris et cliquez sur **Account Wipe Account Mail and PIM from client (Effacer le courrier et le PIM du client)**. L' option *Effacer le compte* est similaire à l' option*Effacer complètement* expliquée ci-dessus, mais au lieu d'effacer toutes les données, elle effacera uniquement les données du compte, telles que ses e-mails, entrées de calendrier, contacts et autres. Le reste, comme les applications, les photos ou la musique, est laissé en l'état.

Autoriser le client

Si l'option "Les nouveaux clients nécessitent une autorisation administrative" de l' écran <u>Paramètres du client ActiveSync</u> [447] est réglée sur l'autorisation, sélectionnez un client et cliquez sur Approuver le client pour la synchronisation, pour l'autoriser à se synchroniser avec le serveur.

Gérer les paramètres clients d'un terminal

L'écran Paramètres clients au niveau de l'appareil vous autorise à gérer les paramètres d'un appareil spécifique.

Client Settings: frank.thomas@company.test/14A65AD03AA182FADF712A69	×
General FolderSync Options Content Handling	
Troubleshooting Log level Use inherited or default Archive transactions as XML WBXML Validate/correct PIM mrk file integrity	
Client Options Enforce protocol restrictions Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation	
Bandwidth reset Day Use inherited or default V	
Security Exempt from Location Screen Dynamically allow remote address Allow clients provisioned/managed by other servers Disallow Factory Reset Wipes	
Preview Runtime Settings OK Cancel Image: Concel Help Image: Concel Image: Concel	

Non (par défaut), toutes les options de cet écran sont définies sur "Utiliser les paramètres hérités ou par défaut", ce qui signifie que chaque option est paramétrée à partir de l'option correspondante de l' écran<u>Paramètres clients de Types clients</u>. Toute modification apportée aux paramètres de cet écran sera répercutée sur cet écran. Inversement, toute modification apportée à cet écran remplacera le paramètre du type de clients pour ce terminal.

Général

Résolution des problèmes

Niveau de journalisation

ActiveSync for MDaemon prend en charge six niveaux de journalisation, du plus élevé au plus faible :

DébogaIl s'agit du niveau de journalisation le plus complet. Il consignegetoutes les entrées disponibles et n'est généralement utilisé que

pour diagnostiquer un problème.

- **Info** Pas de journalisation modérée. Pas de journalisation des opérations générales sans détails. Il s'agit du niveau de journalisation par défaut.
- **Avertis** Les avertissements, les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont consignés dans le journal.
- **Erreur** Les erreurs, les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- **Critiqu** Les erreurs critiques et les événements de démarrage/arrêt sont journalisés.
- Aucun Seuls les événements de démarrage et d'arrêt sont journalisés.
- **Hériter** Non (par défaut), le niveau journalisation est hérité de la hiérarchie des Paramètres clients. Ainsi, les clients héritent leurs paramètres des Types de clients, les Types de clients des Comptes, les Comptes des Groupes, etc. Le Paramètres globaux du client pour cette option est déterminé par le paramètre de niveau de journalisation dans le dialogue<u>Diagnostics</u>[457].

Archiver les transactions en [XML | WBXML]

Utilisez les options d'archivage*XML...* et *WBXML* si vous souhaitez enregistrer ces données, qui peuvent parfois être utiles à des fins de débogage. Les options globales sont désactivées par défaut.

Valider/corriger l'intégrité du fichier mrk PIM

Cette option exécute un processus de validation et de correction des données PIM du client afin de rechercher les problèmes connus susceptibles d'empêcher une synchronisation correcte, tels que des UID iCal en double ou des champs facultatifs vides. L'option globale est désactivée par défaut.

Options client

Appliquer les restrictions de protocole

Activez cette option si vous souhaitez refuser les connexions de tout client qui tente d'utiliser un protocole autre que les *Versions du protocole autorisées* spécifiées pour le client. Non (par défaut), cette option est désactivée, ce qui signifie que les restrictions de protocole n'empêchent pas un client d'utiliser un protocole différent ; elles indiquent simplement au client quels protocoles utiliser. Si un client tente malgré tout d'utiliser un protocole restreint, MDaemon autorisera quand même la connexion. Pour plus d'informations, voir <u>Restrictions de protocole</u> [459] pour plus d'informations.

Répondre à 'Get/UserInformation' en utilisant l'alias de l'identifiant comme 'adresse SMTP principale'

Dans ce cas, le service peut renvoyer un Alias/une adresse secondaire en tant

qu'adresse primaire en réponse à une requête de type Configurer/Gérer/Informations sur l'utilisateur. Cela permet de contourner un problème causé par une mise à jour postérieure à iOS9.x qui faisait que les clients ne pouvaient pas envoyer de courrier à l'aide d'un alias. L'utilisation de cette option résulte en une réponse non conforme aux spécifications à Settings/Get/UserInformation.

Les nouveaux clients doivent recevoir l'autorisation de l'administrateuravant de synchroniser.

Activez cette option si vous souhaitez que les nouveaux clients soient autorisés par un administrateur avant de pouvoir commencer à se synchroniser avec un compte. La liste <u>Clients</u> indique tous les clients en attente d'autorisation, et l'administrateur peut les autoriser à partir du même écran. Ce paramètre est Non (par défaut).

Max. clients par utilisateur

Si vous souhaitez limiter le nombre de clients ActiveSync ou de terminaux qui peuvent être associés à un compte MDaemon, indiquez le nombre souhaité dans cette option. L'option globale est réglée sur "illimité" par défaut. Cette option est disponible sur les écrans Paramètres clients globaux, de domaine et de compte, et non sur les écrans Clients individuels.

Jour de réinitialisation de la bande passante

Utilisez cette option si vous souhaitez réinitialiser les statistiques d'utilisation de la bande passante pour les Terminaux ActiveSync un jour précis de chaque mois. L'événement de réinitialisation a lieu dans le cadre du processus de maintenance nocturne normal et est consigné dans le journal du système comme les autres routines de maintenance. L'option globale est réglée sur "0 (Jamais)" par défaut, ce qui signifie que les statistiques d'utilisation ne seront jamais réinitialisées. Paramétrez les options enfant sur un jour différent si, par exemple, vous souhaitez que le jour de réinitialisation coïncide avec la date de réinitialisation de la facturation de l'opérateur sans fil d'un utilisateur ou d'un client.

Sécurité

Exclure du Filtrage de pays

Activez cette option dans l'écran des paramètres d'un client ActiveSync si vous souhaitez que l'appareil puisse filtrer l' <u>écran de localisation</u> [603]. Cela permet à un utilisateur valide de continuer à accéder à son compte via ActiveSync lorsque, par exemple, il se rend à un endroit où les tentatives d'authentification sont bloquées. Pour que l'appareil soit exempté, il doit s'être connecté et authentifié via ActiveSync dans le délai configuré dans le paramètre<u>Supprimer les clients inactifs</u> après ce nombre de jours [443] situé dans l'écran Régètres.

Autoriser dynamiquement l'adresse distante

Si vous excluez un pays du Filtrage de l'emplacement, activez cette option si vous souhaitez également autoriser l'adresse IP distante à partir de laquelle il se connecte. Cela peut s'avérer utile pour autoriser d'autres clients susceptibles de se connecter à partir de la même adresse IP.

Autoriser les clients gérés par d'autres serveurs

Par défaut, lorsque le serveur ActiveSync envoie des données de

provisionnement/des spécificités de politiques à un client et que celui-ci signale qu'il est également géré par un autre serveur ActiveSync, le client sera toujours autorisé à se connecter à MDaemon. Dans ce cas, il n'y a aucun moyen de s'assurer que les spécificités de votre politique seront appliquées lorsqu'elles entrent en conflit avec la politique de l'autre serveur ActiveSync. En général, les clients utilisent par défaut l'option la plus restrictive en cas de conflit. Désactivez cette option si vous ne souhaitez pas autoriser ces clients à se connecter.

Interdire les réinitialisations aux paramètres d'usine

Si cette option est activée (On/Oui), il ne sera pas possible d'**effacer complètement** un client ActiveSync. Si vous souhaitez pouvoir effectuer un Effacer complètement à distance sur un client, vous devez d'abord désactiver cette option. L'option est désactivée par défaut. Pour plus d'informations, voir : <u>Effacer</u> <u>complètement un client ActiveSync</u> with sur la page Clients.

Options FolderSync

Options de dossier

Exclure

Dossier Expéditeurs bloqués autorisés/ bloqués

Par défaut, les dossiers Expéditeurs autorisés et Dossiers Expéditeurs bloqués de l'utilisateur ne sont pas synchronisés avec les périphériques. Ils ne sont généralement utilisés par MDaemon que dans le cadre de la prévention automatique du spam. C'est pourquoi ils n'ont pas besoin d'être affichés sur les appareils en tant que contacts.

Dossiers de courrier personnalisés (Non par défaut)

Par défaut, tous les Dossiers de courrier créés par l'utilisateur et par défaut peuvent être synchronisés avec le terminal. Activez cette option si vous souhaitez que seuls les dossiers courrier par défaut soient synchronisés, c'està-dire la Boîte de réception, les Éléments envoyés, les Éléments supprimés, les Brouillons, etc. Aucun dossier créé par l'utilisateur ne sera inclus. Cette option est désactivée par défaut.

Dossiers PIM personnalisés non (par défaut)

Par défaut, tous les dossiers PIM de l'utilisateur (contacts, calendrier, notes, tâches, etc.) sont synchronisés avec l'appareil. Activez cette option si vous souhaitez que seuls les dossiers PIM par défaut soient synchronisés. Exemple : si cette option est activée et qu'un utilisateur possède plusieurs dossiers de calendrier, seul le calendrier par défaut sera synchronisé. Cette option est désactivée par défaut.

Inclure

Arborescence Dossiers publics

Cochez cette case si vous souhaitez que les <u>Dossiers publics</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers publics</u> auxquels il a accès. Cette option est autorisée par défaut.

Navigation dans les dossiers publics (affiche les noms de dossiers)

Non par défaut, pour qu'un client puisse synchroniser un sous-dossier public ou y accéder, le compte doit disposer de l'<u>autorisation de Recherche</u> [327] pour le sous-dossier (c'est-à-dire le dossier enfant) et tous les <u>Dossiers publics</u> [325] parents situés au-dessus. Si le compte n'a pas l'autorisation de voir les dossiers parents, il ne peut pas non plus voir le dossier enfant, même s'il en a l'autorisation. Activez cette option si vous souhaitez autoriser le client à accéder à ces dossiers enfants. **Par nom : l** 'activation de cette option doit nécessairement révéler les noms des dossiers parents au client, ce qui pourrait être considéré comme un risque de sécurité. Cette option est désactivée par défaut.

Nombre max de Dossiers publics

Utilisez cette option si vous souhaitez limiter le nombre de Dossiers publics autorisés sur le périphérique. Lorsqu'une limite est définie, le serveur parcourt la liste des dossiers jusqu'à ce que la limite soit atteinte, puis plus aucun dossier n'est envoyé à l'appareil. Il n'existe aucun moyen de garantir l'ordre dans lequel les dossiers seront traités. Non (paramètres par défaut).

Dossiers IMAP partagés

Cochez cette case si vous souhaitez que les <u>dossiers partagés</u> auxquels un utilisateur a accès soient inclus dans la liste des dossiers de l'utilisateur sur les Terminaux ActiveSync. Cette option est activée par défaut.

Autoriser les recherches

Autorise le client à effectuer des recherches dans les <u>Dossiers partagés</u> auxquels il a accès. Cette option est autorisée par défaut.

Gestion du contenu

Options de gestion des e-mails

Créer des tâches/rappels pour les e-mails avec indicateurs

Cette option permet à MDaemon de rappeler à l'utilisateur les éléments marqués, en créant un élément de tâche pour chaque courrier électronique marqué. lorsque le client le demande. L'option globale de ce contrôle est activée par défaut.

Toujours envoyer les mises à jour de réunion lorsque l'événement est modifié

Certains clients n'envoient pas correctement les e-mails de mise à jour des réunions lorsqu'ils modifient une réunion. Cette option indique au service ActiveSync d'envoyer une mise à jour de la réunion lorsqu'un élément de la réunion est mis à jour par l'organisateur. Cette option ne doit être définie que pour les <u>clients</u> and et les <u>types de clients</u> out qui n'envoient pas correctement les mises à jour de réunion, sous peine d'envoyer des mises à jour de réunion en double. Par conséquent, cette option n'est disponible que dans les pages de paramètres pour les Clients et les Types de clients.

Demander des confirmations de lecture pour tous les e-mails envoyés

Activez cette option si vous souhaitez que le serveur demande des confirmations de lecture pour tous les courriers envoyés par un client. Cette option est désactivée par défaut.

Envoyer des confirmations de lecture du serveur lorsque le courrier est marqué comme lu et lorsque l'expéditeur le demande.

Activez cette option si vous souhaitez que le serveur prenne en charge les demandes de confirmation de lecture et délivre un accusé de réception de lecture lorsqu'un message est marqué comme lu par un client. Cette option est désactivée par défaut.

Envoyer avec l'alias spécifié dans ReplyTo

Certains clients peuvent ne pas autoriser un expéditeur à envoyer du courrier à l'aide d'un alias. Cette fonctionnalité a été ajoutée au <u>protocole Exchange</u> <u>ActiveSync (EAS)</u> [459] 16.x, mais certains clients ne supportent pas la version 16.x. Par exemple, Outlook pour Windows n'utilise que EAS 14.0, et bien qu'il permette à un utilisateur de spécifier une autre adresse pour l'envoi, le message généré ne reflète pas correctement les choix de l'utilisateur. Cette faculté permet d'utiliser le champ ReplyTo pour envoyer l'e-mail, à condition que l'adresse ReplyTo soit un <u>alias</u> <u>valide</u> [364] pour cet utilisateur. L'option globale est activée par défaut.

Fusionner virtuellement les contacts publics et les contacts par défaut

Activez cette option si vous souhaitez fusionner les contacts publics avec les contacts par défaut de l'utilisateur sur le terminal. Il s'agit uniquement d'une fusion virtuelle, c'est-à-dire qu'ils ne sont pas réellement copiés dans le dossier des contacts de l'utilisateur. Cela peut être utile sur les clients qui ne prennent pas en charge les recherches dans la liste d'adresses globale (GAL). Non (par défaut).

Dossiers Expéditeurs bloqués lors du déplacement d'un courrier dans le dossier Courriers indésirables

Si cette option est activée, lorsqu'un client déplace un e-mail vers le dossier Courriers indésirables du compte, le service ajoute l'adresse SENDER\$ - adresse de l'expéditeur de cet e-mail au dossier Contacts des expéditeurs bloqués.

Forcer l'envoi des réponses aux réunions lorsqu'une demande de réunion est acceptée/déclinée, etc.

Dans cette option, lorsqu'un client accepte, refuse ou choisit une action en réponse à une demande de réunion, le service envoie une réponse à l'organisateur de la réunion. Cette fonction est destinée aux clients spécifiques qui n'envoient pas correctement ces mises à jour eux-mêmes.

Aperçu des paramètres effectifs

Ce bouton est disponible sur tous les écrans des Paramètres clients enfant (c.-à-d. <u>domaines</u> [462], <u>comptes</u> [479] et <u>clients</u> [488]). Non (par défaut), les options de ces écrans sont définies pour hériter de leurs paramètres d'un écran parent. Utilisez cette fonction pour voir quels paramètres sont actuellement appliqués à l'écran affiché. Voir :

ActiveSync | Paramètres du client 447 ActiveSync | Domaines 462 ActiveSync | Comptes 479

5.2 Groupes & Modèles

5.2.1 Gestionnaire de groupes

🧐 Groups & Templates	
 Group Manager Dept A Dept B Template Manager New Accounts Mail Services Web Services Groups Autoresponder Forwarding Quotas Attachments Allow List Settings Sample Template 	Group Management New group Delete group Rename group Copy group Add or remove accounts from the selected group Count: 2 Groups Dept A Dept B Dept B
	Ok Cancel Apply Help

Le Gestionnaire de groupes (Comptes | Modèles des comptes... | Gestionnaire de groupes) permet de créer des groupes de comptes et de gérer les comptes qui leur appartiennent. Les groupes ont un certain nombre d'utilisations et de fonctions différentes. Exemple : à l'aide de l' écran Propriétés des groupes (autribuer un modèle de [947] compte à un groupe, ce qui vous permet de contrôler divers paramètres de compte pour les membres du groupe. Vous pouvez également contrôler si les membres du groupe ont accès ou non à la Messagerie instantanée de [947] sur les groupes, ce qui vous permet de contenu prend en charge les groupes, ce qui vous permet de créer des conditions de règles basées [997] sur le fait que l'expéditeur ou le destinataire d'un message est ou n'est pas membre d'un groupe spécifique. Enfin, pour les Dossiers IMAPAP partagés [116], vous pouvez attribuer des droits deListe de contrôle d'accès à [327] des Groupes spécifiques, ce qui signifie que tous les membres de ce Groupe partageront ces droits d'accès.

Copyright © 1996-2025. All rights reserved. MDaemon Technologies

Vous pouvez ajouter des comptes à un groupe en sélectionnant le groupe dans la liste ci-dessous, puis en cliquant sur le bouton "*Ajouter ou supprimer des comptes…*". Vous pouvez également ajouter des utilisateurs à des groupes à partir de l'écran Dossier de courrier & Groupes de chaque utilisateur.

Gestion de groupes

Nouveau groupe

Pour créer un nouveau groupe de comptes, cliquez sur *Nouveau groupe*, tapez un nom et une description pour le groupe, puis cliquez sur *OK*. Le nouveau groupe apparaît dans la liste des groupes ci-dessous et dans le volet de gauche.

Supprimer un groupe

Pour supprimer un groupe, sélectionnez-le dans la liste ci-dessous, cliquez sur *Supprimer le groupe* et cliquez sur *Oui* pour confirmer votre décision de supprimer le groupe.

Renommer un groupe

Pour renommer un groupe, sélectionnez-le dans la liste ci-dessous et cliquez sur *Renommer le groupe*. Nom et type du nouveau groupe et cliquez sur *OK*.

Copier un groupe

Si vous souhaitez créer un groupe dont les paramètres correspondent à ceux d'un autre groupe, sélectionnez un groupe dans la liste, cliquez sur ce bouton, puis indiquez un nom et une description pour le nouveau groupe.

Ajouter ou supprimer des comptes du groupe sélectionné

Pour gérer ce compte appartient(x) à un groupe, sélectionnez un groupe dans la liste ci-dessous et cliquez sur ce bouton. Cochez la case en regard des comptes que vous souhaitez ajouter au groupe et décochez la case en regard des membres que vous souhaitez supprimer. Cliquez sur Ok.

Voir :

<u>Dossier de courrier & Groupes</u> ୮୦୦ <u>Création d'une nouvelle règle du Filtre de contenu</u> ଭମ <u>Dossiers IMAP partagés</u> 116

5.2.1.1 Propriétés du groupe

838

🧐 Groups & Templates - Dept A	×
Group Manager Dept A Dept B Dept B New Accounts Mail Services Web Services Groups Autoresponder Forwarding Quotas Attachments Allow List Settings Sample Template	Group Properties Describe this group Users in Department A Account template (optional) Sample Template Active Directory group (optional - must enable AD monitoring feature) Closable MD aemon Instant Messenger Disable MD aemon Instant Messenger Disable instant messaging Priority (1-1000 - lower values have priority over higher ones) Create Client Signature Do Not Disturb Normally mail account access is available at all times. Use this feature to schedule a period of time during which accounts may not be accessed. During this time-frame accounts may continue to receive mail but they can't access it. Enable Do Not Disturb Define Do Not Disturb Define Do Not Disturb Define Do Not Disturb
	Ok Cancel Apply Help

L'écran Propriétés du groupe (Comptes | Modèles et groupes... " [nom du groupe]) permet de configurer les paramètres de chaque groupe que vous avez créé à l'aide du Gestionnaire de groupes (a). Pour ouvrir l'écran Propriétés du groupe à partir du Gestionnaire de groupes, double-cliquez sur le groupe que vous souhaitez modifier ou cliquez sur le nom du groupe dans le volet de gauche. Dans cet écran, vous pouvez attribuer un Modèle de compte (a) à un groupe, ce qui vous permet de contrôler divers paramètres de compte pour les membres du groupe. Vous pouvez également lier le groupe à un groupe Active Directory, contrôler si les membres du groupe ont accès ou non à MDaemon Instant Messenger (MDIM [335]) et à la messagerie instantanée, et définir un niveau de priorité pour le groupe. Pour contrôler l'appartenance à un groupe, utilisez les écrans Gestionnaire de comptes et Dossier courrier & Groupes de [768]

Propriétés du groupe

Décrire ce groupe

Saisissez ici une description du groupe, à titre de référence. Ces informations sont généralement saisies lors de la création du groupe, mais peuvent être modifiées à tout moment à partir de cet écran.

Modèle de compte (facultatif)

Si vous avez créé un <u>Modèle de compte</u> and que vous souhaitez utiliser pour contrôler certains des paramètres des comptes des membres du groupe, utilisez cette liste

déroulante pour sélectionner le modèle souhaité. Lorsqu'un modèle de compte est lié à un groupe, toute catégorie de paramètres de compte désignée dans les <u>Propriétés</u> <u>du modèle</u> and sera utilisée pour tous les comptes appartenant au groupe. Le modèle</u> sera utilisé pour contrôler ces paramètres plutôt que d'utiliser les paramètres individuels du compte dans l'éditeur de compte. Si un compte est retiré d'un groupe qui contrôlait ses paramètres de compte, les paramètres reviendront aux valeurs désignées par le <u>modèle Nouveaux comptes</u>

Si un compte appartient à plusieurs groupes liés à différents modèles, tous les modèles seront utilisés s'il n'y a pas de conflit dans les propriétés du modèle désigné . Si plusieurs modèles sont définis pour contrôler les mêmes propriétés, c'est le premier modèle répertorié qui sera utilisé.

Groupe Active Directory (facultatif - nécessite la surveillance AD)

Utilisez cette option si vous souhaitez lier le groupe à un groupe Active Directory spécifique. Les membres du groupe Active Directory seront automatiquement ajoutés au groupe de comptes. Mais pour que cela fonctionne, vous devez utiliser la fonction de<u>surveillance Active Directory</u>.

Vous pouvez mapper n'importe quel attribut Active Directory que vous souhaitez utiliser comme déclencheur pour l'ajout de comptes à des groupes, bien que l'attribut "memberOf" soit le plus souvent celui à utiliser. Vous pouvez configurer cette fonction en modifiant le fichier ActiveDS.dat dans le bloc-notes. Cette fonctionnalité est désactivée par défaut. Pour l'activer, modifiez ActiveDS.dat et indiquez l'attribut à utiliser pour votre déclencheur de groupe, ou décommentez la ligne "Groups=%memberOf%" dans ActiveDS.dat pour l'utiliser.

Désactiver MDaemon Instant Messenger

Cochez cette case si vous souhaitez désactiver la prise en charge de MDIM pour tous les membres du groupe.

Désactiver la messagerie instantanée

Cochez cette case si vous souhaitez autoriser la prise en charge de MDIM, mais pas sa fonction de messagerie instantanée.

Priorité (1-1000 - les valeurs les plus basses sont prioritaires sur les plus hautes)

Utilisez cette option pour définir un niveau de priorité (1-1000) pour vos groupes, ce qui permet aux comptes d'être membres de plusieurs groupes et d'éviter d'éventuels conflits entre les paramètres des groupes. Exemple : lorsqu'un compte est membre de plusieurs groupes ayant chacun un modèle de compte lié contrôlant les mêmes paramètres, les paramètres du groupe ayant la première priorité seront utilisés. En d'autres termes, un groupe dont la valeur de priorité est "1" aura la priorité sur un groupe dont la valeur est "10". En l'absence de conflit, les paramètres de chaque groupe sont appliqués collectivement. Dans le cas d'une égalité, le premier groupe trouvé l'emporte. Lorsqu'un compte est retiré d'un groupe lié à un modèle de comptes, les paramètres des comptes précédemment contrôlés par le modèle de comptes seront remplacés par les paramètres des comptes désignés par le groupe prioritaire suivant. Si aucun autre groupe ne contrôle ces paramètres, ils reviendront aux paramètres désignés par le modèle Nouveaux comptes

Créer une signature client

Cliquez sur ce bouton si vous souhaitez ajouter une signature client à utiliser pour les membres du groupe. Voir : <u>Signature client du groupe</u>

Ne pas déranger

La fonction Ne pas déranger permet de programmer une période pendant laquelle un compte ne peut pas envoyer de courrier ni être consulté par ses utilisateurs. L'accès pendant une période Ne pas déranger n'est pas autorisé et renvoie une réponse d'erreur appropriée aux demandes d'accès IMAP, POP, SMTP, ActiveSync et Webmail. Mon compte accepte toujours le courrier entrant pour les comptes dans cet état, mais ces comptes ne peuvent pas envoyer de courrier ni être accédés par des clients de messagerie.

Pour appliquer Ne pas déranger à un ou plusieurs comptes :

- 1. Cliquez sur Activer "Ne pas déranger".
- 2. Cliquez sur **Définir la programmation Ne pas déranger**.
- 3. Définissez les dates de début et de fin, les heures de début et de fin et les jours de la semaine pour l'utiliser.
- 4. Cliquez sur **Ok**.
- 5. Utilisez le <u>Gestionnaire des groupes</u> pour affecter à ce groupe tous les comptes qui souhaitent l'utiliser.

Voir :

<u>Gestion de groupes</u> ଛେଗି <u>Dossier de courrier & Groupes</u> ୮୫ଛି <u>Gestionnaire de modèles</u> ଛଣ୍ଟୀ <u>Propriétés du modèle</u> ଛଣ୍ଡି

5.2.1.1.1 Client Signature

Client Signatures	×
This signature can be pushed to Webmail and MDaemon Connector. In Webmail it's called the "System" signature. Groups and domains can have their own signatures, otherwise the default signature is used.	
Plain text signature:	
\$CONTACTFULLNAME\$ \$CONTACTEMAILADDRESS\$	
"Wherever you go, there you are."	
v	
HTML signature (cut-and-paste from your favorite HTML editor): Note: <body>, <html>, and their closing tags will be removed. Plain text signature will be created from HTML when only HTML is given.</html></body>	
_ \$CONTACTFULLNAME\$	
\$CONTACTEMAILADDRESS\$	
<rp><!--</td--><td></td></rp>	
· · · · · · · · · · · · · · · · · · ·	
< >	
Ok Canad Arabi	
UK Lancei Apply Help	

Utilisez cet écran pour créer une signature client pour ce groupe, que vous pouvez transmettre au MDaemon Webmail [366] et au MDaemon Connector [428], afin qu'elle soit utilisée par vos utilisateurs lorsqu'ils composent des messages électroniques. Vous pouvez utiliser les macros [442] listées ci-dessous pour personnaliser la signature, afin qu'elle soit unique pour chaque utilisateur, en incluant des éléments tels que le nom de l'utilisateur, son adresse e-mail, son numéro de téléphone, etc. Si vous avez créé une Signature client par défaut [138] ou une Signature client [216] default [138] >, cette signature sera utilisée à la place de l'une ou l'autre pour les membres du groupe. Utilisez l'option *Transmettre* [366] la signature client si vous souhaitez transmettre la signature client à Webmail et l' option *Transmettre la signature client à Outlook* [428] si vous souhaitez la transmettre à MDaemon Connector. Dans les options de composition de Webmail, la signature client transmise est appelée "Système". Pour MDaemon Connector, vous pouvez désigner un nom pour la signature qui apparaîtra dans Outlook.

Signature en texte clair

Cette zone permet d'insérer une signature en texte brut. Si vous souhaitez désigner une signature html correspondante à utiliser dans la partie text/html des messages multipart, utilisez la zone de*signature HTML* ci-dessous. Si une signature est incluse dans les deux zones, MDaemon utilisera la signature appropriée pour chaque partie du message multipart. Si aucune signature HTML n'est spécifiée, la signature en texte brut sera utilisée dans les deux parties.

Signature HTML (copier-coller à partir de votre éditeur HTML préféré)

Dans cette zone, vous pouvez insérer une signature HTML à utiliser dans la partie texte/html des messages multipart. Si une signature est incluse à la fois dans cette zone et dans la zone de*signature en texte brut* ci-dessus, MDaemon utilisera la signature appropriée pour chaque partie du message multipart. Si aucune signature en texte brut n'est spécifiée, la signature html sera utilisée pour en créer une.

Pour créer votre signature html, saisissez le code html manuellement ou copiez-collez-le directement à partir de votre éditeur HTML préféré. Si vous souhaitez inclure des images en ligne dans votre signature HTML, vous pouvez le faire en utilisant la macro\$ATTACH_INLINE:path_to_image_file\$.

Exemple :

