Benutzerhandbuch

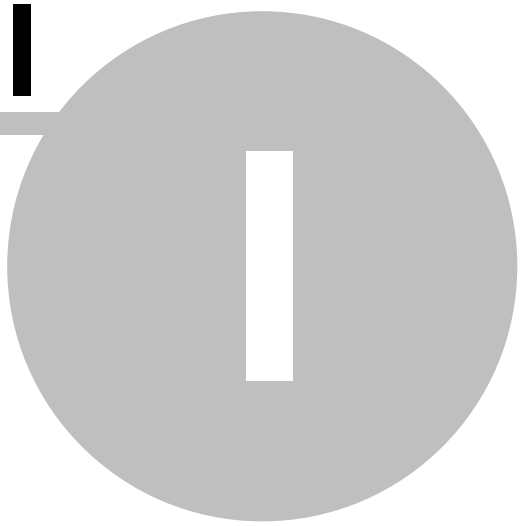
23.0

MDaemon Messaging Server
Benutzerhandbuch

v23.0.0 - März 2024

Inhaltsverzeichnis

Kapitel



1 MDaemon Messaging Server 23.0

Einführung

Der MDaemon Messaging Server, ein Produkt von MDaemon Technologies, ist ein auf Standards basierender Mailserver für die Dienste SMTP, POP3 und IMAP. Er unterstützt die Betriebssysteme Microsoft Windows 7, Server 2008 R2, sowie neuere Versionen dieser Betriebssysteme, und bietet den gesamten Leistungsumfang eines vollständigen Mailservers. MDaemon ist darauf ausgelegt, einer beliebigen Zahl von Nutzern E-Mail-Dienste zur Verfügung zu stellen und enthält leistungsfähige Verwaltungswerkzeuge für E-Mail-Benutzerkonten und Nachrichtenformate. MDaemon enthält skalierbare Mailserver-Dienste für SMTP, POP3 und IMAP4, unterstützt LDAP und Active Directory, enthält einen eigenen browsergestützten E-Mail-Client, verfügt über Inhalts- und Spam-Filter, umfassende Sicherheitsfunktionen und vieles mehr.

Leistungsmerkmale von MDaemon

MDaemon verfügt nicht nur über die Funktionen zur Verarbeitung von E-Mail über SMTP, POP3 und IMAP4 sondern auch über viele weitere Leistungsmerkmale. Die folgende Liste gibt einen Überblick über einen Teil dieser Leistungsmerkmale.

- Umfassende Unterstützung für Virenprüfung und Virenschutz ist für als zusätzlich erhältliches Leistungsmerkmal für Ihre Lizenz für MDaemon oder MDaemon Private Cloud verfügbar. Wenn Sie diese Leistungsmerkmale lizensieren, erhalten Sie hierdurch Zugriff auf Schutz in Echtzeit gegen Massenangriffe, die so genannte Outbreak Protection 643, sowie MDaemon AntiVirus 671. Sie können dann Nachrichten automatisch auf Viren prüfen und infizierte Nachrichten reinigen oder löschen lassen, bevor diese die Empfänger überhaupt erreichen. Sie können MDaemon außerdem veranlassen, Administratoren, Absender und Empfänger von der festgestellten Infektion zu unterrichten.
- MDaemon verfügt über eine umfassende Verwaltung von Mailinglisten und E-Mail-Verteilerlisten. Hiermit lassen sich unbegrenzt viele getrennte E-Mail-Verteiler erstellen, die lokale und außen liegende Mitglieder enthalten können. Die Listen können für die Bestellung durch Nichtmitglied geöffnet werden, sie können öffentlich oder privat geführt werden, Antworten auf Listennachrichten können an den Autor der ursprünglichen Nachricht oder die gesamte Liste geleitet werden, Digest-Funktionen sind verfügbar, und die Listen können mithilfe zahlreicher anderer Leistungsmerkmale angepasst werden.

- Webmail[317] ist ein fester Bestandteil von MDaemon. Dieses Leistungsmerkmal gestattet Ihren Benutzern den Zugriff auf ihre E-Mail-Nachrichten über ihren bevorzugten Web-Browser. Ein E-Mail-Client, der an einen Arbeitsplatz gebunden ist, ist dazu nicht erforderlich. Dieser Client ist besonders gut für Benutzer geeignet, die viel auf Reisen sind oder die für die Bearbeitung ihrer E-Mail keinen Rechner haben, der ihnen fest zugewiesen ist.
- MDaemon Webmail enthält den vollen Leistungsumfang eines E-Mail-Clients. Sie können insbesondere E-Mail senden und empfangen, eine Rechtschreibprüfung durchführen, E-Mail in mehreren persönlichen Ordnern verwalten, die Sprache für die Benutzerschnittstelle aus 18 Sprachen auswählen, Besprechungen und Termine planen, Kalender und Aufgaben für den Zugriff durch andere Benutzer freigeben, die Einstellungen für das MDaemon-Benutzerkonto bearbeiten (hierzu wird auch die Remoteverwaltung[350] benötigt), Kontakte verwalten, und vieles mehr. Ein Bestandteil von Webmail ist der MDaemon Instant Messenger (MDIM)[318], ein kleines Hilfsprogramm, das der Benutzer herunterladen und auf seinem Rechner lokal installieren kann. Es eröffnet einen einfachen Zugang auf Ihre E-Mail-Nachrichten und Ordner und prüft regelmäßig, ob neue Nachrichten vorliegen. Der Web-Browser wird dazu nicht benötigt. Der MDaemon Instant Messenger enthält auch ein vollständiges Instant-Messaging-System, mit dessen Hilfe Benutzer des MDIM und anderer XMPP-Clients[372] untereinander schnell und einfach "chatten" können.
- MDaemon enthält zahlreiche Funktionen, die Ihnen helfen, Ihr E-Mail-System abzusichern. Die Funktionen Spam-Filter und Sperrlisten für DNS helfen Ihnen, die meisten Spam-Nachrichten wirksam auszuschalten, die "Spammer" vielleicht durch Ihre Domäne schleusen wollen. Die IP- und Host-Filter und die Sperrlisten für Adressen ermöglichen die Suche nach bestimmten Adressen und Domänen, die keine Verbindung mit dem E-Mail-Server herstellen oder keine Nachrichten durch das System leiten sollen. Sie gestatten auch die gezielte Freigabe einzelner IP-Adressen, während alle anderen Adressen blockiert werden.
- MDaemon unterstützt das Lightweight Directory Access Protocol (LDAP) und kann daher Ihren LDAP-Server stets mit aktuellen Daten über alle Benutzerkonten versorgen. Sie können hieraus ein immer aktuelles LDAP-Adressbuch bilden, auf das Benutzer zurückgreifen können, deren E-Mail-Clients LDAP ebenfalls unterstützen. Sie können weiter wahlweise ein Active Directory oder einen LDAP-Server als Datenbank für die MDaemon-Benutzerkonten nutzen und sind dann nicht auf eine ODBC-kompatible Datenbank oder die lokale Datendatei `USERLIST.DAT` angewiesen. MDaemon-Server an mehreren Standorten können sich eine gemeinsame Benutzerdatenbank teilen.
- Die umfangreichen Auswertungs- und Parserfunktionen von MDaemon machen es möglich, dass die E-Mail-Nachrichten für ein gesamtes Netzwerk aus nur einem POP3-Postfach abgerufen werden, das der ISP bereitstellt. E-Mail-Dienste können damit zu einem Bruchteil der Kosten realisiert werden, die normalerweise hierfür anzusetzen wären.
- Mithilfe von Adress-Aliasnamen können Sie E-Mail-Nachrichten an eigentlich nicht bestehende Postfächer an gültige Benutzerkonten oder Mailinglisten leiten. Benutzerkonten und E-Mail-Adressen werden so beispielsweise über mehrere E-Mail-Adressen in einer Domäne oder mehreren Domänen erreichbar.
- Sie können mithilfe der Funktionen für Domänen-Gateways getrennte Domänen für verschiedene Abteilungen oder Gruppen einrichten, die jeweils

im lokalen Netzwerk oder an einer anderen über das Internet erreichbaren Stelle angesiedelt sind. Bei Nutzung dieser Funktion legt MDaemon alle Nachrichten an Domänen, für die MDaemon als Gateway arbeitet, im Postfach der jeweiligen Domäne ab. Von dort aus können der MDaemon-Server der Zieldomäne oder ein E-Mail-Client die Nachrichten abrufen und an die Nutzer der Domäne weiterleiten. Mithilfe dieser Funktion kann MDaemon auch als Backup-Mailserver für andere Domänen arbeiten.