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
\Nimages\r_t_and_arnold.jpg$">
```

Il existe également plusieurs façons d'insérer des images en ligne dans les signatures à partir de l'interface web de l'<u>Administration de mote Admin</u> : 376

- Dans l'écran Signature client de MDaemon Remote Admin, cliquez sur le bouton "Image" de la barre d'outils de l'éditeur HTML et sélectionnez l'onglet upload.
- Dans l'écran Signature client de l'administration à distance, cliquez sur le bouton "Ajouter une image " de la barre d'outils de l'éditeur HTML.
- Glisser-déposer une image dans l'éditeur HTML de l'écran Signature client avec Chrome, FireFox, Safari ou MSIE 10+.
- Copier et coller une image du presse-papiers dans l'éditeur HTMLde l'écran Signature client avec Chrome, FireFox, MSIE 11+.

Les balises <body></body> et <html></html> ne sont pas autorisées dans les signatures et seront supprimées lorsqu'elles seront trouvées.

Macros de signature

Les signatures MDaemon prennent en charge les macros qui insèrent dans la signature les Informations de contact de l'expéditeur, extraites du contact de l'expéditeur situé

dans le Dossier public de son domaine. Cela permet de personnaliser les signatures par défaut et par domaine avec les informations de l'expéditeur. Par exemple, \$CONTACTFULLNAME\$ insère le nom complet de l'expéditeur et \$CONTACTEMAILADDRESS\$ insère l'adresse électronique de l'expéditeur. Utilisez Webmail, MDaemon Connector ou ActiveSync pour modifier les contacts publics. Des valeurs vides sont utilisées si aucun contact n'existe pour l'expéditeur. Les macros disponibles sont listées ci-dessous.

Les utilisateurs peuvent contrôler l'emplacement des signatures MDaemon dans leurs courriers électroniques en plaçant l'une des macros**du Sélecteur de signature** dans un message, à l'endroit où ils souhaitent que la signature apparaisse.

Sélecteur de signature	
\$SYSTEMSIGNATURE\$	Place la <u>Signature par défaut</u> [132] ou la <u>Signature du</u> <u>domaine</u> [210] dans un message. Si les deux existent, c'est la signature de domaine qui est utilisée.
SIGNATURE DU CLIENT	Place la <u>Signature client par défaut</u> [138] ou la <u>Signature client par domaine dans</u> [216] un message. Si les deux existent, c'est la Signature client du domaine qui est utilisée.
\$ACCOUNTSIGNATURE\$	Place la <u>signature du compte</u> [807 []] dans le message.
Par noms et identifiants	
Votre nom complet	\$CONTACTFULLNAME\$\$ (NOM DE LA PERSONNE À CONTACTER)
Votre nom	\$CONTACTFIRSTNAME\$ (PRÉNOM DU CONTACT)
Deuxième prénom	\$CONTACTMIDDLENAME\$,
Votre nom	NOM DE FAMILLE \$CONTACTLASTNAME\$
Titre	TITRE \$CONTACTTITLE
Suffixe	SUFFIXE \$CONTACTSUFFIX\$
Surnom	NOM DE FAMILLE DU CONTACT
Votre nom	PRÉNOM DE YOMI \$CONTACTYOMIFIRSTNAME
Votre nom\$ \$contactyomifirstname\$ \$contactyomilastname	NOM DE FAMILLE \$CONTACTYOMILASTNAME\$
Nom du compte	NOM DU COMPTE \$CONTACTACCOUNTNAME\$
ID du client	\$CONTACTCUSTOMERID\$ (IDENTIFIANT DU CLIENT)
Identifiant du gouvernement	ID DU GOUVERNEMENT \$CONTACTGOVERNMENTID
Fichier comme	FICHIER EN TANT QUE \$CONTACTFILEAS\$

Adresses électroniques	
Adresse électronique	ADRESSE ÉLECTRONIQUE \$CONTACTEMAILADDRESS
Cette adresse électronique [2	ADRESSE DE COURRIEL 2\$ \$CONTACTEMAILADDRESS2
Cette adresse électronique 3	\$CONTACTEMAILADDRESS3\$ (ADRESSE DE COURRIER ÉLECTRONIQUE)
Numéros de téléphone et de	fax
Téléphone portable	TÉLÉPHONE PORTABLE \$CONTACTHOMEMOBILE
Téléphone portable 2	\$CONTACTMOBILE2
Téléphone de voiture	\$CONTACTNUMÉRODEVOITURE
Téléphone fixe	\$CONTACT TÉLÉPHONE DOMICILE
Téléphone fixe 2	\$CONTACTHOMEPHONE2\$ \$CONTACTHOMEPHONE3\$ \$CONTACTHOMEPHONE4
Fax à domicile	\$CONTACTHOMEFAX
Autre téléphone	\$CONTACTAUTRETÉLÉPHONE
Messagerie instantanée et W	Veb
Adresse IM	ADRESSE DE MESSAGERIE INSTANTANÉE \$CONTACTTIMADDRESS
Adresse de messagerie instantanée 2	ADRESSE DE MESSAGERIE INSTANTANÉE 2\$ \$CONTACTIMADDRESS2
Adresse IM 3	\$CONTACTIMADDRESS3
Adresse MMS	ADRESSE MMS\$ \$CONTACTMMSADDRESS
Adresse web du domicile	ADRESSE WEB DU DOMICILE \$CONTACTHOMEWEBADDRESS
Adresse de la maison	
Adresse du domicile	\$CONTACTHOMEADDRESS
Ville du domicile	\$CONTACTHOMECITY\$
État du domicile	ÉTAT DU DOMICILE \$CONTACTHOMESTATE
Code postal du domicile	CODE POSTAL DU DOMICILE \$CONTACTHOMEZIPCODE
Pays d'origine	PAYS DU DOMICILE \$CONTACTHOMECOUNTRY

Autre adresse	\$CONTACTAUTREADRESSE
Autre ville	\$CONTACTOTHERCITY\$ (AUTRE VILLE)
Autre état	\$CONTACTAUTREÉTAT\$ AUTRE CODE POSTAL
Autre code postal	\$CONTACTOTHERZIPCODE\$ AUTRE CODE POSTAL
Autre pays	\$CONTACTOTHERCOUNTRY
Entreprise	
Nom de l'entreprise	\$CONTACTBUSINESSCOMPANY\$ (EN ANGLAIS)
Nom de l'entreprise Votre nom	\$CONTACTYOMICOMPANYNAME\$ (NOM DE L'ENTREPRISE)
Titre de l'entreprise	TITRE DE L'ENTREPRISE \$CONTACTBUSINESSTITLE
Bureau de l'entreprise	BUREAU DE L'ENTREPRISE \$CONTACTBUSINESSOFFICE\$
Département de l'entreprise	DÉPARTEMENT DE L'ENTREPRISE \$CONTACTBUSINESSDEPARTMENT
Chef d'entreprise	CONTACT MANAGER D'ENTREPRISE \$CONTACTBUSINESSMANAGER
Assistant(e) commercial(e)	ASSISTANT COMMERCIAL \$CONTACTBUSINESSASSISTANT
Téléphone de l'assistant commercial	TÉLÉPHONE DE L'ASSISTANT D'AFFAIRES \$CONTACTBUSINESSASSISTANT\$
Téléphone principal de l'entreprise	TÉLÉPHONE PRINCIPAL DE L'ENTREPRISE \$CONTACTBUSINESSMAINPHONE\$
Téléphone de l'entreprise	TÉLÉPHONE PRINCIPAL \$CONTACTBUSINESSMAINPHONE\$ TÉLÉPHONE PROFESSIONNEL \$CONTACTBUSINESSMAINPHONE\$ TÉLÉPHONE PROFESSIONNEL \$CONTACTBUSINESSMAINPHONE
Téléphone professionnel 2	TÉLÉPHONE PROFESSIONNEL 2\$ \$CONTACTBUSINESSPHONE2
Téléphone IP professionnel	TÉLÉPHONE IP PROFESSIONNEL \$CONTACTBUSINESSIPPHONE
Fax professionnel	FAX PROFESSIONNEL \$CONTACTBUSINESSFAX
Téléavertisseur professionnel	TÉLÉAVERTISSEUR D'ENTREPRISE \$CONTACTBUSINESSPAGER

Radio professionnelle	RADIO PROFESSIONNELLE \$CONTACTBUSINESSRADIO\$
Adresse professionnelle	ADRESSE DE L'ENTREPRISE \$CONTACTBUSINESSADDRESS
Ville de l'entreprise	VILLE DE L'ENTREPRISE \$CONTACTBUSINESSCITY
État de l'entreprise	ÉTAT DE L'ENTREPRISE \$CONTACTBUSINESSSTATE\$
Code postal de l'entreprise	CODE POSTAL DE L'ENTREPRISE \$CONTACTBUSINESSZIPCODE\$
Pays de l'entreprise	PAYS DE L'ENTREPRISE \$CONTACTBUSINESSCOUNTRY
Adresse web de l'entreprise	ADRESSE WEB DE L'ENTREPRISE \$CONTACTBUSINESSWEBADDRESS
Autre	
Conjoint	\$CONTACTCONJOINT\$
Enfants	\$CONTACTENFANTS\$
Catégories	CATÉGORIES\$ DE CONTACT
Commentaire	COMMENTAIRE\$CONTACT

Voir :

Signatures client par défaut 138 Signatures par défaut 132 Gestionnaire de domaines | Signatures 210 Mon compte | Signature 807 Gestionnaire de domaines | Paramètres de Webmail 197 Paramètres du client MC | Signature 428

5.2.2 Gestionnaire de modèles

 Groups & Templates - Template Manager Group Manager Template Manager New Accounts Mail Services Web Services Groups Autoresponder Forwarding Quotas Attachments Allow List Settings Sample Template 	Template Management New template Delete template Rename template Copy template The "New Accounts" template is applied to all new accounts. Select a template to delete or rename it. Double-click to edit template properties.
	Ok Cancel Apply Help

Avec le Gestionnaire de modèles (Comptes | Paramètres des comptes... | Gestionnaire de modèles), vous pouvez créer et gérer des Modèles de comptes, qui sont des ensembles nommés de paramètres de comptes pouvant être assignés à des groupes sont provide paramètres de compte appartenant à un ou plusieurs de ces groupes verra les paramètres de compte désignés verrouillés, n'étant contrôlés que par les modèles assignés plutôt que par l'éditeur de compte. Les catégories de paramètres de compte qu'un modèle contrôlera sont désignées dans l' écran despropriétés de chaque modèle , auquel on accède en double-cliquant sur le nom du modèle dans la liste ci-dessous, ou en cliquant sur le modèle dans le volet de gauche.

Gestion des modèles

Nouveau modèle

Pour créer un nouveau Modèle de compte, cliquez sur *Nouveau modèle*, tapez un nom pour le modèle et cliquez sur *OK*. Le nouveau modèle apparaît dans la liste des modèles ci-dessous et dans le volet de gauche.

Supprimer un modèle

Pour supprimer un modèle, sélectionnez-le dans la liste ci-dessous, cliquez sur *Supprimer le modèle* et cliquez sur *Oui* pour confirmer votre décision de supprimer le modèle.

Renommer un modèle

Pour renommer un modèle, sélectionnez le modèle dans la liste ci-dessous et cliquez sur *Renommer le modèle*. Tapez un nouveau nom pour le modèle et cliquez sur *OK*.

Copier un modèle

Si vous souhaitez créer un modèle dont les paramètres correspondent à ceux d'un autre modèle, sélectionnez un modèle dans la liste, cliquez sur ce bouton, puis indiquez le nom du nouveau modèle.

Liste des modèles

La liste située en bas du Gestionnaire de modèles contient tous vos modèles. Filtrez un modèle, puis utilisez les boutons en haut de l'écran pour le supprimer ou le renommer. Double-cliquez sur un modèle pour ouvrir son écran de propriétés (au), à partir duquel vous pouvez désigner les catégories de paramètres des comptes qu'il contrôlera. Vous pouvez accéder directement à n'importe quel modèle et à ses paramètres de compte à l'aide des contrôles situés dans le volet de gauche. Le modèle*Nouveaux comptes* est un modèle spécial qui apparaît toujours en premier dans la liste.

Modèle Nouveaux comptes

Le modèle *Nouveaux comptes* est un modèle spécial qui est appliqué à tous les nouveaux comptes lorsqu'ils sont créés. Plutôt que de verrouiller et de contrôler certains paramètres des comptes comme le font d'autres modèles, le modèle *Nouveaux comptes* sert simplement à désigner les paramètres initiaux des nouveaux comptes. Ces paramètres initiaux peuvent ensuite être modifiés normalement en utilisant l'Éditeur de comptes pour modifier les comptes individuels. Certains paramètres du modèle, tels que les options situées dans l' écran<u>Rôles d'administration</u> (875), ne sont pas disponibles dans le modèle Nouveaux comptes.

Voir :

Propriétés du modèle 🕬 Gestion de groupes 📾

5.2.2.1 Propriétés du modèle

	Template Control
E Group Manager	This template controls the following account pattings:
Template Manager	This template controls the following account settings.
	✓ All possible account settings
Mail Services	· · · · · · · · · · · · · · · · · · ·
Web Services	Mail services
Autoropondor	
Eonwarding	
Restrictions	Groups
Quotas	Autoresponders
Attachments	Mail forwarding
Allow List	Restrictions
Settings	
	Attachment handling
	Administrative Roles (not available in New Accounts template)
	Settings & Allow List
	New Account Settings
	Mailbox \$USERFIRSTNAMELC\$.\$USERLASTNAMELC\$
	Mail folder \\\MIKE-P71\MDaemon\Users\\$DDMAIN\$\\$MAILBOX\$\
	Account must change mailbox password before it can connect

Pour accéder à l'écran des propriétés d'un modèle, ouvrez <u>le Gestionnaire de modèles</u> at cliquez sur le nom du modèle dans le volet de gauche. Utilisez l'écran des propriétés de chaque modèle pour désigner les catégories de paramètres des comptes que le modèle contrôlera. Pour tout compte appartenant à un <u>groupe</u> at qui utilise un modèle de compte, les écrans correspondants de l'éditeur de compte seront verrouillés, car ces paramètres seront contrôlés par le modèle. Si un compte appartient à plusieurs groupes liés à différents modèles, tous les modèles seront utilisés s'il n'y a pas de conflit dans les propriétés désignées du modèle. Si plusieurs modèles sont définis pour contrôler les mêmes propriétés, c'est le premier modèle répertorié qui sera utilisé.

Paramètres contrôlés par modèle

Tous les paramètres de compte possibles

Cochez cette case si vous souhaitez que ce modèle contrôle tous les modèles de comptes disponibles pour les <u>Groupes</u> at itilisant le modèle. Tous les écrans du modèle seront utilisés pour les paramètres de compte de chaque membre du groupe au lieu des écrans correspondants du même nom dans l'Éditeur de comptes. Décochez cette case si vous souhaitez utiliser les options*Paramètres des comptes* ci-dessous pour sélectionner des paramètres de compte spécifiques à contrôler.

Paramètres des comptes

Cette section répertorie toutes les catégories de paramètres des comptes que le modèle peut contrôler pour les groupes utilisant le modèle. Chaque option correspond

à l'écran du même nom. Lorsqu'une option est sélectionnée, les paramètres de l'écran du modèle seront utilisés à la place des paramètres de l'écran correspondant de l'éditeur de compte pour les membres du groupe associés.

Nouveaux comptes Paramètres des comptes

Ces options ne sont disponibles que dans le <u>modèle Nouveaux comptes</u> [48]. Elles utilisent une variété de macros spéciales and pour générer automatiquement le dossier de stockage du courrier et la partie boîte aux lettres de l'adresse électronique pour les Nouveaux comptes.

Boîte aux lettres

Utilisez ce champ pour contrôler le Nom a pour céfaut de la Boîte aux lettres de l' adresse électronique qui sera générée pour les Nouveaux comptes. Dans la section Macros de modèle al ci-dessous, vous trouverez une liste des macros qui peuvent être utilisées dans cette chaîne de modèle.

"\$USERFIRSTNAMELC\$.\$USERLASTNAMELC\$" est le modèle par défaut pour cette option. Dans le cas de la création d'un compte pour "Michael Mon" dans le domaine Exemple.com, son adresse sera configurée comme suit "michael.mason@example.com".

Dossier Dossiers de courrier

Utilisez ce champ pour contrôler le *Dossier courrier* 700 par défaut qui sera utilisé pour les nouveaux comptes. Le Dossier Dossiers de courrier de chaque compte est l'endroit où ses messages électroniques seront stockés sur le serveur. Exemple :"... \NDOMAIN\$\NMAILBOX\$\" crée le chemin "...\Nexemple.com\Nmichael.mason\N" pour l'utilisateur "michael.mason@example.com".

MDaemon prend en charge un système de base pour le hachage des dossiers. Sous NTFS, le fait de conserver de nombreux dossiers sous la même racine peut parfois entraîner des problèmes de performances. Si vous avez un grand nombre d'utilisateurs et que vous souhaitez subdiviser les dossiers utilisateurs au-delà de la configuration par défaut \$DOMAIN\$\\$MAILBOX\$\, vous pouvez utiliser la macro \$MAILBOXFIRSTCHARSn\$ pour le faire. Avec cette macro, "n" est un nombre compris entre 1 et 10 et s'étend aux "n" premiers caractères du Nom de la BAL. Si vous modifiez le chemin d'accès à votre *Dossier courrier* par défaut de la manière suivante, vous obtiendrez un système de hachage de dossier décent :

 $C \cdot$ \NMailboxRoot\N\$MAILBOXFIRSTCHARS4\N\$MAILBOXFIRSTCHA RS2\N\$MAILBOX\N\$.

Le compte doit changer de mot de passe avant de se connecter

Cette option contrôle si le nouveau compte doit ou non modifier le mot de passe desa boîte aux lettres avant de pouvoir accéder à POP, IMAP, SMTP, Webmail ou MDaemon Remote Admin. L'utilisateur peut se connecter au Webmail ou au MDaemon
> Comme il peut être difficile ou impossible pour certains utilisateurs de modifier le mot de passe, il convient de faire preuve de prudence avant d'activer cette option.

Macros de modèle

Vous trouverez ci-dessous une référence rapide aux macros disponibles pour automatiser la configuration de votre compte.

\$DOMAIN	Cette variable résoudra le nom de domaine sélectionné pour le compte.
\$DOMAINIP\$ CETTE VARIABLE RÉSOUDRA LE NOM DE DOMAINE SÉLECTIONNÉ POUR LE COMPTE.	Cette variable se résoudra à l'adresse IPv4 associée au domaine actuellement sélectionné pour le compte.
\$DOMAINIP6\$ CETTE VARIABLE SE RÉSOUDRA À L'ADRESSE IPV4 ASSOCIÉE AU DOMAINE ACTUELLEMENT SÉLECTIONNÉ POUR LE COMPTE.	Cette variable se résoudra à l'adresse IPv6 associée au domaine actuellement sélectionné pour le compte.
\$MACHINENAME\$ (NOM DE LA MACHINE)	Cette macro permet de restaurer le Nom d'hôte du Domaine par défaut, à partir de l'écran Nom d'hôte ou adresse IP du Gestionnaire de domaines. Cette macro est désormais utilisée dans le script d'informations du compte par défaut (NEWUSERHELP.DAT) pour les nouvelles installations.
NOM D'UTILISATEUR	Cette variable correspond au Prénom et au nom complet du titulaire du compte. Ce champ est équivalent à "\$USERFIRSTNAME\$ \$USERLASTNAME\$"

\$USERFIRSTNAME\$ (NOM DE FAMILLE DE L'UTILISATEUR)	Cette variable correspond au prénom du titulaire du compte.
\$USERFIRSTNAMELC\$ CETTE VARIABLE INDIQUE LE PRÉNOM DU TITULAIRE DU COMPTE.	Cette variable renvoie au prénom du titulaire du compte, en lettres minuscules.
\$USERLASTNAME\$ CETTE VARIABLE RENVOIE AU NOM DE FAMILLE DU TITULAIRE DU COMPTE, EN LETTRES MINUSCULES.	Cette variable renvoie au nom de famille du titulaire du compte.
\$USERLASTNAMELC\$ CETTE VARIABLE RENVOIE AU NOM DE FAMILLE DU TITULAIRE DU COMPTE, EN LETTRES MINUSCULES.	Cette variable renvoie au nom de famille du titulaire du compte, en lettres minuscules.
\$USERFIRSTINITIAL\$ CETTE VARIABLE INDIQUE LA PREMIÈRE LETTRE DU NOM DU TITULAIRE DU COMPTE, EN MINUSCULES.	Cette variable correspond à la première lettre du prénom du titulaire du compte.
\$USERFIRSTINITIALC\$ CETTE VARIABLE SE RÉSOUT À LA PREMIÈRE LETTRE DU PRÉNOM DU TITULAIRE DU COMPTE.	Cette variable correspond à la première lettre du prénom du titulaire du compte, en minuscules.
\$USERLASTINITIAL\$ (DERNIÈRE LETTRE INITIALE DE L'UTILISATEUR)	Cette variable correspond à la première lettre du Prénom et du nom du titulaire du compte.
\$USERLASTINITIALLC\$ (NOM DE FAMILLE DE L'UTILISATEUR)	Cette variable correspond à la première lettre du Prénom et du nom du titulaire du compte, en minuscules.
\$MAILBOX\$ CETTE VARIABLE INDIQUE LA	Cette variable correspond au Nom de la BAL du compte courant. Cette valeur sera également utilisée comme

5 000	

PREMIÈRE LETTRE DU NOM DE FAMILLE DU TITULAIRE DU COMPTE, EN MINUSCULES.	valeur de la commande USER passée lors des sessions de courrier POP3 entrant.
<pre>\$MAILBOXFIRSTCHARSn\$ (boîte aux lettres)</pre>	Où "n" est un nombre compris entre 1 et 10. Votre nom sera étendu aux "n" premiers caractères du Nom de la BAL.

Voir :

<u>Gestionnaire de modèles</u> ୟମି <u>Gestion de groupes</u> ରେଶି

5.2.2.1.1 Services de messagerie

 Groups & Templates - Mail Services Group Manager Template Manager New Accounts Mail Services Web Services Groups Autoresponder Forwarding Quotas Attachments Allow List Settings Sample Template 	Mail Services Mail Services Enable POP access (Post Office Protocol) but only from LAN IPs Enable IMAP access (Internet Message Access Protocol) but only from LAN IPs enable MD aemon Connector access (requires IMAP) Restrict SMTP access to LAN IPs only Enable ActiveSync access Apply to all accounts now
	Ok Cancel Apply Help

Les options de cet écran de modèle correspondent aux options de l'écran Services de messagerie de l'éditeur de compte. Lorsqu'un modèle est configuré pour <u>contrôler cet</u> <u>écran</u> [243], il contrôlera les options des Services de messagerie pour tout compte appartenant à un <u>groupe</u> [338] qui utilise le modèle.

Services de messagerie

Activer l'accès POP (Post Office Protocol)

Lorsque cette case est cochée, les comptes dont les paramètres sont contrôlés par ce modèle sont accessibles via Post Office Protocol (POP). Pratiquement tous les logiciels de messagerie prennent en charge ce protocole. Décochez cette case si vous ne souhaitez pas autoriser l'accès POP.

... mais seulement à partir d'IP du réseau local

Cochez cette case si vous souhaitez autoriser l'accès aux comptes via POP uniquement lorsque l'utilisateur se connecte à partir d'une <u>adresse IP locale</u> [47].

Activer l'accès IMAP (Internet Message Access Protocol)

Lorsque cette case est cochée, les comptes dont les paramètres sont contrôlés par ce modèle sont accessibles via Internet Message Access Protocol (IMAP). Le protocole IMAP est plus polyvalent que le protocole POP, car il permet de gérer le courrier électronique sur le serveur et d'y accéder à l'aide de plusieurs clients. La plupart des logiciels de messagerie prennent en charge ce protocole.

... mais seulement à partir d'IP du réseau local

Cochez cette case si vous souhaitez autoriser l'accès aux comptes via IMAP uniquement lorsque l'utilisateur se connecte à partir d'une <u>adresse IP locale</u> [47].

...activer l'accès MDaemon Connector (requiert IMAP)

Cette option n'est disponible que sur le modèle Nouveaux comptes. Cliquez sur cette option si vous souhaitez autoriser le compte à se connecter à l'aide de <u>MDaemon Connector</u> [409]. **Remarque :** cette option n'est disponible que lorsque la prise en charge de MDaemon Connector est activée sur votre serveur.

Limiter l'accès SMTP aux IP LAN uniquement

Cochez cette case si vous souhaitez limiter l'accès SMTP aux IP locales uniquement. Cela empêchera les comptes d'envoyer du courrier s'ils ne sont pas connectés à votre réseau. Si le compte tente d'envoyer du courrier à partir d'une adresse IP extérieure, la connexion sera refusée et abandonnée.

Activer l'accès ActiveSync

Cette option n'est disponible que dans le modèle Nouveaux comptes. Cochez cette case si vous souhaitez autoriser les nouveaux comptes à utiliser ActiveSync sur un appareil mobile pour synchroniser le courrier électronique, les contacts, le calendrier et d'autres données avec MDaemon Webmail. Ce paramètre correspond à l' option *Activer les services ActiveSync* pour *cet utilisateur* située dans l'écran ActiveSync pour MDaemon de l'Éditeur de comptes.

Appliquer à tous les comptes maintenant

Cette option n'est disponible que sur le modèle Nouveaux comptes. Cliquez sur ce bouton pour appliquer immédiatement les paramètres de cet écran aux écrans<u>Services de messagerie</u> (769) et <u>ActiveSync for MDaemon</u> (819) de tous les comptes MDaemon existants. Voir :

Propriétés du modèle 849 Propriétés du groupe 833 Modèle Nouveaux comptes 848 Mon compte | Services de messagerie 769

5.2.2.1.2 Services web

Les options de cet écran de modèle correspondent aux options de l'écran Services Web de l'éditeur de compte. Lorsqu'un modèle est défini pour <u>contrôler cet écran</u>, il contrôlera les options des Services Web pour tout compte appartenant à un <u>groupe</u> aqui utilise le modèle.

Services Web et Authentification à deux facteurs

Activer l'accès au webmail

Activez cette case à cocher si vous souhaitez que les comptes contrôlés par ce modèle puissent accéder au <u>Webmail</u> (333), qui permet aux utilisateurs d'accéder à leur courrier électronique, à leurs calendriers et à d'autres fonctionnalités à l'aide d'un navigateur Web.

... mais seulement à partir d'IP du réseau local

Cochez cette case si vous souhaitez autoriser les comptes associés à accéder à Webmail uniquement lorsqu'ils se connectent à partir d'une <u>adresse IP locale</u> [447].

Activer l'accès MDaemon Remote Admin

Cochez cette case si vous souhaitez permettre aux comptes contrôlés par ce modèle de modifier certains paramètres de leur compte via l'<u>administration à</u> <u>distance</u> [376]. Les comptes ne pourront modifier que les paramètres que vous désignez ci-dessous.

Dans le cas où cette fonction est activée et que le serveur Remote Admin est actif, l'utilisateur pourra se connecter à Remote Admin en pointant un navigateur vers le domaine MDaemon désigné et le <u>port assigné à Remote Admin</u> (par ex. http://example.com:1000). Un écran de connexion lui sera d'abord présenté, puis un écran contenant les paramètres qu'il a été autorisé à modifier. Il lui suffit de modifier les paramètres de son choix, puis de cliquer sur le bouton*Enregistrer les modifications.* Il peut ensuite se déconnecter et fermer le navigateur. Si l'utilisateur a accès à Webmail, il peut également accéder à MDaemon Remote Admin à partir du menu Options avancées de Webmail.

Si l'utilisateur est un compte administrateur global ou de domaine (désigné sur l' écran <u>Rôles administratifs</u> [812] de l'éditeur de compte), il verra un écran différent après s'être connecté à l'administration à distance.

... mais seulement à partir d'IP du réseau local

Cochez cette case si vous souhaitez autoriser le compte à accéder à l'Administration à distance uniquement lorsqu'il se connecte à partir d'une <u>adresse IP locale [647</u>].

Activer MDaemon Instant Messenger

Cochez cette case si vous souhaitez activer la prise en charge de <u>MDIM</u> par défaut pour les nouveaux comptes. Cette option n'est disponible que dans le <u>Modèle</u> <u>Nouveaux comptes</u> with. Il existe une option similaire dans les <u>Propriétés du groupe</u> qui peut être utilisée pour contrôler l'accès des membres du groupe à MDIM.

Activer la messagerie instantanée

Cliquez sur cette option si vous souhaitez activer la prise en charge du système de messagerie instantanée du MDIM par défaut pour les nouveaux comptes. Cette option n'est disponible que dans le <u>Modèle Nouveaux Comptes</u> une option similaire dans les <u>Propriétés du groupe</u> au peut être utilisée pour contrôler l'accès des membres du groupe à la messagerie instantanée.

L'utilisateur peut modifier les catégories

Cochez cette case si vous souhaitez autoriser les nouveaux utilisateurs du MDaemon Webmail à modifier les catégories. Cette option est Désactivés par défaut pour les nouveaux utilisateurs. **Note :** Cette option n'est disponible que dans l'interface web de MDaemon Remote Admin.

Ignorer la vérification de la persistance d'IP pour les sessions Webmail

Si l' option <u>Serveur Web de Webmail</u> (339) "Exiger la persistance IP pendant la session Webmail" est activée, vous pouvez cocher cette case si vous souhaitez exempter

les nouveaux utilisateurs de l'exigence de persistance IP. **Note :** Cette option n'est disponible que dans l'interface web de MDaemon Remote Admin.

Activer l'assistant IA pour les e-mails

Si l' option Activer les messages IA est activée dans la boîte de dialogue Webmail [197] d'un domaine de compte , cochez cette case si vous souhaitez permettre aux comptes contrôlés par ce modèle d'utiliser ces fonctions dans MDaemon Webmail ; les fonctions ne seront disponibles pour l'utilisateur que lorsque l'option au niveau du domaine sera activée. **Voir :** "Fonctionnalités des messages AI du Webmail [355]" ci-dessous pour des informations importantes et des mises en garde concernant l'utilisation de ces fonctionnalités.

Authentification à deux facteurs

MDaemon prend en charge l'Authentification à deux facteurs (2FA) pour les utilisateurs qui se connectent à Webmail ou à l'interface web de MDaemon Remote Admin. Les comptes qui se connectent au Webmail via HTTPS peuvent activer l'Authentification à deux facteurs pour ce compte dans l'écran**Options | Sécurité du** Webmail. Dès lors, l'utilisateur doit entrer un code de vérification lorsqu'il se connecte au Webmail ou à MDaemon Remote Admin. Le code est obtenu lors de la Connexion à partir d'une Application d'authentification installée sur l'appareil mobile ou la tablette de l'utilisateur. Cette fonctionnalité est conçue pour tout client qui prend en charge Google Authenticator. Consultez le fichier d'aide du Webmail pour plus d'informations sur la configuration de 2FA pour un compte.

Autoriser l'Authentification à deux facteurs

Par défaut, les Nouveaux comptes sont autorisés à configurer et à utiliser la fonctionnalité d'Authentification à deux facteurs (2FA) de Webmail. Décochez cette case si vous ne souhaitez pas autoriser l'authentification à deux facteurs par défaut pour les Nouveaux comptes. Vous pouvez contrôler ce paramètre pour des comptes spécifiques sur la page Services Web de chaque compte.

Requérir Authentification à deux facteurs

Activez cette option si vous souhaitez forcer tous les nouveaux comptes à utiliser l'Authentification à deux facteurs (2FA) lors de la connexion au Webmail ou à l'interface web d'administration à distance de MDaemon. Lorsque l'authentification àdeux facteursest requise, tout compte qui n'a pas encore été configuré pour l'utiliser sera redirigé vers une page pour la configurer la prochaine fois que le compte se connectera à Webmail. Consultez le fichier d'aide de Webmail pour plus d'informations sur la configuration d'un compte.

MDaemon Remote Admin permet aux utilisateurs de modifier...

...Modifier le nom réel

L'activation de cette fonction permettra aux comptes associés à ce modèle de modifier le paramètre <u>Prénom et Les nom.</u> 765

...modifier la boîte aux lettres

L'activation de cette fonction permet aux utilisateurs de modifier le <u>Nom de la boîte</u> <u>aux lettres</u> $\boxed{165}$.

Comme le *Nom de la Boîte aux lettres* fait partie de l'adresse email du compte, qui est l'identifiant unique et la valeur de connexion pour le compte, le fait de le modifier signifie que l'utilisateur changera son adresse e-mail réelle. Dans ce cas, tout message adressé à l'ancienne adresse risque d'être rejeté, supprimé ou autre.

...Modifier le mot passe

Cochez cette case si vous souhaitez autoriser les comptes à modifier le *mot de passe de la boîte aux lettres*. Pour en savoir plus sur les Exigences relatives aux mots mots passe, voir : <u>Mots de passe state</u>.

...Modifier adresse de transfert

Lorsque cette fonction est activée, les comptes associés au modèle pourront modifier les paramètres de l'adresse de<u>transfert.</u>

...Modifier le transfert avancé

Lorsque cette fonctionnalité est activée, les utilisateurs pourront modifier les paramètres de transfert avancés 7801.

...Modifier les filtres IMAP

Utilisez cette commande pour permettre à chaque utilisateur de créer et de gérer ses propres <u>Filtres IMAP</u> [789].

...Modifier des alias

Activez cette option si vous souhaitez permettre aux titulaires de comptes d'utiliser l'administration à distance pour modifier les <u>alias</u> associés à leurs comptes.

...modifier les mots passe d'application

Par défaut, les utilisateurs peuvent modifier leurs <u>Mots passe d'application</u> at les Désactivez cette case à cocher si vous ne souhaitez pas autoriser l'utilisateur à les modifier.

...Modifier ce compte est privé

Cette option détermine si chacun sera autorisé ou non à utiliser le MDaemon Remote pour modifier l'option "*Compte masqué des listes "Tout le monde", des calendriers partagés et de VRFY*" située dans l'écran Paramètres de l'éditeur de compte.

...Modifier les restrictions de courrier

Cette case à cocher détermine si le compte pourra ou non modifier la restriction Courrier entrant et sortant, située sur l'écran<u>Restrictions</u>

...modifier les paramètres des quotas

Cochez cette case si vous souhaitez autoriser le compte à modifier les paramètres de<u>quotas.</u>

...modifier les paramètres MultiPOP

Cochez cette case si vous souhaitez autoriser le compte à ajouter de nouvelles entrées<u>MultiPOP</u> [792] et à activer/désactiver la collecte MultiPOP pour ces entrées.

...les paramètres autorépondeur

Cochez cette case si vous souhaitez donner à l'utilisateur la permission d'ajouter, de modifier ou de supprimer des <u>autorépondeurs</u> (777) pour son compte.

... Modifier la gestion des pièces jointes

Cochez cette case si vous souhaitez autoriser l'utilisateur à modifier les options de gestion des pièces jointes de son compte, situées dans l'écran Autoriser pièces jointes.

...gestion terminaux mobiles

Cochez cette case si vous souhaitez autoriser le titulaire du compte à utiliser l'administration à distance pour gérer les paramètres spécifiques à son appareil, par exemple pour les appareils ActiveSync.

Appliquer à tous les comptes maintenant

Cette option n'est disponible que dans le <u>Modèle Nouveaux comptes</u> [348]. Cliquez dessus pour appliquer les paramètres de cet écran à tous les comptes MDaemon existants qui ne sont pas spécifiquement contrôlés par un Modèle de compte Services Web.

Appliquer les valeurs par défaut de l'installation

Cette option n'est disponible que sur le <u>Modèle Nouveaux Comptes</u> [348]. Cliquez dessus pour réinitialiser le modèle Nouveaux comptes aux paramètres par défaut de l'installation. Cette option ne modifie que les paramètres du modèle, elle ne modifie pas les comptes existants.

Charger les paramètres du modèle "Nouveaux comptes".

Cette option n'est disponible que pour les modèles personnalisés. Cliquez dessus pour définir les options de cet écran sur les valeurs par défaut désignées dans l'écran Services web du modèle Nouveaux comptes [248].

Fonctionnalités des messages IA du Webmail

Dans la version 23.5.0 de MDaemon, le thème Pro du client Webmail de MDaemon inclut diverses fonctionnalités d'intelligence artificielle (IA) pour aider vos utilisateurs à gérer leur courrier électronique et à augmenter leur productivité. Ces fonctionnalités sont facultatives et désactivées par défaut, mais peuvent être activées pour tout utilisateur de votre choix.

Grâce à ces fonctionnalités, dans le MDaemon Webmail, vous pouvez utiliser l IA pour :

- Vous donner un résumé du contenu d'un message électronique.
- Suggérer une réponse au message, selon plusieurs directives que vous pouvez demander à l'IA d'utiliser. Vous pouvez définir le *ton de* la réponse

(professionnel, respectueux ou décontracté). La position à adopter dans la réponse peut être intéressée ou non, d'accord ou non, ou sceptique. L'*attitude* à *adopter* dans la réponse peut être confiante, enthousiaste, calme ou apologétique. Les derniers peuvent indiquer la *longueur de* la réponse, qui peut être très brève ou détaillée.

 Vous aider à composer un nouveau message électronique, sur la base d'un texte que vous avez déjà inclus. Comme pour l'option *Suggérer* ci-dessus, vous pouvez également définir le ton, la position, l'attitude et la longueur que l'IA utilisera pour rédiger le message.

L' option Activer les fonctions IA pour les messages de la boîte de dialogue principale Paramètres du Webmail (365) permet de déterminer si la prise en charge des fonctions IA est activée par défaut pour vos domaines. Une option du même nom située dans la boîte de dialogue du (197) Gestionnaire de domaines peut être utilisée pour remplacer ce paramètre principal pour des domaines spécifiques. **Remarque :** Activer assistant IA pour les e-mails pour un domaine ne permet pas à tous les utilisateurs de ce domaine d'accéder à ces fonctions. Vous devez activer l' option Activer les options IA pour les *e-mails dans* l'écran Services Web (771) de l'éditeur de compte pour tout utilisateur que vous souhaitez autoriser à les utiliser. Vous pouvez également utiliser les fonctionsModèles de comptes [847] et Groupes [836] pour affecter des utilisateurs à un groupe ayant accès aux fonctions de messages AI.

> Activer les assistants IA pour les e-mails de MDaemon permet aux comptes d'envoyer et de recevoir des informations en provenance et à destination de services d'IA générative tiers, en particulier ChatGPT d'OpenAI. Les administrateurs et les utilisateurs doivent donc être conscients que cela introduit plusieurs problèmes potentiels de confidentialité en raison de la capacité de la fonctionnalité à traiter des données personnelles et à générer des informations potentiellement sensibles. Pour répondre à ces préoccupations, il est essentiel que les organisations forment leurs employés à une utilisation responsable de l'IA. **Remarque :** Les données soumises à/depuis I OpenAI ne sont pas stockées sur le serveur local ou sur notre réseau.

Vous trouverez la politique d'utilisation de l'IA de MDaemon Technologies sur notre <u>page d'information sur l'intelligence</u> <u>artificielle (IA)-la MDaemon</u>. Sur cette même page, il y a également un lien vers les Conditions d'utilisation d'OpenAI. Voir :

<u>Propriétés du modèle</u> ୫4୭ <u>Propriétés du groupe</u> ୫3୭ <u>Modèle Nouveaux comptes</u> ୫4୭ <u>Mon compte | Services Web</u> 771

5.2.2.1.3 Groupes

🧐 Groupes & Modèles - Groupes	×
Gestionnaire de groupes Gestionnaire de modèles Dervices de messagerie Services web Groupes Autorépondeur Transfert Quotas Pièces jointes Liste des exceptions Paramètres	
OK Annuler Appliquer	Aide

Ce compte appartient au(x) groupe(s)

Cet écran n'est disponible que dans le <u>modèle Nouveaux comptes</u> at correspond à la section Appartenance au groupe de l'écran Dossier courrier & Groupes de l'éditeur de comptes. Lorsque vous sélectionnez un ou plusieurs groupes dans cet écran, les nouveaux comptes sont automatiquement ajoutés à ces groupes.

Voir :

 Modèle Nouveaux Comptes

 Gestion de groupes

 Propriétés du groupe

5.2.2.1.4 Autorépondeur

	Autoresponder	
🖅 Group Manager	Autoresponder	
🚊 Template Manager	Enable autoresponder	
New Accounts	Edit autoresponder file Schedule Publish	
Mail Services		
···· Web Services		
Groups	Do not send auto response if message is from one of these addresses	
- Autoresponder	Remove	
Forwarding		
Attachments		
Allow List	New excluded address - wildcards ok	
Settings		
Sample Template	Add	
	· · · · · · · · · · · · · · · · · · ·	_
	Run this program	
	Browse	9
	Pass message to process	
	Add sender to this mailing list	
	Bemove sender from this list	

Les options de cet écran de modèle correspondent aux options de l'écran Autorépondeur de l'éditeur de compte. Lorsqu'un modèle est défini pour <u>contrôler cet</u> <u>écran</u> [243], il contrôlera les options de l'autorépondeur pour tout compte appartenant à un <u>groupe</u> [333] qui utilise le modèle.

Les répondeurs automatiques sont des outils utiles pour faire en sorte que les messages entrants déclenchent automatiquement certains événements, tels que l'exécution d'un programme, l'ajout de l'expéditeur à une liste de diffusion, la réponse à un message généré automatiquement, etc. L'utilisation la plus courante des répondeurs automatiques consiste à répondre automatiquement aux messages entrants par un message défini par l'utilisateur indiquant que le destinataire est en vacances, qu'il n'est pas disponible, qu'il répondra dès que possible, etc. Les utilisateurs de MDaemon disposant d'un <u>accès Web</u> [771] au <u>Webmail</u> [335] ou à l'<u>Administration à distance</u> [376] peuvent utiliser les options fournies pour composer eux-mêmes des messages de réponse automatique et programmer les dates auxquelles ils seront utilisés. Enfin, les messages de réponse automatique sont basés sur le contenu du fichier OOF.mrk, qui se trouve dans le dossier racine de chaque utilisateur . Ce fichier prend en charge un grand nombre de macros, qui peuvent être utilisées pour générer dynamiquement une grande partie du contenu du message, ce qui rend les répondeurs automatiques très polyvalents.

> Les Autorépondeurs sont toujours honorés lorsque le message déclencheur provient d'une source distante. Toutefois, pour les messages provenant provenant du même domaine d'un utilisateur, les autorépondeurs ne seront déclenchés que si vous activez l'option *Les autorépondeurs sont déclenchés par le courrier intra-domaine*, située dans l' écran<u>" Paramètres |</u> <u>des autorépondeurs</u> 2021. Vous pouvez également utiliser une option de cet écran pour limiter les messages de réponse automatique à une réponse par expéditeur et par jour.

Répondeur automatique

Activer l'autorépondeur

Activer ce contrôle pour activer un autorépondeur pour tous les groupes contrôlés par ce modèle. Pour plus d'informations sur les répondeurs automatiques, voir : <u>Répondeurs automatiques</u>.

Modifier le fichier de réponse automatique

Cliquez sur ce bouton pour modifier le fichier de réponse automatique qui sera utilisé pour les groupes associés à ce modèle.

Planification

Cliquez sur ce bouton pour ouvrir la boîte de dialogue Programmer dans laquelle vous pouvez définir une date et une heure de début et de fin pour l'autorépondeur, ainsi que les jours de la semaine où il doit être actif. Laissez la case Schedule vide si vous souhaitez que l'autorépondeur soit actif en permanence.

Schedule			
Schedule Action			
	Erase the 'Start date/time' to deactivate this sched	dule.	
<u> </u>	Start date/time	🏛 at 12 🗸 00 🗸 AM 🗸	
	End date/time	🏥 at 12 🗸 00 🗸 AM 🗸	
	Select days of the week		
	🗹 Monday 🛛 🗹 Saturday		
	🗹 Tuesday 🛛 🗹 Sunday		
	🗹 Wednesday		
	🗹 Thursday		
	🗹 Friday	Ok Cancel	
	☑ Monday ☑ Saturday ☑ Tuesday ☑ Sunday ☑ Wednesday ☑ Thursday ☑ Friday	Ok Cancel	

Publier

Cliquez sur ce bouton si vous souhaitez copier le fichier et les paramètres du répondeur automatique de ce modèle vers un ou plusieurs autres comptes. Sélectionnez les comptes vers lesquels vous souhaitez copier le répondeur automatique, puis cliquez sur **Ok**.

Ne pas envoyer de réponse automatique si le message provient d'une de ces adresses Vous pouvez ici dresser la liste des adresses que vous souhaitez exclure des

réponses initiées par ce répondeur automatique.

Il peut arriver que des messages de réponse automatique soient envoyés à une adresse qui renvoie elle-même une réponse automatique. Cela peut créer un effet "ping-pong" qui fait que les messages sont continuellement renvoyés entre les deux serveurs. Si vous rencontrez l'une de ces adresses, indiquez-la ici pour éviter que cela ne se produise. Il existe également une option, située dans l' écran<u>" Paramètres</u> <u>autorépondeurs "</u> [902], qui peut être utilisée pour limiter les messages de réponse automatique à une réponse par expéditeur et par jour.

Supprimer

Cliquez sur ce bouton pour supprimer toutes les entrées sélectionnées de la liste des adresses exclues.

Nouvelle adresse exclue - jokers acceptés

Si vous souhaitez ajouter une adresse à la liste des adresses exclues, saisissez-la ici, puis cliquez sur le bouton*Ajouter.*

Exécuter un programme suivant.

Exécuter un programme suivant.

Utilisez ce champ pour indiquer le chemin d'accès et le nom de fichier d'un programme que vous souhaitez exécuter à l'arrivée d'un nouveau courrier pour un membre du groupe contrôlé par ce modèle. Il convient de veiller à ce que ce programme se termine correctement et puisse être exécuté sans surveillance. Des paramètres de ligne de commande facultatifs peuvent être saisis immédiatement après le chemin d'accès à l'exécutable, si vous le souhaitez.

Traiter le message

Sélectionnez cette option et le processus spécifié dans le champ *Exécuter ce programme* se verra transmettre le nom du message de déclenchement en tant que premier paramètre de ligne de commande disponible. Dans le cas où le paramètre autorépondeur est défini pour un compte qui transfère le courrier vers un autre endroit et **ne** conserve **pas** de copie locale dans sa propre boîte aux lettres (voir <u>Transfert</u> 786), cette fonction est désactivée.
Non par défaut, MDaemon place le nom du fichier de messages comme dernier paramètre de la ligne de commande. Vous pouvez modifier ce comportement en utilisant la macro \$MESSAGE\$. Dans ce cas, utilisez cette macro à la place du nom du fichier de messages. Cela permet une plus grande flexibilité dans l'utilisation de cette fonctionnalité puisqu'une ligne de commande complexe telle que celle-ci sera possible : logmail /e /j /message=\$MESSAGE\$ /q.

Liste de diffusion

Ajouter l'expéditeur à la liste de diffusion

Si une liste de diffusion est ajoutée dans ce champ, l'expéditeur du message entrant sera automatiquement ajouté en tant que membre de cette liste de diffusion. Il s'agit d'une fonction pratique pour la constitution automatique de listes.

Supprimer expéditeur de cette liste de diffusion

Si une liste de diffusion est indiquée dans ce champ, l'expéditeur du message entrant sera automatiquement supprimé de la liste de diffusion spécifiée.

Voir :

<u>Propriétés du modèle</u> ଜଣ <u>Propriétés du groupe</u> ଛଛ <u>Nouveau Modèles de comptes</u> ଜଣ <u>Mon compte | Répondeur automatique</u> ୮୮୮

5.2.2.1.5 Transfert

866

🧐 Groups & Templates - Forwarding		×
 Groups & Templates - Forwarding Group Manager Template Manager New Accounts Mail Services Web Services Groups Autoresponder Forwarding Quotas Attachments Allow List Settings 	Mail Forwarding Enable mail forwarding Forwarding address(es) (separate each address with a comma) Domain, [Host], or IP AUTH Logon AUTH Password SMTP 'MAIL' Value Port (default = 25) 25	
Settings 	Pot (default = 25) 25	
	Ok Cancel Apply Help	

Les options de cet écran de modèle correspondent aux options de l'écran <u>Transfert de</u> <u>l'</u>[780]éditeur de comptes. Lorsqu'un modèle est défini pour <u>contrôler cet écran</u>[840], il contrôlera les options de transfert pour tout compte appartenant à un <u>groupe</u>[838] qui utilise le modèle.

Transfert de courrier

Activer transfert de courrier

Cochez cette case si vous souhaitez transférer les messages entrants des comptes associés à l'adresse ou aux adresses spécifiées dans l'option Adresses de transfert cidessous. Les utilisateurs de MDaemon ayant un <u>accès web</u> [771] à <u>Webmail</u> [333] ou <u>MDaemon Remote Admin</u> [376] peuvent utiliser les options fournies pour définir euxmêmes les options de transfert, sans avoir à demander à un administrateur de le faire.

Adresses de transfert (séparez chaque adresse par une virgule)

Utilisez ce champ pour désigner les adresses e-mail auxquelles vous souhaitez transférer des copies des messages entrants du compte associé au fur et à mesure de leur arrivée. Une copie de chaque nouveau message arrivant sur le serveur sera automatiquement générée et transférée aux adresses spécifiées dans ce champ, à condition que l' option*Activer le transfert de courrier* ci-dessus soit cochée. Lors de la redirection vers plusieurs adresses, séparez chacune d'entre elles par une virgule.

Domaine, [Hôte] ou IP

Si vous souhaitez Routage des messages Transférer MESSAGE ! via un autre serveur, tel que lesserveurs MX d' un domaine particulier, indiquez ici le domaine ou l'adresse IP. Si vous souhaitez router les messages vers un hôte spécifique, mettez la valeur entre parenthèses (par exemple [host1.example.com]).

Mot de passe AUTH

Saisissez ici les Exigences relatives aux mots passe du serveur vers lequel vous transférez le courrier des utilisateurs associés.

Valeur SMTP 'MAIL' (en anglais)

Si une adresse est spécifiée ici, elle sera utilisée dans l'instruction"MAIL From" envoyée au cours de la session SMTP avec l'hôte acceptant, au lieu d'utiliser l'expéditeur réel du message. Si vous avez besoin d'une instruction SMTP "MAIL From" vide(c'est-à-dire "MAIL FROM<>"), entrez "[poubelle]" dans cette option.

Port (par défaut = 25)

MDaemon enverra les messages transférés en utilisant le port TCP spécifié ici. Le port SMTP par défaut est 25.

Garder une copie locale du courrier transféré

Par défaut, une copie de chaque message transféré est délivrée normalement dans la boîte aux lettres de l'utilisateur local. Si vous décochez cette case, aucune copie locale ne sera conservée.

Planification

Cliquez sur ce bouton pour créer un calendrier de transfert du courrier électronique des comptes associés. Vous pouvez définir une date et une heure de début, une date et une heure de fin, et spécifier les jours de la semaine où le courrier sera transféré.

Voir :

<u>Propriétés du modèle</u> ଖୋ <u>Propriétés du groupe</u> ଛୋ <u>Nouveau Modèles de comptes</u> ଖୋ <u>Éditeur de comptes | Redirection</u> 7ଛମ

5.2.2.1.6 Restrictions

🧐 Groups & Templates - Restrictions	
🖂 Group Manager	Inbound Message Restrictions
En Template Manager	Restrict messages FROM outside domains
New Accounts Mail Services Web Services Groups Autoresponder Forwarding Restrictions Quotas Attachments Allow List Settings Sample Template	except if from one of these addresses New address Add Remove Add Remove Messages from outside domains should be: Refused
	Intestitic messages to outside domains except if to one of these addresses New address Add Remove
	Ok Cancel Apply Help

Les options de cet écran de modèle correspondent aux options de l' écran <u>Restrictions</u> ⁷⁸²de l'éditeur de compte. Lorsqu'un modèle est défini pour <u>contrôler cet</u> <u>écran</u> ⁶⁴³, il contrôlera les options de restrictions pour tout compte appartenant à un <u>groupe</u> ⁶³³ qui utilise le modèle.

Restrictions appliquées aux messages entrants

Refuser les messages PROVENANT DE domaines externes

Cochez cette case pour empêcher ce compte de recevoir des messages électroniques provenant de domaines non locaux.

... sauf si l'expéditeur est l'une de ces adresses

Les adresses spécifiées dans cette zone constituent des exceptions aux Restrictions aux messages entrants. Les caractères génériques sont autorisés. Ainsi, si vous désignez "*@altn.com" comme exception, aucun message entrant provenant d'une adresse de altn.com ne sera restreint.

Nouvelle adresse

Si vous souhaitez ajouter une adresse à la liste des Restrictions aux messages entrants, tapez-la ici et cliquez sur le bouton*Ajouter*.

Ajouter

Après avoir saisi une adresse dans l'option*Nouvelle adresse*, cliquez sur ce bouton

pour l'ajouter à la liste des exceptions.

Supprimer

Si vous souhaitez supprimer une adresse de la liste des restrictions, sélectionnez-la, puis cliquez sur ce bouton.

Les messages provenant d'un domaine externe doivent être...

Les options de cette liste déroulante déterminent ce que MDaemon fera des messages destinés à ce compte mais provenant d'un domaine non local. Vous pouvez choisir l'une des options suivantes :

Refusées - Les messages restreints seront refusés par MDaemon.

Renvoyé à l'expéditeur - Les messages provenant de domaines restreints seront renvoyés à l'expéditeur.

Envoyé au postmaster - Les messages restreints seront acceptés mais livrés au postmaster au lieu de ce compte.

Envoyé à… - Les messages restreints seront acceptés mais livrés à l'adresse que vous indiquez dans la zone de texte à droite.

Restrictions appliquées aux messages sortants

Refuser les messages ENVOYÉS À des domaines externes

Cochez cette case pour empêcher ce compte d'envoyer des messages électroniques à des domaines non locaux.

... sauf si expéditeur est l'une de ces adresses

Les adresses spécifiées dans cette zone constituent des exceptions à la restriction sur les messages sortants. Les caractères génériques sont autorisés. Ainsi, si vous désignez "*@altn.com" comme exception, les messages sortants adressés à n'importe quelle adresse de altn.com ne seront pas restreints.

Nouvelle adresse

Si vous souhaitez ajouter une adresse à la liste des Restrictions aux messages sortants, tapez-la ici et cliquez sur le bouton*Ajouter*.

Ajouter

Après avoir saisi une adresse dans l'option*Nouvelle adresse*, cliquez sur ce bouton pour l'ajouter à la liste des exceptions.

Supprimer

Si vous souhaitez supprimer une adresse de la liste des restrictions, sélectionnez-la et cliquez sur ce bouton.

Les messages envoyés à un domaine externe doivent être...

Les options de cette liste déroulante déterminent ce que MDaemon fera des messages provenant de ce compte mais destinés à un domaine non local. Vous pouvez choisir l'une des options suivantes :

Refusées - Les messages restreints seront refusés par MDaemon.

Renvoyé à l'expéditeur - Les messages à destination de domaines restreints seront renvoyés à l'expéditeur.

Envoyé au postmaster - Les messages restreints seront acceptés mais remis au postmaster au lieu du destinataire désigné.

Envoyé à… - Les messages restreints seront acceptés mais remis à l'adresse que vous indiquez dans la zone de texte à droite.

5.2.2.1.7 Quotas

🧐 Groupes & Modèles - Quotas		x
Groupes & Modèles - Quotas Gestionnaire de groupes Gestionnaire de modèles Services de messagerie Services web Groupes Autorépondeur Transfert Quotas Pièces jointes Liste des exceptions Paramètres	Quotas Activer les restrictions de quotas Si le compte dépasse ces quotas, il ne peut plus recevoir de courrier et un message d'avertissement est placé dans sa boîte aux lettres. Nombre maximal de messages stockés 0 (0 = pas de limite) Espace disque maximal autorisé (en mégaoctets) 0 (0 = pas de limite) Nombre max. de messages envoyés par jour 0 (0 = pas de limite) Nombre max. de messages envoyés par jour 0 (0 = pas de limite) Appliquer à tous les comptes maintenant 0 (0 = pas de limite) Nettoyage Utiliser les valeurs par défaut du domaine Supprimer le compte s'il est inactif depuis (en jours) 0 (0 = jamais) Supprimer les messages de plus de (en jours) 0 (0 = jamais) EFFACER les messages IMAP supprimés de plus de (en jours) 0 (0 = jamais) SUPPRIMER également les anciens messages des dossiers IMAP Appliquer à tous les comptes maintenant	
	OK Annuler Appliquer A	ide

Les options de cet écran de modèle correspondent aux options de l'écran Modèles de comptes. Lorsqu'un modèle est configuré pour <u>contrôler cet écran</u> [44], il contrôlera les options de quotas pour tout compte appartenant à un <u>groupe</u> [338] qui utilise le modèle.

Quotas

Activer les quotas

Cochez cette case si vous souhaitez spécifier un nombre maximum de messages que les comptes contrôlés par ce modèle peuvent stocker, définir un espace disque maximum que les comptes peuvent utiliser (y compris les pièces jointes dans ledossier Documents dechaque compte) ou désigner un nombre maximum de messages que les comptes peuvent envoyer via SMTP par jour. Dans le cas d'une tentative de distribution du courrier qui dépasserait les limites maximales de messages ou d'espace disque, le message sera refusé et un message d'alerte approprié sera placé dans la boîte aux lettres de l'utilisateur. Si une Collecte<u>MultiPOP</u> dépasse lemaximum autorisé pour le compte, un avertissement similaire est émis et lesentrées MultiPOP ducomptesont automatiquement désactivées (mais pas supprimées de la base de données).

Utiliser la fonction *Envoyer un e-mail d'avertissement à l'utilisateur lorsque ce pourcentage de son quota est atteint* dans "Comptes | Paramètres des comptes | Quotas<u>pour</u> qu'un message d'alerte soit envoyé lorsqu'un compte approche de ses limites de quota. Torsque le compte dépasse une valeur de pourcentage désignée de sa restriction*Nombre maximal de messages stockés à* la fois ou *Espace disque maximal autorisé*, un message d'alerte sera envoyé au compte à minuit. Ce message indique le nombre de messages stockés par le compte, la taille de sa boîte aux lettres, ainsi que le pourcentage utilisé et restant. Dans le cas où un message d'alerte existant se trouve dans la boîte aux lettres du compte, il sera remplacé par un message mis à jour.

Nombre maximal de messages stockés à la fois

Cette option permet de désigner le nombre maximal de messages pouvant être stockés pour les comptes. L'utilisation de "0" dans l'option signifie qu'il n'y aura pas de limite au nombre de messages autorisés.

Espace disque maximum autorisé (en Mo)

Cette option permet de définir l'espace disque maximal que les comptes peuvent utiliser, y compris les pièces jointes éventuellement stockées dans le Dossier Pièces dechaque compte.L'utilisation de "0" dans l'option signifie qu'il n'y aura pas de limite à la quantité d'espace disque que les comptes peuvent utiliser.

Nombre max. de messages envoyés par jour

Cette option permet de définir le nombre maximum de messages que chaque compte peut envoyer par jour via SMTP. Si le compte atteint cette limite, le Nouveau compte sera refusé jusqu'à ce que le compteur soit remis à zéro à minuit. Utilisez "0" dans l'option si vous ne souhaitez pas limiter le nombre de messages que le compte peut envoyer.

Appliquer à tous les comptes maintenant

Cliquez sur ce bouton pour appliquer les paramètres de cet écran à tous les comptes MDaemon existants dont les paramètres Paramètres contrôlés par comptes ne sont pas spécifiquement contrôlés par un modèle de compte. Les valeurs de quotas par défaut seront alors rétablies pour tous les comptes. Cette option n'est disponible que sur le <u>Modèle Nouveaux comptes</u> [24].

Élagage

Les options de cette section permettent de déterminer si un compte contrôlé par ce modèle sera supprimé s'il devient inactif. Vous pouvez également indiquer si les anciens messages appartenant au compte seront supprimés après un certain temps. Tous les jours à minuit, MDaemon supprimera tous les messages qui ont dépassé les délais indiqués, ou il supprimera complètement le compte s'il a atteint la limite d'inactivité.

Utiliser les paramètres par défaut du domaine

Les paramètres d'élagage par défaut sont propres à chaque domaine et se trouvent dans l'écran Paramètres du Gestionnaire de domaines. Si vous souhaitez ignorer les paramètres par défaut du domaine pour les comptes contrôlés par un modèle, décochez cette case et définissez les valeurs souhaitées dans les options cidessous.

Supprimer les comptes s'ils sont inactifs depuis plus plus de jours (0 = jamais)

Indiquez le nombre de jours pendant lesquels le compte doit être inactif avant d'être supprimé. Une valeur de "0" dans ce champ signifie que le compte ne sera jamais supprimé pour cause d'inactivité.

Supprimer les messages plus anciens que ce nombre de jours (0 = jamais)

Il s'agit du nombre de jours pendant lesquels un message donné peut rester dans laboîte aux lettres ducompteavant d'être supprimé automatiquement par MDaemon. La valeur "0" signifie que les messages ne seront jamais supprimés en raison de leur ancienneté. Dans cette option, les messages contenus dans les dossiers IMAP ne sont pas pris en compte, sauf si vous activez l'option "Nettoyer les anciens messages des dossiers IMAP également" ci-dessous.

PURGEZ les messages IMAP supprimés qui datent de plus de ce nombre de jours (0 = jamais)

Utilisez cette commande pour spécifier le nombre de jours pendant lesquels vous souhaitez que les messages IMAP marqués pour suppression restent dans les dossiers d'un utilisateur.Les messages marqués pour suppression au-delà de ce nombre de jours seront supprimés. La valeur "0" signifie que les messages marqués pour suppression ne seront jamais supprimés en raison de leur ancienneté.

Nettoyer également les anciens messages des dossiers IMAP

Cochez cette case si vous souhaitez que l'option"*Supprimer les messages effacés depuis plus de ce nombre de jours*" ci-dessus s'applique également aux messages des dossiers IMAP. Lorsque ce contrôle est désactivé, les messages ordinaires contenus dans les dossiers IMAP ne seront pas supprimés en raison de leur ancienneté.

Voir :

Propriétés du modèle 49 Propriétés des groupes 838 Nouveau Modèles de comptes 448 Mon compte | Quotas 784 Paramètres des comptes | Quotas 920

5.2.2.1.8 Pièces jointes

Groupes & Modèles - Pièces jointes		×
Gestionnaire de groupes Gestionnaire de modèles Services de messagerie Services web Groupes Autorépondeur Transfert Quotas <u>Pièces jointes</u> Liste des exceptions Paramètres	Gestion des pièces jointes Ne pas extraire les pièces jointes des messages Extraire les pièces jointes et les enregistrer dans le dossier Documents du compte Utiliser la fonctionnalité Liens vers les pièces jointes Extraire les pièces jointes des messages entrants Extraire les pièces jointes des messages sortants Les liens vers les pièces jointes doivent être activés pour que ces trois dernières options fonctionnent. La fonction de Liens vers les pièces jointes est actuellement ACTIVÉE. Modifier les paramètres des Liens vers les pièces jointes	
	OK Annuler Appliquer Ai	ide

Les options de cet écran de modèle correspondent aux options de l'écran Pièces jointes de l'éditeur de compte. Lorsqu'un modèle est défini pour <u>contrôler cet écran</u>, il contrôlera les options des pièces jointes pour tout compte appartenant à un <u>groupe</u> au qui utilise le modèle.

Gestion des pièces jointes

Ne pas extraire les pièces jointes des messages

Si cette option est sélectionnée, les pièces jointes ne seront pas extraites des messages d'un compte contrôlé par un modèle. Les messages contenant des pièces jointes seront traités normalement, en laissant les pièces jointes intactes.

Extraire les pièces jointes et les enregistrer dans le dossier Documents du compte

Si cette option est activée, MDaemon extraira automatiquement les pièces jointes MIME Base64 présentes dans les messages entrants du compte. Les fichiers extraits sont supprimés du message entrant, décodés et placés dans ledossier Documents ducompte. Une note est alors placée dans le corps du message, indiquant les noms des fichiers qui ont été extraits. Cette option ne fournit pas de lien vers les pièces jointes jointes. <u>Webmail</u> as pour accéder à leur dossier Documents.

Utiliser la fonctionnalité Liens vers les pièces jointes jointes

Sélectionnez cette option si vous souhaitez utiliser la fonctionnalité Liens vers les pièces jointes pour les messages entrants ou sortants contenant des pièces jointes.



Si cette option est sélectionnée mais que la fonction Liens jointes est désactivée dans la boîte de dialogue<u>Liens</u> jointes seront pas extraites.

Extraire les pièces jointes des messages entrants

Lorsque cette option est activée, les pièces jointes sont extraites des messages entrants du compte et stockées à l'emplacement désigné dans la boîte de dialogue Liens jointes. (1) Des liens URL sont alors placés dans le Corps du message, sur lesquels l'utilisateur peut cliquer pour télécharger les fichiers. Pour des raisons de sécurité, ces liens URL ne contiennent pas de chemin d'accès direct aux fichiers. Au lieu de cela, ils contiennent un identifiant unique (GUID) que le serveur utilise pour faire correspondre le fichier au chemin d'accès réel. Ce GUID est stocké dans le fichierAttachmentLinking.dat...

Extraire les pièces jointes des messages sortants

Cochez cette case si vous souhaitez utiliser la fonctionnalité Liens vers les pièces jointes pour extraire les pièces jointes des messages sortants du compte. Lorsque le compte envoie un e-mail, Liens les pièces jointes extrait le fichier, le stocke et le remplace par une URL permettant de télécharger le fichier.

Modifier les paramètres des Liens vers les pièces jointes

Cliquez sur ce bouton pour ouvrir la boîte de dialogue<u>Liens vers les pièces jointes</u>

Voir :

<u>Propriétés du modèle</u> अभे <u>Propriétés du groupe</u> छिछै <u>Nouveau Modèles de comptes</u> अभ् <u>Liens vers les pièces jointes</u> 768 <u>Mon compte | Pièces jointes</u> 787

5.2.2.1.9 Rôles d'administration

🧐 Groups & Templates - Administrative Roles	
Groups & Templates - Administrative Roles Group Manager Template Manager New Accounts Sample Template Mail Services Web Services Autoresponder Forwarding Quotas Attachments Attachments Attachments Attachments Settings	Administrative Roles Account is a global administrator Account is a domain administrator
	Ok Cancel Apply Help

Rôles d'administration

Ce compte est administrateur global

Activez cette case à cocher pour accorder à ces utilisateurs un accès administratif au niveau du serveur. Les administrateurs globaux ont :

- Aucun accès à la configuration du serveur, à tous les utilisateurs et à tous les domaines par l'intermédiaire de l'administration à distance. MDaemon Admin Remote
- Un accès à tous les utilisateurs MDaemon de tous les domaines MDaemon en tant que contacts de messagerie instantanée.
- La possibilité d'envoyer des messages à toutes les listes de diffusion, même si elles sont marquées comme "Lecture seule".
- La possibilité d'envoyer des messages aux listes de diffusion même s'il n'est pas membre.

L'utilisateur aura un accès complet auxfichiers et options de MDaemon. Pour plus d'informations sur les options d'administration de l'interface web d'administration à distance, voir <u>Administration à distance</u> [376].

Ce compte est administrateur de domaine

Cochez cette case pour désigner les utilisateurs comme Administrateurs de domaine. Les administrateurs de domaine sont similaires aux administrateurs globaux, sauf que leur accès administrateur est limité à ce domaine et aux autorisations accordées sur la page<u>Services Web.</u> 771

> Cet écran n'est pas disponible sur le <u>modèle Nouveaux</u> <u>comptes</u> [848]. L'accès administrateur ne peut pas être accordé automatiquement aux Nouveaux comptes. Pour accorder un accès administratif à un compte, associez le compte à un modèle personnalisé qui utilise cet écran pour accorder cet accès, ou désignez manuellement le compte en tant qu'administrateur à partir de l'écran Rôles d'administration de l'éditeur de compte.

Voir :

Propriétés du modèlePropriétés du groupe838Nouveau Modèles de comptes848Mon compte | Rôles d'administration812

5.2.2.1.10 Liste d'autorisation

🧐 Groupes & Modèles - Liste des exceptions 🛛 💦
Gestionnaire de groupes Gestionnaire de modèles
OK Annuler Appliquer Aide

Les options de cet écran de modèle correspondent aux paramètres situés dans l'écran de l'éditeur de compte. Liste d'autorisation de l'est paramétré pour contrôler ce modèle d'ast, il contrôle les paramètres de l'écran and Liste d'admissibilité de tout compte appartenant à un groupe qui utilise le modèle . Paramètres des comptes appartenant à un groupe sui utilise le modèle.

Liste d'autorisation

Le Filtre anti-spam utilise les contacts personnels, les expéditeurs autorisés et les expéditeurs bloqués

L'écranListe d'autorisation (automatique) [739]du Filtre anti-spam contient une option globale qui peut être utilisée pour que le Filtre anti-spam autorise automatiquement un message lorsque l'expéditeur du message est trouvé dans les contacts personnels du destinataire local ou dans le dossier des expéditeurs autorisés. Il bloquera également automatiquement un message lorsque l'expéditeur se trouve dans le dossier Expéditeurs bloqués de l'utilisateur. Si vous avez activé l'option globale du Filtre anti-spammais que vous ne souhaitez pas l'appliquer à ces comptes, décochez cette case pour remplacer le paramètre global. Si l'option globale est désactivée, cette option ne sera pas disponible.

Ajouter automatiquement les destinataires des e-mails aux expéditeurs autorisés Cochez cette option si vous souhaitez mettre à jour ledossier \$SENDER\$ - adresse de l'expéditeur autorisé de chaque comptechaque fois qu'il envoie un message sortant à une adresse e-mail non locale. Dans le cas où le *Filtre anti-spam utilise les contacts personnels, les expéditeurs autorisés et les expéditeurs bloqués,* en conjonction avec l'option ci-dessus, le nombre de faux positifs du Filtre anti-spam peut être considérablement réduit. L'option *Ajouter automatiquement les destinataires des e-mails aux expéditeurs autorisés* située sur l' écranListe expéditeur (automatique)



Cette option est désactivée lorsque le compte utilise un autorépondeur.

Voir :

Propriétés du modèle 449 Propriétés du groupe 838 Nouveau Modèles de comptes 848 Editeur de compte | Liste d'autorisation 813

5.2.2.1.11 Paramètres

Groups & Templates - Settings	Settings Hide account from "Everyone" lists and domain's public contacts folder Automatically place new meeting requests on calendar, marked Tentative Account automatically processes meeting and cancellation requests Automatically decline requests that conflict with an existing event Automatically decline recurring meeting requests Automatically decline recurring meeting requests Automatically decline recurring meeting requests Automatically decline recurring meeting requests Account can use subaddressing to route incoming mail into folders Apply domain signature to all messages from this account Account is exempt from the "Authentication credentials must match those of the email sender" requirement Require app password to log in to SMTP, IMAP, ActiveSync, etc.
	Ok Cancel Apply Help

Les options de cet écran de modèle correspondent aux paramètres situés dans l'écran Paramètres des comptes de l'éditeur de compte. Lorsqu'un modèle est configuré pour <u>contrôler cet écran</u> [44], il contrôlera l'écran Paramètres de tout compte appartenant à un <u>groupe</u> [83] qui utilise le modèle.

Paramètres

Mon compte est masqué dans les listes " Tout le monde ", les calendriers partagés et VRFY

MDaemon crée et maintient automatiquement une liste de diffusion "everyone@ " pour chaque domaine, qui peut être utilisée pour envoyer un message à tout le monde en même temps. Non (par défaut), MDaemon inclut tous les comptes lorsqu'il construit cette liste. Cochez cette case si vous souhaitez exclure de cette liste les comptes contrôlés par ce modèle. Cela masquera également les comptes dans les calendriers partagés et les Aucun résultats.

Placer automatiquement les nouvelles demandes de réunion dans le calendrier, marquées comme provisoires

Par défaut, lorsqu'un compte reçoit une nouvelle demande de réunion, celle-ci est placée dans le calendrier de l'utilisateur et marquée comme *provisoire*. Décochez cette case si vous ne souhaitez pas que ce soit le paramètre par défaut pour les Nouveaux comptes.

Le compte traite automatiquement les demandes de réunion et les annulations de réunion.

Cochez cette case si vous souhaitez que les demandes, les modifications et les annulations de réunion soient traitées automatiquement pour chaque compte. Lorsqu'un compte reçoit un message contenant une demande de réunion, le calendrier du compte est automatiquement mis à jour. Cette option est désactivée par défaut pour tous les comptes.

Refuser automatiquement les demandes qui entrent en conflit avec un événement existant

Si le traitement automatique des demandes et des annulations de réunion est activé, ces demandes de réunion seront automatiquement refusées par défaut lorsqu'elles entrent en conflit avec un événement existant. Décochez cette case si vous souhaitez autoriser la création de l'événement en conflit.

Refuser automatiquement les demandes récurrentes

Cochez cette case si le traitement automatique des demandes récurrentes les demandes et les annulations de réunion est activé mais que vous souhaitez refuser ces demandes lorsqu'elles concernent des réunions récurrentes.

Le compte peut utiliser le sous-adressage pour router le courrier entrant dans des dossiers

Cochez cette case si vous souhaitez autoriser le <u>sous-adressage</u> [817] pour les comptes.

Ajouter la signature de domaine à tous les messages envoyés par ce compte

Lorsqu'il existe une <u>Signature de domaine</u> [210] pour le domaine auquel appartiennent les comptes régis par ce modèle, cette option fait en sorte qu'elle soit ajoutée à tous les e-mails envoyés par ces comptes.

Le compte est exempté de la requiert "Les identifiants doivent correspondre à ceux de l'expéditeur de l'E-mail".

Utilisez cette option si vous souhaitez exempter les comptes régis par ce modèle de l'option globale "*Les informations d'authentification doivent correspondre à celles de l'expéditeur du courriel*" située dans l'écran<u>Authentification SMTP</u> [558].

Exiger un mot de passe d'application pour se connecter à SMTP, IMAP, ActiveSync, etc. Cochez cette case si vous souhaitez que les comptes utilisant ce modèle doivent utiliser des <u>mots de passe d'application</u> al dans les clients de messagerie, pour se connecter à SMTP, IMAP, ActiveSync ou à d'autres protocoles de service de messagerie. Le<u>mot de passe as se service de</u> utilisé pour se connecter au Webmail ou à MDaemon Remote Admin.

Demander des Mots passe d'application peut aider à protéger le mot de passe d'un compte contre les attaques par dictionnaire et par force brute via SMTP, IMAP, etc. Cette méthode est plus sûre car même si une attaque de ce type permettait de deviner le mot de passe réel d'un compte, elle ne fonctionnerait pas et l'attaquant n'en saurait rien, car MDaemon n'accepterait qu'un mot de passe Mon compte correct. De plus, si vos comptes dans MDaemon utilisent l'authentification Active Director et qu'Active Directory verrouille un compte après un certain nombre de tentatives échouées, cette option permet d'éviter que les comptes soient verrouillés, car MDaemon ne vérifiera que les Mots passe d'application, sans essayer de s'authentifier auprès d'Active Directory.

Voir :

 Propriétés du modèle
 Basil

 Propriétés des groupes
 Basil

 Nouveau Modèles de comptes
 Basil

 Éditeur de comptes
 I Paramètres des comptes

5.3 Paramètres de compte

5.3.1 Active Directory

Dans les options Active Directory situées sous Comptes | Paramètres des comptes | Active Directory, MDaemon peut être configuré pour surveiller Active Directory et créer, modifier, supprimer et désactiver automatiquement les comptes MDaemon lorsque leurs comptes associés sont modifiés dans Active Directory. Dans ce cas, MDaemon peut également être configuré pour mettre à jour toutes les fiches de contact public avec les informations les plus récentes stockées dans Active Directory. Les champs communs tels que l'adresse postale d'un compte, les numéros de téléphone, les coordonnées professionnelles, etc. peuvent être renseignés dans les fiches de contact public et mis à jour chaque fois qu'ils sont modifiés dans Active Directory.

Création de comptes

Lorsqu'il est configuré pour surveiller Active Directory, MDaemon recherche les modifications à un intervalle donné, puis crée un nouveau compte utilisateur MDaemon dès qu'il constate qu'un nouveau compte Active Directory a été ajouté. Ce nouveau compte utilisateur MDaemon est créé à partir du Nom complet, de la Boîte aux lettres (identifiant), de la boîte aux lettres, de la description et de l'état activé/désactivé trouvés dans Active Directory.

Par défaut, les nouveaux comptes MDaemon créés suite au contrôle d'Active Directory seront ajoutés au Domaine défaut - Domaine deMDaemon.Vous pouvez également choisir d'ajouter ces comptes au domaine indiquédans l'attribut Active Directory "UserPrincipalName" ducompte. Si un compte a besoin d'un domaine qui n'existe pas encore dans MDaemon, un nouveau <u>domaine</u> 1841 sera automatiquement créé.

Vous pouvez également configurer votre *filtre de recherche* pour qu'il surveille un groupe dans Active Directory, de sorte que l'ajout d'un utilisateur au groupe ou d'un groupe à l'utilisateur entraînera la création de l'utilisateur dans MDaemon, et la suppression d'un utilisateur d'un groupe entraînera la désactivation (et non la suppression) du compte dans MDaemon.

Suppression de comptes

MDaemon peut être configuré pour prendre l'une des mesures suivantes lorsqu'un compte est supprimé d'Active Directory : ne rien faire, supprimer le compte MDaemon associé, désactiver le compte MDaemon associé ou geler le compte MDaemon associé

(c'est-à-dire que le compte peut toujours recevoir du courrier, mais l'utilisateur ne peut pas le collecter ou y accéder).

Mise à jour des comptes

Dans le cas où MDaemon détecte des changements dans les comptes Active Directory, il met automatiquement à jour les propriétés associées dans le compte MDaemon correspondant.

Synchronisation de MDaemon avec Active Directory

L'option"*Effectuer une analyse complète d'Active Directory maintenant*" permet à MDaemon d'interroger la base de données d'Active Directory, puis de créer ou de modifier les comptes utilisateurs de MDaemon si nécessaire. Lorsqu'un compte Active Directory correspondant à un compte MDaemon existant est trouvé, le compte MDaemon est lié à ce dernier. . then, any future changes made to the Active Directory accounts will be propagated to the MDaemon accounts automatically.

Authentification Active Directory

Les comptes ajoutéspar la fonctionnalité Active Directory deMDaemonsont configurés par défaut pour l'authentification Active Directory (AD). Avec l'authentification AD, MDaemon n'a pas besoin de stocker lemot de passe ducomptedans sa propre base de données d'utilisateurs. Au lieu de cela, le titulaire du compte utilisera ses identifiants Windows et MDaemon les transmettra à Windows pour l'authentification du compte associé.

Pour utiliser l'authentification AD avec Active Directory, un nom de domaine Windows doit être présent dans l'espace prévu à cet effet sur le <u>Moniteur</u> (1877). C'est le domaine Windows que MDaemon utilisera lorsqu'il tentera d'authentifier les comptes. Dans la plupart des cas, MDaemon détecte automatiquement ce Nom de domaine Windows et le renseigne pour vous. Cependant, vous pouvez utiliser un autre domaine dans cette option si vous le souhaitez, ou vous pouvez utiliser "NT_ANY" si vous souhaitez autoriser l'authentification dans tous les domaines Windows au lieu de la limiter à un domaine spécifique. Si vous laissez cette option vide, MDaemon n'utilisera pas l'authentification AD lors de la création de nouveaux comptes. Il générera un mot de passe aléatoire que vous devrez modifier manuellement pour que les utilisateurs puissent accéder à leurs comptes de messagerie.

Surveillance persistante

La surveillance d'Active Directory continue de fonctionner même lorsque MDaemon est arrêté. Toutes les modifications apportées à Active Directory sont suivies et MDaemon les traite au redémarrage.

Sécurité des fichiers Active Directory

Il est important de noter queles fonctionnalités deMDaemonrelatives à Active Directory ne modifient en rien les fichiers de schéma d'Active Directory - la surveillance s'effectue à sens unique, d'Active Directory vers MDaemon. MDaemon ne modifie pas votre annuaire.

Modèle Active Directory

Lorsque MDaemon ajoute ou modifie des comptes suite à la surveillance et à l'analyse d'Active Directory, il utilise un modèle Active Directory

("MDaemon/app/ActiveDS.dat") pour lier certains noms d'attributs Active Directory aux champs des comptes de MDaemon.Exemple : MDaemon lie par défaut l'attribut Active Directory "cn" au champ"FullName"de MDaemon. Ces liens ne sont pas codés en dur. Vous pouvez facilement modifier ce modèle à l'aide du Bloc-notes si vous le souhaitez et changer les liens entre les champs par défaut. Exemple : "FullName=%givenName% %sn%" pourrait remplacer le paramètre par défaut : "FullName=%cn%". Voir ActiveDS.dat pour plus d'informations.

Mise à jour des carnets d'adresses publics

La surveillance d'Active Directory peut être utilisée pour interroger périodiquement Active Directory et mettre à jour toutes les fiches de contacts publics dans MDaemon avec les informations les plus récentes. Les champs communs tels que l'adresse postale d'un compte, les numéros de téléphone, les coordonnées professionnelles, etc. seront renseignés dans leur fiche de contact public, et ces données seront mises à jour à chaque fois qu'elles seront modifiées dans Active Directory. Pour activer cette fonctionnalité, utilisez l'option "*Surveiller Active Directory et mettre à jour le(s) carnet(s) d'adresses public(s)*" située à l'adresse suivante : <u>Active Directory |</u> <u>Surveillance</u>.

De nombreux champs de la fiche de contact peuvent être surveillés à l'aide de cette fonctionnalité. Pour obtenir la liste complète des champs Fichier public qui peuvent être mis en correspondance avec des attributs Active Directory, consultez le fichier ActiveDS.dat. Ce fichier contient plusieurs nouveaux modèles de mappage qui vous permettent de spécifier un ou plusieurs attributs Active Directory à partir desquels un champ particulier de la fiche de contact doit être renseigné (par exemple, %fullName% pour le champ Fullname, %streetAddress% pour le champ Adresse, et ainsi de suite).

MDaemon doit faire correspondre l'adresse électronique d'un compte à un attribut d'Active Directory pour savoir quelle fiche contact mettre à jour. Si cette correspondance n'est pas trouvée, il ne fait rien. Par défaut, MDaemon tente de construire une adresse électronique en utilisant les données de l'attribut associé au modèle de boîte aux lettres (voir ActiveDS.dat), auxquelles il ajoute en interne le nom de <u>domaine par défaut</u> (164), comme il le ferait lors de la création et de la suppression de comptes à partir des données d'Active Directory. Vous pouvez cependant décommenter le modèle "abMappingEmail" dans ActiveDS.dat et le lier à n'importe quel attribut Active Directory (comme %mail%, par exemple). Notez toutefois que la valeur de cet attribut doit contenir une adresse électronique qui sera reconnue comme un compte d'utilisateur local valide.

Cette fonction créera les enregistrements de contact à la volée s'ils n'existent pas encore et mettra à jour les enregistrements de contact existants. En outre, veuillez noter qu'elle écrasera toute modification effectuée en dehors d'Active Directory. Les champs des fiches de contact qui ne sont pas mappés ne sont pas modifiés. Par conséquent, les données existantes qui ne sont pas soumises à ce processus ne seront ni modifiées ni perdues. Enfin, les comptes MDaemon dont la valeur est définie sur ne sont pas soumis à la création ou à la mise à jour de leurs fiches de contact.

Menu Comptes	883

Voir :

Active Directory | Surveillance

5.3.1.1 Authentification

Account Settings - Authentication	×
- Active Directory	Active Directory Authentication & Search User name or Bind DN
Monitoring LDAP Aliases	Password Use secure authentication
. Other	Base entry DN Leave blank for default LDAP://rootDSE.
	LDAP://rootDSE
	Search filter Test
	(&(objectClass=user)(objectCategory=person))
	Contact search filter
	(&(objectClass=user)(objectCategory=person))
	Search scope: Base DN only 1 level below base DN Base DN and all children Verbose AD logging
	Ok Cancel Apply Help

L'accès à Active Directory peut nécessiter des autorisations spéciales pour que toutes les fonctionnalités fonctionnent.

Authentification Active Directory & Recherche

Nom d'utilisateur ou DN de liaison

Il s'agit de l'identifiant de connexion ou du DN du compte Windows que MDaemon utilisera pour se lier à Active Directory. que MDaemon utilisera pour se lier à Active Directory à l'aide de LDAP. Active Directory autorise l'utilisation d'un compte Windows ou d'un UPN lors de la liaison.



Dans le cas où vous utilisez un DN dans cette option plutôt qu'un logon Windows, vous devez désactiver/effacer

l'option "Utiliser l'authentification sécurisée" ci-dessous.

Mot de passe

Il s'agit du mot de passe correspondant au DN ou à l'identifiant Windows utilisé dans l' option*DN de liaison* ci-dessus.

Utiliser l'authentification sécurisée

Cochez cette case si vous souhaitez utiliser une authentification sécurisée lors de vos recherches dans Active Directory. Vous ne pouvez pas utiliser cette option si vous utilisez un DN plutôt qu'une connexion Windows dans l' option*DN de liaison* cidessus.

Utiliser l'authentification SSL

Cochez cette case si vous souhaitez utiliser l'authentification SSL lors de vos recherches dans Active Directory.

L'utilisation de cette option nécessite un serveur SSL et une infrastructure sur votre réseau Windows et Active Directory. Contactez votre service informatique si vous n'êtes pas sûr que votre réseau soit configuré de cette manière, et pour savoir si vous devez activer cette option.

Chercher dans Active Directory

Entrée base DN

Il s'agit du Distinguished Name (DN) ou point de départ dans l'arborescence Directory Information Tree (DIT) à partir duquel MDaemon cherchera des comptes et des modifications dans Active Directory. Non (par défaut), MDaemon commencera à chercher au DSE racine, qui est l'entrée la plus élevée de votre hiérarchie Active Directory. Le fait de désigner un point de départ plus précis, plus proche de l'emplacement des comptes d'utilisateurs dans l'arborescence d'Active Directory, peut réduire le temps nécessaire pour chercher des comptes et des modifications de comptes dans le DIT. Laissez ce champ vide pour restaurer les paramètres par défaut LDAP par : //rootDSE.

Filtre de recherche

Il s'agit du filtre de recherche LDAP qui sera utilisé lors du contrôle ou de la recherche de comptes et de modifications de comptes dans votre Active Directory. Utilisez ce filtre pour localiser plus précisément les comptes utilisateurs que vous souhaitez inclure dans la surveillance d'Active Directory.

Vous pouvez également configurer votre filtre de recherche pour surveiller un groupe au sein d'Active Directory. Ainsi, l'ajout d'un utilisateur au groupe ou d'un groupe à l'utilisateur entraînera la création de l'utilisateur dans MDaemon, et la suppression d'un utilisateur d'un groupe entraînera la désactivation (et non la suppression) du compte dans MDaemon. Exemple : un filtre de recherche approprié pour un groupe appelé 'MonGroupe' pourrait ressembler à ceci :

```
(|(&(ObjectClass=group)(cn=MyGroup))(&(objectClass=user)
(objectCategory=person)
(memberof=cn=MyGroup,ou=me,dc=domain,dc=com)))
```

Remplacez les éléments 'ou=' et 'dc=' par des éléments appropriés à votre réseau.

Filtre de recherche de contacts

Utilisez cette option pour spécifier un filtre de recherche distinct pour les recherches de contacts. Si vous utilisez dans ce champ le même texte que dans l'option*Filtre de recherche* ci-dessus, une seule requête est utilisée pour mettre à jour toutes les données. Lorsque les filtres de recherche sont différents, deux requêtes distinctes sont nécessaires.

Test

Utilisez les boutons*Test* pour tester les paramètres de vos filtres de recherche.

Étendue de la recherche :

Il s'agit de la portée ou de l'étendue de vos recherches dans Active Directory.

DN de base uniquement

Cherchez cette option si vous souhaitez limiter votre recherche au DN de base spécifié ci-dessus. La recherche ne sera pas effectuée en dessous de ce point de l'arborescence (DIT).

1 niveau inférieur au DN de base

Utilisez cette option si vous souhaitez étendre votre recherche Active Directory à un niveau inférieur au DN fourni dans votre DIT.

DN de base et tous les enfants

Cette option permet d'étendre la portée de votre recherche du DN fourni à tous ses enfants, jusqu'à l'entrée enfant la plus basse de votre DIT. Il s'agit de l'option sélectionnée par défaut, qui, combinée au paramètre DSE racine par défaut cidessus, signifie que l'ensemble du DIT situé en dessous du DSE racine sera cherché.

Pas de journalisation AD verbeuse

Non (par défaut), MDaemon utilise la Pas de journalisation par défaut pour Active Directory. Décochez cette case si vous souhaitez utiliser une pas de journalisation Active Directory moins poussée.

5.3.1.2 Surveillance

Ø Account Settings - Monitoring	
Active Directory Authentication Monitoring DAP Aliases Autoresponders Other	Active Directory Monitoring Monitor Active Directory and create/update MD aemon accounts Monitor Active Directory and update public address book(s) Use Active Directory domain names when creating accounts Query Active Directory for new data every 30 seconds Windows domain for AD authentication EXAMPLE Valid values are a Windows domain, NT_ANY, or leave blank for randomly generated passwords. When accounts are deleted in Active Directory do nothing (leave the MD aemon account untouched) delete them from MD aemon account (account can't send or receive mail) disable the MD aemon account (account can't send or receive mail) freeze the MD aemon account (account can receive but can't collect mail) freeze MD aemon account (account can receive but can't collect mail) freeze MD aemon accounts when they are disabled in Active Directory When accounts are deleted in AD remove from public address book(s) Accounts deleted outside AD are not recreated by AD monitoring Perform full Active Directory scan now
	Ok Cancel Apply Help

Surveillance d'Active Directory

Surveiller Active Directory et créer/mettre à jour les comptes MDaemon

Cliquez sur cette option pour activer la surveillance d'Active Directory, qui créera et mettra à jour les comptes MDaemon au fur et à mesure des mises à jour d'Active Directory.

Surveiller Active Directory et mettre à jour le(s) carnet(s) d'adresses public(s)

Activez cette option si vous souhaitez utiliser Active Directory pour mettre à jour toutes les fiches de contact publiques avec les informations les plus récentes stockées dans Active Directory. Les champs communs tels que l'adresse postale d'un compte, ses numéros de téléphone, ses coordonnées professionnelles, etc. seront renseignés dans sa fiche de contact public et ces données seront mises à jour chaque fois qu'elles seront modifiées dans Active Directory. De nombreux champs de la fiche de contact seront ainsi contrôlés. Pour obtenir la liste complète des champs de la fiche de contact publique qui peuvent être associés à des attributs Active Directory, consultez le fichier ActiveDS.dat. Voir : <u>Mise à jour des carnets</u> <u>d'adresses publics</u> 2007, pour plus d'informations.

Utiliser les noms de domaine Active Directory lors de la création de comptes

Utilisez cette option si vous souhaitez que les nouveaux comptes créés à la suite de la surveillance d'Active Directory soient ajoutés au domaine indiqué dans l'attribut Active Directory "UserPrincipalName" du compte. Si un compte nécessite un domaine qui n'existe pas encore dans MDaemon, un nouveau domaine domaine souhaitez que automatiquement créé. Effacez ou désactivez cette option si vous souhaitez que tous les nouveaux comptes soient ajoutés au Domaine par défaut de MDaemon.

Interroger Active Directory pour obtenir de nouvelles données toutes les [xx] secondes Il s'agit de l'intervalle auquel MDaemon surveille les modifications apportées à Active Directory.

Domaine Windows pour l'authentification AD

Indiquez ici un nom de domaine Windows si vous souhaitez utiliser l'authentification Active Directory pour les comptes créés par la surveillance d'Active Directory. Si vous laissez ce champ vide, les nouveaux comptes se verront attribuer des mots de passe aléatoires. Vous devrez alors modifier ces mots passe manuellement pour pouvoir accéder aux comptes.

Lorsque des comptes sont supprimés dans Active Directory...

L'option sélectionnée ci-dessous détermine l'action que MDaemon entreprendra lorsquele compte Active Directory associé à un compteMDaemonest supprimé.

...ne rien faire

Choisissez cette option si vous ne souhaitez pas que MDaemon apporte des modifications à un compte MDaemon lorsque son compte associé est supprimé d'Active Directory.

...les supprimer également de MDaemon

Si vous choisissez cette option, le compte MDaemon sera supprimé lorsque le compte qui lui est associé sera supprimé d'Active Directory.

0

Le compte MDaemon associé sera alors complètement supprimé. Tous les messages, dossiers de messages, carnets d'adresses, calendriers, etc. du compte seront supprimés.

...désactiver le compte DÉSACTIVÉ

Lorsque cette option est sélectionnée et qu'un compte Active Directory est supprimé, le compte MDaemon correspondant est désactivé. Cela signifie que le compte MDaemon existera toujours sur le serveur, mais qu'il ne pourra ni envoyer ni recevoir de courrier électronique et que personne n'y aura accès.

...Figer les comptes MDaemon

Lorsque cette option est sélectionnée, MDaemon continue d'accepter lecourrier entrant ducomptemais le "verrouille" de manière à ce que personne n'y ait accès. Dans ce cas, le courrier entrant adressé à ce compte ne sera ni rejeté ni supprimé par MDaemon, mais le titulaire du compte ne pourra pas récupérer ce courrier ni y accéder tant que le compte est figé.

Figer les comptes MDaemon lorsqu'ils sont désactivés dans Active Directory

Par défaut, lorsque vous désactivez un compte dans Active Directory, MDaemon désactive également le compte associé dans MDaemon. Le compte devient alors inaccessible et MDaemon n'acceptera ni ne délivrera de messages pour ce compte. Toutefois, si vous préférez que le compte MDaemon associé soit figé plutôt que désactivé, activez cette option. MDaemon acceptera toujours les messages pour les comptes figés, mais les utilisateurs ne pourront pas accéder à ces comptes pour collecter ou envoyer leur courrier électronique.

Lorsque les comptes sont ajoutés à AD, les supprimer du ou des carnets d'adresses publics

Non (par défaut), un contact de dossier public est supprimé lorsque le compte qui lui est associé est supprimé d'Active Directory. Toutefois, le contact n'est supprimé que s'il a été <u>créé à l</u> a fonction d'intégration d'Active Directory aprile. Désactivez cette option si vous ne souhaitez pas supprimer les contacts lorsque les comptes associés sont supprimés dans Active Directory.

Les comptes ajoutés en dehors d'AD ne sont pas recréés par le contrôle d'AD

Lorsque vous supprimez un compte MDaemon en dehors d'Active Directory (par exemple, en le supprimant manuellement à l'aide de l'interface MDaemon), par défaut le compte ne sera pas recréé par la fonctionnalité de surveillance d'Active Directory. Désactivez cette option si vous souhaitez que ces comptes soient recréés.

Effectuer une analyse complète d'Active Directory maintenant

Cliquez sur ce bouton pour que MDaemon interroge la base de données Active Directory, puis crée, modifie ou supprime des comptes si nécessaire. Lorsqu'un compte Active Directory correspondant à un compte MDaemon existant est trouvé, le compte MDaemon est lié à ce dernier.

Voir aussi

<u>Active Directory</u> ब्लो <u>Active Directory | Authentification</u> ब्लो

5.3.1.3 LDAP

Account Settings - LDAP			×
		D 1-1 1	
Manitarian	U store account data in an LUAP accessible store		
Use LDAP server for address book and remote verification			1
	Host name or IP	RDN filter	
Autoresponders		mail=\$EMAIL\$	
• Other	Bind DN	Bind password	Port
			389
	Base entry DN (database)	Base entry DN (addre	ss book)
	Object class (database)	Object class (address book)	
	MDaemonUser	MDaemonContact	
	Base entry DN (remote verification	1)	
	Server is protocol version 3	Cache LDAP look	up results
	Chase referrals	Export full name w	ith aliases
	See the MDaemon Users Manual LDAP fields.	for an explanation of these	Configure
	Ok	Cancel Ap	ply Help

MDaemon prend en charge la fonctionnalité LDAP (Lightweight Directory Access Protocol). Cliquez sur "Comptes | Paramètres des comptes | LDAP " pour accéder à l'écran LDAP utilisé pour configurer MDaemon afin qu'il tienne à jour votre serveur LDAP pour tous ses comptes utilisateurs. MDaemon peut maintenir une base de données LDAP précise et continuellement à jour en communiquant avec votre serveur LDAP chaque fois qu'un compte MDaemon est ajouté ou supprimé. Cela permet aux utilisateurs disposant de clients de messagerie compatibles avec LDAP de "partager" un carnet d'adresses global contenant les entrées de tous les utilisateurs de MDaemon ainsi que d'autres contacts que vous aurez inclus.

Vous pouvez également utiliser votre serveur LDAP comme <u>base de données des</u> <u>utilisateurs de MDaemon</u> plutôt que son système local USERLIST.DAT ou une base de données compatible ODBC. Vous pouvez utiliser cette méthode de gestion des informations sur les utilisateurs si vous avez plusieurs serveurs MDaemon à différents endroits mais que vous souhaitez qu'ils partagent une seule base de données des utilisateurs. Chaque serveur MDaemon sera configuré pour se connecter au même serveur LDAP afin de partager les informations sur les utilisateurs plutôt que de les stocker localement.

LDAP

Stocker les données des comptes dans un annuaire LDAP

Cochez cette case si vous souhaitez que MDaemon utilise votre serveur LDAP comme base de données utilisateurs plutôt qu'ODBC ou son systèmelocal USERLIST.DAT. Vous pouvez utiliser cette méthode pour maintenir vos informations utilisateur si vous avez plusieurs serveurs MDaemon à différents endroits mais que vous souhaitez qu'ils partagent une seule base de données utilisateur. Chaque serveur MDaemon sera configuré pour se connecter au même serveur LDAP afin de partager les informations sur les utilisateurs plutôt que de les stocker localement.

Utiliser un serveur LDAP pour le carnet d'adresses et la vérification à distance

Si vous utilisez ODBC ou la méthode pardéfaut USERLIST.DAT pour maintenir votre base de données de comptes plutôt que la méthode du serveur LDAP, vous pouvez toujours maintenir un serveur LDAP à jour avec tous les noms, adresses électroniques et alias de vos utilisateurs en activant cette case à cocher. Ainsi, vous pouvez toujours maintenir un serveur LDAP à jour pour l'utiliser comme système de carnet d'adresses global pour les utilisateurs de clients de messagerie qui prennent en charge les carnets d'adresses LDAP.

Vous conserverez ainsi une base de données de vos boîtes aux lettres, alias et listes de diffusion que vos serveurs de sauvegarde distants pourront interroger pour la vérification à distance des informations d'adresse. Pour plus d'informations, reportezvous à la section *DN de base (vérification distante)* ci-dessous.

Propriétés du serveur LDAP

Nom d'hôte ou IP

Indiquez ici le Nom hôte ou l'Adresse IP de votre serveur LDAP.

Filtre RDN

Cette commande est utilisée pour générer le RDN pour chaqueentrée LDAP d'unutilisateur.Le nom distinctif relatif (RDN) est le composant le plus à gauche dunom distinctif (DN) dechaque entrée.Pour toutes les entrées homologues (celles qui partagent un parent immédiat commun), le RDN doit être unique, c'est pourquoi nous suggérons d'utiliser l'adresse électronique de chaque utilisateurcomme RDN afin d'éviter les conflits éventuels. Dans ce contrôle, l'utilisation de la macro \$EMAIL\$ comme valeur de l'attribut (c'est-à-dire mail=\$EMAIL\$) entraînera son remplacement par l'adresse électronique de l'utilisateurlors de la création de son entrée LDAP.Le DN de l' utilisateursera composé du RDN et du *DN d'entrée base* cidessous.

DN de liaison

Ajoutez le DN de l'entrée à laquelle vous avez accordé un accès administratif à votre serveur LDAP afin que MDaemon puisse ajouter et modifier les entrées de vos utilisateurs MDaemon. Il s'agit du DN utilisé pour l'authentification dans l'opération de liaison.

Mot de passe de liaison

Ce mot de passe sera transmis à votre serveur LDAP avec la valeur du*DN de liaison* pour l'authentification.

Port

Indiquez le port que votre serveur LDAP surveille. Monaemon utilisera ce port lorsqu'il publiera des informations du compte.

DN de base (base de données)

Entrez l'entrée base (root DN) qui sera utilisée dans toutes les entrées utilisateur de MDaemon lorsque vous utilisez le serveur LDAP comme base de données utilisateur plutôt que le fichier USERLIST.DAT. Le DN de l'entrée base est combiné avec le RDN (voir le *filtre RDN* ci-dessus) pour constituer lenom distinctif (DN) de chaque utilisateur.

DN de base (carnet d'adresses)

Lors de la mise en miroir des informations du compte dans le carnet d'adresses d'une base de données LDAP, entrez l'entrée de base (base DN) qui sera utilisée dans toutes les entrées du carnet d'adresses de l'utilisateur de MDaemon. Le DN de l'entrée base est combiné avec le RDN (voir le *filtre RDN* ci-dessus) pour constituer lenom distinctif (DN) de chaque utilisateur.

Classe d'objet (base de données)

Permet de spécifier la classe objet à laquelledoit appartenir l'entrée de la base de données de chaque utilisateur de MDaemon. Chaque entrée contiendra l'attributobjectclass= avec cette valeur.

Classe d'objet (carnet d'adresses)

Indique la classe d'objet à laquelledoit appartenir l'entrée du carnet d'adresses LDAP de chaque utilisateur de MDaemon. Chaque entrée contiendra l'attributobjectclass= avec cette valeur.

DN de base (vérification distante)

Un problème courant avec les passerelles de domaine et les serveurs de sauvegarde est qu'ilsn'ont généralement pas de méthode pour déterminer si le destinataire d'un message entrant est valide ou non. Exemple : si un message arrive auserveur de sauvegarde de example.compour user1@example.com, le serveur de sauvegarde n'a aucun moyen de savoir s'il existe réellement une boîte aux lettres, un alias ou une liste de diffusion à example.com pour "user1". Le serveur de secours n'a donc d'autre choix que d'accepter tous les messages. MDaemon contient une méthode permettant de vérifier ces adresses et de résoudre ce problème. En spécifiant un DN d'entrée base qui sera utilisé pour toutes les Boîtes Boîtes, Alias et Listes de diffusion, votre serveur LDAP peut être tenu à jour avec toutes ces informations. Ensuite, votre serveur de sauvegarde peut simplement interroger votre serveur LDAP chaque fois qu'un message arrive pour votre Domaine et vérifier si l'adresse du destinataireest valide ou non.Si ce n'est pas le cas, le message sera rejeté.

Utiliser la version 3 du protocole

Cochez cette case si vous souhaitez que MDaemon utilise le protocole LDAP version 3 avec votre serveur.

Suivre les referrals

Il arrive qu'un serveur LDAP ne dispose pas de l'objet demandé, mais qu'il ait une référence croisée à son emplacement, vers laquelle il peut renvoyer le client. Si vous

souhaitez que MDaemon suive ces referrals, activez cette option. Cette option est désactivée par défaut.

Mettre en cache les résultats des vérifications LDAP

Par défaut, MDaemon met en cache les vérifications LDAP les résultats. Désactivez cette option si vous ne souhaitez pas les mettre en cache.

Exporter le nom complet avec les alias

Les alias exportés vers un carnet d'adresses LDAP contiennent le Nom complet du compte dans le champ À :. Dans les alias, c'est l'adresse électronique actuelle du compte (sans alias) qui est placée dans le champ CN. Cochez cette case si vous souhaitez que le nom complet du compte (s'il est connu) soit placé dans le champ CN. Cette option est désactivée par défaut.

Configurer

Cliquez sur ce bouton pour ouvrir le fichier de configurationLDAP.dat dans un éditeur de texte. Ce fichier est utilisé pour désigner les noms des attributs LDAP qui correspondront à chaque champ Mon compte de MDaemon.

Voir :

Options de compte

5.3.2 Alias

5.3.2.1 Alias

🧐 Paramètres de compte Alias	
Active Directory Alias Paramètres Autorépondeurs Autres	Alias MD aemon@\$L0CALDOMAIN\$ = MD aemon@company.test ListServ@\$L0CALDOMAIN\$ = MD aemon@company.test ListServer@\$L0CALDOMAIN\$ = MD aemon@company.test postmaster@company.test = michael.mason@company.test abuse@company.test = michael.mason@company.test Haut Bas Double-cliquez sur une entrée pour la modifier Modifier Fichier
	Nouvel alias - Caractères jokers ? et * autorisés Alias E-mail actuel michael.mason@company.test (Micha V & Ajouter
	OK Annuler Appliquer Aide

Les alias vous permettent de créer d'autres noms de boîtes aux lettres pour vos comptes ou vos listes de diffusion, ce qui est utile lorsque vous souhaitez que plusieurs noms de boîtes aux lettres correspondent à un seul compte ou à une seule liste d'utilisateurs. Sans les alias, vous devriez créer des comptes utilisateurs distincts pour chaque adresse, puis transférer les messages ou utiliser des règles de filtrage complexes pour les associer à d'autres comptes.

Exemple : si userl@example.com gère toutes les demandes de facturation pour votre domaine, mais que vous voulez dire à tout le monde de les envoyer à billing@example.com, vous pouvez créer un Alias pour que les messages adressés à billing@example.com aillent en fait à userl@example.com. Si vous hébergez plusieurs domaines et que vous souhaitez que tous les messages adressés au Postmaster (quel que soit le domaine) soient envoyés à userl@example.com, vous pouvez utiliser un caractère générique pour associer l'alias Postmaster@* à son adresse.

Alias actuels

Cette fenêtre contient tous les alias actuels que vous avez créés.

Supprimer

Cliquez sur ce bouton pour supprimer une entrée sélectionnée de la liste Alias actuels.

Haut de page

Les alias sont traités dans l'ordre dans lequel ils sont listés. Vous pouvez déplacer un alias vers une position plus élevée dans la liste en le sélectionnant puis en cliquant sur ce bouton.

Vers le bas

Les alias sont traités dans l'ordre dans lequel ils sont listés. Vous pouvez déplacer un alias vers une position inférieure dans la liste en le sélectionnant et en cliquant ensuite sur ce bouton.

Modifier le fichier

Cherchezce bouton si vous souhaitez ouvrir le fichier Éditeur'd alias dans un éditeur de texte, afin d'y effectuer une recherche manuelle ou de le modifier. Après avoir effectué les modifications souhaitées, quittez l'éditeur de texte, puis MDaemon rechargera le fichier.

Alias

Saisissez l'adresse électronique que vous souhaitez transformer en alias de l'"Adresse électronique actuelle". listée ci-dessous. Les caractères génériques "?" et "*" sont acceptés, et vous pouvez utiliser "@\$LOCALDOMAIN\$" dans l'alias comme un caractère générique qui ne correspondra qu'à vos domaines locaux. Exemple : "userl@example.*", "*@\$LOCALDOMAIN\$" et "userl@\$LOCALDOMAIN\$" sont tous valables dans un alias.

E-mail actuel

Sélectionnez un compte dans la liste déroulante, utilisez l'icône Compte pour rechercher un compte ou saisissez une nouvelle adresse e-mail ou une liste diffusion dans cet espace. Il s'agit de l'adresse E-mail actuelle qui recevra le message lorsqu'il est adressé à un alias correspondant.

Ajouter

Cliquez sur le bouton*Ajouter* pour ajouter l'alias à la liste. Les valeurs *Alias* et l'*E-mail actuel* seront combinés et placés dans la fenêtre*Alias actuels*.

Voir :

Alias | Paramètres 🕬 Mon compte | Alias 78

5.3.2.2 Paramètres

Ø Account Settings - Settings	
Aliases Aliases Settings Autoresponders Other	Settings □ It's OK to relay mail for aliases that include foreign domains □ Fully qualified aliases (no wildcards) are allowed to be list members □ Mail from 'Postmaster', 'abuse', 'webmaster' requires authentication □ IP Shield honors aliases ○ Replicate aliases to LDAP address book □ Alias processing stops when result matches an existing account or list This option must be enabled when using subaddressing or there is a chance that subaddressed addresses will not be handled properly. □ Use recursive aliasing When enabled, any match to the alias list causes the resulting value to be reprocessed back through the entire alias listing again. With this option you can layer your aliases up to 10 levels deep. ☑ Allow logon using aliases
	Ok Cancel Apply Help

Paramètres

Autoriser le relais du courrier aux alias qui comportent des domaines externes Cochez cette case si vous souhaitez autoriser MDaemon à relayer le courrier pour ces domaines locaux. Cette option remplace l' option *Ne pas autoriser le relais de messages* dans le <u>Contrôle des relais</u> [546] pour ces alias.

Autoriser les alias complets (sans caractères jokers) à s'abonner à une liste

Cochez cette case si vous souhaitez autoriser les alias à être membres des listes de diffusion de MDaemon. Seuls les comptes actifs peuvent être membres d'une liste si cette option n'est pas activée. **Remarque :** les alias contenant des caractères génériques ne sont pas autorisés à être membres de la liste même si cette option est activée.

Le courrier provenant de 'Postmaster', 'abuse', 'webmaster' doit être authentifié requise. Lorsque cette option est activée, MDaemon requiert l'authentification des messages provenant de vos alias ou comptes " postmaster@... ", " abuse@... " ou " webmaster@... " avant de les accepter. Les spammeurs et les pirates informatiques

savent que ces adresses peuvent exister et peuvent donc tenter d'utiliser l'une d'entre elles pour envoyer du courrier via votre système. Cette option les empêchera, ainsi que d'autres utilisateurs non autorisés, de le faire. Pour votre commodité, cette option est également disponible sur l'écran <u>Authentification</u> <u>SMTP</u> situé à l'adresse suivante : Sécurité | Paramètres de sécurité. Si vous modifiez le paramètre ici, il sera également modifié dans cet écran.

Le Bouclier IP honore les alias

Par défaut, le <u>Bouclier IP</u> is respecte les alias lorsqu'il vérifie la validité des paires domaine/IP dans les messages entrants. Le Bouclier IP traduit un alias en véritable compte vers lequel il pointe et l'honore donc s'il passe le bouclier. Si vous décochez cette case, le Bouclier IP traitera chaque Alias comme s'il s'agissait d'une adresse indépendante du compte qu'il représente. Ainsi, si l'adresse IP d' un Alias viole un Bouclier IP, le message sera refusé. Cette option est reproduite sur l'écran du Bouclier IP : si vous modifiez le paramètre ici, vous le modifierez également dans cet écran.

Dupliquer les alias dans le carnet d'adresses LDAP

Cochez cette case si vous souhaitez que les alias soient dupliqués dans le carnet d'adresses LDAP. La réplication des alias est nécessaire pour que la fonction de vérification à distance du LDAP fonctionne de manière fiable, mais si vous n'utilisez pas cette fonction, il est inutile de dupliquer les alias dans le carnet d'adresses LDAP. Si vous n'utilisez pas la vérification à distance, vous pouvez désactiver cette fonction pour gagner du temps. Pour plus d'informations sur la vérification à distance de LDAP, voir : LDAP

Le traitement des alias s'arrête lorsqu'une correspondance est trouvée avec un compte ou une liste existant(e).

Lorsque cette option est activée, le traitement des alias s'arrête lorsque le destinataire du message entrant correspond à un compte ou une liste de diffusion existant(e). Cela s'applique généralement aux alias qui contiennent un caractère générique. Exemple : si l'alias "*@example.com=user1@example.com"est défini, cette option permet d'appliquer l'alias uniquement aux adresses qui n'existent pas sur votre serveur. Si vous disposez également du compte"user2@example.com", les messages adressés à l'utilisateur 2 lui seront toujours transmis, car l'alias ne sera pas appliqué à ces messages. En revanche, les messages adressés à un compte ou à une liste inexistante seront envoyés à"user1@example.com", car l'alias générique sera appliqué à ces messages. Cette option est activée par défaut.



Elle doit être activée lorsque vous utilisez le <u>sous-adressage</u> and , afin d'éviter les problèmes potentiels liés à la gestion de ces messages.

Utiliser la création d'alias récursifs

Cochez cette case si vous souhaitez traiter les alias de manière récursive. Toute correspondance d'alias entraîne le retraitement de la valeur résultante dans l'ensemble de la Liste d'alias. Il est possible d'imbriquer les alias jusqu'à 10 niveaux de profondeur. Exemple : vous pouvez mettre en place quelque chose comme ceci :