- Der Server kann über die Remoteverwaltung[350] ferngewartet werden. Die Remoteverwaltung ist ein fester Bestandteil von MDaemon und Webmail und erlaubt es Ihren Benutzern, die Einstellungen für ihre Benutzerkonten mithilfe eines Webbrowsers einzusehen und zu bearbeiten. Sie legen dabei fest, welche Einstellungen ihre Benutzer bearbeiten dürfen, und sie bestimmen die Zugangsrechte auf der Ebene der Benutzerkonten. Der Systemverwalter (sowie andere Benutzer, die Sie dazu berechtigen) kann die Remoteverwaltung nutzen, um alle Einstellungen von MDaemon sowie Dateien einzusehen und zu bearbeiten, die Sie für die Bearbeitung durch die Remoteverwaltung zur Verfügung stellen.
- Ein internes System zum Nachrichtentransport, das System der RAW-Nachrichten, eröffnet eine einfache Möglichkeit, Nachrichten in den E-Mail-Fluss einzusteuern. Die Entwicklung benutzerdefinierter Mail-Software wird dadurch erheblich einfacher. Mithilfe von RAW ist es möglich, ein vollständiges Mail-System nur aus einem Text-Editor und einigen Batchdateien zu erstellen.
- Ein äußerst vielseitiger Inhaltsfilter erlaubt es Ihnen, das Verhalten des Servers anhand des Inhalts eingehender und abgehender E-Mail-Nachrichten genau zu bestimmen. Sie können den Nachrichten Kopfzeilen hinzufügen, Kopfzeilen aus ihnen löschen, den Nachrichten Fußtexte und Signaturen anfügen, Dateianlagen entfernen, Kopien an andere Benutzer leiten, Instant Messages auslösen, Programme ausführen, und vieles mehr.

MDaemon Private Cloud

MDaemon Private Cloud (MDPC) ist eine besondere Version des MDaemon Messaging Servers, die speziell für Reseller und IT-Dienstleister entwickelt wurde, damit diese ihren Kunden gehostete E-Mail-Dienste auf Basis von MDaemon anbieten können. Anders als die für den Einsatz in der hausinternen Infrastruktur lizensierten Version MDaemon wurde MDPC auf Grundlage eines neuen Lizenzmodells und einer neuen Kodebasis speziell für den Einsatz in Hostingumgebungen entwickelt. MDaemon Private Cloud enthält alle Leistungsmerkmale von MDaemon und zusätzlich die folgenden Leistungsmerkmale:

- neues Lizenz- und Abrechnungsmodell (je Nutzer/je Monat)
- Unterstützung für Microsoft Outlook
- Verbesserte Steuerung mehrere Domänen
- Branding nach Domänen getrennt (White Label)
- Berichterstellung nach Domänen getrennt
- Test-Benutzerkonten ohne Berechnung (Konten werden in den Abrechnungszahlen nicht berücksichtigt)
- Outbreak Protection, MDaemon AntiVirus und das AntiVirus-Plugin ClamAV (zusätzliche Leistungsmerkmale gegen gesondertes Entgelt)

- ActiveSync für MDaemon (zusätzliches Leistungsmerkmal gegen gesondertes Entgelt)

Systemanforderungen

Sie erhalten die jeweils neuesten Informationen über die Systemanforderungen, die für den Betrieb von MDaemon zu erfüllen sind, und die empfohlene Systemausstattung, auf der Seite Systemanforderungen der Website mdaemon.com.

Marken

Siehe auch:

Neuigkeiten MDaemon 23.0 15
Die Umstellung auf MDaemon 23.0.0 65
Die Haupt-Benutzeroberfläche von MDaemon 74
So erhalten Sie Hilfe 71

1.3 Neuigkeiten in MDaemon 23.0

Neuigkeiten MDaemon 23.0

Änderungen und neue Leistungsmerkmale

MDaemon Server

- Im Menü Server-Einstellungen steht der neue Konfigurationsdialog MultiPOP 145 zur Verfügung. Von hier aus können Sie den MultiPOP-Server von MDaemon aktivieren und deaktivieren und die Option "*MultiPOP löscht abgerufene Nachrichten immer von allen Servern*" konfigurieren (diese Option war früher Teil des Konfigurationsdialogs Abruf über MultiPOP 382), um damit die Option *Nachrichten nach Abruf nicht vom POP3-Server löschen* 739 für alle Benutzer festzulegen. Die neue Seite unterstützt auch Optionen für OAuth 2.0 für den Abruf von Nachrichten aus Gmail und Microsoft (Office) 365 über MultiPOP.

  MultiPOP OAuth 2.0 unterstützt jetzt den Abruf von Nachrichten aus Gmail und Microsoft (Office) 365 146 — OAuth 2.0 ist ein Verfahren zur modernen Authentifizierung, das Gmail und Microsoft (Office) 365 bereits erfordern oder in nächster Zeit erfordern werden. Es löst die herkömmlichen Verfahren zur Anmeldung und Authentifizierung (die sog. legacy oder basic authentication) ab. Damit MDaemon mithilfe von OAuth 2.0 über MultiPOP Nachrichten von Gmail oder Microsoft (Office) 365 für Ihre Benutzer abrufen kann, müssen Sie Ihren MDaemon-Server bei Google oder Microsoft registrieren und eine Applikation nach dem Standard OAuth 2.0 erstellen. Sie nutzen dafür die Google-API-Konsole oder das Microsoft Azure Active Directory. Die

Vorgehensweise ähnelt der Vorgehensweise, die Ihre Webmail-Benutzer zur Dropbox-Integration[336] anwenden.

- Der IMAP-Server von MDaemon unterstützt jetzt Kennzeichnungen (Flags) für Schlüsselwörter. E-Mail-Clients wie etwa Mozilla Thunderbird können damit Nachrichtentags auf dem Server speichern, die dann über alle Instanzen des Clients verfügbar sind.
- Die Leistung des IMAP-Server beim Öffnen großer Nachrichten-Ordner wurde verbessert.

Sicherheit

- Im Konfigurationsdialog für den Dynamischen Filter[612] steht die neue Option *IPs bei Verstoß gegen Anmelderichtlinien sperren* zur Verfügung, mit deren Hilfe alle IP-Adressen gesperrt werden können, die Anmeldungen ohne vollständige E-Mail-Adresse als Benutzernamen versuchen. Diese Option ist per Voreinstellung abgeschaltet. Nähere Informationen über die hiermit verbundene Option *POP-/IMAP-Server verlangen zur Echtheitsbestätigung die vollständige E-Mail-Adresse* finden Sie auf der Seite System[495].
- Die Option *Wiederholte Versuche zur Echtheitsbestätigung mit denselben Kennwörtern nicht mehrfach zählen* wurde um eine zusätzliche Option "*jedoch nur bei gültigen Benutzerkonten*" erweitert. Beide Optionen finden Sie auf der Seite Verfolgung fehlgeschlagener Echtheitsbestätigungen[616]. Diese neue Option bewirkt, dass wiederholte Versuche zur Echtheitsbestätigung mit denselben Kennwörtern nur dann nicht mehrfach gezählt werden, wenn dabei die Anmeldung an einem gültigen Benutzerkonto versucht wird. Ein Beispiel zur Vorgehensweise, wenn dies Option aktiv ist: Aktualisiert ein Benutzer ein geändertes Kennwort auf einem Client, lässt es aber auf einem anderen Client unverändert, so versucht dieser andere Client, sich mit dem veralteten Kennwort anzumelden. Diese Anmeldeversuche schlagen fehl. Sie werden aber nicht mehrfach gezählt, da jeweils ein gültiger Benutzername übermittelt wird. Versucht dagegen ein Bot die Anmeldung und probiert dabei dasselbe Kennwort in Kombination mit wahllosen nicht bestehenden Anmeldenamen aus, dann werden diese Anmeldeversuche mehrfach gezählt. Das Kennwort ist im Beispiel zwar stets gleich, aber die Anmeldenamen sind nicht gültig. Der Bot wird daher gesperrt, sobald die Höchstzahl der zulässigen fehlgeschlagenen Anmeldeversuche erreicht ist. Der Vorgang DynamicScreen des XML-API wurde aktualisiert, um die neuen Leistungsmerkmale zu berücksichtigen.
- Im Konfigurationsdialog Inhaltsfilter » Dateianlagen[662] steht eine neue Option "*Warnmeldung am Beginn des Nachrichtentexts einfügen, falls Dateianlagen entfernt wurden*" zur Verfügung. Entfernt MDaemon eine Dateianlage aus einer Nachricht, etwa, weil ein Virus gefunden wurde, so fügt MDaemon am Beginn des Nachrichtentexts eine entsprechende Warnmeldung ein. Mithilfe der Schaltfläche **Warnmeldung** können Sie den Inhalt dieser Warnmeldung einsehen und bearbeiten. Die Option ist per Voreinstellung abgeschaltet.
- Für die AntiVirus-Prüfung steht die neue Option *Gateways von der AntiVirus-Prüfung ausnehmen*[671] zur Verfügung.
- MDaemon sendet jetzt Warnhinweise per E-Mail an die Administratoren, wenn SSL-Zertifikate[577], die für die Nutzung durch MDaemon[579], Webmail[582] oder die Remoteverwaltung[586] konfiguriert sind, demnächst ablaufen.
- MTA-STS[592] wurde um eine Ausnahmeliste erweitert. Hiermit können Domänen, bei denen MTA-STS zu Problemen führt, einzeln ausgenommen