```
user2@example.com = user1@example.com
EXEMPLE : user1@example.com = user5@example.net
```

user5@example.net = user9@example.org

Ce système est logiquement identique à l'alias simple :

user2@example.com = user9example.org

Cela signifie également que :

user1@example.com = user9example.org

Autoriser la connexion à l'aide d'alias

Par défaut, les utilisateurs sont autorisés à se connecter à leur compte en utilisant l'un des <u>alias de alias</u> leur compte au lieu du nom réel de leur boîte aux lettres. Décochez cette case si vous ne souhaitez pas l'autoriser.

Voir :

Alias 894

5.3.3 Autorépondeurs

5.3.3.1 Comptes

🧐 Paramètres de compte Comptes	.
Active Directory Alias Autorépondeurs Pièces jointes Liste des exceptions Paramètres Autres	Domaines Image: Company.test Image: Company.test
	OK Annuler Appliquer Aide

Les autorépondeurs sont des outils utiles pour faire en sorte que les messages entrants déclenchent automatiquement certains événements, tels que l'exécution d'un programme, l'ajout de l'expéditeur à une liste de diffusion, l'envoi d'un message généré automatiquement, etc. L'utilisation la plus courante des répondeurs automatiques consiste à répondre automatiquement aux messages entrants par un message défini par l'utilisateur indiquant que le destinataire est en vacances, qu'il n'est pas disponible, qu'il répondra dès que possible, etc. Les utilisateurs de MDaemon disposant d'un <u>accès</u> Web mil au Webmail au Vebmail au où à l'Administration à distance automatique et programmer les dates auxquelles ils seront utilisés. Enfin, les messages de réponse automatique et dossier racine de chaque utilisateur . Ce fichier prend en charge un grand nombre de macros, qui peuvent être utilisées pour générer dynamiquement une grande partie du contenu du message, ce qui rend les répondeurs automatiques très polyvalents.

Les Autorépondeurs sont toujours honorés lorsque le message déclencheur provient d'une source distante. Toutefois, pour les messages provenant provenant du même domaine d'un utilisateur, les autorépondeurs ne seront déclenchés que si vous activez l'option *Les autorépondeurs sont déclenchés par le courrier intra-domaine*, située dans l' écran<u>"</u> <u>Paramètres | des autorépondeurs</u> 902]. Vous pouvez également utiliser une option de cet écran pour limiter les messages de réponse automatique à une réponse par expéditeur et par jour.

Liste des comptes

Cette zone répertorie toutes les Boîtes aux Lettres disponibles qui peuvent héberger un répondeur automatique. Double-cliquez sur un compte dans cette liste pour ouvrir l'écran<u>Répondeur automatique</u> rrricorrespondant, qui permet de configurer un répondeur automatique pour ce compte.

Voir :

Autorépondeurs | Liste des exceptions de l'autorépondeur Autorépondeurs | Paramètres de l'autorépondeur <u>Création de messages de réponse automatique</u> <u>Mon compte | Répondeurs automatiques</u>

5.3.3.2 Pièces jointes

900

🧐 Paramètres de compte Pièces jointes 🗾 🗾	3
Active Directory Alias Autorépondeurs Comptes Comptes Comptes Comptes Comptes Comptes Contras Comptes Contras Comptes Contras Contras Comptes Contras Comptes Contras Comptes Contras Comptes Contras Comptes Contras Contras Comptes Comptes Comptes Comptes Contras Comptes Contras Comptes Comptes Contras Comptes Comptes Comptes Contras Comptes Contras Contras Comptes Contras Contres Contras Contras Contras Cont	
OK Annuler Appliquer Aide]

Indiquez ici les Chemins du fichier complet de tous les fichiers que vous souhaitez autoriser à être utilisés comme pièces jointes dans les <u>scripts d'autorépondeur</u>. Dans le script de réponse automatique, utilisez la macro de remplacement**% SetAttachment%** pour joindre le fichier.

Voir :

 Autorépondeurs | Comptes

 Autorépondeurs | Liste des exceptions de l'autorépondeur

 Autorépondeurs | Paramètres

 Création de scripts de réponse automatique

 Mon compte | Autorépondeurs
5.3.3.3 Exceptions

Paramètres de compte Liste des excepti	ions	×
Active Directory Alias Autorépondeurs Comptes Pièces jointes Iste des exceptions Paramètres Autres	# Liste des exceptions de l'autorépondeur # Ce fichier liste les adresses e-mail ne devant pas recevoir # de réponses automatiques. Vous pouvez préciser des paires en-tête/valeur # qui, si elles sont présentes dans le message, classeront ce dernier dans les exceptions. # Toutes les adresses système doivent figurer dans ce fichier. # Toutes les adresses système doivent figurer dans ce fichier. # Ex : MD aemon@*, Mailer-D aemon@* ou Precedence: bulk, X-List *. MDaemon@* Mailer-Daemon@* X-Spam-Flag: Yes X-Mailing-List * Precedence: bulk Precedence: junk Return-Path: <>	*
	OK Annuler Appliquer Ai	de

Utilisez la liste d'exceptions des autorépondeurs pour configurer des exceptions globales auxautorépondeurs. pour configurer des exceptions globales aux autorépondeurs. Les messages provenant des entrées de cette liste ne recevront pas de répondeur automatique. Cette liste peut contenir à la fois des adresses électroniques et des paires d'en-têtes/valeurs. Saisissez une adresse ou une paire d'en-tête/valeur par ligne. Les caractères génériques sont autorisés.



Voir :

Autorépondeurs | Comptes Autorépondeurs | Paramètres <u>Création de scripts de réponse automatique</u> Mon compte | Autorépondeurs 777

5.3.3.4 Paramètres

Account Settings - Settings	
Active Directory Aliases Autoresponders Accounts Attachments Exempt List Settings Other	Settings Autoresponders are triggered by intra-domain mail Limit auto responses to one per day per recipient Undeliverable autoresponse emails are simply deleted (no retry queue) Edit the default autoresponder file (OutOfOffice.rsp)
	Ok Cancel Apply Help

Paramètres

Appliquer l'autorépondeur au courrier local

Non (par défaut), les courriers locaux et distants déclenchent des autorépondeurs. Décochez cette case si vous ne souhaitez pas déclencher les autorépondeurs lorsque le message entrant provient du même domaine que l'utilisateur.

Limiter les réponses automatiques à une par jour et par destinataire

Non (par défaut), les répondeurs automatiques ne génèrent qu'un seul message de réponse par jour pour une adresse donnée. Cela permet d'éviter que des personnes reçoivent le même message de réponse automatique redondant le même jour, à chaque fois qu'elles vous envoient un e-mail. Décochez cette case si vous souhaitez envoyer des messages de réponse automatique chaque fois que quelqu'un vous envoie un message, même s'il en a déjà reçu un ce jour-là.



Cette option permet également d'éviter les boucles de messages, qui peuvent se produire lorsque votre message de

réponse automatique est renvoyé à une adresse où un autorépondeur est également actif. Au lieu de permettre aux deux adresses d'envoyer constamment des messages de réponse automatique l'une à l'autre, cette option permet d'envoyer un seul message par jour à cette adresse.

Supprimer les réponses automatiques non distribuables (pas de file de relance)

Activez cette option si vous souhaitez supprimer les messages de réponse automatique non distribués lorsqu'ils arrivent à expiration dans la file distante, plutôt que de les placer dans le système de<u>file d'attente de relance.</u>

Modifier le fichier d'autorépondeur par défaut (OutOfOffice.rsp)

Il s'agit du fichier de messages du répondeur automatique par défaut. Le contenu de ce fichier sera copié dans <u>le fichier oof.mrk d'</u> \overline{m} un <u>compte</u> \overline{m} si son fichier est manquant ou vide.

Voir :

Autorépondeurs | Comptes Autorépondeurs | Liste des exceptions de l'Exceptions Création de scripts de réponse automatique Mon compte | Autorépondeurs 777

5.3.3.5 Créer des scripts de réponse automatique

Les fichiers OOF.mrk sont des fichiers texte ASCII contenus dans le dossierracine de chaque utilisateur . Ils définissent les messages renvoyés à la suite d'un autorépondeur. Lorsqu'un message de réponse automatique est déclenché par un répondeur automatique, le fichier est traité et analysé à la recherche de macros, qui seront alors remplacées par les données réelles du message entrants qui a déclenché la réponse. Les lignes commençant par le caractère "#" sont ignorées et servent de commentaires. Deux exemples de messages sont présentés ci-dessous.

Macros de réponse automatique

\$HEADERS\$: DANS L'EN-TÊTE FROM: : LES LIGNES COMMENÇANT PAR LE CARACTÈRE "#" SONT IGNORÉES ET UTILISÉES POUR LES COMMENTAIRES.	Cette macro sera remplacée par tous les en-têtes du message entrants. Le texte précédant immédiatement cette macro sera dupliqué au début de chaque ligne développée.
EN-TÊTE FROM :	Cette macro fait en sorte que la valeur de l'en-
\$HEADER:XX\$ CETTE	tête spécifiée à la place de "xx" soit développée

MACRO EST REMPLACÉE PAR TOUS LES EN- TÊTES DU MESSAGE ENTRANT.	<pre>dans le message. Exemple : Si le message entrant contient "TO : joe@example.com", la macro\$HEADER:TO\$ le remplacera par "joe@example.com". Si le message d'origine contient "OBJET :Ceci est le sujet", la macro\$HEADER:SUBJECT\$ sera remplacée par le texte "Ceci est le sujet".</pre>
\$BODY\$	Cette macro sera remplacée par l'ensemble du corps du message. Dans le but de préserver les jeux de caractères des différentes langues, MDaemon lira le corps du message sous forme de données binaires plutôt que sous forme de texte pur, permettant ainsi une copie octet par octet du corps du message.
\$BODY-AS-TEXT\$ (CORPS DU MESSAGE SOUS FORME DE TEXTE)	Comme la macro\$BODY\$, cette macro sera remplacée par le corps du message entier, mais sous forme de texte plutôt que de données binaires. Le texte précédant immédiatement cette macro sera dupliqué au début de chaque ligne développée. Ainsi, l'utilisation de">>\$BODY-AS- TEXT\$" dans un texte placerait chaque ligne du message original dans le message généré, mais chaque ligne commencerait par ">>". Du texte peut également être ajouté à droite de cette macro.
\$SENDER\$ (EXPÉDITEUR)	Cette macro renvoie à l'adresse complète contenue dans l'en-tête "From :" du message entrant.
BOÎTE AUX LETTRES DE L'EXPÉDITEUR	Cette macro renvoie à la boîte aux lettres de l'expéditeur. La boîte aux lettres est la partie de l'adresse électronique située à gauche du symbole "@".
\$SENDERDOMAIN\$ (DOMAINE DE L'EXPÉDITEUR)	Cette macro renvoie au domaine de l'expéditeur. Il s'agit de la partie de l'adresse électronique située à droite du symbole "@".
\$RECIPIENT\$ (DESTINATAIRE)	Cette macro renvoie à l'adresse complète du destinataire du message.
\$RECIPIENTMAILBOX\$ (BOÎTE AUX LETTRES DU DESTINATAIRE)	Cette macro renvoie à la boîte aux lettres du destinataire du message. La boîte aux lettres est la partie de l'adresse électronique située à gauche du symbole "@".

\$RECIPIENTDOMAIN\$ (DOMAINE DU DESTINATAIRE)	Cette macro renvoie au domaine du destinataire du message. Le domaine est la partie de l'adresse électronique située à droite du symbole "@".
\$SUBJECT	Cette macro renvoie à la valeur de l'en-tête "Subject :".
\$MESSAGEID\$ CETTE MACRO SE RÉFÈRE À LA VALEUR DE L'EN-TÊTE "SUBJECT :".	Cette macro correspond à la valeur de l'en-tête "Message ID".
\$CONTENTTYPE\$ CETTE MACRO SE RÉFÈRE À LA VALEUR DE L'EN-TÊTE "MESSAGE-ID".	Cette macro correspond à la valeur de l'en-tête "Content-Type".
\$PARTBOUNDARY\$ CETTE MACRO SE RÉFÈRE À LA VALEUR DE L'EN-TÊTE "CONTENT-TYPE".	Cette macro correspond à la valeur de l'en-tête MIME "Part-Boundary" dans l'en-tête"Content- Type" pour les messages multipartites.
\$DATESTAMP	Cette macro se développe en une ligne d'horodatage de type RFC-2822.
\$ACTUALTO	Certains messages peuvent contenir un champ"ActualTo" qui représente généralement la boîte aux lettres et l'hôte de destination tels qu'ils ont été saisis par l'utilisateur d'origine avant tout reformatage ou conversion d'alias. Cette macro s'étend à cette valeur.
\$ACTUALFROM\$ (CHAMP DE DESTINATION RÉEL)	Certains messages peuvent contenir un champ"ActualFrom" qui représente généralement la boîte aux lettres et l'hôte d'origine avant tout reformatage ou conversion d'alias. Cette macro se développe en fonction de cette valeur.
\$REPLYTO	Cette macro se résout à la valeur trouvée dans l'en-tête"ReplyTo".
\$PRODUCTID\$ CETTE MACRO SE DÉVELOPPE EN FONCTION DE LA VALEUR TROUVÉE DANS L'EN-TÊTE "REPLYTO".	Cette macro se développe en chaîne d'information sur la version de MDaemon.
\$AR_START	Renvoie la date et l'heure de début du répondeur automatique.

\$AR_END Renvoie la date d'arrêt du répondeur automatique.

Macros de remplacement de l'en-tête From: : Les macros énumérées ci-dessous contrôlent l'en-tête TO :.

Les macros énumérées ci-dessous contrôlent les en-têtes du message de réponse automatique.

%SetSender%

ex : %SetSender%=mailbox@example.com

Pour les besoins du message de réponse automatique, cette macro réinitialise l'expéditeur du message d'origine avant de construire les en-têtes du message de réponse automatique. Ainsi, cette macro contrôle l'en-tête TO du message de réponse automatique. Exemple : si l'expéditeur du message original était"user2@example.org" et que le répondeur automatique du destinataire a utilisé la macro%SetSender% pour le remplacer par "user1@example.com", l' en-têteTO du message de réponse automatique sera alors "user1@example.com".

%SetRecipient%

Exemple : %SetRecipient%=mailbox@example.com

Pour les besoins du message de réponse automatique, cette macro réinitialise le destinataire du message original avant de construire les en-têtes du message de réponse automatique. Ainsi, cette macro contrôle l'en-tête FROM du message de réponse automatique. Exemple : si le destinataire du message d'origine était"michael@example.com" et que le compte de Michael disposait d'un autorépondeur utilisant la macro%setRecipient% pour le remplacer par "michael.mason@example.com",l'en-tête FROM du message d'autoréponse serait défini comme étant "michael.mason@example.com".

%SetReplyTo%

Exemple : %SetReplyTo%=mailbox@example.com Contrôle la valeur de l' en-têteReplyTodu message de réponse automatique .

%SetSubject% (Définir l'objet)

ex : %SetSubject%=Texte de l'objet Remplace la valeur de l'objet dumessage original.

%SetMessageId%

ex : %SetMessageId%=Chaîne ID Modifie la chaîne d'identification du message.

%SetPartBoundary% (Définir la limite de la partie)

ex : %SetPartBoundary%=Chaîne de délimitation Modifie la limite de la partie.

%SetContentType%

ex : %SetContentType%=typeMIME Modifie le type de contenu du message en fonction de la valeur déclarée.

%SetAttachment%

ex : %SetAttachment%=filespec Force MDaemon à joindre le fichier spécifié au message de réponse automatique nouvellement généré. Dans l'application MDaemon, seuls les fichiers spécifiés dans l'écran<u>Attachments</u> mi peuvent être joints aux autorépondeurs.

5.3.3.5.1 Exemples de scripts de réponse automatique

Un simple message de réponse automatique oof.mrk utilisant plusieurs macros de réponse automatique :

Salutations \$SENDER\$ Votre message concernant '\$SUBJECT\$' ne sera pas lu par moi car je suis en vacances. Hourra !!! Je vous prie d'agréer, Madame, Monsieur, l'expression de mes sentiments distingués,

\$RECIPIENT\$

Vous pouvez également utiliser certaines des macros de remplacement d'en-tête pour étendre ce script et contrôler les en-têtes qui seront générés lorsque le message de réponse automatique sera renvoyé à \$SENDER\$:

```
Salutations $SENDER$
Votre message concernant '$SUBJECT$' ne sera pas lu par moi car je
suis en vacances. Hourra !!!
Je vous prie d'agréer, Madame, Monsieur, l'expression de mes
salutations distinguées,
$RECIPIENT$
%SetSubject%=RE : $SUBJECT$
%SetAttachment%=c:\photos\me on vaction.jpg
```

À l'aide de ce script, le message de réponse automatique comportera "RE : " au début de l'objet et le fichier joint spécifié.

La ligne"%SetSubject%=RE : \$SUBJECT\$" est traitée comme suit :

1. La partie^{\$SUBJECT\$} est développée et remplacée par le texte de l'objet du message original. La chaîne est donc équivalente à :

%SetSubject%=RE : Texte de l'objet original

2. MDaemon remplace le sujet original, qu'il a stocké dans ses tampons internes, par le nouveau sujet calculé. Dans ce cas, toute utilisation de "\$SUBJECT\$" dans le script renverra le nouveau résultat.

Notez l'emplacement des nouvelles macros - elles sont énumérées au bas du script de réponse. Cela est nécessaire pour éviter les effets de bord. Exemple : si la macro % SetSubject% était placée avant la macro \$SUBJECT\$, qui apparaît à la deuxième ligne du script de réponse, le texte du sujet aurait déjà été modifié au moment où la macro \$SUBJECT\$ serait développée. Par conséquent, au lieu de remplacer \$SUBJECT\$ par le contenu de l'en-tête "Subject :" du message d'origine, il serait remplacé par la valeur que vous avez attribuée à%SetSubject%.

Voir :

Autorépondeurs | Comptes Autorépondeurs | Liste des exceptions de l'autorépondeur Autorépondeurs | Paramètres | Autorépondeurs Mon compte | Répondeurs automatiques 777

5.3.4 Autres

5.3.4.1 Base de données des comptes

🧐 Paramètres de compte Base de donnée	: des comptes 🧮	3
 Paramètres de compte Base de donnée Active Directory Alias Autorépondeurs Autres Mots de passe Quotas Minger 	 tes comptes Type de base de données Stocker les données des comptes dans le fichier USERLIST.DAT USERLIST.DAT est le fichier de stockage standard des données de compte dans MDaemon. Il ne requiert aucune configuration spéciale. La plupart des données de compte sont enregistrées dans un seul fichier stocké en mémoire pour plus de rapidité. Stocker les données des comptes dans un annuaire LDAP Configurer Les serveurs LDAP sont souvent utilisés pour le stockage de données. Ils répondent plus rapidement aux requêtes mais ils sont plus lents en termes de mise à jour ou d'insertion de données. Stocker les données des comptes dans une base ODBC Les outils des bases de données ODBC simplifient l'ajout, la modification ou la suppression des données des comptes. 	
	OK Annuler Appliquer Aide]

La boîte de dialogue Base de données des comptes (située sous Comptes | Paramètres des comptes) permet de définir la méthode que MDaemon doit utiliser pour gérer les comptes utilisateurs : ODBC, LDAP ou le système local USERLIST.DAT.

Type de base de données des comptes

Stocker les données de compte dans le fichier disque USERLIST.DAT

Choisissez cette option si vous souhaitez que MDaemon utilise son fichierinterne USERLIST.DAT comme base de données des comptes.Il s'agit duparamètre par défaut de MD aemon. Toutes les informations des comptes utilisateurs de MDaemon sont stockées localement. La plupart des informations sont stockées dans un seul fichier, qui est résident en mémoire afin d'augmenter l'efficacité et la vitesse.

Stocker les données des comptes dans un annuaire LDAP accessible

Choisissez cette option si vous souhaitez que MDaemon utilise votre serveur LDAP comme base de données des utilisateurs de MDaemon plutôt qu'ODBC ou son systèmelocal USERLIST.DAT. Vous pouvez utiliser cette méthode pour gérer les données de vos comptes utilisateurs si vous avez plusieurs serveurs MDaemon à différents endroits mais que vous souhaitez qu'ils partagent une seule base de données utilisateurs. Chaque serveur MDaemon sera configuré pour se connecter au même serveur LDAP afin de partager les informations sur les utilisateurs plutôt que de les stocker localement. Les serveurs LDAP répondent généralement de manière rapide et efficace aux requêtes, mais sont plus lents à mettre à jour ou à insérer de nouvelles données.

Configurer

Lorsque l'option Mon compte LDAP est sélectionnée, cliquez sur ce bouton pour ouvrir l'<u>écran LDAP</u> and afin de configurer les paramètres de votre serveur LDAP.

Stocker les données de compte dans un magasin accessible par ODBC

Choisissez cette option si vous souhaitez utiliser une base de données compatible ODBC comme base de données des comptes MDaemon.

Configurer

Lorsque l'option Données de compte ODBC est sélectionnée, cliquez sur ce bouton pour ouvrir l'<u>Assistant sélecteur ODBC</u> pour sélectionner et configurer votre base de données compatible ODBC.

5.3.4.1.1 Assistant de sélection ODBC

Utilisez l'assistant de sélection ODBC pour sélectionner ou configurer une source de données compatible ODBC à utiliser comme base de données de comptes MDaemon.

Migration de votre base de données de comptes vers un magasin accessible par ODBC

 Dans la boîte de dialogue Base de données des comptes (Comptes | Paramètres des comptes | Base de données des comptes), cliquez sur Stocker les données des comptes dans une base de données accessible par ODBC, puis sur Configurer pour ouvrir l'assistant de sélection ODBC.

ODBC Selector Wiz	zard	×
	First, select a data source. MS Access Database Excel Files dBASE Files My Data Source	
	Some data sources require a logon and password. Logon Password <back next=""> Cancel</back>]

- Sélectionnez la source de données que vous souhaitez utiliser pour votre base de données de compte. Si aucune source de données compatible n'est répertoriée, cliquez sur New DSN (Nouveau DSN), puis suivez les instructions indiquées sous <u>Creating a New ODBC Data Source (Création d'une nouvelle source de</u> <u>données ODBC)</u>
- 3. Si nécessaire, entrez le Logon et le Mot de passe de la source de données.
- 4. Cliquez sur Next (Suivant).
- Si la source de données contient déjà les tables requises par AM, passez à l'étape
 Sinon, cliquez sur Exécuter un script pour créer les tables nécessaires...

ODBC Selector Wiz	zar d		×
	Data source name:	My Data Source	
	This data source cont	ains the following tables:	
	Contacts MDaemon has detect present.	ed that the required tables are not	
	Run a script to	o create the necessary tables	
	< Ba	ck Finish Cancel	

6. Utilisez le Chemin du fichier (ou Parcourez) vers le fichier script que vous souhaitez utiliser pour créer les tables pour votre application de base de données. Le dossier\MDaemon\app contient des scripts pour plusieurs des applications de base de données les plus populaires.

Create Database Tables	
Select a script to create the database tables.	
C:\MDaemon\App\AccountsDB-Access.sql	Browse
Click the 'Create database tables' to run the script and crea tables MDaemon needs in order to use the DSN you have :	te the selected.
Run script and create database tables now	Close

- 7. Cliquez sur **Exécuter le script et créer les tables de la base de données** maintenant, cliquez sur **OK**, puis sur **Fermer**.
- 8. Cliquez sur **Terminer**, puis sur **OK** pour fermer la boîte de dialogue Base de données des comptes.
- Unoutil de migration de base de données va migrer tous vos comptes utilisateurs vers la source de données ODBC, puis fermer MDaemon. Cliquez sur OK, puis redémarrez MDaemon en cours et commencez à utiliser la nouvelle base de données de comptes ODBC.

Voir :

Base de données des comptes 908 Création d'une nouvelle source de données ODBC 912

5.3.4.1.1.1 Créer une source de données

Pour créer une nouvelle source de données ODBC :

- Dans la boîte de dialogue Base de données des comptes (Comptes | Paramètres des comptes | Base de données des comptes), cliquez sur Stocker les données de compte dans un magasin accessible par ODBC, puis sur Configurer pour ouvrir l'assistant de sélection ODBC.
- 2. Cliquez sur **New DSN** pour ouvrir la boîte de dialogue Select Data Source.

ODBC Selector Wiz	ard	×
	First, select a data source. MS Access Database Excel Files dBASE Files My Data Source Some data sources require a logon and password. Logon Password	
	< Back Next > Cancel	

3. Passez à l'onglet **Machine Data Source**, puis cliquez sur **New...** pour ouvrir la boîte de dialogue Create New Data Source (Créer une nouvelle source de données).

Sele	ct Data Source			? 🗙
File	Data Source Machine Data	Source		
	Data Source Name dBASE Files Excel Files MS Access Database WebAdmin	Type User User User System	Description WebAdmin Database	
				New
	A Machine Data Source is spe "User" data sources are speci sources can be used by all use	cific to this fic to a use ers on this	s machine, and cannot be share er on this machine. "System" da machine, or by a system-wide se	d. ta rvice.
			OK Cancel	Help

4. Sélectionnez System Data Source (Source de données système) et cliquez sur Next (Suivant).



5. Sélectionnez le **pilote debase de données** pour lequel vous souhaitez configurer la source de données, puis cliquez sur **Next (Suivant)**.

Select a driver for which you want to set up a data so Name Driver da Microsoft para arquivos texto (*.txt; *.csv) Driver do Microsoft Access (*.mdb) Driver do Microsoft Base (*.dbf) Driver do Microsoft Excel(*.xls) Driver do Microsoft Paradox (*.db) Driver do Microsoft Visual FoxPro Microsoft Access Driver (*.mdb) Microsoft Access-Treiber (*.mdb) Microsoft dBase Driver (*.dbf) Microsoft dBase Driver (*.dbf)	burce.
A Back Nevts Ca	incel

 Cliquez sur Finish pour afficher la boîte de dialogue de configuration spécifique au pilote. L'apparence de cette boîte de dialogue varie en fonction du pilote que vous avez sélectionné (boîte de dialogue de configuration de Microsoft Access illustrée ci-dessous).

ODBC Microsoft Access Setup		? 🔀
Data Source Name:	MDaemon Accounts	ОК
Description:	MDaemon Accounts Data Source	Cancel
– Database Database:		Help
Select	Create Repair Compact	Advanced
- System Database -		
• None		
🔿 Database:		
	System Database	Options>>

- Désignez un nom de source de données pour votre nouvelle source de données et fournissez toute autre information requise par la boîte de dialogue spécifique au pilote (comme la création ou la spécification d'une base de données, le choix d'un répertoire ou d'un serveur, etc.)
- 8. Cliquez sur **OK** pour fermer la boîte de dialogue spécifique au pilote.
- 9. Cliquez sur **OK** pour fermer la boîte de dialogue Select Data Source.

Voir : Mon compte

Assistant de sélection ODBC - Base de données des comptes 📟

5.3.4.2 Mots de passe

Active Directory Aliases Autoresponders Cother Account Database Passwords Units Minger	Strong Passwords ✓ Require strong passwords Strong passwords must meet length and complexity requirements and not be found in the bad passwords file. See Help for details. Minimum password length (at least 8 characters) 10 ✓ Password must contain a special character Edit the bad password file Force weak passwords to change
	Password Settings Passwords expire after this many days 0 (0 = passwords never expire) Warn users of password expiration each day for 5 days (0 = never) Be careful using these options. If a user's password expires they will not be able to check or send mail until the password is changed, which may not be easy for them to do. Accounts setup for AD authentication are not subject to password expiration. Remember this many old passwords 0 (0 = none) Store mailbox passwords using non-reversible encryption Not compatible with APOP or CRAM-MD5 authentication or other features that depend on MD aemon being able to decrypt passwords. Do not allow passwords found in third-party compromised passwords list Check for compromised password at login and send warning email every Enable app passwords 0 days (0 = never) Penable app passwords 0 days (0 = never)

Mots de passe sécurisés

Demander des mots de passe forts

Par défaut, MDaemon demande des mots de passe forts lors de la création de nouveaux comptes ou de la modification de mots de passe existants. Décochez cette case si vous souhaitez désactiver l'exigence de mots de passe forts.

Les mots passe forts doivent :

- Respecter une longueur minimum.
- Contenir des majuscules et des minuscules.

- Contenir des lettres et des chiffres.
- Contenir un caractère spécial (si l'option de caractère spécial est définie cidessous).
- Ne pas contenir le nom complet de l'utilisateur ou le nom de la boîte aux lettres.
- Ne pas être enregistré dans la liste des mots passe incorrects.

Longueur minimum du mot de passe (au moins 8 caractères)

Cette option permet de définir la longueur minimale demandée aux mots passe forts. Cette valeur doit être d'au moins 8 caractères, mais une valeur plus élevée est recommandée. La valeur par défaut pour les nouvelles installations de MDaemon est de 10 caractères. Modifier ce paramètre ne déclenche pas automatiquement un changement de mot de passe pour les comptes dont le mot de passe est plus court que le nouveau minimum, mais lors du prochain changement de mot de passe de ces utilisateurs, ce paramètre sera appliqué.

> Indépendamment du paramètre minimal, les mots de passe peuvent comporter plus de 72 caractères lorsque l'option"*Stocker les mots de passe des boîtes aux lettres en utilisant un chiffrement unrement unique*" ci-dessous est activée. Si cette option est désactivée, les mots de passe ne peuvent pas dépasser 15 caractères.

Les mots passe doivent contenir un caractère spécial.

Par défaut pour les nouvelles installations de MDaemon, les mots de passe forts requièrent également au moins un des caractères spéciaux suivants : !"#\$%&'()*+,-./:;<=>?@[\]^_`{|}~. Désactivez cette option si vous ne souhaitez pas demander un caractère spécial dans les mots passe forts.

Modifier le fichier des mots de passe incorrects

Cliquez sur ce bouton pour modifier le fichier des mots de passe incorrects. Les entrées répertoriées dans ce fichier sont insensibles à la casse et ne peuvent pas être utilisées comme mots de passe. Si vous souhaitez créer des entrées plus complexes ou polyvalentes, vous pouvez utiliser des <u>expressions régulières</u> ⁷⁰³. Les entrées commençant par " !" sont traitées comme des expressions régulières.

Forcer la modification des mots de passe faibles

Cliquez sur ce bouton si vous souhaitez forcer tous les comptes dont le mot de passe est faible à modifier leur mot de passe. Tous les comptes dont le mot de passe est faible seront bloqués jusqu'à ce que le mot de passe soit modifié. Le mot de passe peut être modifié par un administrateur via l'interface MDaemon, ou un utilisateur bloqué peut modifier le mot de passe via Webmail ou l'interface d'administration à distance. Dans le cas où l'utilisateur tente de se connecter en utilisant l'ancien mot de passe, il lui sera demandé d'en créer un nouveau avant de continuer. **Remarque :** Cette option n'est pas disponible lorsque vous utilisez l'option "*Stocker les mots passe boîtes aux lettres en utilisant un chiffrement non réversible*" ci-dessous.

Rapport de mots de passe peu sécurisés

Cliquez sur ce bouton pour générer un rapport de tous les comptes MDaemon dont le mot de passe est faible. Le rapport sera envoyé à l'adresse électronique que vous aurez spécifiée après avoir cliqué sur OK. **Remarque :** Cette option n'est pas disponible si vous utilisez l'option "*Stocker les mots passe boîtes aux lettres en utilisant un chiffrement non réversible*" ci-dessous.

Paramètres de passe

Les mots de passe expirent après cebre jours (0=mots de passe n'expirent jamais) Utilisez cette option si vous souhaitez définir un nombre maximal de jours pendant lesquels un compte est accessible avant qu'il ne soit nécessaire de modifier son mot passe. La valeur par défaut de cette option est "0", ce qui signifie que les mots de passe n'expirent jamais. Mais si vous la fixez à 30 jours, par exemple, l'utilisateur disposera de 30 jours pour modifier son mot de passe, à compter de la dernière modification du mot de passe du compte. Par conséquent, lorsque vous définissez initialement une valeur d'expiration, tout compte dont le mot de passe n'a pas été modifié dans le nombre de jours spécifié aura immédiatement un mot de passe expiré. Lorsque le mot de passe d'un utilisateur expire, celui-ci ne pourra pas accéder aux services POP, IMAP, SMTP, Webmail ou MDaemon Remote Admin. L'utilisateur peut toutefois encore se connecter à Webmail ou au MDaemon Remote Admin, où il lui sera alors demandé de changer son mot de passe avant de continuer. Les clients de messagerie tels que Outlook, Thunderbird et autres ne peuvent pas être utilisés pour modifier le mot passe. En outre, de nombreux clients n'affichent même pas de message d'erreur utile aux utilisateurs, qui peuvent donc avoir besoin de l'aide de l'administrateur pour comprendre pourquoi leur connexion échoue.

> Pour que les utilisateurs puissent modifier leur mot de passe via le Webemon ou le MDaemon Remote Admin, ils doivent d'abord obtenir l'autorisation d'accès web "...modifier le mot de passe" sur l'écran des Services Web. En outre, comme il peut être difficile ou impossible pour certains utilisateurs de modifier leur mot de passe, il convient de faire preuve de prudence avant d'utiliser cette option.

Avertir les utilisateurs de l'expiration du mot passe chaque jour pendant [xx] jours (0 = jamais)

Les comptes dont le mot de passe est sur le point d'expirer peuvent recevoir chaque jour un courriel de rappel indiquant que le mot de passe doit être modifié. Utilisez cette option pour indiquer le nombre de jours avant l'expiration du mot de passe pendant lesquels MDaemon doit commencer à envoyer ces e-mails quotidiens.

Retenir cebre anciens mots passe (0 = aucune)

Utilisez cette option pour indiquer le nombre d'anciens mots de passe que vous souhaitez que MDaemon retienne pour chaque utilisateur. Lorsque les utilisateurs modifient leur mot de passe, ils ne sont pas autorisés à réutiliser les anciens mots de passe. Cette option a la valeur "0" (désactivé) par défaut. Stocker les mots de passe de boîtes aux lettres en utilisant un chiffrement à sens unique Cochez cette case si vous souhaitez que MDaemon stocke les mots de passe à l'aide d'un cryptage non réversible. Cela permet d'éviter que les mots de passe soient décryptés par MDaemon, l'administrateur ou un éventuel pirate. Pour ce faire, MDaemon utilise la fonction de hachage de mots de passe <u>***</u>, qui permet d'utiliser des mots de passe plus longs (jusqu'à 72 caractères) et de conserver les mots de passe sans les révéler lors de l'exportation et de l'importation de comptes. Certaines fonctionnalités ne sont toutefois pas compatibles avec cette option, comme la détection des mots de passe peu sécurisés et l' authentification<u>APOP & CRAM-</u> <u>MD5</u>[90[†]], car elles dépendent de la capacité de MDaemon à décrypter les mots de passe. L'option Mots de passe non réversibles est activée par défaut.

Mots de passe compromis

MDaemon peut comparer le mot de passe d'un utilisateur à une liste de mots de passe compromis provenant d'un service tiers. Si le mot de passe d'un utilisateur figure dans la liste, cela ne signifie pas que le compte a été piraté. Cela signifie que quelqu'un, quelque part, a utilisé les mêmes caractères que son mot de passe et que celui-ci est apparu dans une violation de données. Les mots de passe publiés peuvent être utilisés par des pirates dans des attaques par dictionnaire, mais les mots de passe uniques qui n'ont jamais été utilisés ailleurs sont plus sûrs. Pour plus d'informations, voir <u>Pwned Passwords (Mots de passe publiés</u>).

Ne pas autoriser les mots de passe trouvés dans la liste des mots passe compromis tierce partie

Cochez cette case si vous ne souhaitez pas que le mot de passe d'un compte soit défini sur un mot de passe figurant dans la liste des mots de passe compromis.

Vérifier la présence d'un mot de passe compromis lors de la connexion et envoyer un email d'alerte à tous les [xx] jours (0 = jamais)

Dans cette option, vous pouvez vérifier automatiquement le mot de passe de chaque utilisateur par rapport à la liste des mots de passe compromis une fois tous les jours spécifiés, lorsque chaque utilisateur se connecte. S'il s'avère qu'il utilise un mot de passe compromis, un e-mail de notification est envoyé au compte et au postmaster. Les messages d'alerte peuvent être personnalisés en modifiant les fichiers de modèles de messages dans le dossier Destinataire des messages d'alerte. Dans la mesure où les instructions relatives à la manière dont un utilisateur doit modifier son mot de passe peuvent varier selon que le compte utilise un mot de passe stocké dans MDaemon ou qu'il utilise l' authentification <u>Active Directory</u>, il existe deux fichiers modèles : CompromisedPasswordMD.dat et CompromisedPasswordAD.dat. Des macros peuvent être utilisées pour personnaliser le message, modifier l'objet, changer les destinataires, etc.

Mots de passe d'application

Mots passe d'application at une option qui peut être utilisée pour rendre les comptes plus sécurisés en créant des mots de passe très forts, générés de manière aléatoire, à utiliser uniquement dans les clients de messagerie et les apps de messagerie, puisque ces apps ne peuvent pas être sécurisées par l'<u>Authentification à deux facteurs</u> [771] (2FA). Voir : <u>Mots de passe d'application</u> [804].

Activer les mots passe d'application

Tous les utilisateurs peuvent créer des Mots de passe d'application pour leurs comptes par défaut, lorsqu'ils sont connectés au Webmail à l'aide de l'Authentification à deux facteurs. Si vous souhaitez désactiver la prise en charge des Mots mots passe d'application pour un utilisateur spécifique, vous pouvez le faire avec l' option...modifier les mots passe d'application mil sur la page Services Web de l'utilisateur.

Exiger l'authentification en deux étapes pour configurer les mots de passe d'application

Par défaut, les utilisateurs doivent être connectés au Webmail à l'aide de l'Application d <u>'authentification à deux facteurs</u> [771] (2FA) pour pouvoir créer un nouveau mot de passe d'appli. Il n'est pas recommandé de désactiver cette exigence. <u>Les Administrateurs globaux</u> [812] sont exemptés de cette exigence dans MDaemon Webmail, mais il est tout de même recommandé qu'ils utilisent toujours l'authentification à deux facteurs lorsqu'ils se connectent à MDaemon Webmail ou à MDaemon Webmail.

Supprimer les mots de passe d'application lorsque le mot de passe du compte est modifié

Par défaut, lorsque le mot de passe d'un compte est modifié, tous les mots de passe des applications seront supprimés, obligeant l'utilisateur à en créer de nouveaux s'il souhaite les utiliser ou s'il est requis de le faire par le paramètre"*Demander mots passe...*" (voir note ci-dessous).

Il existe une option de compte sur la page<u>Paramètres de</u> <u>l'éditeur de compte</u> at que vous pouvez utiliser pour "*Exiger un mot de passe d'appli pour se connecter à SMTP, IMAP, ActiveSync, etc.*"

Demander des Mots passe d'application peut aider à protéger le mot de passe d'un compte contre les attaques par dictionnaire et par force brute via SMTP, IMAP, etc. Cette solution est plus sûre car même si une attaque de ce type permettait de deviner le mot de passe réel d'un compte, elle ne fonctionnerait pas et l'attaquant n'en saurait rien, car MDaemon n'accepterait qu'un Mot passe Mon compte correct. De plus, si vos comptes dans MDaemon utilisent l' authentification<u>Active Directory</u> and et que Active Directory verrouille un compte après un certain nombre de tentatives échouées, cette option permet d'éviter le verrouillage des comptes, car MDaemon ne vérifiera que les Mots passe d'application, et n'essaiera pas de s'authentifier auprès d'Active Directory.

Voir aussi :

Éditeur de comptes | Informations générales sur les comptes Mon compte | Services web Mon compte | Mots de passe d'application Expression régulière 703

5.3.4.3 Quotas

Account Settings - Quotas	
Active Directory Aliases Autoresponders Other Account Database Passwords Quotas Minger	Quota Settings Include all email folders in quota calculation (needed for IMAP users) Include calendar, contacts, tasks, documents, folders as well Refuse incoming messages sent to over quota accounts Refuse outgoing messages sent from over quota accounts SMTP server sends 552 when account is over quota (otherwise sends 452) Recalculate all quota values once per day
	Quota Report and Warnings
	Inactive Accounts Disable accounts after this many inactive days (0 = never) Exempt list
	Ok Cancel Apply Help

Paramètres de quotas

Inclure tous les dossiers de courrier dans le calcul des quotas (requis pour les utilisateurs IMAP)

Lorsque cette case est cochée, tous les fichiers de messages de tous les dossiers de messagerie ducompte d'un utilisateur sontpris en compte dans les limitations de taille ou de nombre de messages imposées à ce compte. Dans le cas contraire, seuls les fichiers de messages de la boîte de réception seront pris en compte dans ces limitations. Cette fonction n'est généralement nécessaire que pour les utilisateurs IMAP.

...inclure les dossiers Calendrier, Contacts, Tâches, Documents et Documents également

Cochez cette case si vous souhaitez inclure tous les dossiers Calendrier, Contacts, Tâches et Documents dans le calcul des quotas.

Refuser les messages destinés à des comptes ayant dépassé leur quota

Par défaut, lorsqu'un compte est soumis à une restriction de quota de messages et que le quota est atteint, MDaemon n'accepte plus de messages entrants pour ce compte jusqu'à ce que le titulaire du compte supprime certains de ses messages stockés. Décochez cette case si vous ne souhaitez pas refuser les messages entrants pour les comptes dont le quota est dépassé.

Refuser les messages envoyés par des comptes ayant dépassé leur quota

Cochez cette case si vous souhaitez refuser les messages sortants envoyés à partir d'un compte ayant atteint son quota. Un compte ayant dépassé son quota ne pourra plus envoyer de courrier tant que certains de ses messages stockés n'auront pas été supprimés. Cette option est désactivée par défaut.

Le serveur SMTP envoie un code 552 lorsqu'un compte a dépassé son quota (452 par défaut)

Non (par défaut), MDaemon envoie le code d'erreur 452 (i.e. "Requested action not taken : insufficient system storage") pendant le processus SMTPlorsqu'un compte dépasse le <u>quota</u> (74). Ce code signifie généralement que le serveur doit réessayer plus tard. Cochez cette case si vous souhaitez envoyer le code d'erreur 552 ("Requested mail action aborted : exceeded storage allocation").

Recalculer les valeurs des quotas une fois par jour

Par défaut, les valeurs de quota mises en cache ne sont réinitialisées que lorsque l'option "*Envoyer un rapport de quota quotidien…*" ci-dessous est activée et envoyée. Cochez cette case si vous souhaitez au contraire que les valeurs de quota soient recalculées dans le cadre de la routine de maintenance quotidienne.

Rapports de quotas et avertissements

Envoyer un avertissement à l'utilisateur lorsque ce pourcentage de quota est atteint Si, au cours de la <u>maintenance et du nettoyage quotidiens</u> [525], MDaemon détermine qu'un compte dépasse ce pourcentage du *Nombre maximal de messages stockés à la fois* ou de l'*Espace disque maximal autorisé* indiqué dans l'Éditeur de compte [784], un message d'avertissement sera envoyé à ce compte. Utilisez l' option *Texte l'objet* (proche du quota) ci-dessous pour définir l'objet du message. Le message indiquera le nombre actuel de messages stockés par le compte, la taille de sa boîte aux lettres, ainsi que le pourcentage utilisé et le pourcentage restant. Dans le cas où un message d'alerte existant se trouve dans la boîte aux lettres du compte, il sera remplacé par un message actualisé. Chaque fois qu'un nouveau message d'alerte est placé dans la boîte aux lettres de l'utilisateur, une entrée est créée dans le journal du système pour signaler que cela a été fait. Aucune entrée du journal n'est créée lorsque le message existe déjà et qu'il est simplement mis à jour. Si une entrée du journal est ajoutée à plusieurs reprises, cela indique que l'utilisateur supprime le message de sa boîte de réception. Désactivez cette option si vous ne souhaitez pas envoyer le message d'avertissement sur les quotas aux utilisateurs.

> Le modèle de message Near Quota (situé à l'adresse : MDaemonapp\NearQuota.dat) est utilisé pour créer le message d'alerte Near Quota. Tous les Modèles de comptes utilisateurs (par exemple \$EMAIL\$, \$MAILBOX\$, \$DOMAIN\$, etc.) peuvent être utilisés dans le modèle.

Texte de l'objet (proche du quota)

Ce texte est l'Objet du message d'avertissement envoyé à tous les utilisateurs qui dépassent le pourcentage de quota indiqué ci-dessus. Ces messages sont envoyés chaque jour lors de l'événement de maintenance et de nettoyage quotidien, qui a lieu à minuit par défaut.

Texte de l'objet (hors quota)

Tout comme le message d'alerte "near quota", un autre message est envoyé lorsque le compte d'un utilisateur dépasse le quota. Ce texte est l'Objet du message d'alerte "hors quota".

Envoyer un rapport quotidien sur les quotas aux administrateurs globaux et de domaine Cochez cette case et indiquez une valeur si vous souhaitez envoyer un rapport quotidien sur les quotas à tous les Administrateurs globaux et de domaine. Le rapport contiendra des Statistiques de quota pour tous les utilisateurs ayant atteint ou dépassé le pourcentage désigné de leur restriction de quota. Utilisez "0" comme valeur si vous souhaitez que le rapport contienne des statistiques sur les quotas de tous les utilisateurs.

Ne pas inclure les comptes figés ou désactivés

Par défaut, les rapports sur les quotas n'incluent pas les comptes désactivés ou figés. Décochez cette case si vous souhaitez les inclure.

Texte de l'objet (rapport quotidien)

Utilisez cette option si vous souhaitez personnaliser le texte de l'objet du rapport quotidien sur les quotas que MDaemon envoie aux administrateurs. Si vous souhaitez personnaliser le rapport lui-même, consultez QuotaReport.dat dans le dossierMDaemon\APP.

Comptes inactifs

Désactiver les comptes après ces jours d'inactivité [xx] (0 = jamais)

Utilisez cette option si vous souhaitez désactiver automatiquement les comptes inactifs depuis plus d'un certain nombre de jours. Lorsque le nombre maximal de jours d'inactivité est atteint, le compte est désactivé et un e-mail est envoyé au postmaster. Ce compte est ACTIVÉ en répondant à l'e-mail. Le traitement est effectué dans le cadre du nettoyage de minuit chaque nuit. La valeur par défaut est 0 (désactivé).

Liste des exceptions

Les comptes ajoutés à cette liste de sont exemptés de la fonction de désactivation des comptes inactifs.

Voir :

 Mon compte | Quotas

 Gestionnaire de modèles | Quotas

 870

5.3.4.4 Minger

🧐 Paramètres de compte Minger	
Active Directory Alias Autorépondeurs Autorépondeurs Autres Base de données des comptes Mots de passe Quotas Minger	Avec Minger, les autres serveurs peuvent envoyer des requêtes au votre afin de déterminer si une adresse est active, désactivée ou inconnue. Activer le serveur Minger Écouter les connexions Minger sur ce port UDP 4069 Exiger un mot de passe Il doit s'agir d'une chaîne comportant au moins 16 caractères. Les serveur Minger accepte les requêtes anonymes Il est possible d'autoriser les requêtes anonymes mais dans ce cas n'importe qui peut obtenir le statut d'une adresse e-mail. En effet, Minger indique le statut des adresses e-mail (actives, désactivées ou inconnues). Minger considère les résultats des vérifications Minger
	OK Annuler Appliquer Aide

Situé sous Comptes | Paramètres des comptes, Minger est un protocole de vérification des adresses électroniques créé par MDaemon Technologies. Basé à l'origine sur le protocole Finger, Minger est principalement destiné à fournir un mécanisme simple et efficace pour permettre à d'autres personnes d'interroger votre serveur afin de vérifier si une adresse électronique est valide ou non. Pour des raisons d'efficacité, Minger utilise UDP plutôt que TCP, et pour des raisons de sécurité, il peut requérir une authentification, bien qu'il prenne également en charge les requêtes anonymes. La boîte de dialogue Activer les requêtes Minger permet d'activer ou de désactiver le serveur Minger de MDaemon, de désigner le port qu'il utilisera (4069 par défaut) et de choisir de requérir une authentification via un système de secret partagé ou d'autoriser les requêtes anonymes.

MDaemon dispose également d'un client Minger, qui est intégré au système Domain Gateways (voir <u>Vérification</u> 270). Chaque domaine pour lequel MDaemon joue le rôle de passerelle ou de serveur de secours peut être configuré pour utiliser Minger afin que MDaemon se connecte au serveur distant et vérifie si les destinataires des messages entrants pour ce domaine sont valides ou non. Cela vous évite de devoir supposer que tous les destinataires sont des adresses valides.

Vous trouverez la dernière version du protocole Minger à l'adresse suivante

http://tools.ietf.org/html/draft-hathcock-minger-06

Serveur Minger

Activer le serveur Minger

Cochez cette case pour activer le serveur Minger de MDaemon.

Écouter les connexions Minger sur le port UDP

Il s'agit du port sur lequel le serveur Minger écoutera les connexions. L' IANA (<u>Internet Assigned Numbers Authority</u>) a réservé et attribué le port TCP et UDP 4069 pour utiliser les clients et les serveurs Minger. Il n'est pas recommandé de modifier ce port, car il a été réservé exclusivement à l'utilisation Minger.

Exiger un mot de passe

Si vous souhaitez que l'authentification soit requise via un système de secret partagé, choisissez cette option et saisissez une chaîne de texte d'au moins 16 caractères. Lorsque cette option est choisie, le serveur Minger refusera les requêtes non authentifiées.

Le serveur Minger accepte les requêtes anonymes

Choisissez cette option si vous souhaitez prendre en charge les requêtes Minger anonymes : le client connecté n'est pas tenu de s'authentifier avant d'effectuer des requêtes de vérification d'adresse. Ceci est similaire à ce qui peut être accompli par les sources utilisant la commandeSMTP VRFY ou SMTP "call back" ou "call forward", mais c'est beaucoup plus efficace et n'entraîne pas de nombreuses sessions SMTP abandonnées sur TCP, des journaux SMTP encombrés de sessions abandonnées, et d'autres problèmes similaires inhérents à ces méthodes.

Minger considère les alias inconnus comme des adresses actives

Si cette case est cochée, Minger traitera les alias étrangers (alias qui pointent vers des adresses externes) comme si c'étaient des adresses connues actives. De plus, ce comportement est forcé lorsqu'une requête provient de <u>SecurityGateway</u> vers MDaemon, quel que soit le réglage de cette option.

Mettre les résultats des vérifications Minger en cache

Par défaut, MDaemon met les résultats des vérifications Minger en cache. Si vous ne souhaitez pas les mettre en cache, désactivez cette option.

5.4 Importation de comptes

1

5.4.1 Importer des comptes depuis un fichier texte

Cliquez sur le menu Comptes | Importer... | Importer des comptes à partir d'un fichier texte délimité par des virgules... pour accéder à cette fonction de génération de comptes. Vous pouvez également y accéder en cliquant sur le bouton *Importer* dans le Gestionnaire des comptes. Il s'agit d'une méthode simple pour importer et générer automatiquement des comptes de messagerie. MDaemon lira un fichier texte et générera de nouveaux comptes de messagerie en utilisant simplement le Prénom et le Nom de l'utilisateur. Si vous prenez soin de configurer correctement les chaînes de vos Modèles de comptes (voir Modèle des Nouveaux Comptes [848]), vous pouvez générer des comptes uniques en utilisant uniquement le Prénom et le Nom, mais vous pouvez également inclure de nombreuses autres options pour les paramètres spécifiques de l'utilisateur si vous souhaitez outrepasser les nouveaux comptes par défaut. Tous les champs doivent être séparés par des virgules.

Chaque ligne du fichier texte délimité par des virgules ne doit contenir qu'une seule entrée d'utilisateur. La première ligne doit être une ligne de base indiquant les noms et l'ordre des champs dans les lignes suivantes. Un exemple de fichier ressemblerait à ceci