werden. MTA-STS muss dann nicht mehr insgesamt deaktiviert werden, wenn diese Probleme sich auf die Zustellung von Nachrichten auswirken.

- Das AntiVirus-Modul ClamAV wurde auf Version 0.105.1 aktualisiert.

Webmail

- Einbindung von Google Drive 339 — MDaemon Webmail kann den Benutzern Optionen anbieten, mit denen sie Dateianlagen aus Nachrichten direkt in ihre Google-Drive-Benutzerkonten speichern können. Sie können außerdem dort gespeicherte Dokumente bearbeiten und verwalten. Um diese Leistungsmerkmale zu aktivieren, sind ein **API-Schlüssel**, eine **Client-ID** und ein **Client-Schlüssel** erforderlich. Diese Daten werden direkt von Google bezogen. Hierzu muss in der Google-API-Konsole eine App erstellt, und es muss Ihre MDaemon-Installation bei Google registriert werden. Eine Komponente dieser App ist die Anmeldung über OAuth 2.0. Sie gestattet Ihren Webmail-Benutzern, sich bei Webmail anzumelden und dann den Zugriff auf ihre Google-Drive-Benutzerkonten durch MDaemon freizugeben. Sobald diese Freigabe erteilt ist, können die Benutzer ihre in Google Drive gespeicherten Ordner und Dateien einsehen. Sie können Dateien auch hochladen, herunterladen, verschieben, kopieren, umbenennen und löschen. Sie können außerdem Dateien nach und aus den lokalen Dokumentordnern kopieren und verschieben. Wenn Benutzer Dokumente bearbeiten wollen, so können Sie die Dokumente in Google Drive betrachten und Änderungen vornehmen, soweit sie in Google Drive die entsprechenden Berechtigungen haben. Die Vorgehensweise zum Einrichten des Google Drive ähnelt der Vorgehensweise bei der Integration von Dropbox 336 und MultiPOP-OAuth 145 in MDaemon. Nähere Informationen hierzu finden Sie unter Einbindung von Google Drive 339.
- In allen Designs außer Lite steht die neue Option "*Ziehen und Ablegen (Drag and Drop) zum Verschieben von Ordnern aktivieren*" zur Verfügung. Sie finden die neue Option in Webmail im Menü Optionen auf der Seite **Ordner**. Die Option ist per Voreinstellung aktiv.
- Session Cookies werden nutzen jetzt HTTPS und sind dadurch sicherer.
- Benachrichtigungen über Änderungen an Kategorien werden jetzt an MDaemon versandt.
- WorldClient ändert die Datei robots.txt nicht mehr beim Programmstart.
- Der eingebaute Web-Server verhindert jetzt das Herunterladen von DLL-Dateien aus dem HTML-Verzeichnis.
- Das Eingabefeld für Kennwörter wurde um einen Hinweis auf die höchstzulässige Länge erweitert. Wenn das Kennwort die Höchstlänge von 15 Zeichen überschreitet, erscheint ein entsprechender Hinweis.
- Anmeldeversuche, bei denen als Benutzername nicht die vollständige E-Mail-Adresse übermittelt wird, werden jetzt gemeldet. Dies ist für die Funktion der neuen Option IPs bei Verstoß gegen Anmelderichtlinien sperren 612 des Dynamischen Filters erforderlich.

Design Pro

- Lesebestätigungen werden jetzt unterstützt.
- Mithilfe einer neuen Option kann das Kontextmenü des HTML-Editors deaktiviert werden.

- Die Ordnerliste kann jetzt in der Größe verändert werden.

MDaemon-Remoteverwaltung (MDRA)

- Im Domänen-Manager steht jetzt eine Webmail-Einstellung[345] "*Benutzern den Empfang von Bestätigungskodes für die Zwei-Faktor-Authentifizierung per E-Mail gestatten*" zur Verfpgung. Benutzer können damit die Bestätigungskodes über eine gesonderte E-Mail-Adresse empfangen und müssen nicht die App Google Authenticator nutzen. Diese Option ist per Voreinstellung aktiv.
- Beim Hinzufügen einer neuen Zugriffskontrollliste (ACL) werden jetzt per Voreinstellung die Berechtigungen Anzeigen und Lesen gesetzt.
- Die Schaltflächen **Test** in den Konfigurationsdialogen Spam-Filter » DNS-BL » Hosts[704] und Einstellungen » Active Directory » Echtheitsbestätigung[818] sind jetzt abgeblendet, solange Tests ausgeführt werden.
- Der eingebaute Web-Server verhindert jetzt das Ausführen und das Herunterladen von DLL-Dateien im Verzeichnis Templates.

- Die Benutzer können das Aussehen der Benutzerschnittstelle der Remoteverwaltung jetzt ihren Wünschen anpassen. Sie klicken dazu auf ihren Benutzernamen (z.B. frank.thomas) in der oberen rechten Ecke des Fensters. Sie können mithilfe der dann zur Verfügung stehenden Optionen die Benutzerschnittstelle auf den **Dunklen Modus** umstellen, die **Schriftgröße** ändern und ihre bevorzugte **Sprache** auswählen.

  - Die Bestätigung über das Löschen von Benutzerkonten wurde angepasst und nutzt jetzt eine individuell angepasste Bestätigung.
  - Der Dynamische Filter meldet jetzt Anmeldeversuche, bei denen nicht die vollständige E-Mail-Adresse als Benutzername übermittelt wird.

ActiveSync

- Der Abschnitt Client-Einstellungen wurde um die Option *Absender sperren, wenn Nachricht in Ordner Junk-Email verschoben wird*[422] erweitert. Ist diese Option aktiv, so wird die Absender-Adresse (Felder Sender und From) einer E-Mail-Adresse in den Kontaktordner für gesperrte Absender eingetragen, sobald ein Client die zugehörige E-Mail-Nachricht in den Ordner für Spam-Nachrichten verschiebt.
- Sie können für ActiveSync jetzt die Schaltfläche zum Zurücksetzen in den Auslieferungszustand[464] deaktivieren. Sie können dann die ActiveSync-Geräte nicht mehr ferngesteuert vollständig löschen, falls Sie nicht zunächst die neue Option Löschen der Clients (Zurücksetzen in den Auslieferungszustand) nicht zulassen[422] deaktivieren.
- Die Daten aus dem Datenfeld BodyPreferences sind jetzt im Klartext lesbar. Hierdurch wird die Fehlersuche bei Synchronisierungsproblemen einfacher.
- Beim Synchronisieren besonders großer Postfächer durch Clients ist jetzt die Leistung beim Beenden der Vorgänge verbessert.
- Die Ordner für Postfächer und die öffentlichen Ordner können jetzt mit benutzerdefinierten Anzeigenamen versehen werden.
- Die Leistung beim Beenden des Programms ist verbessert.
- ActiveSync-Clients können jetzt Nachrichten an persönliche Verteilerlisten senden, die in den Kontakt-Ordnern gespeichert sind.

- Die Struktur des Konfigurationsdialogs Client-Einstellungen auf der Benutzeroberfläche wurde geändert. Sie bietet jetzt Platz für neue, zusätzliche Einstellungen.

Weiteres

- Beim Hinzufügen einer neuen Zugriffskontrollliste (ACL) über die Benutzeroberfläche von MDaemon werden jetzt per Voreinstellung die Berechtigungen Anzeigen und Lesen gesetzt.
- In der Benutzeroberfläche von MDaemon erscheint jetzt eine Warnmeldung, falls Sie versuchen, für Webmail, die Remoteverwaltung oder den XMPP-Bosh-Server Portnummern einzugeben, die einander überschneiden.
- XMLAPI - Mithilfe des neuen Vorgangs "Editor" können jetzt die verschiedenen INI-Dateien von MDaemon bearbeitet werden.
- Einige Plugins wurden geändert, sodass jetzt auch neuere Versionen ausgeführt werden können. Kunden können somit mögliche Hotfixes und Patch-Versionen erproben.

Versionsinformationen zu MDaemon Server

Sie finden eine vollständige Liste aller neuen Leistungsmerkmale, Änderungen und Fehlerbehebungen in MDaemon 23.0.0 in der Datei `RelNotes.html` im MDaemon-Verzeichnis `\Docs\`.

Neuigkeiten MDaemon 22.0

Änderungen und neue Leistungsmerkmale

Webmail

Design Pro

- Beim Betrachten einer Nachricht können Sie den Mauszeiger auf dem Namen des Absenders stehenlassen. Es erscheint dann ein Popup mit Optionen, um den Absender in die Kontakte oder die Freigabe- und Sperrlisten einzutragen.
- Ansichten zum Verfassen von Nachrichten, zum Lesen von Nachrichten und für Kalendereinträge, Kontakte, Aufgaben und Notizen können jetzt in einem neuen Fenster geöffnet werden.
- Sie können jetzt in der Nachrichtenvorschau und beim Lesen von Nachrichten die jeweils nächste ungelesene Nachricht öffnen.
- Wenn die Nachrichtenliste im Mehrzeilenmodus angezeigt wird, erscheinen jetzt auch Ausschnitte aus den Nachrichten, sog. Snippets.
- Sie können den Benutzern des Designs Pro jetzt die neue Option *Anzeigenamen für Aliasnamen bearbeiten* zugänglich machen. Die Option finden Sie unter Einstellungen » E-Mail verfassen. Hiermit können die Benutzer die Anzeigenamen für alle Aliasnamen bearbeiten, die mit ihren Benutzerkonten verbunden sind. Falls Sie den Benutzern die Nutzung dieser Option gestatten wollen, aktivieren Sie unter Webmail-Einstellungen 345 die Option *Benutzern das Bearbeiten der Anzeigenamen für ihre Aliasnamen*

gestatten. **Beachte:** Diese Option ist nur in der Webschnittstelle der MDaemon-Remoteverwaltung (MDRA) 350 verfügbar.

- Optionen und Verknüpfungen, die such auf "Weiße Listen" oder "Schwarze Listen" für Absender beziehen, wurden umbekannt. Die neu eingeführten Begriffe lauten Freigabelisten und Sperrlisten. Die früheren Ordner für die Weißen und Schwarzen Listen heißen jetzt "Freigegebene Absender" und "Gesperrte Absender".
- Die Nachrichtenliste kann jetzt auch nach der Spalte Kennzeichnung sortiert werden.
- In der Aufgabenliste erscheinen überfällige Aufgaben jetzt in roter Farbe.
- Der XMPP-Client wurde auf Version 4.4.0 aktualisiert.

Weiteres

- Wenn starke Kennwörter erzwungen werden, dann wird dem Benutzer jetzt während der Eingabe eines neuen Kennworts eine Liste der Anforderungen an die Kennwörter angezeigt. Alle Anforderungen, die das Kennwort erfüllt, erscheinen während der Eingabe schritthaltend in grüner Schrift und als abgehakt. Die Fehlermeldung, mit der unzulässige Kennwörter beim Speichern abgewiesen werden, wurde geändert und gibt jetzt klarer Auskunft darer, warum das Kennwort beanstandet wird.
- Die Optionen zum Verfassen von E-Mail-Nachrichten enthalten jetzt Einstellungen zur Auswahl der Standard-Absenderadresse ("Von:"). Die hier ausgewählte Adresse wird beim Verfassen von, Antworten auf und Weiterleiten von Nachrichten verwendet.
- Auf der Seite Optionen » Benutzeranpassung steht für das Intervall zur Aktualisierung der Nachrichtenliste jetzt auch die Option "1 Minute" zur Verfügung.
- Die Anmeldeseite für Webmail unterstützt jetzt CSRF-Token zum Schutz gegen Cross-Site-Request-Forgery. Sie sind aktiv, wenn in der MDaemon-Remoteverwaltung auf der Seite Webmail-Einstellungen » Web-Server 322 die Option "*Token zum Schutz gegen Cross-Site-Request-Forgery aktivieren*" aktiv ist. Falls Sie in Webmail benutzerdefinierte Vorlagen verwenden, fügen Sie dem Anmeldeformular ein verdecktes Eingabefeld nach folgendem Schema hinzu: `<input type="hidden" name="LOGINTOKEN" value=<$LOGINTOKEN$> />`
- Öffentlicher Kalender - Die Listenansicht wurde geändert. Sie beginnt jetzt mit dem jeweils aktuellen Tag und zeigt die folgenden 30 Tage an.
- URLs werden jetzt in der Nachrichtenansicht automatisch in Hyperlinks umgewandelt.
- Die Namen der Standard-Ordner (Entwürfe, Gesendete Elemente usw.) werden jetzt in die Sprache übersetzt, die der Webmail-Benutzer jeweils verwendet. Diese Übersetzung findet nicht nur für Englisch sondern für alle Sprachen statt, die MDaemon enthält.
- Die Anmeldekodes der Zwei-Faktor-Authentifizierung können mithilfe einer neuen Option jetzt auch an E-Mail-Adressen gesandt werden.
- Designs LookOut und WorldClient - Die Art, wie die Kategorien in Listen dargestellt werden, wurde vereinheitlicht.

- Für die Ordner Zugelassene Absender und Gesperrte Absender werden jetzt besondere Symbole angezeigt. Diese weisen darauf hin, dass es sich um besondere Ordner handelt.

MDaemon-Remoteverwaltung (MDRA)

- Die Remoteverwaltung wurde um eine Ausnahmeliste für IPs für Zwei-Faktor-Authentifizierung erweitert, für die keine Zwei-Faktor-Authentifizierung verlangt wird. Die Ausnahmen gelten für Webmail und die Remoteverwaltung und nur für Verbindungen, die von den hier erfassten IP-Adressen ausgehen.
- In der MDaemon-Remoteverwaltung steht unter Webmail-Einstellungen 345 die neue Option "*Benutzern das Bearbeiten der Anzeigenamen für ihre Aliasnamen gestatten*" zur Verfügung. Mithilfe dieser Option können Sie den Benutzern gestatten, die Anzeigenamen für alle Aliasnamen zu bearbeiten, die ihren Benutzerkonten zugeordnet sind. Sie können diese Anzeigenamen mithilfe der Option *Anzeigenamen für Aliasnamen bearbeiten* im Webmail-Design Pro bearbeiten.
- Für die Kennwortfelder wurde der Parameter autocomplete="off" in autocomplete="new-password" geändert. Hierdurch soll verhindert werden, dass Mozilla Firefox Kennwortfelder außerhalb der Anmeldeseite automatisch ausfüllt.
- Die Benachrichtigungen können jetzt über einen neuen Editor auf der Seite Benachrichtigungen 664 des Inhaltsfilters bearbeitet werden.
- Die Anmeldeseite unterstützt jetzt CSRF-Token zum Schutz gegen Cross-Site-Request-Forgery. Sie sind aktiv, wenn in der MDaemon-Remoteverwaltung auf der Seite Einstellungen zur MDaemon-Remoteverwaltung die Option "*Token zum Schutz gegen Cross-Site-Request-Forgery aktivieren*" aktiv ist.
- Falls Sie externe und lokale benutzerdefinierte Warteschlangen 869 erstellt haben, können Sie diese ab jetzt in der MDaemon-Remoteverwaltung im Abschnitt Nachrichten und Warteschlangen verwalten.