```
"Mailbox", "FullName", "MailDir", "AllowAccess"
"arvel", "Arvel Hathcock", "C:\Mail\Arvel", Y
"michael", "Michael Mason", "C:\Mail\Michael\", N
```



Utilisez les valeurs suivantes dans la ligne de base pour établir une correspondance avec les champs du compte MDaemon :

Nom du champ À :	Type de champ
MailBox	chaîne
Domaine	chaîne
Nom complet	chaîne
MailDir	chaîne
Mot de passe	chaîne
AutoDecode	bool
IsForwarding	bool
AllowAccess	bool
AllowChangeViaEmail	bool
KeepForwardedMail	bool
HideFromEveryone	bool
EncryptMail	bool
ApplyQuotas	bool
ActiverMultiPOP	bool
MaxMessageCount	int
MaxDiskSpace	int
FwdAddress	chaîne
FwdHost	chaîne
FwdSendAs	chaîne
FwdPort	chaîne
NTAccount	chaîne
MailFormat	chaîne
AutoRespScript	chaîne
AutoRespProcess	chaîne
AddToList	chaîne
RemoveFromList	chaîne
PassMessageToProcess	bool
MaxUIDLCount	int
MaxMessageSize	int
RecurseIMAP	bool

MaxInactive	int
MaxMessageAge	int
MaxDeletedIMAPMessageAge	int
Commentaires	chaîne de caractèr es
Défini par l'utilisateur	chaîne de caractèr es

Voir :

Comptes intégrés de Windows

5.4.2 Intégration de comptes Windows

MDaemon prend en charge l'intégration des comptes Windows. Ce support consiste en un moteur d'importation SAM/Active Directory, accessible depuis le menu Comptes de MDaemon (Comptes | Importer... | Importer des comptes depuis SAM/Active directory...). En outre, MDaemon prend en charge les éléments suivants Active Directory (AD) des utilisateurs est intégrée au code de gestion des utilisateurs de MDaemon. Il est possible de spécifier un domaine Windows dans le champ "Domaine" d'un compte, puis MDaemon authentifiera dynamiquement ces comptes en temps réel, en utilisant le système de sécurité du domaine Windows spécifié. Dans un tel schéma, le fait de modifier le mot de passe du compte dans la gestion des utilisateurs Windows mettra automatiquement à jour MDaemon. Par conséquent, vos utilisateurs n'auront à se souvenir que d'un seul jeu d'identifiants d'authentification. Cela facilite également la création de nouveaux comptes pour les nouvelles installations.



👲 SAM	I/Active Directory Account Importer
Domain	8
	PDC/BDC machine name
mary	Windows domain name EXAMPLECOM
	MDaemon domain name example.com
Accoun	its
6	Windows accounts Selected accounts
<u> 1</u>	Administrator >>
	LabManager Australia
	>>
Options	
50	✓ Make account mailboxes equal to the SAM/AD account name
l les	
0.454	Windows will not release account passwords to MDaemon. Please select the method MDaemon will use to create or authenticate
	account passwords.
	Use the account templates to generate passwords
	C Set account passwords equal to account names
	Make every password equal to
	C Authenticate passwords dynamically using SAM/AD
	Authenticate on this Windows domain
	Addienceare on this windows domain
	Import Selected Accounts

Importateur de comptes SAM/Active Directory

Domaines

PDC/BDC Nom de la machine

Ce champ vous permet de spécifier le nom de la machine à partir de laquelle MDaemon lira les informations de la base de données des comptes Windows. Vous pouvez spécifier Non (par défaut) et MDaemon lira les données de la machine locale.

Actualiser

Cliquez sur ce bouton pour actualiser la liste des comptes Windows.

Nom de domaine Windows

Nom et type du domaine Windows à partir duquel vous souhaitez importer des comptes.

Nom de domaine MDaemon

Choisissez dans la liste déroulante le domaine MDaemon dans lequel les comptes seront importés.

Mon compte

Comptes Windows

Cette fenêtre contient une liste de tous les noms de comptes collectés dans la base de données des comptes Windows.

Comptes sélectionnés

Cette fenêtre contient tous les noms de comptes que vous avez sélectionnés et que vous souhaitez importer.

>>

Cliquez sur ce bouton pour déplacer les noms de comptes en surbrillance de la fenêtre "Comptes Windows" vers la fenêtre "Comptes sélectionnés".

<<

Cliquez sur ce bouton pour supprimer les entrées en surbrillance de la fenêtre "Comptes sélectionnés".

Options

Faire en sorte que les boîtes aux lettres des comptes soient égales au nom du compte SAM/AD.

Cliquez sur ce commutateur pour forcer l'utilisation du nom de compte Windows de chaque utilisateur importécomme valeur de sa Boîte aux lettres. Avec cette méthode, vous n'aurez pas à vous soucier de configurer correctement les macrosdu Modèle Nouveaux comptes.

Utiliser le Modèle de compte pour générer des mots de passe

Cette option permet à MDaemon de générer des mots de passe pour les comptes importés en utilisant les paramètres du modèle de compte (voir Paramètres par défaut des comptes).

Définir les mots de passe de compte égaux aux noms de compte

Cette option fait que MDaemon utilise le nom du compte comme mot de passe du compte.

Faire en sorte que chaque mot de passe soit égal à...

Ce compte utilise une valeur de mot de passe statique qui sera utilisée par tous les comptes importés.

Authentifier les mots de passe dynamiquement à l'aide de SAM/AD

Ce commutateur active l'authentification l'authentification AD des comptes ajoutés. Dans ce cas, plutôt que de spécifier un mot de passe, MDaemon authentifie simplement les valeurs USER et PASS fournies par le client de messagerie en utilisant la base de données NT en temps réel.

Authentifier sur ce domaine Windows

Par nom de domaine Windows que MDaemon utilisera pour authentifier les connexions de manière dynamique. Il ne s'agit pas du nom de la machine du contrôleur de domaine. Il s'agit du Nom du domaine Windows.



Lorsque les comptes sont configurés pour une AD, le nom du domaine Windows précédé de deux barres obligues inverses est utilisé dans le champ PASSWORDdu compte et est stocké en clair dans le fichierusERLIST.DAT. Exemple, si un compte est configuré pour l'authentification AD sur un domaine Windows appelé AD sur un domaine Windows appelé ALTN, lechamp Mot de passe du comptecontiendra la valeur \\NALTN. Les deux barres obliques inverses précédant le nom du domaine signifient à MDaemon que le champ du mot de passe contient en fait le nom d'un domaine Windows et que MDaemon doit tenter d'authentifier les valeurs USER et PASS fournies par le client de messagerie à l'aide de la base de données du compte dece domaine.De ce fait, vous ne devez pas faire commencer un mot de passe par deux caractères barre obligue inverse, sauf si le compte est configuré pour l'authentification AD comme décrit ci-dessus. l'authentification AD comme décrit ci-dessus. En d'autres termes, vous ne pouvezpas avoir des mots de passe ordinaires qui commencent par deux barres obligues inverses. Les mots de passe commençant par deux barres obliques inverses sont toujours supposés fournir un Nom de domaine Windows et non un mot de passe.

Vous pouvez saisir les deux barres obliques inversées et la combinaison du nom de domaine Windows dans le champ dumot de passe d'un compte sur l'écran <u>Détails du compte de</u> [765] l'Éditeur de comptes. Il n'est pas nécessaire de se limiter à l'utilisation de l'importateur pour configurer les comptes pour l'authentification AD.

Voir :

Importation de comptes à partir d'un fichier texte Editeur de compte | Compte

Section

6 Menu Files d'attente

6.1 Files d'attente

6.1.1 File de relance

🧐 Queues - Retry Queue	
Mail Queues 	Retry Queue Keep message in the remote queue for at least 60 minutes Delay delivery after an SMTP temp error for 3 minutes Retry sending undeliverable mail once every 240 minutes Inform the sender when message delivery is delayed 1 minutes Inform the sender when previously delayed messages are delivered Undeliverable Mail Route message to bad queue if hop count exceeds 20 (5-100) If a message is still undeliverable after 2 days them: Route message to the bad message queue 2 days them: Route message to the bad message could not be delivered 1 inform the postmaster that the message could not be delivered Inform the postmaster that the message could not be delivered unless it's an MD aemon auto-generated message Route messages with no recipients to the bad message queue Route messages with no recipients to the bad message queue
	Ok Cancel Apply Help

La boîte de dialogue File de relance, située sous Files d'attente | Files d'attente de messagerie, permet de déterminer comment MDaemon va traiter les messages qui ne peuvent pas être distribués en raison d'une erreur non fatale, par exemple lorsque le serveur de réception est temporairement indisponible.

File de relance

Conserver le message dans la file distante au moins [xx] minutes

Dans ce paramètre, la durée pendant laquelle un message reste dans la file distante avant d'être retiré et placé dans la file de relance est déterminée. En règle générale, la file distante tentera de livrer le message plus fréquemment que la file d'attente de relance.

Après une erreur SMTP temporaire, retarder la distribution pendant [xx] minutes

Lorsque MDaemon rencontre une erreur SMTP temporaire (4xx) lors d'une tentative de distribution d'un message, il retarde de ce nombre de minutes chaque tentative ultérieure de distribution de ce message. Cela permet d'éviter que MDaemon n'essaie

de délivrer le message trop rapidement. Non par défaut, le délai est fixé à 3 minutes. Si vous souhaitez désactiver le délai, définissez la valeur à "0".

Tenter de renvoyer le courrier toutes les [xx] minutes

Ce paramètre détermine la fréquence de traitement des messages dans le File de relance.

Informer l'expéditeur lorsque la distribution du message est retardée

Par défaut, MDaemon informe l'expéditeur lorsqu'un message n'a pas pu être distribué en raison d'une erreur temporaire, ce qui le place dans la file d'attente de relance. Décochez cette case si vous ne souhaitez pas informer l'expéditeur du retard.

Informer l'expéditeur lorsque des messages dont la distribution a été retardée sont distribués

Cochez cette case si vous souhaitez informer l'expéditeur de la remise d'un message retardé. Cette option est désactivée par défaut.

Courrier non distribuable

Routage des messages dans la file d'attente des messages erronés si le nbre de sauts dépasse (5-100)

Les normes RFC stipulent qu'un serveur de messagerie doit apposer un cachet sur chaque message à chaque fois qu'il est traité. Ces cachets peuvent être comptés et utilisés comme mesure palliative contre les boucles de courrier récursives qui peuvent parfois être causées par des configurations erronées. Si elles ne sont pas détectées, ces boucles de distribution de messages épuisent vos ressources. Dans le processus de comptage du nombre de fois où le message a été traité, de tels messages peuvent être détectés et placés dans le répertoire des mauvais messages. Si un message n'est pas parvenu à son destinataire après avoir été traité par un certain nombre de serveurs de messagerie, c'est qu'il y a probablement une boucle de messagerie en cours. Selon toute vraisemblance, le paramètre par défaut de ce contrôle devrait suffire à empêcher les boucles de courrier et ne devra pas être modifié.

Si un message ne peut toujours pas être distribué après [xx] jours then :

Ce paramètre détermine le nombre de jours pendant lesquels un message peut rester dans le File de relance avant d'être supprimé. Si vous entrez "0" jours dans cette option, le message sera renvoyé après la première tentative. Le paramètre par défaut est de 2 jours.

Placer en file des messages erronés

Dans cette option, un message sera déplacé vers la file d'attente des mauvais messages une fois qu'il aura atteint la limite de temps définie dans l'option "*Si le message ne peut toujours pas être distribué après [xx] jours, alors :*".

Informer l'expéditeur que le message n'a pas pu être distribué

Dans le cas où un message a atteint la limite de temps fixée dans l'option "*Si un message peut toujours être remis après [xx] jours then :*", MDaemon enverra un message de<u>Notification d'état de distribution a</u> à l'expéditeur pour l'informer que le message a été définitivement supprimé du serveur.

Informer le postmaster lorsque le message n'a pas pu être distribué

Si ce commutateur est activé, le postmaster sera informé lorsqu'un message a été définitivement supprimé du système de relance.

.. sauf s'il s'agit d'unmessage généré automatiquement par MDaemon

Par défaut, le système de relance n'informera pas le postmaster lorsqu'un message n'a pas pu être distribué alors qu'il s'agit d'un message généré automatiquement par MDaemon. Décochez cette case si vous souhaitez informer le postmaster de l'échec de ces messages également. Exemples de messages générés automatiquement : avis de renvoi, messages générés par un répondeur automatique, résultats du traitement d'un compte, etc.

Routage des messages sans destinataires dans la file des messages erronés

Lorsque cette option est activée, les messages sans données sur les destinataires sont placés dans la file d'attente des mauvais messages. Lorsqu'elle est désactivée, ils sont supprimés. Cette option est activée par défaut.

6.1.2 File temporaire

🧐 Files d'attente - File d'attente temporaire	
Files d'attente File de relance File d'attente temporaire Files personnalisées Restaurer les files Paramètres DSN Pré/post-traitement	Les messages qui produisent des erreurs lors de l'analyse de contenu, de la recherche de virus ou de spam sont placés dans la file temporaire Activer et utiliser la file temporaire Garder le courrier si le Filtre anti-spam rencontre une erreur de traitement Garder le courrier si le compte expéditeur ou destinataire est désactivé ou figé Traiter la file temporaire après chaque mise à jour des signatures antivirus E-mails de résumé Envoyer un résumé de la file temporaire aux adresses ci-dessous Envoyer un résumé de la file des messages incorrects aux adresses ci-dessous Envoyer un résumé de la file de quarantaine aux adresses ci-dessous Postmaster (séparez plusieurs adresses par des virgules) Envoyer un résumé toutes les 120 minutes Remarque : MDaemon envoie un résumé au démarrage et à l'arrivée du premier message dans la file d'attente.
	OK Annuler Appliquer Aide

La file d'attente, située sous Files d'attente | Files d'attente de courrier, peut être utilisée pour recevoir des messages qui provoquent des exceptions logicielles lors du traitement de l'AntiVirus, de l'AntiSpam ou du Filtre de contenu. Si une erreur logicielle se produit lors du traitement d'un message, celui-ci sera placé dans la file d'attente et ne sera pas distribué.

Les messages placés dans la file d'attente y resteront jusqu'à ce que l'administrateur prenne des mesures pour les supprimer. Il existe un bouton Traiter la file d'attente dans la barre d'outils de MDaemon et une option identique dans la barre de menuFiles d'attente. Vous pouvez également traiter les messages en cliquant avec le bouton droit de la souris sur la file d'attente dans l'interface principale, puis en sélectionnant " Remettre en file d'attente " dans le menu contextuel. Le traitement de la file d'attente déplacera tous ses messages dans les files d'attente distante ou locale pour le traitement normal du courrier. Si l'erreur qui a entraîné le placement d'un message dans la file d'attente existe toujours, ce message sera replacé dans la file d'attente lorsque l'erreur se reproduira. Si vous souhaitez tenter de distribuerles messages de la file d'attente sans tenir compte des erreurs éventuelles, vous pouvez le faire en cliquant avec le bouton droit de la souris sur la file d'attente dans l'interface principale, puis en sélectionnant "Distribuer" dans le menu du clic droit. Lors de la libération des messages de la file d'attente, une boîte de confirmation s'ouvre pour vous rappeler que les messages peuvent contenir des virus ou ne pas pouvoir être filtrés correctement par le Filtre de contenu, l'AntiSpam et/ou l'AntiVirus.

File d'attente

Activer et utiliser la file temporaire

Cochez cette case pour activer la file d'attente. Les messages qui provoquent des exceptions logicielles lors du traitement par l'AntiVirus et le Filtre de contenu seront déplacés vers cette file d'attente chaque fois qu'une erreur se produit.

Garder le courrier si le Filtre anti-spam rencontre une erreur de traitement Cochez cette option si vous souhaitez déplacer vers la file d'attente les messages qui provoquent des erreurs lors du traitement par le Filtre anti-spam.

Garder le courrier si le compte expéditeur ou destinataire est désactivé ou figé Lorsque cette option est activée, MDaemon met automatiquement en attente les messages lorsque le compte d'envoi ou de réception est désactivé ou figé.

Traiter la file temporaire après chaque mise à jour des signatures antivirus

Lorsque cette option est activée, la file d'attente est traitée automatiquement à chaque mise à jour des signatures de l'<u>Activer AntiVirus</u>

E-mails de résumé

Envoyez par e-mail un résumé de la file d'attente aux adresses électroniques cidessous.

Si vous souhaitez envoyer un résumé des messages contenus dans la file d'attente à une ou plusieurs adresses électroniques à intervalles réguliers, cliquez sur cette option et indiquez les adresses dans l'espace de texte ci-dessous.

E-mails de résumé de la file d'attente des mauvais messages aux adresses électroniques ci-dessous

Si vous souhaitez envoyer régulièrement un résumé des messages contenus dans la file d'attente des messages indésirables à une ou plusieurs adresses électroniques, cliquez sur cette option et dressez la liste des adresses dans l'espace texte prévu à cet effet.

E-mails de résumé de la file d'attente de la quarantaine aux adresses électroniques ci-dessous

Activez cette option si vous souhaitez envoyer un résumé de la file d'attente de la quarantaine à l'intervalle désigné ci-dessous.

Destinataires du message récapitulatif

Utilisez la zone de texte pour spécifier les adresses électroniques auxquelles vous souhaitez envoyer les résumés du contenu de la file d'attente désignés dans les deux options précédentes. Lorsque vous indiquez plusieurs adresses, séparez-les par des virgules.

Les messages de notification sont envoyés au démarrage de MDaemon, la première fois qu'un message est placé dans la file d'attente, et à l'intervalle spécifié dans l'option *Envoyer le résumé toutes les [xx] minutes* ci-dessous.



Si un message de notification provoque une erreur logicielle, il se peut qu'il ne soit pas envoyé aux destinataires distants. Il sera cependant toujours envoyé aux destinataires locaux.

Envoyer un résumé aux destinataires des notifications du Filtre de contenu

Cliquez sur cette option si vous souhaitez qu'une copie supplémentaire de chaque message de notification soit envoyée aux <u>destinataires</u> [714] de notification désignés par le Filtre de contenu .

Inclure un lien d'action (libérer, remettre en file d'attente, supprimer) dans l'email résumé

Par défaut, les e-mails de résumé pour la file d'attente, la quarantaine et la mauvaise file d'attente contiennent des liens pour libérer, remettre en file d'attente ou supprimer chaque message. L'E-mails résumé de la file d'attente des mauvais messages contient un lien supplémentaire permettant de supprimer tous les messages. Désactivez cette option si vous ne souhaitez pas inclure les liens dans les E-mails de résumé.



Dans le but de générer les liens, le paramètre <u>URL de</u> <u>MDaemon Remote Admin</u> [377] doit être défini.

Envoyer le résumé toutes les [xx] minutes

Utilisez cette option pour indiquer le nombre de minutes qui s'écouleront avant que MDaemon n'envoie un message de notification de file d'attente à chaque adresse spécifiée ou aux destinataires du Filtre de contenu.
6.1.3 Files personnalisées

🧐 Queues - Custom Queues				×
Mail Queues Active Queue Custom Queues Restore Queues DSN Settings Pre/Post Processing	Queue type	Queue path		H
	New queue name	ated under the root \MDa	emon\Queues\ folder	Remove
	This queue contains:	Host or IP		
	remote mail	AUTH Logon		
	🔘 local mail	AUTH Password		
	Add	SMTP 'MAIL' value Port (default = 25)	25	
	Local mail queues are Adding or deleting ent	not eligible for custom del ries cannot be undone by	ivery schedules. clicking 'Cancel'.	
		Ok C	ancel Apply	Help

Utilisez la boîte de dialogue Files personnantes sous Files d'attente | Files d'attente pour créer des files d'attente locales personnalisées et des files d'attente de courrier distant. La prise en charge des files personnalisées permet à MDaemon de surveiller plusieurs emplacements à partir desquels le courrier est envoyé. Vous pouvez créer de nouvelles files d'attente et les désigner comme locales ou distantes, puis utiliser les règles du Filtre de contenu pour que les messages soient automatiquement placés dans vos files d'attente personnalisées. Pour les files personnalisées, vous pouvez utiliser le <u>Planificateur d'événements</u> pour contrôler la fréquence de traitement de ces files d'attente.

Files personnalisées

Cette zone affiche une entrée pour chaque file personnalisée, indiquant son chemin de fichier et s'il s'agit d'une file locale ou distante.

Supprimer

Si vous souhaitez supprimer une file d'attente de la liste, sélectionnez son entrée, puis cliquez sur le bouton*Supprimer.*



Lorsque vous supprimez une file personnalisée, toutes les programmations personnalisées ou les règles de filtrage du contenu associées à cette file sont également supprimées.

Nom de la nouvelle file d'attente

Saisissez ici le nom de la nouvelle file d'attente. La file d'attente sera créée dans le dossierMDaemon \NMaemon\NQueuesues\N.

Cette file d'attente contient...

...du courrier distant

Choisissez cette option si vous souhaitez que la file d'attente personnalisée soit utilisée pour le courrier distant.

Références de la file d'attente

Vous pouvez spécifier un *Hôte ou une IP*, un *Mot de passe AUTH*, une *Valeur SMTP 'MAIL' et un Port pour n'importe quel courrier distant*. Si ces informations sont fournies, tous les messages de la file d'attente seront distribués à l'aide de ces paramètres. Dans certaines circonstances, il est toutefois possible que des messages individuels de la file d'attente aient leurs propres données de distribution et, si c'est le cas, ces données auront la priorité sur ces paramètres. **REMARQUE :** Lorsque vous utilisez un nom d'hôte dans l' option*Nom d'hôte ou IP*, MDaemon effectue une recherche d'enregistrement MX sur le nom d'hôte. Si vous souhaitez que MDaemon effectue une recherche dans l'enregistrement A, vous devez mettre le nom d'hôte entre parenthèses (par exemple, [mail.exemple.com]).

...courrier local

Choisissez cette option si vous souhaitez que la file d'attente locale personnalisée soit utilisée pour le courrier local. **Remarque :** les Files d'attente locales personnalisées ne peuvent pas être utilisées pour les programmes de distribution personnalisés.

Ajouter

Après avoir choisi le Nom et le type de votre file d'attente, cliquez sur le bouton*Ajouter* pour l'ajouter à la liste des files d'attente personnalisées.

6.1.4 Restaures les files



Restaurer l'emplacement par défaut des files d'attente

Par défaut, une nouvelle installation de MDaemon stocke les files d'attente de messages telles que Remote, Local, Raw, etc. dans le sousdossier\MDaemon\Queuesues\. Les versions précédentes de MDaemon stockaient les files d'attente ailleurs. Si votre installation de MDaemon utilise les anciens dossiers et que vous souhaitez déplacer vos files d'attente vers cette structure mieux organisée, cliquez sur ce bouton et toutes les files d'attente, ainsi que les fichiers et les messages qu'elles contiennent, seront déplacés pour vous. Après avoir cliqué sur ce bouton, vous devrez redémarrer MDaemon pour que les modifications soient prises en compte.



<u>Files personnalisées</u> and ne seront pas déplacées par cette fonctionnalité.

6.1.5 Paramètres DSN

940

🧐 Files d'attente - Paramètres DSN	
Files d'attente File de relance File d'attente temporaire Files personnalisées Restaurer les files Paramètres DSN Pré/post-traitement	Contenu des notifications d'état de remise (DSN) Objet du message de distribution retardée (512 caractères max.) AVERTISSEMENT : distribution du message retardée Objet du message d'erreur permanente de distribution (512 caractères max.) AVERTISSEMENT : échec de distribution du message
	Paramètres des notifications d'état de remise Ne pas inclure les transcriptions de sessions dans les notifications d'état de remise V Ne pas générer de notifications pour le courrier transféré non distribuable Placer les notifications non distribuables dans la file des messages incorrects Envoyer les notifications d'état de remise via le Filtre de contenu et le filtre anti-spam
	OK Annuler Appliquer Aide

Lorsque MDaemon rencontre un problème de livraison d'un message, qu'il s'agisse d'un échec temporaire ou permanent, un message de Notifications d'état de remise (DSN) est envoyé à l'expéditeur du message. Cet écran contient diverses options relatives à ces messages DSN. Il se trouve à l'adresse suivante : Files | Files d'attente / DSN... | Paramètres des notifications DSN.

Contenu des notifications DSN

Objet du message de distribution retardée (512 caractères max.)

Dans ce cas, il s'agit de l'objet du message DSN qui sera envoyé en cas de problème transitoire entraînant un retard dans la distribution du message. Exemple : si le serveur de messagerie du destinataire n'est pas disponible lorsque MDaemon tente de distribuer un message, MDaemon continuera d'essayer de l'envoyer à intervalles réguliers et enverra ce message DSN pour informer l'expéditeur du problème. Voir : <u>Personnalisation des messages DSN</u>

Objet du message d'erreur permanente de distribution (512 caractères max.)

Il s'agit de l'objet du message DSN qui sera envoyé en cas de problème empêchant MDaemon de délivrer un message. Par exemple, si le serveur de messagerie qui reçoit le message le rejette en indiquant que l'adresse électronique du destinataire n'existe pas, MDaemon cessera d'essayer de livrer le message et enverra un message DSN informant le destinataire que le message ne peut pas être livré. Voir : <u>Personnalisation des messages DSN</u>

Paramètres des notifications (DSN)

Ne pas inclure les transcriptions de session dans les messages DSN

Cliquez sur cette option si vous ne souhaitez pas inclure les transcriptions de session SMTP dans les messages d'erreur et d'avertissement relatifs à la distribution. "Destinataire des messages d'alerte" est désactivé par défaut. Cette option est désactivée par défaut.

Ne pas générer de DSN pour le courrier transféré non distribuable

Lorsque cette option est activée, les messages transférés qui rencontrent des erreurs de distribution permanentes et fatales ou qui expirent de la File de relance seront déplacés dans la file d'attente des mauvais messages, sans qu'aucun message DSN ne soit envoyé à l'expéditeur d'origine. Cette option est activée par défaut.

Placer les notifications non distribuables dans la file des messages incorrects

Cochez cette case si vous souhaitez placer les messages DSN non distribuables dans la file d'attente des files d'attente des messages erronés plutôt que de les relancer.



Cela ne s'applique qu'aux messages DSN générés par MDaemon.

Envoyer les notifications d'état de remise via le Filtre de contenu et le Filtre anti-spam Activer cette option si vous souhaitez envoyer les messages DSN à travers les filtres anti-spam et de contenu. Cette option est désactivée par défaut.

Personnalisation des messages DSN

La partie "lisible par l'homme" des messages DSN transitoires (retard) et permanents (échec) peut être personnalisée en créant un fichier appelé respectivement DSNDelay.dat ou DSNFail.dat dans le dossier CréationaemonApp\. Modifiez-les à l'aide d'un éditeur de fichiers texte tel que Notepad et saisissez le texte que vous souhaitez utiliser. Les macros suivantes peuvent être utilisées dans votre texte personnalisé :

\$SESSIONID\$ - se développe en chaîne d'identification de la session de livraison

\$QUEUEID\$ - renvoie à la chaîne d'identification de la file d'attente du message.

\$MESSAGEID\$ - se développe en fonction de la valeur de l'En-tête ID du message.

\$RETRYDAYS\$ - durée de la file d'attente (en jours)

\$RETRYHOURS\$ - durée de la file d'attente (en heures)

Redémarrage de MDaemon en cours pour que les modifications apportées à ces fichiers soient prises en compte.

Voir :

File de relance 932

6.2 Pré/Post-traitement

🧐 Files d'attente - Pré/post-traitement		
■- Files d'attentePré/post-traitement	File D'attente Locale Exécuter ce programme juste Suspendre les opérations du	avant le traitement de la file locale: Parcourir
	serveur pendant : -1 secondes.	Ne pas exécuter quand la file d'attente est vide Forcer l'arrêt du programme Exécuter le programme dans une fenêtre masquée
	File D'attente Distante Lancer ce programme avant c	le traiter la file d'attente distante :
	Suspendre les opérations du serveur pendant :	Ne pas exécuter quand la file d'attente est vide
	-1 secondes. Remarque : en saisissant -1 dans toute l'exécution du programme.	Exécuter le programme dans une fenêtre masquée s le champ, les opérations du serveur sont suspendues pendant La valeur 0 n'implique aucune attente.
		OK Annuler Appliquer Aide

Pré/Post-traitement des files locales et REMOTE

Lancer ce programme avant de traiter la file d'attente du courrier local ou distant Ce champ indique le chemin et le nom d'un programme qui sera exécuté juste avant le traitement et la distribution des messages RFC-2822 qui pourraient se trouver dans les files d'attente locales ou distantes. Si le chemin d'accès complet n'est pas indiqué, MDaemon cherchera d'abord l'exécutable dans le répertoire MDaemon, puis dans le répertoire Windows System, ensuite dans le répertoire Windows et enfin dans les répertoires listés dans la variable d'environnement PATH.

Lors de l'exécution de ce processus, le serveur doit suspendre les opérations du serveur pendant [xx] secondes

La valeur saisie ici détermine lecomportement deMDaemon pendant que le programme spécifié est en cours d'exécution. MDaemon peut être configuré pour suspendre son fil d'exécution pendant le nombre de secondes spécifié, en attendant que le fil d'exécution du processus revienne. Si le processus revient avant que le nombre de secondes ne soit écoulé, MDaemon reprendra immédiatement son fil d'exécution. Si vous entrez "0" dans cette option, MDaemon ne suspendra pas du tout les opérations. Si vous entrez "-1", MDaemon attendra jusqu'à ce que le processus revienne, quelle que soit la durée de cette attente.

942

Ne pas exécuter lorsque la file d'attente est vide

Activez ce commutateur si vous ne voulez pas que le programme spécifié s'exécute lorsque la file d'attente est vide.

Forcer le processus à terminer

Il arrive que le processus que vous devez exécuter ne se termine pas de lui-même. Dans ce cas, MDaemon forcera la session à se terminer une fois que le temps spécifié dans la section...*Suspendre toutes les opérations pendant [xx] secondes*. Ce commutateur ne fonctionne pas si l'intervalle de temps écoulé est fixé à "-1".

Exécuter le programme dans une fenêtre masquée

Cochez cette case si vous souhaitez que le programme s'exécute dans une fenêtre masquée.

6.3 Gestionnaire de files d'attente et de statistiques

La Gestion des files d'attente et des statistiques de MDaemon est accessible à partir de MDaemon, dans le menu Files sélectionnées" Gestion des files d'attente et des statistiques. La Gestion des files d'attente et des Statistiques est constituée d'une boîte de dialogue de quatre pages. Chacune de ces pages a été conçue pour servir un objectif distinct et spécifique, tout en conservant un format simple qui les rend très faciles à utiliser.

Page File d'attente

L'onglet par défaut est la page File d'attente. Depuis cette page, vous pouvez facilement gérer toutes les Boîtes aux lettres aux Lettres de MDaemon, ainsi que les Dossiers courrier de Mon compte. En cliquant simplement sur la file d'attente ou l'utilisateur de votre choix, une liste de tous les fichiers de messages contenus dans la file d'attente spécifiée s'affiche, ainsi que plusieurs informations pertinentes sur chaque message : l'expéditeur, le destinataire, le contenu de l'en-tête "Deliver-To", l'objet du message, sa taille et depuis combien de temps il se trouve à l'endroit où il se trouve. En outre, des commandes permettent de copier ou de déplacer facilement les messages d'un dossier à l'autre, ou de les supprimer complètement.

Page utilisateur 948

Aucun utilisateur n'affiche une liste de tous les utilisateurs de MDaemon. Cette liste comprend leur Nom complet, le nom de leur boîte aux lettres, le nombre de messages dans leur boîte aux lettres, l'espace disque occupé par leur compte et la date à laquelle ils ont consulté leur courrier pour la dernière fois. Cette liste peut également être enregistrée sur le disque sous forme de fichier texte ou au format délimité par des virgules pour une utilisation avec des bases de données.

Pas de journalisation 950

Cette boîte de dialogue permet d'afficher les Fichiers journaux de MDaemon sous forme de liste simple. Cette fonction est très utile pour examiner rapidement l'historique destransactions de messagerie de MDaemoncar elle condense le *Fichier journal* sélectionné en une liste à

colonnes qui contient : le Type du message (POP Inbound, DomainPOP, RFC2822, etc.), l'Hôte auquel MDaemon s'est connecté pendant la transaction, l'expéditeur, le destinataire, la taille du message, la date à laquelle chaque message a été traité avec succès ou non. Vous pouvez également examiner la partie détaillée du journal concernant n'importe quelle entrée de la liste en double-cliquant sur l'entrée souhaitée. Cela affichera la partie du journal où la transaction a été effectuée. Les Fichiers journaux affichés sur la *page des journaux* peuvent être sauvegardés sous forme de fichier texte ou au format délimité par des virgules pour une utilisation avec des bases de données.

Page Rapport

La dernière page est la *page des rapports*. Ce texte permet de produire un rapport contenant tous lesparamètres de configuration de MDaemon, dans un format lisible en texte clair. Dans la mesure où MDaemon dispose d'un grand nombre de paramètres et de configurations optionnels, cette fonction permet d'accélérer considérablement le processus d'administration des changements de configuration et d'aider à diagnostiquer d'éventuels problèmes de configuration. De plus, ce texte est affiché dans un format éditable qui permet de copier/coller les informations qu'il contient (en utilisant le menu contextuel du clic droit), ou d'ajouter des annotations ou d'autres informations au fichier avant de l'enregistrer.

6.3.1 Files d'attente

🌾 Queue/St	ats Manager					- • •
Queue Page	User Page	Log Page Report Pa	age			
C:\MDaem	on\Queues\Lo	cal\ (0 messages, 0 kl	B)			
Filename		From	То	Deliver-To	Subject	Size
			III			4
Bemote	Queue					Coort
Local Q	ueue					Cobà
Retry Qi	ueue	=				Move
- Holding - LAN Qu	Queue eue	-				Delete
- RAW Q	ueue					
- Bad Qu	eue					
Inbound	l Queue	-				<u>R</u> efresh

Page de liste de la file d'attente

Dansla zone*Messages et files d*' attente ou dans la liste d'utilisateurs située à côté, une liste de tous les fichiers de messages contenus dans la file d'attente sélectionnée est

affichée dans la zone de liste principale de cette page. Cette liste contient lenom du fichier de chaque message, l'expéditeur, le destinataire, le contenu de l'en-tête "Deliver-To", l'objet du message, sa taille et depuis combien de temps il se trouve à son emplacement actuel (listé par date et heure).

Au-dessus de cette boîte, le chemin d'accès complet au répertoire actuellement affiché est indiqué, ainsi que le nombre de messages affichés et la taille du répertoire.

Vous pouvez copier, déplacer ou supprimer un ou plusieurs fichiers en les sélectionnant dans la liste et en cliquant ensuite sur le bouton approprié situé en dessous.

Le contenu de ces fichiers peut également être modifié directement à partir de la liste des*pages de la file d'attente*. Il vous suffit de double-cliquer sur le fichier que vous souhaitez modifier (ou de choisir "Editer" dans le menu contextuel du clic droit) et le fichier s'ouvrira dans le Bloc-notes pour être édité.

Si vous souhaitez que le Gestionnaire de files d'attente et de statistiques ouvre par défaut un éditeur autre que le Blocnotes, vous devez modifier le fichier mdstats.ini situé dans le dossier MDaemon\Napp. Modifiez la clé "Editor="située sous le titre de la section [QueueOptions] en Editor=MyEditor.exe. Si le Chemin du fichier *.exe ne se trouve pas dans votre chemin d'accès actuel, vous devrez inclure le chemin d'accès dans le nom du fichier.

Vous pouvez naviguer dans la zone de liste en utilisant les barres de défilement verticales ou horizontales, ou en cliquant n'importe où dans la zone de liste et en utilisant les touches FLECHE pour la navigation. Vous pouvez trier les informations contenues dans la zone de liste*Page de file d'attente en* fonction de la colonne de votre choix. Il suffit de cliquer une fois sur la colonne souhaitée pour la trier dans l'ordre croissant (A-Z, 1-2), ou de cliquer deux fois pour la trier dans l'ordre décroissant (Z-A, 2-1). Les colonnes peuvent également être redimensionnées en plaçant le pointeur sur la ligne entre les titres des colonnes jusqu'à ce qu'elle change de forme, puis en faisant glisser la colonne jusqu'à la largeur souhaitée.

Sélection de fichiers

Pour sélectionner des fichiers individuellement Cliquez sur le fichier souhaité.

Pour sélectionner des fichiers contigus Cliquez sur le premier fichier de la liste

contiguë de fichiers que vous souhaitez sélectionner, puis, tout en maintenant la touche MAJ enfoncée, cliquez sur le dernier fichier contigu de la liste souhaitée.

Vous pouvez également utiliser les touches FLECHE, ACCUEIL, FIN, PAGE HAUT et PAGE BAS, tout en maintenant la touche MAJ enfoncée, pour sélectionner les fichiers dans un ordre contigu. Pour sélectionner des fichiers non contigus Cliquez sur les fichiers souhaités dans la colonneNom du fichier tout en maintenant la touche CTRL enfoncée.

Messages et files d'attente

Cliquez sur une file d'attente dans le volet inférieur gauche et une liste de tous les fichiers contenus dans la file d'attente spécifiée s'affichera dans la zone de liste *Queue Page (Page de file d'attente).* Si vous cliquez sur l'option *Dossiers utilisateurs*, une liste de tous les utilisateurs de MDaemon sera affichée *dans la zone de liste des utilisateurs* à droite de la section*Files d'attente de messages.*

Liste des utilisateurs

Cette boîte affiche une liste de tous les utilisateurs de MDaemon lorsque l'option *Dossiers utilisateurs* est cliquée dans la section*Files d'attente des messages* (volet inférieur gauche). Cliquez sur lenom d' un utilisateurpour afficher la liste de tous les fichiers de messages actuellement contenus dans le dossier de la boîte aux lettres de l'utilisateur.

Rafraîchissement

Les files d'attente étant dynamiques lorsque MDaemon est actif - des fichiers de messages y étant constamment transférés - vous devez régulièrement cliquer sur ce bouton pour actualiser la liste des fichiers que vous avez pu afficher.

Vous pouvez modifier le fichier MDstats.ini pour que les listes affichées se rafraîchissent automatiquement. Pour cela, ouvrez le fichierMDstats.ini situé dans le répertoire de MDaemon et modifiez la clé AutoRefresh sous le titre[QueueOptions] pour indiquer le nombre de secondes qui doivent s'écouler entre deux actualisations. La valeur "0" signifie que vous ne souhaitez pas que la liste soit actualisée automatiquement. Exemple : AutoRefresh=15 (la liste sera rafraîchie toutes les 15 secondes).

Copie

Lorsqu'un ou plusieurs fichiers sont sélectionnés, cliquez sur ce bouton pour copier les fichiers sélectionnés dans une autre file d'attente ou dans le dossier de la boîte aux lettres d'unutilisateur. Après avoir cliqué sur ce bouton, la boîte de dialogue*Copier message(s) s* 'ouvre, dans laquelle vous pouvez sélectionner l'emplacement dans lequel vous souhaitez copier les fichiers sélectionnés.

Déplacer

Lorsqu'un ou plusieurs fichiers sont sélectionnés, cliquez sur ce bouton pour déplacer les fichiers sélectionnés vers une autre file d'attente ou un autre dossier de la boîte aux lettres de l'utilisateur. Après avoir cliqué sur ce bouton, la boîte de dialogue*Déplacer le(s) message(s) s* 'ouvre, dans laquelle vous pouvez sélectionner l'emplacement vers lequel vous souhaitez déplacer les fichiers sélectionnés.

Les fichiers copiés/déplacés vers d'autres files d'attente conserveront rarement leur nom d'origine. Pour éviter d'écraser des fichiers du même nom qui se trouvent déjà dans la file d'attente, MDaemon calcule toujours le nom du fichier dedestination suivant en se basant sur le fichierHIWATER.MRK situé dans le dossier de destination.

Supprimer

Dans la liste de l'État des files d'attente, lorsqu'un ou plusieurs fichiers sont sélectionnés , cliquez sur ce bouton pour supprimer les fichiers sélectionnés. Si vous cliquez sur ce bouton, une boîte de confirmation s'ouvre pour vous demander si vous souhaitez vraiment supprimer les fichiers sélectionnés.



6.3.2 Utilisateurs

😓 Queue/Stats Manager 🚽						- • •
Queue Page User Page L	.og Page Report f	Page				
User Information (7 users) -						
Full Name	Mailbox	Domain	Msg Count	Disk Space	Quota	Forwarding A
🕵 Arvel Hathcock	Arvel.Hathcock	example.com	1	5	(n/a)	(n/a)
🕵 Bill Farmer	Bill.Farmer	example.com	1	5	(n/a)	(n/a)
👲 Frank Thomas	Frank.Thomas	example.com	2	5	(n/a)	(n/a)
🕵 Kevin Beatty	Kevin.Beatty	example.com	1	5	(n/a)	(n/a)
📓 👲 MDaemon Server	MDaemon	example.com	0	0	(n/a)	(n/a)
👷 Michael Mason	michael.mason	example.com	708	7,674	(n/a)	(n/a)
🕵 Randy Peterman	Randy.Peterm	example.com	1	5	(n/a)	(n/a)
		III				P
				(Refresh	Save

Infos utilisateur

Lorsque l'on choisit la page Utilisateur, une liste de tous les comptes MDaemon est chargée dans la zone de listeInfos utilisateur. Cette liste contient lenom complet de chaque utilisateur, le nom de sa boîte aux lettres, le domaine auquel le compte appartient, le nombre de messages qu'il contient, son format de courrier, la quantité d'espace disque (en kilo-octets) que le compte occupe, son adresse de transférer, et enfin, la date à laquelle son courrier a été vérifié pour la dernière fois. Dans la mesure où les informations contenues dans cette liste sont en constante évolution, elles peuvent être facilement mises à jour en cliquant sur le boutonActualiser.

Vous pouvez naviguer dans la zone de liste en utilisant les barres de défilement verticales et horizontales, ou vous pouvez cliquer n'importe où dans la zone de liste et utiliser les touches FLECHE pour la navigation. Vous pouvez trier les informations contenues dans la zone de liste *Infos utilisateur* en fonction de la colonne de votre choix. Il vous suffit de cliquer une fois sur la colonne souhaitée pour la trier par ordre croissant (A-Z), ou de cliquer deux fois pour la trier par ordre décroissant (Z-A). Les colonnes peuvent également être redimensionnées en plaçant le pointeur sur la ligne entre les titres des colonnes jusqu'à ce qu'elle change de forme, puis en faisant glisser la colonne jusqu'à la largeur souhaitée. En outre, vous pouvez double-cliquer sur n'importe quelle entrée et MDStats passera à la *page de file d'attente* avec le contenu de son dossier de boîte aux lettres affiché.



Les Dossiers utilisateurs contiennent un fichier appelé "hiwater.mrk" qui est utilisé pour déterminer certaines de ces informations sur l'utilisateur. Évitez de supprimer ce fichier inutilement, car cela empêchera le Gestionnaire des files d'attente et des statistiques d'obtenir certaines des informations figurant dans la liste*lnfos utilisateur* .

Rafraîchir

Les statistiques relatives aux utilisateurs, telles que le nombre de messages contenus dans leurs boîtes aux lettres et l'espace disque utilisé par leurs comptes, sont en constante évolution. Vous pouvez facilement mettre à jour les informations contenues dans la liste *Infos utilisateur* en cliquant sur le bouton*Actualiser*. Toutes les informations affichées seront alors immédiatement mises à jour.

Indicateur de progression

Comme les listes d'*Infos utilisateur* peuvent parfois être très volumineuses, une barre d'indicateur de progression se trouvesous la liste *d'Infos utilisateur*. Elle indique visiblement que le programme fonctionne toujours lorsque des fichiers volumineux sont en cours de chargement.

Sauvegarde

Les informations contenues dans la liste *Infos utilisateur* peuvent être enregistrées dans un fichier au format délimité par des virgules pour une utilisation avec des bases de données, ou dans un fichier texte ASCII en cliquant sur le bouton*Enregistrer*. Après avoir choisi un nom et un emplacement pour ce fichier dans la boîte de dialogue Enregistrer sous de Windows, il vous sera demandé si vous souhaitez enregistrer le fichier au format délimité par des virgules ou en tant que fichier texte brut.

6.3.3 Journaux

🍥 Queue/Stats Mai	nager				- • •
Queue Page User	Page Log Page F	leport Page			
C:\MDaemon\Log:	s\MDaemon-2010120	16-all.log			
Туре	Host	From	То	Subject	Bytes Da
•					•
,					
				Open Log	Save

Rapport de journalisation

La liste Fichiers journaux affiche les fichiers journaux détaillés de MDaemonque vous sélectionnez à l'aide du bouton *Ouvrir le journal* et de la boîte de dialogue Ouvrir de Windows qui suit. L'affichage du *rapport de journal* permet de consulter rapidement et facilement l'historique des transactions de courrier traitées par MDaemon, sans avoir à trier le grand volume d'informations que les fichiers journaux de MDaemon peuvent parfois contenir. Lorsqu'un *rapport de journalisation* est affiché dans cette liste, le Gestionnaire de files d'attente et de statistiques le décompose dans un format simple contenant : le Type de message (POP Inbound, DomainPOP, RFC2822, etc.), l'Hôte auquel MDaemon s'est connecté pendant la transaction, l'expéditeur, le destinataire, la taille du message, la date à laquelle chaque message a été traité, si oui ou non la transaction a été réussie.

Vous pouvez également examiner la partie détaillée du journal concernant n'importe quelle entrée de la liste en double-cliquant sur l'entrée souhaitée. Cela affichera la partie du journal où la transaction a été effectuée. En utilisant le menu contextuel du clic droit, vous pouvez copier/coller cette partie détaillée du journal dans un éditeur de texte pour la sauvegarder ou la modifier si vous le souhaitez.

Vous pouvez naviguer dans la zone de liste en utilisant les barres de défilement verticales et horizontales, ou vous pouvez cliquer n'importe où dans la zone de liste et utiliser les touches FLECHE pour la navigation. Vous pouvez redimensionner lescolonnes de lazone de listeen plaçant le pointeur sur la ligne entre les titres des colonnes jusqu'à ce qu'elle change de forme, puis en faisant glisser la colonne jusqu'à la largeur souhaitée.

La page de journalisation affiche les fichiers journaux qui ont été compilés à l'aide de l' option Journalisation des sessions de courrier électronique détaillées ou de l' option Journalisation des sessions de courrier électronique résumées, qui se trouvent sous la rubrique Journalisation | Mode journal. Toutefois, nous vous recommandons vivement d'utiliser l' option Journalisation des sessions de courrier électronique détaillées. Dans ce dernier cas, vous constaterez que très peu d'informations seront affichées dans votre rapport de journalisation. En effet, le Fichier journaux condense le journal détaillé en une vue synthétique de l'activité de MDaemon, tout en permettant de consulter la vue détaillée de chaque transaction si nécessaire (en doublecliquant sur une entrée journal). Il n'est donc pas nécessaire que MDaemon résume le fichier journal lors de sa compilation.

Ouvrir le journal

Cliquez sur ce bouton pour ouvrir la boîte de dialogue Ouvrir de Windows afin de choisir le fichier journal que vous souhaitez consulter. Si vous cliquez sur ce bouton alors qu'un *Fichier journal* est déjà affiché dans la liste*Rapport de journal*, vous aurez la possibilité d'ajouter le nouveau fichier à celui qui est déjà affiché.

Après l'affichage d'un journal, une boîte de message contenant un résumé du journal sélectionné s'ouvre. Lors de l'enregistrement d'un rapport de journalisation sous forme de fichier texte, ce résumé de la journalisation lui sera annexé.

Log Sun	imary 🛛 🔀
(į)	Start Date : 2010-01-14 00:00:12 End Date : 2010-01-15 00:00:18
	SMTP Inbound : 2815 SMTP Outbound : 10 MultiPOP : 185 IMAP : 486
	ОК

Indicateur de progression

Les *Fichiers journaux* pouvant être très volumineux, une barre d'indicateur de progression se trouvesous la liste des*Rapports journaux*. Elle indique de manière visible que le programme est toujours en cours d'exécution lorsque des fichiers volumineux sont en cours de chargement ou d'enregistrement.

Sauvegarde

Les informations contenues dans la liste *Fichiers journaux* peuvent être enregistrées dans un fichier au format délimité par des virgules pour une utilisation avec des bases de données, ou dans un fichier texte ASCII en cliquant sur le bouton*Enregistrer*. Après avoir choisi un nom et un emplacement pour ce fichier dans la boîte de dialogue Enregistrer sous de Windows, il vous sera demandé si vous

souhaitez enregistrer le fichier au format délimité par des virgules ou en tant que fichier texte brut.

6.3.4 Rapport

😓 Queue/Stats Manager	
Queue Page User Page Log Page Report Page	
Report	
Configuration Report	<u>^</u>
Registration Information	
Product ID : MDaemon PRO v16.5.0 Version : 16.5.0 Registration Name : Arvel Hathcock Registration Company: Alt-N Technologies Registration Key : ABCDEFG-HIJKLMNOP-QRSTUV	
Product ID : SecurityPlus for MDaemon Version : 4.5.1 Registration Key : ABCDEFG-HIJKLMNOP-QRSTUV	
Product ID : ActiveSync for MDaemon Version : 16.5.0.16b Registration Key : ABCDEFG-HIJKLMNOP-QRSTUV	
<	4
	Refresh Save

Rapport

Dans *la page Rapport*, un rapport complet est produit. Il répertorie tous les paramètres de MDaemon dans un format texte facile à lire. Cette fonction réduit considérablement le temps nécessaire à l'administrateur pour vérifier les nombreux paramètres de configuration de l' Administration de MDaemon() et permet de résoudre rapidement d'éventuels problèmes de configuration.

Vous pouvez naviguer dans ce rapport à l'aide des barres de défilement ou des touches du CURSEUR, et l'affichage durapport est également un éditeur de texte - ce qui permet d'insérer des notes ou des informations supplémentaires dans le rapport avant de l'enregistrer dans un fichier. En outre, vous pouvez utiliser le menu contextuel pour couper, copier et coller dans et à partir de cet affichage en cliquant avec le bouton droit de la souris et en effectuant la sélection souhaitée dans le menu qui s'ouvre.

Actualiser

Cliquez sur ce bouton pour mettre à jour les Paramètres de*rapports de* MDaemonactuellement affichés .

Indicateur de progression

Dans la même optique que les autres onglets de la Gestion des files d'attente et des Statistiques, la *page Rapport* contient une barre d'indicateur de progression qui sert à

indiquer de manière visible que le programme est toujours en cours de fonctionnement pendant le chargement ou l'enregistrement de fichiers volumineux.

Sauvegarder

Cliquez sur ce bouton pour enregistrer le *rapport*affiché . Après avoir cliqué sur ce bouton, une boîte de dialogue standard Enregistrer sous s'ouvre pour vous permettre de désigner un nom de fichier et l'emplacement où vous souhaitez l'enregistrer.

6.3.5 Personnaliser le Gestionnaire de files d'attente et de statistiques

6.3.5.1 Fichier MDstats.ini

Personnalisation de la Gestion des files d'attente/Statistiques

Voici la liste des fichiers qui peuvent être modifiés dans le fichierMDstats.ini situé dans le répertoire\app\de MDaemon:

[MDaemon]

AppDir=C: \Nmdaemon\Napplicatio n	Emplacement durépertoire \NApp deMDaemon.
[QueueOptions]	
Editor=NOTEPAD.EXE	Éditeur à utiliser lorsqu'un message est double- cliqué, ou lorsqu'un message est cliqué avec le bouton droit de la souris et que l'option Modifier est sélectionnée.
LockOnEdit <i>=</i> No	Création ou non d'un fichier LCK lors de la modification d'un message. Cela permet d'éviter qu'un message ne soit déplacé hors de la file d'attente pendant qu'il est en cours de modification.
AutoRefresh=Oui	Temps (en secondes) entre les actualisations automatiques de la liste des messages. O signifie qu'il n'y a pas d'actualisation automatique.
ShowDirectories=Oui	Affiche les sous-répertoires des files d'attente dans la zone de liste en plus des messages. Les répertoires apparaissent sous la forme <nomdurépertoire>.</nomdurépertoire>
[Options d'utilisateur]	
ShowQuota=Oui	Détermine si la liste utilisateur affiche des informations sur les quotas (nombre de messages

et espace disque, comme MDaemon le calcule) o	วน
des informations sur les fichiers (nombre de	
fichiers et espace disque total).	

[LogOptions]

ShowUnknown=Yes	Affiche les sessions dont MDStats n'a pas pudéterminer si elles étaient entrantes ou sortantes, SMTP ou POP.
ShowSmtpInbound=Oui	Affiche les sessions SMTP entrantes.
ShowPopInbound=Oui	Affiche les sessions POP entrantes (vérification du courrier).
ShowSmtpOutbound=O ui	Affiche les sessions SMTP sortantes.
ShowPopOutbound=Oui	Affiche les sessions POP sortantes (MultiPOP, DomainPOP).
ShowRFC822=Oui	Affiche les distributions du courrier local RFC822.
ShowSmtpHelo=Oui	Pour les sessions SMTP entrantes, afficher le domaine HELO dans la colonne Host.
IgnoreEmptyPop=Oui	Ignore les contrôles de courrier lorsque aucun courrier n'a été distribué.
ShowImap=Oui	Affiche les sessions IMAP.
[Remap]	Remappage des lettres de lecteur ; pour exécuter MDStats à partir d'une machine différente de celle sur laquelle MDaemon est installé.
C:=\\server\c	Lors de la lecture du fichier MDaemon.ini, Remplacer "C :" par "\Nserveur\c".
[Spécial]	
OnlyOneInstance=No	Autorise l'exécution d'une seule instance de MDStats. Si vous tentez de l'ouvrir à nouveau, l'instance déjà en cours d'exécution sera activée.

Voir :

Paramètres de la ligne de commande de MDStats

6.3.5.2 Paramètres de ligne de commande MDStats

<u>Remarque</u> : tous les paramètres de la ligne de commande <u>ne sont pas</u> sensibles à la casse.

Numéro 1 à 8	Affiche la file d'attente spécifiée dans la page File d'attente.
	= File distante
	= File locale
	= File de relance
	= File LAN
	= File File RAW
	= Bad Queue
	= File d'attente SmtpIn
	= File d'attente de sauvegarde
/L[N] [InputFile] [OutputFile]	Produit un rapport sous forme de fichier journal. Le fait de spécifier un "N" après le "L" signifie qu'il ne faut pas sauvegarder dans un fichier délimité par des virgules.
/A	Si vous produisez un rapport sous forme de fichier journal, ajoutez les nouvelles informations au fichier de sortie plutôt que de les écraser.

Section

7 Autres fonctionnalités de MDaemon

7.1 MDaemon et fichiers texte

MDaemon utilise un certain nombre de fichiers texte pour stocker certaines de ses données, les modèles de messages générés par le système et les paramètres de configuration, ce qui lui confère une grande souplesse. Vous pouvez créer de nouveaux fichiers texte à partir de MDaemon en utilisant le menu Fichier | Nouveau ". Cela peut être utile pour créer rapidement des fichiers de données à utiliser avec les répondeurs automatiques et diverses autres fonctionnalités de MDaemon, telles que les fichiers RAW.

Modifier les fichiers de MDaemon

Les différents fichiers de données de MDaemon sont en texte brut et peuvent être édités dans le Bloc-notes. Vous pouvez facilement ouvrir n'importe lequel de ces fichiers depuis MDaemon en utilisant le menu Fichier | Ouvrir " Fichier texte vide. Non (par défaut), MDaemon recherche les fichiers *.txt dans le dossier \app\ de MDaemon . Dans la liste déroulante*Fichiers de type :*, sélectionnez "Tous les fichiers" pour afficher le reste des fichiers contenus dans ce dossier.

7.2 Contrôle du serveur à distance par e-mail

Il est possible d'accéder à distance à de nombreuses fonctions de MDaemon en utilisant le système de transport de courrier électronique lui-même, en envoyant un e-mail spécialement formaté au compte système de MDaemon, "MDaemon@<Domaine de MDaemon>". Les messages envoyés au serveur sont stockés dans le répertoire des messages du serveur, comme pour n'importe quel autre utilisateur.

Certains de ces messages de commande nécessitent un compte valide sur le serveur. Pour les commandes qui nécessitent un compte valide, le message doit être authentifié au cours du processus SMTP à l'aide de SMTP AUTH.

Il existe deux grandes catégories de commandes qui peuvent être utilisées dans les messages électroniques : <u>Liste de diffusion</u>, et le <u>courrier électronique général</u>.

Voir :

 Contrôle des listes de diffusion

 Commandes générales de courrier électronique

7.2.1 Contrôle des listes de diffusion et catalogues

Aucune de ces commandes ne nécessite l'ouverture d'un compte sur le serveur. Les paramètres contenus entre [crochets] sont facultatifs. Exemple : "nom [adresse]" peut être saisi comme "Michael" seul ou avec le paramètre facultatif ajouté : "Michael user1@example.com". Les messages doivent être envoyés à "mdaemon@[MDaemon

959

domain]" avec chaque commande et les paramètres associés contenus sur une seule ligne dans le corps du message.

COMMAND ES	PARAMÈTRES	DESCRIPTIONS
SUBSCRIB E	listname [address] [{real name}] [(pass)]	L'expéditeur est ajouté aux membres de la liste spécifiée, à condition que cette liste existe et qu'elle autorise les abonnements à distance. Si une adresse facultative est spécifiée après le nom de la liste, c'est cette adresse qui est ajoutée aux membres de la liste et non l'adresse figurant dans le champ FROM : du message d'abonnement. Dans ce cas, un Nom réel peut être ajouté pour l'abonné en l'incluant entre accolades (par exemple {Bill F}. Si le mot de passe de la liste suit cette commande (les parenthèses sont nécessaires), la commande sera honorée même si la fonction d'abonnement de cette liste est désactivée.
		Exemple : SUBSCRIBE list@example.com SUBSCRIBE list@example.com me@example.com {BillF} SUBSCRIBE list@example.com you@example.org (PASS)
UNSUBSCR IBE ou SIGNOFF	listname [address] [(pass)]	L'auteur est radié de la liste spécifiée, à condition que cette liste existe et qu'elle contienne l'auteur en tant que membre actuel. Si une adresse facultative est spécifiée après le Nom de la liste, c'est cette adresse qui est supprimée de la liste et non l'adresse figurant dans le champ À : du message de désabonnement. Si le mot de passe de la liste suit cette commande (les parenthèses autour du mot de passe sont nécessaires), la commande sera honorée même si la fonction de désabonnement de cette liste est désactivée. Exemple :
		UNSUBSCRIBE list@example.com (listPASS) SIGNOFF list@example.com me@example.com
DIGEST	nom de la liste [adresse]	L'expéditeur est configuré pour recevoir le courrier de la liste au format "digest". Si une adresse facultative est spécifiée après

		le nom de la liste, cette adresse est configurée en mode condensé. Exemple : DIGEST list@example.com DIGEST list@example.com user1@example.com
NORMAL	nom de la liste [adresse]	L'expéditeur est configuré pour recevoir le courrier de la "liste" au format normal (non digéré). Si une adresse optionnelle est spécifiée après le nom de la liste, cette adresse est configurée pour recevoir le courrier au format normal à la place de l'expéditeur.
		Exemples : NORMAL list@example.com
		NORMAL list@example.com userl@altn.com
NOMAIL	nom de la liste [adresse]	Cette commande configure l'adresse en mode nomail. Le compte entrera dans un état de suspension et ne recevra plus de trafic de liste. Si aucune adresse n'est spécifiée, c'est l'expéditeur du message qui sera utilisé.
		Exemple :
		NOMAIL list@example.com me@example.com
MAIL	nom de la liste [adresse]	Cette commande permet à l'adresse de revenir du mode nomail au mode normal. Si aucune adresse n'est spécifiée, c'est l'expéditeur du message qui sera utilisé. Exemple :
		MES LISTES DE DIFFUSION list@example.com MES LISTES DE DIFFUSION list@example.com m¢
NOM RÉEL	nom de la liste [adresse] {nom réel}	Cette commande configure le Nom réel de l'"adresse" qui est membre de la liste "listname" à la valeur donnée. Votre nom réel doit être entouré des caractères { et }. Exemple :
		REALNAME list@example.com {Bill Farmer}
LIST	[Mot de passe de liste] [list password]	Fournit des informations sur une liste de diffusion. Si le Nom de la liste n'est pas fourni, un résumé de toutes les listes est renvoyé. Si le mot de passe de la liste est fourni, des informations plus détaillées sur la liste sont renvoyées.

Exemple : LIST list@example.com Lz\$12

Voir :

<u>Contrôle d'un serveur distant par courrier électronique</u>

7.2.2 Commandes générales

Il s'agit de commandes générales qui peuvent être envoyées au Compte système par email. Les messages doivent être envoyés à "mdaemon@[MDaemon domain]" avec chaque commande et les paramètres associés contenus sur une seule ligne dans le corps du message.

COMMANDES	PARAMÈ TRES	DESCRIPTIONS
AIDE	aucun	Une copie du fichier NEWUSERHELP.DAT est traitée et renvoyée à l'auteur du message.
STATUS	aucun	Un rapport d'état sur les opérations du serveur et les états actuels sera envoyé à l'expéditeur du message. Dans la mesure où les informations contenues dans ce rapport d'état sont considérées comme privées, l'utilisateur qui demande le rapport doit être authentifié en tant qu'administrateur.
		Exemple : STATUS

Voir :

<u>Contrôle de serveurs distants par courrier électronique</u>

7.3 Spécification des messages RAW

7.3.1 Spécification des messages RAW

MDaemon prend en charge un format de message simple et puissant appelé RAW mail. L'objectif du système de courrier RAW est de fournir un format simple et standard que les logiciels tels que MDaemon peuvent utiliser pour créer des messages beaucoup plus complexes conformes à la norme RFC-2822. L'utilisation d'agents de transport de courrier tels que RAW permet au logiciel client de se décharger sur le serveur de toutes les tâches compliquées liées au respect des normes de courrier Internet. Le courrier RAW se compose d'une série d'en-têtes de texte obligatoires et facultatifs, suivis d'un corps du message. La plupart des en-têtes sont constitués d'un jeton suivi d'une valeur entourée de symboles <>. Chaque ligne d'en-tête se termine par une combinaison de caractères <CRLF>. Les en-têtes sont séparés du corps du message par une ligne vide et sont insensibles à la casse. Les en-têtes*from* et *to* sont les seuls à être obligatoires. Tout le texte, les en-têtes et le corps du message, est du texte ASCII brut et doit être contenu dans un fichier qui se termine par l'extension ".raw" (par exemple "mon-message.raw"). Dans ce cas, pour mettre le message en file d'attente, placez le fichier*.raw dans lafile RAW de MDaemon(généralement située à "C:MDaemon\Queues\Raw").

Contourner le filtre de contenu

Non (par défaut), les messages RAW passent par le Filtre des contenus comme des messages normaux. Si vous souhaitez qu'un message RAW donné contourne le filtre, commencez le nom du fichier par "p" ou "P". Exemple : "P_mon-message.raw" contournera le Filtre de contenu, mais "mon-message.raw" sera traité normalement.

Le fait de contourner le Filtre de contenu empêchera les messages d'être signés DKIM. Connexion. Si vous avez configuré MDaemon pour qu'il signe tous les messages, cela peut entraîner des problèmes de distribution. Si vous souhaitez que MDaemon signe les messages RAW configurés pour contourner le Filtre de contenu, vous pouvez utiliser l' optionxflag=sign décrite ci-dessous.

En-têtes RAW From : dans l'en-tête FROM

De <mailbox@example.com></mailbox@example.com>	Ce champ contient l'adresse e-mail de l'expéditeur.
To <mailbox@example.com [,<br="">mailbox@example.com]></mailbox@example.com>	Ce champ contient l'adresse électronique du ou des destinataires. Il est possible de spécifier plusieurs destinataires en les séparant par une virgule.
ReplyTo <mailbox@example.com></mailbox@example.com>	Une adresse électronique facultative à laquelle les réponses à ce message seront acheminées.
CC <maibox@example.com[, mailbox@example.com]></maibox@example.com[, 	Liste facultative des destinataires de la copie to de ce message. Il est possible de spécifier plusieurs destinataires en les séparant par une virgule.
Objet <texte></texte>	Objet du message facultatif.
En-tête <header :="" valeur=""></header>	Permet de placer explicitement des combinaisons En-tête/valeur dans le message. Cela vous permet de placer des

en-têtes personnalisés ou non standard dans vos messages *.raw.

Champs spéciaux pris en charge par RAW

Fichier joint et encodage

x-flag=attach <filepath, method> [-x]

Exemple : x-flag=attach <c:\utils\pkzip.exe, MIME> -x

Ce X-FLAG spécifie la valeur "ATTACH" ainsi que deux paramètres compris dans les caractères <>. Le premier paramètre est un Chemin du fichier qui doit être joint au message. Le second paramètre, séparé du premier par une virgule, spécifie la méthode de codage à utiliser pour joindre le message. MDaemon prend en charge deux valeurs pour ce paramètre. La méthode MIME indique au serveur d'utiliser la méthode d'encodage des messages Base64, standard sur Internet. La méthode ASCII indique au serveur d'importer simplement le fichier dans le message. Un paramètre -X facultatif à la fin de la chaîne indique au serveur de supprimer le fichier du disque une fois qu'il a été joint.

Notification d'état de remise