Sicherheit

- Das Modul Cyren AV 671 wurde um den Dienst Cyren Threat Lookup erweitert. Erkennt das AV-Modul eine verdächtige Datei, die nicht durch die Virendefinitionen erfasst ist, so erstellt es einen Hash der Datei und fragt den Dienst Cyren Threat Lookup ab. Der Dienst Cyren Threat Lookup ist eine vollständig cloudbasierte Lösung, mit deren Hilfe MDaemon auf Grundlage der durch Cyren weltweit über Bedrohungen gesammelten Erkenntnisse Dateien prüfen und jederzeit neueste Bewertungen von Bedrohungen durch Malware erhalten kann.
- MDaemon unterstützt auf neueren Versionen von Microsoft Windows jetzt TLS 1.3. Auf Microsoft Windows Server 2022 und Microsoft Windows 11 ist TLS 1.3 per Voreinstellung aktiv. Microsoft Windows 10 beinhaltet ab Version 2004 (Build 19041) experimentelle Unterstützung für TLS 1.3. Sie kann für eingehende Verbindungen durch Bearbeiten des folgenden Schlüssels in der System-Registrierungsdatenbank aktiviert werden:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityPro
   viders\SCHANNEL\Protocols\TLS 1.3\Server

DisabledByDefault (DWORD) = 0

Enabled (DWORD) = 1
```

- MDaemon protokolliert jetzt die in den SSL-/TLS-Verbindungen jeweils verwendete Chiffrensammlung (englisch "Cipher Suite", z.B. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384).
- Mithilfe einer neuen Option im Konfigurationsdialog Kennwörter[847] kann jetzt festgelegt werden, dass starke Kennwörter mindestens ein Sonderzeichen (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~) enthalten müssen. Diese Option ist bei Neuinstallationen per Voreinstellung aktiv und bei bestehenden Installationen per Voreinstellung abgeschaltet.
- AV-Postfachprüfung - Infizierte Nachrichten, die während der Postfachprüfung gefunden werden, werden jetzt im Zähler für infizierte Nachrichten von MDaemon ebenfalls gezählt.
- AntiVirus - ClamAV wurde auf Version 0.104.3 aktualisiert.

ActiveSync

- Die Leistung für die Synchronisierung von Ordnern (FolderSync) wurde verbessert.
- Das Kontextmenü im Fenster für den Verbindungsmitschnitt in ActiveSync-Verbindungen wurde um einen Menüpunkt erweitert, mit dessen Hilfe eine Verbindung getrennt und ein Client gesperrt werden können.
- In Microsoft Outlook können Nachrichten jetzt unter einem Alias versandt werden. Hierzu dient eine neue Option im Konfigurationsdialog Client-Einstellungen[464]. Falls als Reply-To-Adresse ein gültiger Alias für das Benutzerkonto eingetragen ist, das die Nachricht versendet, so wird die Nachricht unter diesem Alias versandt.
- Der Befehl "Find" aus der Version 16.1 des Protokolls Exchange ActiveSync (EAS) wird jetzt unterstützt. Die Protokollbeschränkung[434], durch die verhindert wurde, dass iOS-Clients die EAS-Version 16.1 nutzten, wurde entfernt.

Weiteres

- Inhaltsfilter - Der Inhaltsfilter unterstützt jetzt die Makros $CONTACT...$ für die Aktion "Unternehmenssignatur anfügen[651]". Mithilfe dieser Makros kann die Signatur durch Informationen aus dem Kontakteintrag des Absenders im Ordner für öffentliche Kontakte angepasst werden. Eine vollständige Liste der Makros, die in Signaturen zulässig sind, finden Sie unter Makros für Signaturen[136].
- Inhaltsfilter - Mithilfe einer neuen Option können jetzt Dateianlagen aus Nachrichten entnommen[651] und durch die Verlinkung von Dateianlagen[364] verarbeitet werden.
- Die per E-Mail versandten Übersichten[866] über die Inhalte der Störungs-, Quarantäne- und Defekt-Warteschlangen können jetzt Verknüpfungen enthalten, mit denen jede Nachricht zur Zustellung freigegeben, erneut in die Warteschlange eingestellt oder gelöscht werden kann. Die hierfür neu eingeführte Option "*Aktions-Verknüpfungen (...) einfügen*" ist per Voreinstellung aktiv. **Beachte:** Die Verknüpfungen werden nur erstellt, wenn der URL für die Remoteverwaltung[352] konfiguriert ist.
- LetsEncrypt[596] - Das Skript wurde aktualisiert und funktioniert jetzt auch in PowerShell 7.

- Die Optionen zur zeitversetzten Zustellung im Konfigurationsdialog Zurückrufen von Nachrichten[124] wurden um eine Option erweitert. Mit ihrer Hilfe kann die Datumskopfzeile ("Date:") mit einem aktuellen Zeitstempel versehen werden. Dieser Zeitstempel weist Datum und Uhrzeit aus, zu der die Nachrichten aus der Warteschlange für zeitversetzte Zustellung freigegeben wurde. Diese Option ist per Voreinstellung abgeschaltet.
- MDaemon Connector[385] wurde auf Version 7.0.7 aktualisiert.
- XMLAPI - Die Zeitplanung für Weiterleitungen wird jetzt unterstützt.

Versionsinformationen zu MDaemon Server

Eine Liste aller Änderungen an MDaemon finden Sie in den Versionsinformationen zu MDaemon 22.0.3.

Neuigkeiten in MDaemon 21.5

Besonders wichtige neue Leistungsmerkmale

App-Kennwörter[750]

App-Kennwörter sind sehr starke, zufällig erzeugte Kennwörter, die in E-Mail-Clients und E-Mail-Apps eingesetzt werden können. Sie erhöhen die Sicherheit Ihrer E-Mail-Apps, da diese Apps nicht durch die Zwei-Faktor-Authentifizierung[720] (2FA) geschützt werden können. Die 2FA ist ein sicheres Anmeldeverfahren, das die Benutzer für Webmail und die MDaemon-Remoteverwaltung (MDRA) nutzen können. Dieses Verfahren ist aber für E-Mail-Apps nicht einsetzbar, da diese Apps im Hintergrund auf Ihre E-Mail-Nachrichten zugreifen müssen, ohne dass Sie dazu einen Kode aus Ihrer Authentifizierungs-App eingeben. Das Leistungsmerkmal App-Kennwörter gestattet Ihnen die Erstellung starker, sicherer Kennwörter, die Sie in Ihren Apps einsetzen können, während Ihr eigentliches Kennwort für das Benutzerkonto durch die Zwei-Faktor-Authentifizierung geschützt ist. App-Kennwörter können nur in E-Mail-Apps eingesetzt werden. Für die Anmeldung an Webmail oder der MDaemon-Remoteverwaltung sind sie dagegen nicht nutzbar. Selbst wenn ein App-Kennwort daher kompromittiert werden würde, könnte eine unberechtigte Person sich damit nicht an Ihrem Benutzerkonto anmelden, um etwa Ihr Kennwort oder andere Einstellungen zu ändern. Sie selbst können sich aber mit dem Kennwort für Ihr Benutzerkonto und der Zwei-Faktor-Authentifizierung an Ihrem Benutzerkonto anmelden, das kompromittierte App-Kennwort löschen und nötigenfalls ein neues App-Kennwort erstellen.

Anforderungen an und Empfehlungen für App-Kennwörter

- App-Kennwörter können nur erstellt werden, wenn für das betreffende Benutzerkonto die Zwei-Faktor-Authentifizierung aktiv ist (diese Anforderung können Sie aber deaktivieren[847], falls gewünscht).
- App-Kennwörter können nur in E-Mail-Apps verwendet werden. Sie sind für die Anmeldung an Webmail oder der MDaemon-Remoteverwaltung nicht nutzbar.
- Jedes App-Kennwort wird nur einmal angezeigt, und zwar unmittelbar nach der Erstellung. Später kann das App-Kennwort nicht mehr angezeigt oder abgerufen werden. Die Benutzer müssen daher darauf vorbereitet sein, das App-Kennwort unmittelbar nach der Erstellung in die App einzugeben.

- Die Benutzer sollen für jede E-Mail-App ein eigenes App-Kennwort verwenden. Sie sollen App-Kennwörter, widerrufen (löschen), falls sie die zugehörige App nicht mehr verwenden, oder falls ein Gerät verlorengeht oder gestohlen wird.
- Für jedes App-Kennwort wird aufgeführt, wann es erstellt wurde, wann es zuletzt verwendet wurde, und von welcher IP-Adresse aus die Verbindung mit dem Benutzerkonto hergestellt wurde. Falls ein Benutzer Unregelmäßigkeiten beim Zeitpunkt der letzten Nutzung oder der protokollierten IP-Adresse bemerkt, sollen das betroffene App-Kennwort widerrufen und ein neues App-Kennwort erstellt werden.
- Bei Änderungen am Kennwort des Benutzerkontos werden alle App-Kennwörter des Benutzerkontos automatisch gelöscht. Die Benutzer können die zuvor gültigen App-Kennwörter dann nicht mehr verwenden.

Anmeldung an SMTP, IMAP, ActiveSync usw. nur über App-Kennwörter zulassen

Auf der Seite Einstellungen des Benutzerkonten-Editors 760 finden Sie eine Einstellung, mit deren Hilfe Sie die "*Anmeldung an SMTP, IMAP, ActiveSync usw. nur über App-Kennwörter zulassen*" können. Diese Option bewirkt, dass die Benutzerkonten in E-Mail-Clients, für die Anmeldung an SMTP, IMAP, ActiveSync und anderen E-Mail-Diensten App-Kennwörter 750 verwenden müssen. Die normalen Kennwörter 847 der Benutzerkonten müssen für die Anmeldung an Webmail oder der MDaemon-Remoteverwaltung weiterhin genutzt werden.

Wenn Sie die Nutzung von App-Kennwörtern für die genannten Anwendungsfälle erzwingen, so kann dies helfen, das Kennwort für ein Benutzerkonto gegen Brute-Force-Angriffe über SMTP, IMAP und andere Dienste zu schützen. Die Sicherheit ist in diesem Fall erhöht, da selbst bei Bekanntwerden des Kennworts für das Benutzerkonto ein Angriff über die genannten Dienste nicht möglich wäre. Ein Angreifer würde dabei nicht einmal erkennen, dass das Kennwort für das Benutzerkonto entdeckt wurde, da MDaemon für die Anmeldung an den genannten Diensten nicht das Kennwort des Benutzerkontos sondern nur ein gültiges App-Kennwort akzeptiert. Ein weiterer Vorteil ergibt sich bei der Echtheitsbestätigung mithilfe des Active Directory. Benutzerkonten im Active Directory 815 werden nach einer bestimmten Anzahl fehlerhafter Anmeldeversuche automatisch gesperrt. Die Nutzung der App-Kennwörter kann solche Sperren verhindern, da MDaemon bei aktivierter Option nur die App-Kennwörter prüft, aber keine Echtheitsbestätigung über das Active Directory versucht.

Weitere neue Leistungsmerkmale und Verbesserungen

Design Pro

- Das Design Mobile wurde in **Pro** umbenannt. Es wurde erweitert und verbessert, und es ist jetzt ein responsives und anpassbares Design, das auf verschiedenen Arten von Endgeräten und Bildschirmformaten genutzt werden kann, ohne dass dabei Funktionen verlorengehen.
- Zum Schutz gegen Cross-Site-Request-Forgery (website-übergreifende Fälschung von Anforderungen) können jetzt Token eingesetzt werden. Hierdurch wird die Sicherheit der Verarbeitung erhöht. Dieses Leistungsmerkmal ist per Voreinstellung abgeschaltet. Um dieses Leistungsmerkmal über die MDaemon-Remoteverwaltung zu aktivieren, rufen Sie die Seite Hauptmenü » Webmail-Einstellungen » Web-Server 322 auf, und

aktivieren Sie die Option "*Token zum Schutz gegen Cross-Site-Request-Forgery aktivieren*".

- Die Seite Einstellungen » Benutzeranpassung wurde um eine Option zum Aktivieren des Dunklen Modus erweitert.
- In geöffneten Nachrichten wird jetzt unter bestimmten Voraussetzungen eine Verknüpfung "Sendungsverfolgung" angezeigt.
  - Es werden per Voreinstellung die Sendungsnummern folgender Versanddienstleister ausgewertet: US Postal Service (USPS), UPS, OnTrac, FedEx und DHL.
  - Die Konfigurationsdatei mit den voreingestellten Versanddienstleistern ist unter `\MDaemon\WorldClient\package_tracking.json` gespeichert.
  - Die Administratoren können weitere Versanddienstleister hinzufügen, indem sie eine Datei `\MDaemon\WorldClient\package_tracking.custom.json` mit den entsprechenden Konfigurationsdaten erstellen. Format und Inhalt dieser Konfigurationsdatei müssen der Konfigurationsdaten für die voreingestellten Versanddienstleister, `package_tracking.json`, entsprechen. Folgende Daten sind mindestens erforderlich: Name des Versanddienstleisters, URL für die Sendungsverfolgung und mindestens ein gültiger regulärer Ausdruck.
- Die Konfiguration für die Zusammenstellung der Nachrichtenliste ist jetzt auch bei kleineren Browserfenstern eingeschränkt möglich. Es erscheint nur die Option für die Konfiguration der Anzeigedichte der Nachrichtenliste.
- Das Design wurde um eine Anzeige für die Stärke des Kennworts erweitert.
- In der Nachrichtenansicht ist jetzt das Leistungsmerkmal Diashow verfügbar.
- Die Kontakte können jetzt als Visitenkarten angezeigt werden.
- Bei Darstellung in der Fenstergröße für Desktop-Anwendungen erscheint die Schaltfläche für neue Elemente jetzt nicht mehr in der Symbolleiste sondern oberhalb der Ordnerliste.
- In der Kalenderansicht erscheint neben den persönlichen Kalendern jetzt ein Pluszeichen. Durch Anklicken dieses Pluszeichens können neue Kalender erstellt werden.
- In Kalendereinträgen wurden neue Tooltipps hinzugefügt. Mit ihrer Hilfe können Optionen bearbeitet und E-Mail-Nachrichten an Besprechungsteilnehmer gesandt werden.
- Bei Fensterbreiten der Browserfenster von mindestens 1200 Bildpunkten ist jetzt die Suchleiste immer sichtbar.
- Mithilfe eines neuen Konfigurationsdialogs können Benutzer Kontakte aus den Schwarzen Listen entfernen, wenn sie sie in die Weißen Listen eintragen. Auch der umkehrte Vorgang ist möglich.
- Falls beim Erstellen oder Umbenennen eines Ordners ein Fehler auftritt, erscheint jetzt eine entsprechende Fehlermeldung.
- HTML wird jetzt für Notizen in Kalendereinträgen, Kontakten, Aufgaben und Notizen unterstützt.
- Der bisherige HTML-Editor (CKEditor) wurde durch Jodit ersetzt.
- In der Standard-Ansicht für die Kopfzeilen erscheint jetzt auch die Zeile Von (From) mit der E-Mail-Adresse des Absenders.

- Die Sprachaufzeichnung wurde hinzugefügt.

Weitere Verbesserungen für Webmail

- Wenn eine Nachricht die Kopfzeile "List-Unsubscribe" enthält, dann erscheint jetzt neben der Absenderadresse (Von:) eine Verknüpfung zum Abbestellen der betreffenden Mailingliste. Diese Verknüpfung kann unter Einstellungen » Benutzeranpassung abgeschaltet werden.
- In eine jeweils bearbeitete Mailingliste können jetzt E-Mail-Nachrichten importiert werden.
- Die Dropbox-Integration wurde aktualisiert. Sie nutzt jetzt zur Wiederherstellung der Verbindung für Benutzer die durch Dropbox bereitgestellte Methode refresh_token. Eine Interaktion mit dem OAuth-Dialog ist dabei nicht erforderlich. Sobald die Gültigkeitsdauer für den access_token abläuft, versucht Webmail, mithilfe des refresh_tokens einen neuen access_token zu erhalten. Einige nicht mehr benötigte Einstellungen wurden aus dem Konfigurationsdialog Cloud-Apps entfernt. Die Administratoren brauchen an der Dropbox-App auf dropbox.com keine Änderungen vorzunehmen.
- Suchanfragen, die sich auf alle Ordner und Unterordner beziehen, berücksichtigen jetzt nicht abonnierte Ordner dann nicht mehr, wenn die nicht abonnierten Ordner ausgeblendet sind.