```
x-flag=confirm delivery
```

Lors de la conversion d'un message RAW contenant cet indicateur en courrier RFC-2822, la chaîne est transformée en "Return-Receipt-To : <sender@example.com>".

Placement de combinaisons d'en-tête/valeur spécifiques dans le message RFC-2822

En-tête <en-tête : valeur>

Si vous souhaitez placer une combinaison en-tête/valeur spécifique dans le message RFC-2822 qui sera généré à partir d'un fichier RAW, vous devrez utiliser la macro HEADER énumérée dans la section En-têtes RAW ci-dessus. Exemple : si vous voulez que l'en-tête "Delivered-By : mail-machine@example.com" soit placé dans le message RFC-2822, vous devez placer ceci : "header <Delivered-By : mail-machine@example.com>" dans le message RAW. Notez que la macro "en-tête" requiert à la fois le champ et la valeur. Vous pouvez placer autant de macros "header" que nécessaire dans un en-tête TO :.

Messages RAW signés par DKIM

x-flag=sign

Dans un fichier*.raw, cette commande spéciale entraîne la signature DKIM du message RAW. Cette commande ne doit être utilisée que dans les messages RAW que vous avez configurés pour contourner le Filtre de contenu (en commençant leur nom de fichier par "p" ou "P"). Vous ne devez pas utiliser cette commande dans les messages RAW normaux qui sont traités par le filtre. Ces messages seront signés normalement.



Tous les messages RAW générés par le Filtre de contenu utiliseront automatiquement la commandex-flag=sign.

Exemples de messages RAW

```
Exemple 1:
```

de <mdaemon@altn.com> à <user01@example.com>

Bonjour John !

Exemple 2 :

```
de <user01@example.com>
à <user09@example.net>
objet <Fichiers demandés>
X-FLAG=CONFIRM DELIVERY
X-FLAG=ATTACH <c:\docs\files\data01.zip, MIME> -X
```

Voici tous les fichiers que vous avez demandés.

7.4 Fichiers sémaphores

MDaemon prend en charge les Fichiers sémaphores, qui peuvent être utilisés à diverses fins, notamment pour permettre à MDaemon d'effectuer des actions spécifiques. Périodiquement, MDaemon recherche l'existence de ces fichiersdans le sousdossier\APP\. S'il en trouve un, le comportement associé est déclenché et le fichier sémaphore est supprimé. Il s'agit d'un mécanisme simple qui permet aux administrateurs et aux développeurs de manipuler MDaemon sans avoir à s'occuper de l'interface. Voici une liste des sémaphores et de leur fonction :

NOM DE ACTION FICHIER

- ACLFIX.SE Exécute la routine de nettoyage des fichiers ACL. М

ADDUSER.S Ce sémaphore crée de Nouveaux comptes. Il est utilisé pour forcer MDaemon à ajouter de nouveaux enregistrements à la fin du fichier ЕM USERLIST. DAT sans provoquer une reconstruction complète de la base de données des utilisateurs, ce qui pourrait prendre du temps. Chaque ligne de ce fichier doit être un enregistrement complet du type spécifié dans la section Fonctions de Gestion des Comptes de l'API de MDaemon (voir MD-API.html dans le sous-dossier

\docs\API de MDaemon). Plusieurs Nouveaux comptes peuvent être spécifiés - un enregistrement de compte par nouvelle ligne. MDaemon traitera le fichier une ligne à la fois et ajoutera chaque nouveau compte. Vous pouvez créer ADDUSER.LCK pour verrouiller le fichier pendant que vous le mettez à jour. MDaemon ne touchera pas à ADDUSER.SEM tant qu'il n'aura pas supprimé ADDUSER.LCK. Pour voir un exemple de fichier ADDUSER.SEM, ouvrez ADDUSER.SMP dans votre répertoire APP avec un éditeur de texte.

ALERT.SEM Affiche dans une fenêtre pop-up le contenu du fichier sémaphore à tous les utilisateurs du Webmail qui sont fichés au moment de la création du fichier. Aucun utilisateur n'est cependant affiché à tous les utilisateurs immédiatement - il est affiché à chaque utilisateur individuellement la prochaine fois que son navigateur envoie une requête au serveur de messagerie Web.

Note : Contrairement aux autres fichiers sémaphores, ce fichier est spécifique au Webmail. Dans ce cas, au lieu de le placer dans le répertoire \app, il doit être placé dans le répertoire\MDaemon\WorldClient\.

- ALIAS.SEM Recharge le(s) fichier(s) de données d'alias.
- AUTORESPE Recharge le(s) fichier(s) d'exception de l'autorépondeur.
- BATV.SEM Recharge le(s) fichier(s) de données de la protection contre la rétrodiffusion (BATV).
- BAYESLEAR Ce SEM lance manuellement le processus d'apprentissage bayésien. N.SEM Cela revient à cliquer sur le bouton Apprendre dans l'onglet Bayesian du Filtre anti-spam. De : ceci démarre la procédure d'apprentissage bayésien même si l'apprentissage bayésien est désactivé.
- BLOCKLIST Recharge les fichiers de données de la liste de blocage.
- CFILTER.SRecharge les règles du Filtre anti-spam, efface les données mises en
cache du Filtre anti-spam, recharge le fichier Liste d'autorisation
(pas de filtrage) 742
- CLEARQUOTLes résultats des contrôles de quotas d'utilisateurs sont conservésACOUNTS.Sdans le fichier quotacounts.dat. Si vous souhaitez effacer laEMvaleur de quota mise en cache pour un utilisateur, ajoutez l'adresse
électronique de l'utilisateur à ce fichier SEM et placez-le ensuite

dans le dossier Dossiers. Si un astérisque (*) est présent sur une ligne, le fichier entier sera supprimé, ce qui aura pour effet d'invalider tous les quotas mis en cache.

CREDSMATC Recharge la liste des exceptions en matière de correspondance des HEXEMPTLI données d'identification 559.

DELUSER.S Vous pouvez utiliser ce fichier sémaphore pour supprimer un ou plusieurs comptes utilisateurs. Créez un fichier texte contenant les adresses de chaque compte à supprimer (une adresse par ligne), nommez le fichier DELUSER.SEM, puis placez-le dans le répertoire \app\ de MDaemon . MDaemon supprimera les comptes puis le fichier DELUSER.SEM. Si vous souhaitez supprimer un compte mais pas son Dossier courrier, ajoutez "^" à l'adresse (par exemple frank@example.com^).

- DMARCEXEM Recharge la <u>liste des exceptions DMARC</u> [560]. PTLIST.SE
 - DNS.SEM Recharge les <u>serveurs DNS de Windows</u> at les paramètres DNS du Filtre anti-spam.
- DOMAINSHA Recharge le fichier de données de partage de domaine.

RING.SEM

EDITUSER. Ce sémaphore est utilisé pour mettre à jour des enregistrements d'utilisateurs spécifiques dans le fichier USERLIST. DAT sans SEM reconstruire complètement le système, ce qui pourrait prendre beaucoup de temps. Pour mettre à jour des enregistrements d'utilisateurs spécifiques dans USERLIST. DAT, créez un fichier nommé EDITUSER.SEM qui comprend un enregistrement de remplacement complet, un enregistrement par ligne, pour tous les enregistrements d'utilisateurs que vous souhaitez modifier. Chaque enregistrement doit être construit selon le format USERLIST. DAT décrit dans l'article de la *** connaissancesUserlist File FormatMDaemon mais il doit commencer par l'adresse électronique de l'enregistrement d'origine, suivie d'une virgule. MDaemon traite le fichier EDITUSER.SEM ligne par ligne. Vous pouvez créer EDITUSER.LCK pour verrouiller le fichier pendant que vous le mettez à jour. MDaemon ne touchera pas à EDITUSER.SEM tant que EDITUSER.LCK n'aura pas été supprimé. Pour voir un exemple de fichier EDITUSER.SEM, OUVREZ EDITUSER.SMP dans votre répertoire \APP \ avec un éditeur de texte.

EXITNOW.S Ferme MDaemon.

ΕM

N.SEM

SEM

- GATEWAYS. Pour des performances optimales, MDaemon conserve sa liste de SEM passerelles en mémoire. Créez un fichier GATEWAYS.SEM dans le répertoire APP de MDaemon pour qu'il recharge le fichier gateways.dat.
- GREYLIST. Recharge le(s) fichier(s) de données de la liste grise.
- GROUPS.SE Recharge le(s) fichier(s) de données de regroupement de comptes.
- GRPLIST.S Recharge le cache interne des noms de Liste de diffusion.
- HANGUPG.S Force un raccrochage conditionnel du dispositif RAS. MDaemon EM attend que toutes les sessions de messagerie en cours soient fermées, puis raccroche la session RAS.
- HANGUPR.SForce le raccrochage inconditionnel du dispositif RAS. Dans ce cas,EMla fermeture est immédiate et inconditionnelle, sans tenir compte
des sessions de courrier en cours sur la connexion.
- HOSTSCREE Recharge le(s) fichier(s) de données de l'Écran d'hôte.
- IPSCREEN. Recharge le(s) fichier(s) de données de l'Écran IP.
- IPSHIELD. Le fichier IPShield.dat est mis en cache dans la mémoire pour SEM augmenter la vitesse d'accès. Utilisez IPSHIELD.SEM pour recharger le fichier en mémoire.
- LDAPCACHE Recharge le(s) fichier(s) de données de l'utilisateur LDAP et de la .SEM passerelle.
- LOCKSEMS. Empêche tout traitement du fichier sémaphore jusqu'à ce que SEM l'utilisateur le supprime.

LOGSETTIN GS.SEM	Recharge les paramètres des fichiers de journalisation.
MDSPAMD.S EM	Recharge la Liste anti-spam (autorisation) du Filtre anti-spam (destinataires) et MDSPAMD, ce qui l'oblige à réinitialiser toutes ses données de configuration.
MINGER.SE M	Redémarre les serveurs.
MXCACHE.S EM	Recharge le(s) fichier(s) de données du MX Cache.
NODNSBL.S EM	Recharge le fichier de liste d'autorisation DNSBL.
NOPRIORIT Y.SEM	Force MDaemon à recharger le fichier NoPriority.dat.
ONLINE.SE M	MDaemon crée ce fichier sémaphore dès qu'il réussit à établir une connexion RAS avec le fournisseur d'accès. MDaemon supprime le sémaphore une fois la connexion terminée. Si vous souhaitez savoir quand MD utilise le sous-système RAS, ce fichier est utile.
POSTDIAL. SEM	MDaemon crée ce fichier immédiatement après la fermeture d'une connexion établie par MDaemon.
PREDIAL.S EM	MDaemon crée ce fichier juste avant d'essayer d'utiliser RAS/DUN. Cela permet à d'autres logiciels de détecter le moment où ils doivent libérer le port d'accès à distance pour que MDaemon puisse l'utiliser.
PRIORITY. SEM	Recharge le(s) fichier(s) de données du Courrier prioritaire.
PROCBAD.S EM	Lance la distribution du contenu de la mauvaise file d'attente.
PROCDIG.S EM	Lance la construction et la diffusion des listes Listes de diffusion.
PROCHOLDI NG.SEM	Lance la livraison du contenu de la file d'attente.

PROCNOW.S EM	Vérifie la présence de courrier distant et distribue le courrier distant en file d'attente.
PROCREM.S EM	MDaemon passe immédiatement en mode de traitement du courrier et traite tout le courrier distant.
PROCRETR. SEM	Déclenche la distribution du contenu de la File de relance.
PRUNE.SEM	Recharge les paramètres d'élagage automatique.
PUBLICSUF FIX.SEM	Recharge le fichier de <u>suffixe public.</u>
QUEUE.SEM	Ce fichier sémaphore est utilisé pour activer/désactiver les Files d'attente. Le fichier peut contenir un nombre quelconque de lignes, mais chacune d'entre elles doit contenir l'une des chaînes suivantes (une par ligne) : Activer en entrée, Activer à distance, Activer localement, ou Désactiver en entrée, Désactiver à distance, Désactiver localement.
RCPTBLOCK LIST.SEM	Recharge la <u>liste de blocage des destinataires</u> [597].
RESTART.S EM	Arrête puis démarre MDaemon.
RESTARTCF .SEM	Arrête et redémarre CFEngine.exe (l'exécutable du filtre de contenu).
RESTARTWC .SEM	Redémarrer de Redémarrez MDaemon Webmail. Cela ne fonctionne que lorsque le Webmail est exécuté à l'aide de son propre <u>serveur</u> <u>Web intégré</u>
RELOADCAC HE.SEM	Recharge tous les paramètres et fichiers de données mis en cache, à l'exception des paramètres et fichiers du Filtre de contenu.
REVERSEEX CEPT.SEM	Recharge le fichier d'exception des recherches inversées.
SCHEDULE. SEM	Recharge le(s) fichier(s) de données de planification.

SENDERBLO CKLIST.SE M	Recharge la <u>liste de blocage des expéditeurs</u> [595].
SPAMHONEY POTS.SEM	Recharge le(s) fichier(s) de données sur les pots de miel de spam.
SPF.SEM	Recharge les fichiers de données SPF, DKIM et VBR.
SUPPRESS. SEM	Recharge les paramètres de la Liste de blocage et efface les paramètres de domaines mis en cache.
TARPIT.SE M	Recharge les fichiers de données tarpit et d'Écran dynamique.
TRANSLAT. SEM	Recharge les fichiers d'en-tête d'une traduction.
TRAY.SEM	Redessine l'icône de MDaemon dans la barre d'état système.
TRUST.SEM	Les domaines ou adresses IP autorisés sont conservés en mémoire pour des performances optimales. Si vous devez recharger ces paramètres manuellement, vous pouvez créer TRUST.SEM pour le faire.
UPDATEAV. SEM	Lance la mise à jour des définitions de l'antivirus.
UPDATESA. SEM	Mises à jour du Filtre anti-spam.
USERLIST. SEM	Recharge le fichier USERLIST.DAT. Utilisez cette option lorsque vous modifiez le fichier USERLIST.DAT et que MDaemon doit le recharger.
WATCHDOG. SEM	MDaemon vérifie et retire ce sémaphore du répertoire APP à des intervalles d'environ 10 à 20 secondes. Ce fichier peut être utilisé par des applications externes pour vérifier si MDaemon est en cours d'exécution. Si ce fichier reste dans le répertoire APP pendant plus de 20 secondes, c'est une bonne indication que MDaemon n'est plus en cours d'exécution.

7.5 Re-routage

Un fichier de message en attente dans une file d'attente contient généralement dans ses en-têtes toutes les informations nécessaires pour que le message soit délivré à l'endroit voulu. Certains en-têtes stockés dans le fichier (comme l'en-tête X-MDaemon-Deliver-To) fournissent à MDaemon des instructions sur l'endroit et le destinataire du message. Cependant, il est parfois nécessaire ou utile d'outrepasser ces informations et de fournir des alternatives spécifiques à l'endroit et à la personne à qui un message doit être envoyé. Les feuilles de route constituent justement un tel mécanisme. Une feuille de route est un fichier qui fournit à MDaemon des instructions très précises sur l'endroit et le destinataire d'un message. Si une feuille de route est présente pour un fichier de message particulier, ce sont les paramètres de la feuille de route, et non ceux du fichier .MSG lui-même, qui contrôlent où et à qui le message est envoyé.

Les feuilles de route se terminent par l'extension .RTE. Dans un exemple, si un fichier de messages en attente d'envoi s'appelle "MD0000.MSG", le fichier de feuille de route correspondant à ce message s'appellera MD0000.RTE et devra se trouver dans le même dossier (file d'attente) que le fichier de messages.

Le format d'une feuille de route est le suivant :

[RemoteHost] DeliverTo=example.net

Cette section d'une feuille de route indique à MDaemon le serveur auquel le fichier.MSGcorrespondant doit être envoyé. MDaemon tentera toujours d'établir une connexion directe avec cet hôte en essayant de router le message dans un délai aussi court que possible. Un seul hôte peut être spécifié.

```
[Port]
Port=xxx
```

Ce commutateur indique le port sur lequel la connexion TCP/IP et la tentative de livraison doivent être effectuées. Le Port 25 est le Non (par défaut = 25) pour le courrier électronique SMTP.

```
[LocalRcpts]
Rcpt0=address@example.com
Rcpt1=other-address@example.com
Rcpt2=yet-another-address@example.com
[RemoteRcpts]
Rcpt0=address@example.net
Rcpt1=other-address@example.net
Rcpt2=yet-another-address@example.net
```

Ces sections de la feuille de route vous permettent de spécifier un nombre quelconque de destinataires locaux et distants qui doivent recevoir une copie du fichier

.MSGassocié. Les adresses distantes et locales des destinataires doivent être séparées et placées dans les sections[LocalRcpts] et [RemoteRcpts] correspondantes.

Les feuillets de route constituent un bon mécanisme pour délivrer ou rediriger le courrier électronique, mais ils ne sont généralement pas nécessaires. MDaemon utilise les feuilles de route dans le cas des courriers de listes de diffusion " routés ". Lorsqu'une liste de diffusion est configurée pour acheminer une seule copie du message de la liste vers un Hôte distant, un bordereau de route est utilisé pour accomplir cette tâche. Il s'agit d'une méthode de distribution du courrier très efficace lorsque vous avez des adresses de masse à distribuer, puisqu'une seule copie du message est nécessaire et qu'il est possible de spécifier un nombre illimité de destinataires. Cependant, tous les Hôte distants ne permettent pas ce type de routage. Comme ce sont eux qui doivent distribuer une copie du fichier de messages à chaque adresse, certains hôtes imposent une limite supérieure au nombre de destinataires qu'ils vous autorisent à spécifier.
Section

8 Création et utilisation de certificats SSL

Lorsque vous utilisez la boîte de dialogue SSL & TLS pour créer des certificats, MDaemon génère des certificats auto-signés. Dans ce cas, l'émetteur du certificat, ou Autorité de Certification (AC), est le même que le propriétaire du certificat. Ceci est parfaitement valide et autorisé, mais comme l'autorité de certification ne figure pas dans la liste des autorités de certification de confiance de vosutilisateurs, chaque fois qu'ils se connectent à l'URL HTTPS de Webmail ou de MDaemon Remote Admin, il leur est demandé s'ils souhaitent ou non se rendre sur le site et/ou installer le certificat. Une fois qu'ils auront accepté d'installer le certificat et qu'ils auront fait confiance audomaine devotre Webmailen tant qu'autorité de certification valide, ils ne verront plus le message d'alerte de sécurité lorsqu'ils se connecteront à Webmail ou à MDaemon Remote Admin.

En revanche, lorsqu'ils se connectent à MDaemon via un client de messagerie tel que Microsoft Outlook, ils n'ont pas la possibilité d'installer le certificat. Ils pourront choisir de continuer à utiliser le certificat temporairement, même s'il n'est pas validé. Chaque fois qu'ils démarreront leur client de messagerie et se connecteront au serveur, ils devront choisir de continuer à utiliser le certificat non validé. Pour éviter cela, vous pouvez soit obtenir un certificat auprès d'une autorité de certification, telle que Let's EncryptLet' [632], ou exporter votre certificat auto-signé et le distribuer à vos utilisateurs par courrier électronique ou par un autre moyen. Ils pourront alors installer manuellement votre certificat et s'y fier afin d'éviter les messages d'alerte à venir.

Création d'un certificat

Pour créer un certificat à partir de MDaemon :

- Ouvrez la boîte de dialogue SSL & TLS dans MDaemon (cliquez sur Sécurité | Paramètres de sécurité | SSL & TLS | MDaemon).
- 2. Cochez la case Activer SSL, STARTTLS et STLS.
- 3. Cliquez sur Créer un certificat.
- 4. Dans la zone de texte intitulée **Nom d'hôte**, entrez le domaine auquel le certificat appartient (par Exemple, "*mail.example.com*").
- 5. Dans la zone de texte intitulée "*Nom de l'organisation/entreprise*", saisissez le nom de l'organisation ou de la société propriétaire du certificat.
- 6. Dans "Alternative host names...", tapez tous les autres noms de domaine que vos utilisateurs utiliseront pour accéder à votre serveur (par exemple, "*.example.com", "example.com", "mail.altn.com", et ainsi de suite).
- 7. Choisissez une longueur de clé de cryptage dans la liste déroulante.
- 8. Choisissez le Pays/région où réside votre serveur.
- 9. Cliquez sur OK.

Utilisation de certificats émis par une autorité de certification tierce

Si vous avez acheté ou généré un certificat à partir d'une source autre que MDaemon, vous pouvez toujours utiliser ce certificat en utilisant la console de gestion Microsoft pour l'importer dans le magasin de certificats utilisé par MDaemon. Pour ce faire, sous Windows, procédez comme suit

- 1. Ouvrez la console de gestion Microsoft (tapez "mmc" dans la zone de texte sous le menu **Démarrer de** Windows et appuyez sur **Entrée**).
- 2. Cliquez sur Fichier | Ajouter/Supprimer un Snap-in... dans la barre de menus (ou appuyez sur Ctrl+M sur votre clavier).
- 3. Dans le volet *Snap-ins disponibles*, cliquez sur **Certificats**, puis sur **Ajouter**.
- 4. Dans la boîte de dialogue *Snap-in Certificats*, choisissez **Compte de l'ordinateur**, puis cliquez sur **Suivant**.
- 5. Dans la boîte de dialogue *Sélectionner un ordinateur*, choisissez **Ordinateur local**, puis cliquez sur **Terminer**.
- 6. Cliquez sur OK.
- Sous Certificats (ordinateur local), si le certificat que vous importez est autosigné, cliquez sur Autorités de certification racine de confiance, puis sur Certificats. Si le certificat n'est pas auto-signé, cliquez sur Personnel.
- 8. Dans le volet Actions, cliquez sur **Autres actions** | **Toutes les tâches** | **Importer**. .., puis sur **Suivant**.
- 9. Saisissez le chemin d'accès au fichier du certificat que vous souhaitez importer (en utilisant le bouton Parcourir si nécessaire), puis cliquez sur **Suivant**.
- 10. Cliquez sur Suivant, puis sur Terminer.

12 AM n'affiche que les certificats dont les clés privées utilisent le format d'échange d'informations personnelles (PKCS #12). Si votre certificat importé n'apparaît pas dans la liste, il se peut que vous deviez importer un fichier*.PEM, qui contient à la fois une clé de certificat et une clé privée. L'importation de ce fichier en suivant la même procédure que celle décrite ci-dessus le convertira au format PKCS #12.

Utiliser Let's Encrypt pour gérer votre certificat

Let's Encrypt est une autorité de certification (AC) qui fournit des certificats gratuits via un processus automatisé conçu pour éliminer le processus actuellement complexe de création, de validation, de signature, d'installation et de renouvellement manuels des certificats pour les sites web sécurisés.

Dans le cadre de l'utilisation du processus automatisé de Let's Encrypt pour gérer un

certificat, l'écran <u>Let's Encrypt</u> and est fourni pour vous aider à configurer et à exécuter facilement le script PowerShell inclus dans le dossier

"MDaemon\LetsEncrypt". L'exécution du script permet de tout configurer pour Let's Encrypt, y compris de placer les fichiers nécessaires dans le dossier HTTP du Webmail pour relever le défi http-01. Il utilise le <u>nom d'hôte SMTP</u> [167] du <u>domaine par défaut</u> [184] comme domaine pour le certificat, inclut tout <u>autre nom d'hôte que</u> vous avez spécifié, récupère le certificat, l'importe dans Windows et configure MDaemon pour qu'il utilise le certificat pour MDaemon, Webmail et Remote Admin. Dans le dossier "MDaemon\Logs\", le script crée un fichier journal appelé LetsEncrypt.log. Ce fichier journal est supprimé et recréé à chaque fois que le script est exécuté, et il inclut la date et l'heure début du script. De plus, des e-mails de notification seront envoyés lorsque des erreurs se produisent si vous spécifiez un *E-mail de l'administrateur pour les notifications*. Voir la rubrique Let's Encrypt

Voir :

SSL & TLS 613

977

Index

- 2 -

2FA 771

- A -

AC MDaemon 974 Accès aux ressources du réseau 537 ACL 327.797 Activation Collecte du courrier DomainPOP 152 Dossiers publics 118 Serveur Webmail 339 Activation de MDaemon Connector 410 Active Directory 880, 884 884 Authentification 880 Authentification dynamique Création de comptes 880 Mise à jour des comptes 880 Modèle 880 Port (passerelle) 270 Sécurité des fichiers 880 Serveur (Passerelle) 270 Suppression de comptes 880 Surveillance 887 Surveillance permanente 880 Synchronisation 887 Synchronisation avec MDaemon 880 Utilisation avec les listes de diffusion 315 Vérification (Passerelle) 270 ActiveSync Activation 441 Activer/désactiver le domaine 225 Affectation de paramètres clients à des groupes 497 Assignation de paramètres clients à des Types de clients 504 Attribuer des Politiques 462 Clients 488 Clients (Domaine) 252 Débogage 457 Désactivation 441 Diagnostics 457

Domaine (Clients) 252 Domaines 462 Effacer complètement 488 Effacer des terminaux 488 Effacer données 488 Effacer partiellement 488 Effacer un terminal à distance 488 Éléments du menu d'accès rapide 441 Fichiers dumpers 457 Gérer les clients 447 Groupes 497 Liste blanche 454 Liste noire 454 Mon compte 243, 479 Mon compte Clients 827 443.457 Options avancées Options de compte 819 Paramètres avancés de la politique 441 Paramètres client (globaux) 447 Paramètres clients 488.827 Paramètres clients de domaines 226 Paramètres clients des comptes 820 Paramètres clients globaux 443 Paramètres clients pour les domaines 233 Paramètres de domaine 226, 233 Paramètres globaux 447 Pas de journalisation 457 488 Périphériques Périphériques (Domaine) 252 Politique attribuée 242 470 Politiques Politiques par défaut 462 Politiques pour les domaines 242 Restrictions 459 Restrictions de protocoles 459 Sécurité 454 Service de découverte automatique 441 Sondages 457 Suppression d'appareils 488 Suppression de périphériques 488 Tuning 443 Types de clients 504 315 AD Administrateur Domaine 812 Global 812 Administrateurs 875 Administrateurs au niveau du serveur 812

978

Administrateurs de domaine 812 Admins/Attachments 708 Adresse Liste de blocage 595.597 Suppression 595.597 Adresse distante : vérification d'adresse 923 Adresse distante : vérification des adresses 270 Adresse e-mail du compte système 525 Adresses IP De confiance 554 Adresses IP bloquées 654 ADSP 564 Affichage 70, 78 Affichage des informations d'identification WebAuthn 765 afficher la police de caractères 521 Aide de WorldClient 337 Aide en ligne 65 337 Aide sur WorldClient Ajout de comptes MDaemon Connector 412 ajouter des membres de la liste 289 Alias 795, 894 Alias d'adresse 795 Alias d'adresses 894 Alias de compte 894 ALL USERS:<domaine> macro liste 287 Amélioration des performances 17 Analyse Noms précédant l'adresse électronique [... 160 Ancien élagage du courrier 784 AntiSpam 688 280 Analyse des domaines de la passerelle AntiVirus 402, 403, 688, 693, 718, 723 Afficher le rapport de mise à jour 723 analyse de virus 718 Analyse des domaines de la passerelle 280 Configurer l'utilitaire de mise à jour 723 Malware 723 Message de test EICAR 723 Mise à jour 723 Mises à jour urgentes 402, 403, 723 Paramètres du proxy 167 Planificateur 402, 403, 723 Quarantaine 718 Test 402. 403. 723 Updater 402, 403 AntiVirus supporté 693 APOP 90

Appareils Domaine (ActiveSync) 252 Domaines ActiveSync (Domaine) 252 Apprentissage Bayésien 734 Apprentissage automatique 734 Apprentissage bayésien 725, 730 ARC 572 Archivage 128 Archivage du courrier dans un pré 162 Arrêt d'un message 120 Assassin de spam 736 ATRN 106, 208, 275 AUTH 208, 558 Authentification 558 Active Directory 887 Authentification à 2 facteurs 771 Authentification à deux facteurs 197, 365, 771 Authentification Active Directory 927 Authentification AD 884, 887, 927 Authentification de l'expéditeur Paramètres ARC 572 Authentification de l'hôte 123 Authentification SMTP 93. 558 Auto Discover ActiveSync 441 Autodécouverte des Paramètres du client MC 413 Automatique Écran IP 641 Journalisation et archivage des journaux 175 Autorisations pour les comptes 771 Autoriser les comptes MDaemon Connector 412 AV AntiVirus 718 MDaemon AntiVirus 723 Mises à jour AntiVirus 723 Paramètres du proxy 167

- B -

290 BadAddress.txt balise fo 583 balise rf 583 **Bannières** 375 barre des tâches 521 barre d'état système 521 Barre d'outils 70.78 BATV 634, 635 Bayésien

Copyright © 1996-2025. All rights reserved. MDaemon Technologies

Bayésien Apprentissage 734 Apprentissage automatique 734 Blocage de comptes 654 **Bloc-notes** 958 Boîte de dépôt Intégration avec Webmail 352 Boîte de dialogue Créer une règle 703 **Bouclier IP** 555

- C -

Cache IP 111 Cache IPs 111 Cadre de politique d'expéditeur 560 CalDAV 393 Calendrier 195, 348 Calendrier et planification 333 Calendriers CalDAV 393 569 Canonicalisation Caractéristiques des messages AI Non (Paramètres par défaut) 365 Paramètres des comptes Modèles de comptes 855 CardDAV 393 Carnets d'adresses CardDAV 393 Catégories Créer 363 domaine 363 Modifier vos 363 Personnel 363 Traduire 363 Certificat 632 Certification 588.590 Certification des messages 588.590 Certificats 342, 384, 613, 614, 617, 621 SSL 974 Utilisation d'un tiers 974 Webmail 974 Certificats SSL 974 974 Certificats tiers Cette liste est modérée par par les listes de diffusion 306 Cette liste modérée par par la liste 306 Changements dans MDaemon 17 Chiffrement 677

Choix de la base de données du compte 908 ClamAV 693 Classification Classification bayésienne 730 Classification bayésienne 725 Clés Chiffrement 677 Privé 677 Public 677 Clés privées 677 Clés publiques 677 **Client MDaemon Connector** 413 Envoyer/Recevoir 422 Signature 428 Clients ActiveSync (Domaine) 252 Domaine (ActiveSync) 252 Collecte de courrier POP 150 Collecte du courrier DomainPOP 150 Collecte du courrier SMTP stocké 208 Commande ESMTP SIZE 90 Commande ISP LAST 152 Commande POP DELE 90 Commandes ESMTP VRFY 90 Compilation 303 Compression de fichier 715 Comptes **MDaemon Connector** 412 Comptes intégrés 927 Comptes intégrés dans Windows 927 Comptes POP des FAI 152 Conditions d'utilisation 388 Confiance Domaines 553 Hôtes 553 Configuration Écran IP 598 Paramètres du DomainPOP 150 Configuration à distance 376, 377 Configuration de la Liste de blocage globale 595, 597 Configuration de l'écran Écran IP 598 Configuration de l'IP Shield Bouclier IP 555 Configuration de MDaemon 376 Configuration à distance 376 MDaemon Remote Admin 376

980

Configuration des 163 903 Messages de réponse automatique Paramètres RAS 163 RAS 163 Configuration du cache Cache IP 111 Configuration d'un cluster MDaemon 434 Configuration d'une grappe MDaemon 438 Configuration d'une source de données Source de données ODBC pour une liste 319 Configuration requise 14 Configuration Web 376 Configurer Bouclier IP 555 Configurer les Alias d'adresse 896 Connexion 566 Connexion des messages 563 Connexion DK et DKIM 566 Connexion sans mot passe 377 Contacts CardDAV 393 Contrôle d'accès 325 Contrôle d'accès à distance 958, 961 Contrôle des relais 546 Contrôles généraux de la messagerie 961 Conversion en-tête FROM: : Exceptions Exceptions 127 Cookies 339 Copie d'une règle de courrier IMAP sur tous les comptes d'un domaine 789 Copier le courrier avant de l'analyser 162 Copier un autorépondeur vers d'autres comptes 777 Corrections 529 Correspondance de noms 160 Courrier Élagage 784 files d'attente 116 Files personnalisées 937 Réexpédition 780 Courrier en double 154 Courrier étranger 159 Courrier identifié par des clés de domaine 563 Courrier identifié par DomainKeys 564 Courrier inconnu 102 Courrier non distribuable 932 Courrier prioritaire 124 CRAM-MD5 90 Création de messages

Messages de réponse automatique 903 Création de modèles de comptes 847 Création d'un site Politique du site 648 Création d'une Nouvelle Règles du Filtre de contenu 697 912 nouvelle source de données ODBC nouvelle source de données système 321 Source de données ODBC 912 Créer et utiliser des certificats SSL 974 Cryptage dans le Webmail 333 Cryptographique 563, 566 Connexion Vérification 563. 564 CSP 588, 590

- D -

736 Daemon Dans l'En-tête FROM : Convertir les En-têtes 126 Data Query Service (DQS) 760 De confiance Adresses IP : 554 De DeClient. 337 Débogage ActiveSync 457 Décryptage 677 Dédoublonnage du courrier 154 Définition des administrateurs du filtre de contenu 708 Définition des indicateurs de dossier IMAP 118 Définition des limites de taille des téléchargements 152 Délais de livraison 405 démarrage 521 Destinataires bloqués 597 Détection de piratage 605 Détection de spambots 607 Détection des boucles 100 Déverrouiller l'interface MDaemon 83 Diagnostics ActiveSync 457 Distribution 93 Distribution différée 120 Divers 535 563, 588, 590 DKIM ADSP 564 balises 569

Copyright © 1996-2025. All rights reserved. MDaemon Technologies

DKIM 563, 588, 590 Balises de signature 569 Canonicalisation 569 Clés privées 566 Clés publiques 566 Connexion 566 DNS 566 inclus dans les rapports DMARC 587 Options 569 Sélecteurs 566 Signatures 564 Vérification 564 Vue d'ensemble 563 DMARC balises 583 Création d'un enregistrement DNS 573 Effet sur les listes de diffusion 290 Effets sur les listes de diffusion 294 Enregistrement DNS 573 enregistrements 583. 587 et les listes de diffusion 573 Fichier de suffixe public 587 Filtrage des messages vers le courrier indésirable 580 inclusion de DKIM dans les rapports 587 Pas de journalisation 587 politiques restrictives 580 Rapports 583. 587 rapports d'échec 583, 587 rapports globaux 583 Refusées les messages qui n'ont pas abouti. 580 Vérification 580 Vue d'ensemble 573 DN racine 315, 884 DNS Adresse IP du serveur 104 Enregistrement DMARC 573 Liste de blocage Exceptions 753 Listes de blocage 751 Serveur 104 DNS-BL 751.760 752 Hôtes Liste d'autorisation 753 754 Options DNSSEC 631 Documents 355, 359 Domaine (par défaut) Domaine - Domaine

Archivage 128 **Domaine Passerelles** 634 Domaines 646 Administrateurs 812 Création 184 De confiance 553 FQDN 184 113 Partage Renommer 184 Suppression 184 Domaines approuvés 593 Domaines autorisés 546 Domaines LAN 646 **Domaines multiples** 113 DomainKeys Courrier identifié 566 DomainPOP 150 Collecte du courrier 150 Correspondance de noms 160 Courrier étranger 159 Hôtes & Paramètres 152 Parsing 154 Règles de routage 157 Sécurité 162 Traitement 156 Dossier 768 Courrier Dossier Dossiers de courrier : 768 Dossier spam 754 Dossier spam IMAP 754 Dossiers 116. 325 Dossiers de documents Autoriser 116 Autoriser ou bloquer des types de fichiers 116 Limitation de la taille des documents 116 Dossiers de documents WorldClient 116 Dossiers Dossiers de courrier : Partager des dossiers courrier 116 Dossiers IMAP partagés 116, 118, 325, 796 **Dossiers** publics 116, 118, 796 Élagage 131 Liste de diffusion 314 Dossiers publics IMAP 116 **Dossiers** utilisateurs 116 Dossiers utilisateurs partagés 327, 797 DQS 760 Drapeaux 325 Drapeaux de messages IMAP 325 Droits d'accès 327, 797

Droits d'accès aux dossiers 327, 797 DSE racine 884

- E -

Écran d'hôte 601 Écran dynamique Adresses IP bloquées 654 654 Blocage de comptes Diagnostics 662 Exceptions NAT du domaine 669 Exemptions de routeur pour les domaines 669 Fichiers dumpers 662 Filtre SMTP 603 Filtrer par emplacement 665 Filtrer par SMTP 665.667 Liste d'autorisation 665 Liste d'autorisation dynamique 665 Liste de blocage 667 Liste de blocage dynamique 667 Liste des Comptes Bloqués 674 Liste des comptes exemptés 671 Notifications 658 Options 650 Options avancées 662 Options avancées de journalisation 650 Pas de journalisation 662 Personnalisation 650 Protocoles 657 Rapports 658 Suivi des échecs d'authentification 654 Tarpitting 665 Écran IP 598 Automatique 641 Écran SMTP 603 Éditeur d'alias 894 Editeur de domaine de la passerelle Active Directory 270 ESMTP ETRN 275 LDAP 270 270 Minger Quotas 279 Vérification 270 Éditeur de domaines de passerelle Paramètres 280 Éditeur de filtres de contenu 695 Éditeur de politiques ActiveSync 470 Editeur du domaine de la passerelle

Paramètres de domaine 268 Redirection 274 Effacer le nombre de messages au démarrage 521 131, 784 Élagage Élagage des comptes 784 eM Client 538 538 Activations du client Activations gratuites 538 Licences 538 Enregistrement SRV 75 En-tête "List-Unsubscribe" (désinscription) 306 En-tête "Received" : dans l'en-tête FROM 154 En-tête Authentification-Results : dans l'en-tête FROM 564 En-tête dans-tête FROM : 306 En-tête dans-tête FROM : List-Post 306 En-tête de priorité 530 En-tête du message bienvenue sujet de bienvenue : dans l'en-tête FROM : 530 En-tête en-tête FROM : List-Help 306 En-tête En-tête From : List-Subscribe header 306 En-tête From : Conversion en-tête FROM : Conversion des en-têtes 126 En-tête From : dans l'en-tête FROM 306. 535 290 List-ID En-tête From : dans l'en-tête FROM : List-Subscribe 535 En-tête From : En-tête de désabonnement 306 En-tête From : List-Owner header 306 En-tête From : TO : dans l'en-tête FROM 126 En-tête From: : dans l'en-tête FROM 154.311 535 Listes auxquelles vous êtes inscrit List-Unsubscribe (désabonnement) 535 En-tête From: : L'en-tête FROM Liste de désabonnement 306 Liste de diffusion 306 306 Liste-Archive Liste-Post 306 Listes auxquelles vous êtes inscrit 306 List-Help 306 List-ID 306 Propriétaire de la liste 306 En-tête ID du message 530 En-tête Listes auxquelles vous êtes inscrit : Dans l'en-tête FROM 535 En-tête Return-Receipt-To 530 En-tête TO : dans l'en-tête TO 611 En-tête X-RBL-Warning 530 En-tête-ID : dans l'en-tête FROM 306

Index 983

En-têtes DMARC et les listes de diffusion 294 Liste de 294 Liste de diffusion 294 Liste Reply-To 294 Liste To 294 Entrée base DN 315.884 Envoi de courrier à divers utilisateurs 157 Envoi et collecte de courrier 405 431, 434, 436, 438 Équilibrage de charge 90, 208, 275 **ESMTP** espace 527 Espace disque 527 Faible 527 Paramètres 527 Surveillance 527 Espace disque disponible 527 Espace disque faible 527 étiquette ri 583 étiquette rua 583 étiquette ruf 583 ETRN 208.275 Exceptions NAT du domaine 669 Exclusion d'adresses du filtrage 742 Exemples de scripts de réponse automatique 903, 907 Exemptions de routeur pour les domaines 669 Exiger une acceptation des conditions d'utilisation 388 EXPN 90 Expression régulière 703 expressions 703 expressions balisées 703 Extension de la pièce jointe 525 Extensions de sécurité DNS 631 Extensions SMTP 628 MTA-STS 628 REQUIRETLS 628 TLS Reporting 628 Extraction de la bande passante 639 Extraire les pièces jointes automatiquement 389 Extraire les pièces jointes jointes 389, 787

- F -

Fausses routes971Fax350Fenêtre de connexion85

Fenêtre de connexion SMTP 85 Fenêtre de session 85 Fenêtre de suivi des événements 70, 78 Fenêtre principale 70. 78. 521 Fermer la session RAS 163 Fichier d'adresses erronées 168 Fichier de bienvenue 311 Fichier de mauvaise adresse 290 Fichier GatewayUsers.dat 270 Fichier MDStats.ini 953 Fichier suffixe public 587 Fichiers de support 311 Fichiers en quarantaine suppression 131 787 Fichiers joints Fichiers oof.mrk 898.903 Fichiers sémaphores 964 Fichiers texte 958 File d'attente 934 934 Contenu E-mails de résumé 934 Files d'attente 70, 78, 116, 932, 939 File d'attente 934 Personnalisées 937 Restaurer les paramètres par défaut 939 Filetage 97 Fils de discussion 97 Fils de session 97 Fils de session entrants 97 Fils de session sortants 97 Filtrage des messages 693, 695, 789 Filtre anti-spam 725, 726, 749, 754 Analyse des domaines de la passerelle 280 Apprentissage bayésien automatique 734 Filtre anti-spam 749 Liste d'autorisation 742 742 Liste d'exceptions MDSpamD 736 Mises à jour 746 Rapports 747 Spam Daemon 736 Utilisation d'un Spam Daemon externe 736 Filtre de contenu 693 Actions 697 Administrateurs 708, 714 Conditions 697 Éditeur 695 Récipiendaires 714

Filtre de contenu 693 règles 703 Filtrer en-tête From : dans l'en-tête FROM 611 Filtrer par 542.598 Détection des spambots 607 En-tête TO : Dans l'en-tête FROM : Filtrer 611 Localisation 609 Pays 609 SMTP 603 Filtrer par emplacement Liste d'autorisation dynamique 665 Filtrer par localisation 609 Filtrer par SMTP 665.667 Filtres 789 Filtres 789 789 Règles Flux de travail SMTP 86 Flux de travail SMTP de MDaemon 86 Fonctionnalités de MDaemon 14 Fonctionnalités des messages Al Activation pour les domaines 197 Ce compte est ACTIVÉ 771 Fournisseurs de services de certification 588, 590

- G -

Garantie par référence 588. 590 Génération automatique d'un dossier et d'un filtre anti-spam 754 184 Gestion de domaines Calendrier 195 Fonctionnalités des messages AI 197 Paramètres 222 Paramètres de MDaemon Webmail 197 Gestion de groupes 836 Gestion de l'API 515 Gestion de l'API XML 515 Gestion des files d'attente et des statistiques 943 Gestion personnalisée des files d'attente/statistiques 953 Gestionnaire de domaines 184 ActiveSvnc 225 Hôte de relais 189 Messagerie instantanée MDaemon 193 Mon compte 191 Nom d'hôte & IP 187 Signatures 210 Signatures client 216

Signatures de domaine 210 Signatures du MDaemon Connector 216 Signatures du webmail 216 Gestionnaire de dossiers publics 325 Gestionnaire de modèles 847 Paramètres contrôlés par modèle 849 Propriétés du modèle 849 Gestionnaire de passerelles 261 Domaines 261 Editeur 261 Gestionnaire des comptes 762 Global Administrateurs 812 Auth 558 Liste de blocage 595, 597 Google Drive 355 Greylisting 643 GROUP:<nomdugroupe> macro de liste 287 Groupes 768 ActiveSvnc 497 Affectation des Paramètres du client ActiveSync 497 836 Création d'un compte Messagerie instantanée 838 Messagerie instantanée MDaemon 838 Modèle 861 Mon compte ajouté 836 Mon compte Modèles de comptes 838 Ne pas déranger 838 Priorité 838 Suppression 836 Suppression d'un compte 836 Groupes de comptes 836, 838

- H -

Health Check 545 Heuristique 726 Hôte de relais 189 Non (par défaut) 93 Hôtes 752 Hôtes RBL 752 HTTPS 342, 384, 617, 621

- | -

Icône de la barre d'état 83

Copyright © 1996-2025. All rights reserved. MDaemon Technologies

ID de l'expéditeur 588, 590 Identifiant Profil de la connexion 165 IIS 339 Images dans les signatures 132, 138, 210, 216, 838, 841 IMAP 100, 106, 765, 769 Dossiers 325 Droits d'accès aux dossiers 327, 797 Filtres 789 Règles de messagerie 789 Importation Mon compte 927 Importation de Comptes à partir d'un fichier texte 925 Mon compte 925 Indexation indexation des Dossiers publics 511 indexation des messages en temps réel 511 indexation des messages pour Chercher 511 indexation quotidienne des messages 511 Indexation des messages Diagnostic 513 Fichiers dumpers 513 indexation des Dossiers publics 511 indexation des messages en temps réel 511 indexation des messages pour les recherches 511 indexation quotidienne des messages 511 Options 511 Options avancées 513 Pas de journalisation 513 Personnalisation 511 Indicateurs de message 325 Indicateurs par utilisateur 325 Inscription 297 Inscription aux listes de diffusion 299 Intégration 927 Intégration avec Dropbox 333 Intégration OneDrive 359 Interface 70.78 Interface d'aide 70, 78 INTERFACE GRAPHIQUE 70.78 Interface graphique de MDaemon 70, 78 Introduction 14 IP locales 647 IPv6 109, 110, 187 IU 521

· J -

Jabber 398 Journal des événements 174 Journalisation 170, 175 Archivage 175 Journal des événements 174 Journal des événements Windows 174 Journal détaillé 170 Maintenance 175 Mode de journalisation 168 Paramètres 177, 181 Rapports 172 Sauvegardes 175 Statistiques Pas de journalisation 172 Journalisation et archivage des journaux 175

- L -

Laisser le courrier chez le FAI 152 Largeur de bande 637 LDAP 315, 890 DN d'entrée racine 315 DN racine 884 DSE racine 884 Entrée base DN 315, 884 270 Port (passerelle) Serveur (Passerelle) 270 Vérification (passerelle) 270 Vérification de la passerelle 264 Let's Encrypt 342, 617, 632, 974 110. 187 Liaison Liaison de sockets 110 Licences eM Client 538 Liens vers les pièces jointes jointes 389.787 Liens vers les pièces jointes jointes automatiquement 389 Limite de la taille des messages 222 Limiter la bande passante 637 Limites 152, 784 limites d'espace disque 279 Liste blanche 725.749 ActiveSync 454 Liste d'autorisation Automatique 813

Liste d'autorisation DNS-BL 753 Filtre anti-spam 742 Modèle 876 Liste d'autorisation (automatique) 739 Liste d'autorisation (par destinataire) 743 Liste d'autorisation (par l'expéditeur) 744 Liste de blocage 745, 751 Adresse 595. 597 Liste de blocage en temps réel 751 Liste de contrôle d'accès 327.797 Liste de diffusion 958 303 Compilation Création 281 Dans l'en-tête FROM : List-Unsubscribe header 535 DMARC 290 DMARC et les listes de diffusion 294 Dossiers publics 314 En-tête Listes vous êtes inscrit : dans l'en-tête FROM 535 En-tête List-ID : dans l'en-tête FROM 290 En-têtes 294 Fichiers de support 311 Modifier 281 Notifications 304 ODBC 318 Paramètres 290 Refus des messages DMARC restrictifs 290 Routage 308 Votre nom 290 Liste de macro ALL USERS 287 Liste des Exceptions STARTTLS 626 Liste des exceptions de l'autorépondeur 901 Liste des paramètres de sécurité 545 Liste d'exceptions 742, 901 DNS-BL 753 Répondeurs automatiques 901 Liste d'exceptions de l'autorépondeur 901 Liste noire 725 ActiveSync 454 Liste STARTTLS 627 Liste STARTTLS obligatoire 627 Listes de blocage DNS 752 Listes de diffusion Abonnements 297 Active Directory 315

ajouter des membres 289 ALL USERS:<domaine> macro de liste 287 Basculement de digest 287 Cette liste est modérée par par les listes de diffusion 306 DMARC 573 En-tête From : TO 306 GROUP:<nom du groupe> macro liste 287 Lecture seule 287 Macros de liste ALL USERS 287 Membres 287 Post Only toggle 287 Rappels d'inscription 301 Sécurité 306 Type d'abonnement 287 URL 306 Utilisation d'Active Directory avec des 315 Listes noires 751 littéraux 703 Livraison basée sur des informations autres que l'adresse 160

- M -

Macros Liste de diffusion 287 Message 710, 711 pour les groupes 287 pour les listes 287 pour les Paramètres du client MC 415 Signature 132 Signature client 138 Macros dans les messages de listes de diffusion 308 Macros de message 710.711 Maintenance de la base de données 175 Marguer des messages comme spam 752 Mauvais messages 932 Mauvaise adresse.txt 168 Max. domaines listés 521 279 messages nombre de comptes affichés 521 nombre de lignes de journalisation affichées 521 MDaemon 614 Mise à jour 60 MDaemon Admin Remote 771

Index 987

MDaemon AntiVirus 688. 693. 718 Afficher le rapport de mise à jour 723 Configurer l'utilitaire de mise à jour 723 Malware 723 Message de test EICAR 723 Mise à jour 723 Mises à jour urgentes 402, 403, 723 Planificateur 402, 403, 723 402, 403, 723 Test 402, 403 Updater MDaemon Connector 409.769 Activation 410 412 Ajout d'utilisateurs Autoriser les utilisateurs 412 Création de Dossiers IMAP partagés 410 Dossiers de contacts 410 Mon compte 412 Options 410 Paramètres clients 413 410 Restreindre les utilisateurs Suppression d'utilisateurs 412 MDaemon Connector Client Avancé 419 Base de données 426 Compléments 429 Divers 424 Dossiers 421 415 Macros MDaemon et les fichiers texte 958 MDaemon Remote Admin Certificats 384. 621 HTTPS 384, 621 SSL 384. 621 MDIM 346 Domaines 193 MDPGP 677 **MDSpamD** 736 287 Membres Menu 70.78 83 Menu raccourci Message de Notification d'état de remise 940 Message d'état Notifications remise 940 Message DSN 940 Messagerie instantanée 193. 333. 346. 398 Messagerie instantanée MDaemon 333 Domaines 193 Messages de réponse automatique 903

Messages des tests de détection de virus EICAR 723 Messages en quarantaine suppression 131 703 métacaractères 359 Microsoft OneDrive Migration de la base de données de comptes vers ODBC 909 Minger 113, 270, 923 Vérification de la passerelle 264 Minuterie 405 Mise à jour des définitions de virus 402, 403 Mise à niveau de MDaemon 60 Mise en file d'attente 208.275 Mise en file d'attente AUTH 208 Mise en file d'attente des messages de la passerelle 275 Mise en file d'attente du courrier 208, 209, 275 Mise en file d'attente ETRN 275 Mise en place DomainPOP Mail Collection 150 Mise en place d'un cluster MDaemon 431, 436 Mises à jour 533, 746 Mises à jour AntiVirus 402.403 Mises à jour automatiques 533 Mises à jour urgentes 402.403 Mode de journalisation 168 Modèle Mon compte Restrictions 868 Modèle de restrictions de comptes 868 Modèles Création 847 Nouveaux comptes 847 Renommer 847 Suppression 847 Modifier la règle 703 Modifier les mots de passe 765 Modifier les paramètres du port de WorldClient 337 Modifier une règle 703 Modifier une règle du Filtre de contenu existante 703 Modifier vos En-tête From: : Dans l'en-tête FROM :.. 126 Passerelles 261 Mon compte 925. 927 ActiveSync 479 ActiveSync activé/désactivé 819 Alias 795

Mon compte 925. 927 Assistant de sélection ODBC - Base de données des comptes 909 Clients ActiveSync 827 Comptes Domaines ActiveSync 243 DomainePOP 152 Dossier 768 Dossier de courrier : 768 Dossiers IMAP partagés 796 Filtres 789 Gestionnaire de domaines 191 Groupes 768. 836. 838 Liste d'autorisation 813 Mon compte Informations générales 765 Mots de passe d'application 804 MultiPOP 792 Options de la base de données 908 Paramètres 815 Paramètres du client ActiveSync 820 Périphériques mobiles 827 Pièces jointes 787 Politiques ActiveSync 826 Quotas 784, 920 Répondeur automatique 777 Répondeurs automatiques 898 Restrictions 782 769 Services de messagerie Services Web 771 Transfert 780 Mon compte Autoresponder 777 Mon compte Détection de détournement de compte 605 Mon compte Informations générales 765 Mot de passe 165 Compte de courrier POP 152 Comptes POP des FAI 152 Mots de passe 915 Expiration 915 Fort 915 Mots de passe d'application 804 Non réversible 915 Mots de passe d'application 804 **MultiPOP** 144, 406, 769, 792 MultiPOP et Gmail 144 MultiPOP et Office365 144 144 OAuth 2.0 Suppression des messages du serveur après la collecte 144

- N -

Ne pas déranger 838 431, 434, 436, 438 Nœuds Nœuds de cluster 431, 434, 436, 438 Nom d'affichage de l'alias dans le Webmail 365 Nom d'hôte & IP 187 Non en-tête From) dans l'en-tête FROM :.. 154 Notes de version 17 Notifications 304.710 DSN 940 Notifications d'état remise 940 Nouveautés de MDaemon 17 Nouveaux Modèles de comptes 847 Nouvelles fonctionnalités 17

- 0 -

OAuth 2.0 355.359 Obtenir de l'aide 65 ODBC Assistant de sélection - Base de données de 909 comptes Base de données de compte 909 Liste de diffusion 318 Source de données 909, 912 Source de données du système ODBC 319 ODMR 106, 208, 275 OneDrive 359 OpenPGP 677 Option de base de données LDAP 908 OPTION DE BASE DE DONNÉES ODBC Option de base de données 908 Option de base de données Userlist.dat 908 Options Répondeurs automatiques 902 Services de disponibilité 349 Options avancées ActiveSync 443, 457 Débogage 457 Diagnostic 457 Dumps 457 Fichiers dumpers 457 Pas de journalisation ActiveSync 443 Pas de journalisation d'ActiveSync 457 Tuning 443

Options de compte 909 Mots de passe 915 Options de distribution 93 Options de la base de données 908, 909 908 Options de la base de données des comptes 349 Options de serveur libre/occupé **Options l'autorépondeur** 902 **Options LDAP** 890 **Options LDAP/Carnet d'adresses** 890 Ordre de traitement 86 Outlook Connector pour MDaemon 409 OutOfOffice.rsp 902

- P -

Page d'attente 944 Page de rapport 952 Page d'utilisateur 948 Par nom 165 Par taille Message 222 **Paramètres** Alias 896 Gestion de domaines 222 Modèle 878 Paramètres clients ActiveSync 447 Domaines ActiveSync 226, 233 447 Global Paramètres contrôlés par modèle 849 Paramètres de connexion 163. 165 Paramètres de connexion ISP 165 Paramètres de distribution du courrier 157 Paramètres de domaine 268 Paramètres de file de relance 932 Paramètres de la ligne de commande MDStats 955 Paramètres de liste de diffusion 284 Paramètres de MDaemon Webmail 197 Paramètres de répulsion 641 Paramètres de sécurité Health Check 545 545 Valeurs par défaut Paramètres de serveur Courrier inconnu 102 Distribution 93 DNS 104 Fils de discussion 97 Ports 106

100 Temporisation Paramètres des alias 896 Paramètres des notifications (DSN) 940 Paramètres du client ActiveSync global 443 Paramètres du client MC Avancées 419 426 Base de données Compléments 429 Divers 424 Dossiers 421 Envoyer/Recevoir 422 Macros 415 Paramètres clients en auto-découverte 413 428 Signature Paramètres du proxy 167 Paramètres du relais 546 Paramètres globaux des passerelles 264 Paramètres RAS Dialup Paramètres de connexion ISP 165 Post-connexion 166 Paramètres serveur Élagage 131 Mise en file d'attente 208 Parsing 154 analyse Dédoublonnage du courrier 154 Liste des En-tête From : dans l'en-tête FROM :. 154 Sauter 154 Partage de calendriers 393 Partage de domaine 113 Partage de domaines 113 Partage de réseau 537 Pas de cache 111 Pas de iournalisation 950 ActiveSync 443 Enregistrements DMARC 587 Pas de journalisation de WorldClient 337 Pas de paramètres de journalisation 177, 181 Passerelle 261.635 Création automatique 266 280 Paramètres Paramètres de domaine 268 Paramètres globaux des passerelles 264 Quotas 279 Vérification 923

Vérification des adresses

923

Serveurs

90

Copyright © 1996-2025. All rights reserved. MDaemon Technologies

Passerelles 634 Passerelles 266 Passerelles de domaine 261, 635 Permissions d'accès au web 771 Personnalisation des images des bannières du webmail 375 Personnalisation des messages DSN 940 PGP 677 Pièces jointes Modèle 873 Répondeurs automatiques 900 Supprimer restriction 131 Pièces jointes interdites 708 Pied de page 311 Pièges à spam 758 Planificateur 405.746 Files personnalisées de planification des files d'attente 405 Mises à jour du Filtre anti-spam 746 Programmation de courrier distant 405 Programmation d'événements 405 Politique d'ActiveSync Politique de compte 826 Politique du site 648 Politique du site en matière de sécurité 648 Politiques ActiveSync 462, 470 Affectation à un domaine 242 POP avant SMTP 552 **POP3 ENTRANT** 769 Ports 106 MultiPOP 792 Ports SSL 106 Postconnexion 166 Postmaster informé en cas d'échec de la connexion 163 Recevoir résumé de non 159 pourriel Filtrage 744 Liste d'autorisation 744 Préférences Corrections 529 Divers 535 En-têtes 530 527 Espace INTERFACE UTILISATEUR 521 533 Mises à jour 533 Mises à jour automatiques

MultiPOP 406 920 Quotas Serveurs 90 Système 525 942 Prétraitement Pré-traitement des listes diffusion 525 Prétraitement en file d'attente 942 Prévention des messages en double 154 Processus 166 Profil 165 Profil de connexion 165 Programmation de courrier distant 405 403. 405. 407 Programmation d'événement Programmation d'événements 405 405, 407 Programme de courrier Programmes 166 Propriétés des modèles Rôles d'administration 875 Propriétés du groupe 838 Signatures client 838.841 Propriétés du modèle 849 Groupes 861 Liste d'autorisation 876 Paramètres 878 Pièces jointes 873 870 Quotas 862 Répondeur automatique Services de messagerie 853 Services Web 855 Transfert 866 Protection Virus 693 Protection contre la rétrodiffusion 634.635 Contre la rétrodiffusion 635 Protection contre la rétrodiffusion - Aperçu Contre la rétrodiffusion 634 Protection contre le phishing 611 611 Protection contre le spam Protection instantanée 688 Protocole de chaîne de réception authentifiée 572 Protocole Secure Sockets Layer 342, 613, 614, 617, 626, 974 Publication de filtres IMAP sur tous les comptes d'un domaine 789 Publication d'un autorépondeur vers d'autres comptes 777

- Q -

QSND 208 Quotas 279, 784, 920 Modèle 870 Quotas de courrier 920

- R -

Rappel de message 120 Rappel de message simple 120 Rappel d'email 120 Rappel SMTP 923 Rappels 348 Liste de diffusion 301 Rappels de tâches 348 Rappels d'inscription 301 Rapport Quota 920 Rapports 172.747 Rapports simples 747 RAS Dialup 163 Moteur 163 Paramètres 163 Paramètres de numérotation 163 RAW 961 Champs spéciaux pris en charge par Contourner le filtre de contenu 961 Exemples de messages 961 Spécification des messages 961 RBL 751 Recherche de virus 718 Recherche d'un ISP 208 548 Recherche inversée Récipiendaires 714 Récupération du courrier SMTP stocké 208 Redémarrer le Filtre anti-spam 726 Redirection automatique des messages ! REDIRIGER LEESSAGE ! 789 Refusées non 159 789 Règles Règles de routage 157 Régulation de la bande passante 637, 639 Rejeter le spam 726.749 Relais du courrier à la demande 208, 275 Relais du courrier à la demande (ODMR) 208.209

RelayFax Intégration avec Webmail 350 Remplacement de nom de domaine 156 Renommer des modèles de comptes 847 Répondeur automatique Modèle 862 Répondeurs automatiques 777, 898, 903, 907 Liste des comptes 898 Pièces jointes 900 Vue d'ensemble 898 Responsable 762 Ressources 70, 78 Restaurer 939 Restreindre les adresses IP 110 Restriction des adresses IP 187 Restrictions Modèle 868 Mon compte 782 Restrictions de protocoles ActiveSync 459 Restrictions relatives aux comptes 782 Retrait de file d'attente 208 Retrait du fichier d'attente 208.209 Retransmission 780 Retry 932 Réunions 348 812 Rôles Rôles d'administration 812 Modèle 875 Routage 308 Routage de listes 308 93 Routage des messages Routage du courrier vers différents utilisateurs 157

- S -

S'abonner 297, 299 Saut de message maximum 100 Sauter 154 Sauvegarde du courrier 162 Scheduler Mises à jour AntiVirus 402, 403 Se désabonner 297 Sécuriser le DNS 631 Sécurité 162.927 BATV 634, 635 Détection de piratage 605 Filtre SMTP 603 Filtrer par localisation 609

Sécurité 162.927 Fonctionnalités 542 Liste de diffusion 306 Paramètres 542 Protection contre la rétrodiffusion 635 Protection contre la rétrodiffusion - Aperçu 634 Sécurité des listes 306 Serveur Webmail 333 Serveur BOSH 398 Serveur de messagerie MDaemon 14 Serveur de sauvegarde 270 Serveur LDAP distant 270 Serveur POP 152 Serveur Web 339 Serveurs 90 Service 537 Service de cluster 431, 434, 436, 438 Service de découverte automatique 75 Service Windows 537 Services de disponibilité 348 Services de messagerie 769 Modèle 853 Services Web Modèle 855 Seuil Rejet du spam 726 Seuil SMTP RCPT 641 Seuil Tarpit 641 Si le nombre de tentatives d'appel est défini 163 Signalement du spam 726 Signaler le spam 749, 752 Signalisation au FAI de la mise en file d'attente du courrier 208 Signature du client Transmettre la signature client à Outlook 428 Signature du compte 807 Mon compte 807 Signatures Ce texte 132, 210 Client 216 Domaine 210 Groupe de clients 838.841 HTML 132, 210, 216 Insérer des images 132.210 Insertion d'images 216 Macros 132 Macros pour les signatures client 138

Non (par défaut) 132, 138 pour MDaemon Connector 216 pour Outlook 138 pour Webmail 138, 216 pousser vers Outlook 138 pousser vers Webmail 138 Texte brut 216 Signatures client 216, 838, 841 Macros 138 Non (par défaut) 138 138 pour Outlook pour Webmail 138 Signatures de domaine 210 SMTP call-forward 923 Socket binding 187 Source de données 909.912 Source de données du système 912 Sous-adressage 815 Spam 758 Adresses Apprentissage bayésien 730 Classification 730 Classification des faux positifs 730 Classification faussement négative 730 Filtrage 726, 739, 743, 745, 749 Insertion d'une balise dans l'objet 726 749 Liste blanche Liste d'autorisation 743 Liste d'autorisation automatique (automatique) 739 Liste de blocage 745 749 Liste noire Notation 726 Pièges 758 Rapport simple 747 Rapports 747 Rejet 749 Rejeter 726 Répertoire 730 Répertoire de non-spam 730 Score requis 726 Seuil 726 Suppression 726, 749 SpamD 736 Spamhaus DQS 760 SPF 560, 588, 590 SSL 342, 384 SSL & TLS

SSL & TLS CA 632 Certificat 632 DNSSEC 631 Extensions SMTP 628 Let's Encrypt 632 Liste STARTTLS 627 MDaemon 614 MDaemon Remote Admin 621 Pas de Liste STARTTLS 626 **STARTTLS** 626 TLS 626 Webmail 617 SSL et certificats 342, 613, 614, 617, 974 SSL pour le courrier électronique 614 SSL pour les courriels 613 STARTTLS 613, 614, 626 Statistiques 70.78 Statistiques de journalisation 172 613, 614 STLS Support technique 65 Support technique MDaemon 65 311 Suppression 847 Suppression de modèles de comptes Suppression du courrier 157 Suppression du courrier POP après la collecte 152 Surveillance d'Active Directory 887 Synchronisation 333 393 Synchronisation des calendriers Synchronisation des contacts 393 System Service 537 Système 525

- T -

Tâches CalDAV 393 Tags DKIM 569 DMARC 583 fo 583 fr 583 ri 583 583 rua ruf 583 Tarpitting 665 TCP 106 Téléchargement

Limites 152 Par taille 152 Télécharger Limites 784 Limites de taille 784 100 Temporisateurs Temps de latence 100 Tentatives de tentatives 163 TLS 613, 614, 626 Traitement 156 Traitement de file d'attente locale pré/post traitement 942 Transférer les messages à MESSAGE ! 789 Transfert Passerelle 264 vers un domaine de passerelle 274 Transfert de courrier 157, 780 vers un domaine de la passerelle 274 Transmission Modèle 866 Tuning 443 Types de clients ActiveSync 504

- U -

UDP 106 Utilisateurs bloqués 595 Utilisateurs supprimés 595 Utilisation des expressions régulières 703

- V -

Valeurs par défaut des paramètres de sécurité 545 VBR 588.590 Vérification Adresse distante : 270 Passerelles 270 via Active Directory 270 via LDAP 270 via le fichier GatewayUsers.dat 270 via Minger 270 Vérification de la norme DKIM 564 Vérification de l'adresse 923 Vérification de l'adresse (passerelle) 270 Vérification des signatures 563

Vérification DKIM 564 Verrouillage de l'interface MDaemon 83 Virus 688 Mise à jour 402, 403 VRFY 90, 923 Vue d'ensemble 14

- W -

WebAdmin 376, 377 Rapports 172 WebAthn 197, 365 Webauth 377 WebDAV 393 Webmail 333, 771 Authentification à deux facteurs 365 Branding 375 Calendrier 348 Carnet d'adresses 365 Catégories 363.365 Dropbox 352 Exécution sous IIS 339 Format de la date 365 HTTPS 342, 617 Intégration de RelayFax 350 Jabber 398 MDIM 346 Messagerie instantanée 346, 398 Messagerie instantanée Webmail 398 Modifier le nom d'affichage de l'alias 365 Non (par défaut) 365 Options de domaine 346 Paramètres 365 Paramètres de domaine 197, 365 Paramètres personnalisés 365 Personnalisation des bannières 375 Port HTTPS 342, 617 Rappels 348 Rappels de tâches 348 Réunions 348 Serveur Web 339 SSL 342, 617 SSL et certificats 974 WebAuthn 365 XMPP 398 winmail.dat 715 WorldClient CalDAV 393

CardDAV 393 Connexion 337 De... WorldClient 337 Obtenir de l'aide 337 **Options Free/Busy** 349 Pas de journalisation 337 SSL 613 WorldClient SSL 613

- X -

XMPP 398