- Mithilfe der neuen Option "Für Suche überspringen" können bestimmte Ordner aus den Suchanfragen ausgeschlossen werden, die sich auf alle Ordner und Unterordner beziehen.
- Die Remoteverwaltung wurde um eine Option ergänzt, mit deren Hilfe die Option zum Speichern der Anmeldung bei Nutzung der Zwei-Faktor-Authentifizierung ausgeblendet werden kann.
- Nach Ablauf der Sitzung eines Benutzers erscheint der Hintergrund jetzt verschwommen.
- Die Seite Einstellungen » E-Mail verfassen wurde um ein Leistungsmerkmal zum automatischen Hinzufügen von CC- und BCC-Feldern erweitert.
- Mithilfe einer neuen Option kann das Verfassen von Nachrichten mit einem Aliasnamen als Absender unterbunden werden. Die Einstellung befindet sich in der Datei `WorldClient\Domains.ini` im Abschnitt `[Default:Settings]` und heißt `PreventComposeWithAlias`. Die Einstellung ist per Voreinstellung abgeschaltet.
- Design Lite - Im Editor für neue Nachrichten können Entwürfe jetzt automatisch gespeichert werden.
- Die Seite Optionen » Ordner wurde um eine Option erweitert, mit deren Hilfe die Benutzer die Kontaktordner aus der Suche durch die Funktion Autovervollständigen ausschließen können. Diese Option ist auch über das Kontextmenü erreichbar.
- Bei Anmeldungen von Benutzern an Webmail wird jetzt auch der User-Agent im Protokoll vermerkt.
- Beim Verfassen von Nachrichten erscheint jetzt ein Hinweis, falls für einen lokalen Empfänger ein Autobeantworter aktiv ist.
- Design WorldClient - Bei Darstellung von Kalendereinträgen als Kacheln erscheint jetzt in Einträgen mit Dateianlagen das Symbol einer Büroklammer.

- Bei Neuinstallationen wird die höchstzulässige Größe der Dateianlagen jetzt auf 25 MB gesetzt.
- Der Vorgang "Alle löschen" für Ordner wurde in "Ordner leeren" umbenannt.
- Design WorldClient - Die Seite Sicherheit wurde um die Schaltflächen "Kennwort ändern" und "E-Mail-Adresse für Kennwort-Wiederherstellung ändern" ergänzt.

MDaemon-Remoteverwaltung (MDRA)

- Die Regeln des Inhaltsfilters können jetzt mit Ziehen und Ablegen (Drag and Drop) bearbeitet werden. Die Schaltflächen Kopieren, Bearbeiten und Löschen werden jetzt für alle Regeln dargestellt.
- Es wurden Token zum Verhindern der Cross-Site-Request-Forgery hinzugefügt, um die Verarbeitungssicherheit zu erhöhen. Das entsprechende Leistungsmerkmal ist per Voreinstellung aktiv. Um es abzuschalten, rufen Sie die Seite Hauptmenü » Einstellungen zur Remoteverwaltung » Einstellungen, und deaktivieren Sie die Option "*Token gegen Cross-Site-Request-Forgery verwenden*".
- Einige Kennwortfelder wurden um eine Anzeige für die Stärke des Kennworts erweitert.
- Für Webmail und die Remoteverwaltung steht jetzt die Option zum Speichern von Anmeldungen für die Zwei-Faktor-Authentifizierung zur Verfügung. Sie ist nach Domänen getrennt konfigurierbar und über Einstellungen » Domänen-Manager » Bearbeiten » Webmail-Einstellungen 194 and Hauptmenü » Webmail-Einstellungen » Einstellungen 345 erreichbar.
- Der Dynamische Filter wurde um Berichte über gesperrte IP-Adressen und Verbindungen von abgewiesenen IP-Adressen erweitert.
- Im Abschnitt ActiveSync erscheinen jetzt Übersichten über Gruppen 474 und Client-Typen 481.
- Die ActiveSync-Konfigurationsdialoge Diagnose 432 und Anpassung 418 wurden aktualisiert.
- Die Seite Berichte » Datenverkehr » Statistik für Webmail-Anmeldungen wurde um Übersichtsdiagramme und -tabellen für verwendete Browser-Typen und Betriebssysteme erweitert.
- Mithilfe neuer Schaltflächen können beim Hinzufügen von Benutzern und Gruppen zu Mailinglisten auf der Seite Hauptmenü » Mailinglisten » Bearbeiten » Neu 275 Popup-Fenster aufgerufen werden, in denen die Benutzer und Gruppen zum Hinzufügen durchsucht werden können. Diese neuen Schaltflächen sind nur für Domänen-Administratoren und globale Administratoren 757 verfügbar.
- Den Seiten Hauptmenü » Mein Benutzerkonto » ActiveSync-Clients und ActiveSync » Client-Verwaltung 464 wurden Optionen zum Fernlöschen bestimmter Daten hinzugefügt.
- Alle Änderungen, die über die Remoteverwaltung vorgenommen werden, werden jetzt protokolliert.
- Die Funktionen zum Zurückrufen von Nachrichten 124 wurden aktualisiert und entsprechen jetzt denen auf der Benutzeroberfläche von MDaemon.
- Die Seite Sicherheit » Inhaltsfilter » Komprimierung 668 wurde um eine Option zur Entnahme von Dateianlagen aus Dateien des Typs winmail.dat erweitert.

- Die MDaemon-Remoteverwaltung steht jetzt auch in slowenischer Sprache zur Verfügung.

Weitere Verbesserungen für MDaemon

- Das SMTP Command Pipelining (die Verkettung von SMTP-Befehlen nach RFC 2920) wird jetzt unterstützt. MDaemon sendet ab jetzt die Befehle MAIL, RCPT und DATA nicht mehr getrennt sondern als verkettete Befehle im Stapelbetrieb. Hierdurch wird die Leistung bei Netzwerkverbindungen mit hoher Latenz erhöht. Das SMTP Command Pipelining ist für eingehende Verbindungen stets aktiv. Es ist für abgehende Verbindungen per Voreinstellung aktiv und kann im Konfigurationsdialog Einstellungen » Server-Einstellungen » Server und Zustellung » Server 94 abgeschaltet werden.
- Das SMTP Chunking (die blockweise Verarbeitung übermittelter Befehle nach RFC 3030) wird jetzt unterstützt. Das Chunking gestattet die Übermittlung nicht-zeilengetrennter Nachrichten. Es ist für eingehende Verbindungen per Voreinstellung aktiv und für abgehende Verbindungen per Voreinstellung abgeschaltet. Reine Zeilenvorschübe (line feeds oder LF) in empfangenen Nachrichten werden per Voreinstellung in Zeilenvorschübe mit Wagenrücklauf (carriage return line feeds oder CRLF) umgewandelt. Diese Voreinstellungen können durch Bearbeiten der Optionen `SMTPChunkingInbound=Yes/No`, `SMTPChunkingOutbound=Yes/No` und and `SMTPChunkingAllowBareLF=Yes/No` im Abschnitt `[Special]` der Datei `\MDaemon\App\MDaemon.ini` geändert werden.
- Inhaltsfilter - Die voreingestellte Liste für die gesperrten Dateianlagen 662 wurde aktualisiert.
- Inhaltsfilter - Mithilfe einer neuen Regeln können Dateianlagen in Nachrichten eingefügt werden 651.
- Die Meldungen beim Starten und Beenden des ActiveSync-Servers werden jetzt in das MDaemon-Protokoll System eingetragen.
- Cluster-Betrieb - Terminerinnerungen können jetzt von Sekundärknoten aus synchronisiert werden.
- Dynamischer Filter - Die Länderdaten können mithilfe einer neuen Option jetzt wahlweise auch als Codes nach ISO-Standard 3166 612 und nicht mehr nur als vollständige Namen protokolliert werden.
- XMLAPI - Die ActiveSync-Einstellung AlwaysSendMeetingUpdates wird jetzt unterstützt.
- XMLAPI - Die Erstellung von Signal- oder Semaphoredateien wird jetzt unterstützt.
- XMLAPI - Einstellungen des Konfigurationsdialogs Einstellungen » Server-Einstellungen » Protokollierung können jetzt als Berichte ausgegeben und geändert werden.
- MDaemon Instant Messenger - Die Leistungsmerkmale für den Chat in Konferenzräumen wurden verbessert; es können jetzt mehrere Kontakte für einen Chat in einem Konferenzraum gleichzeitig ausgewählt werden. Darüber hinaus können die Benutzer jetzt Aufforderungen, einen Konferenzraum zu betreten, automatisch akzeptieren.
- Mithilfe einer neuen Option für den Länder-Filter 574 kann bestimmt werden, ob den Nachrichten die Kopfzeile "`X-MDOrigin-Country`" hinzugefügt wird. Diese Option ist per Voreinstellung aktiv.

- Der Konfigurationsdialog Benutzerkonten » Benutzerkonten-Einstellungen » Aliasnamen » Einstellungen[829] wurde um eine Option erweitert, die bestimmt, ob Aliasnamen zur Anmeldung verwendet werden dürfen. Diese Option ist per Voreinstellung aktiv.
- MDaemon Connector wurde auf Version 7.5.0 aktualisiert.
- Die Standard-Nachricht für die Bestätigung von Zustellungen (sie ist gespeichert unter \MDaemon\App\Receipt.dat) wurde geändert. In ihr wird jetzt das Makro `$HEADER:X-RCPT-TO$` und nicht mehr, wie bisher, das Makro `$RECIPIENT$` verwendet. Hierdurch wird die Offenlegung der E-Mail-Adresse vermieden, in die ein Aliasname im jeweiligen Fall umgewandelt wird.

Versionsinformationen zu MDaemon Server

Eine Liste aller Änderungen an MDaemon finden Sie in den Versionsinformationen zu MDaemon 21.5.2.

Neuigkeiten in MDaemon 21.0

Besonders wichtige neue Leistungsmerkmale

Dauerhaft eingerichtete Konferenzräume[374]

Der XMPP-Server von MDaemon unterstützt jetzt dauerhaft eingerichtete Konferenzräume, die auch als ständige Konferenzräume bezeichnet werden. Solche Konferenzräume müssen nicht neu eingerichtet werden, auch wenn zuvor alle Benutzer die Konferenzräume verlassen haben. Sie können diese Konferenzräume unter Einstellungen | Web- & IM-Dienste | XMPP konfigurieren.

Berichte über Falschbewertung von Viren und Spam

In den Übersichten der Benutzeroberfläche von MDaemon für die Warteschlangen für Quarantäne, defekte Nachrichten und die Spam-Fallen steht jetzt in den durch Rechtsklick erreichbaren Kontextmenüs eine neue Option zur Verfügung. Mit ihrer Hilfe können Nachrichten als falsch positiv oder falsch negativ an MDaemon.com gemeldet werden. Die MDaemon-Remoteverwaltung wurde um ähnliche Optionen erweitert. Die so gemeldeten Nachrichten werden analysiert und auch an Dritte weiter übermittelt, damit diese entsprechende Korrekturen veranlassen können.

Grafische Benutzeroberfläche (GUI) für den ActiveSync Migration Client (ASMC)

Für den ActiveSync Migration Client (ASMC) steht jetzt eine grafische Benutzeroberfläche (`ASMCUI.exe` im Verzeichnis `\app\` unter dem Hauptverzeichnis von MDaemon) zur Verfügung, die seine Benutzung erleichtern soll. Mit ihrer Hilfe können Sie Optionen auch speichern und später erneut abrufen. ASMC unterstützt die Migration von Nachrichten, Kalendern, Aufgaben, Notizen und Kontakten von ActiveSync-Servern, die die Protokollversion 14.1 unterstützen. Eine Dokumentation hierzu steht im Verzeichnis Docs unter dem Hauptverzeichnis von MDaemon zur Verfügung. Der Pfad lautet `\MDaemon\Docs\ActiveSync Migration Client.html`.

Verbesserungen für das Webmail-Design Mobile

Das Design Mobile für die Webmail-Nutzer wurde erheblich erweitert und verbessert. Sie finden eine vollständige Liste der zahlreichen neuen Leistungsmerkmale in der Datei `RelNotes.html` im Verzeichnis `\Docs\` unter dem Hauptverzeichnis von MDaemon.

Verbesserungen für den Cluster-Betrieb

Der Cluster-Dienst von MDaemon wurde erheblich verbessert:

- Das Routing von Nachrichten kann jetzt durch mehrere Knoten durchgeführt werden. Hierzu werden die Nachrichten-Warteschlangen durch die Knoten eines Clusters gemeinsam genutzt. Diese arbeitsteilige Verarbeitung und Zustellung der Nachrichten durch mehrere Server gestattet eine gleichmäßigere Auslastung der Knoten und verhindert beispielsweise, dass Nachrichten in den Warteschlangen ausgefallener Knoten steckenbleiben.
- SSL-Zertifikate werden durch den Primär-Knoten auf die Sekundär-Knoten repliziert.
- Während der ersten Replikation der Daten werden die Warteschlangen auf Sekundär-Knoten eingefroren. Hierdurch erhöht sich die Antwortgeschwindigkeit während des Programmstarts.
- Wenn MDaemon beendet wird, wird die Replikation jetzt unterbrochen. Hierdurch werden Verzögerungen bei der Beendigung von MDaemon beseitigt, die sich aus dem Cluster-Betrieb ergeben.
- Knoten können jetzt auch durch Angabe von IP-Adressen oder DNS-Namen in den Cluster aufgenommen werden.
- Die Pfade für die Netzwerkfreigaben können jetzt mithilfe des neuen Konfigurationsdialogs Pfade für Netzwerkfreigaben einfacher verwaltet werden.
- Die Leistungsmerkmale zur Protokollierung und zur Diagnose werden jetzt auf dem neuen Konfigurationsdialog Diagnose bereit gestellt.

Weitere neue Leistungsmerkmale und Änderungen

MDaemon-Remoteverwaltung (MDRA)

Die MDaemon-Remoteverwaltung wurde um zahlreiche Optionen erweitert. Sie finden eine vollständige Liste dieser neuen Optionen und weiterer Änderungen an der Remoteverwaltung in der Datei `RelNotes.html` im Verzeichnis `\Docs\` unter dem Hauptverzeichnis von MDaemon.

Inhaltsfilter

Gesperrte Dateianlagen können jetzt auch in Archiven des Formats 7-Zip gesucht und erkannt werden.

Autobeantworter

Die Autobeantworter unterstützen jetzt Unicode (UTF-8). Die Texte für die Autobeantworter können daher jetzt in beliebigen Sprachen abgefasst sein.

IMAP-Filter 736

Die Filterregeln für die IMAP-Filter können jetzt die Nachrichtentexte nach bestimmten Zeichenketten durchsuchen.

Webmail

- In den Designs LookOut und WorldClient können Kalendereinträge über das Kontextmenü an neue E-Mail-Nachrichten angehängt werden. Im Design Mobile ist dies in der Vorschau für den Kalendereintrag möglich.
- Alle Leistungsmerkmale zur Erstellung neuer Benutzerkonten wurden entfernt.
- Beim Veröffentlichen eines Kalenders (etwa durch Verteilen einer Verknüpfung für den öffentlichen Zugriff) können Sie jetzt mithilfe neuer Optionen die Standardansicht für den Kalender bestimmen (Monat/Woche/Tag) und auch eine Verknüpfung zu den Frei/Gebucht-Informationen veröffentlichen.
- Einzelne Webmail-Benutzer können jetzt von dem Erfordernis ausgenommen werden, dass ihre IP-Adresse während der Verbindung gleich bleiben muss. In der MDaemon-Remoteverwaltung bearbeiten Sie zum Aktivieren dieser Ausnahme das gewünschte Benutzerkonto, rufen Sie die Seite Web-Dienste auf, und aktivieren Sie die Option "Prüfung auf gleichbleibende IP-Adresse während Webmail-Verbindung überspringen".
- Die erweiterte Suche kann jetzt auch das Feld CC durchsuchen.
- In den Kontingentdaten erscheint jetzt auch die Höchstzahl der täglich versandten Nachrichten 731.

Benutzeroberfläche

- Der Konfigurationsdialog Einstellungen | Verwaltung für mobile Endgeräte wurde entfernt und durch den ActiveSync-Konfigurationsdialog ersetzt, der über Einstellungen | ActiveSync erreichbar ist.
- Der Konfigurationsdialog für die ActiveSync-Client-Einstellungen wurde entfernt. Sie können die Client-Einstellungen über die Konfigurationsdialoge Anpassung, Domänen, Gruppen, Benutzerkonten und Clients konfigurieren.
- Der Konfigurationsdialog für die Client-Typen für ActiveSync wurde um Menüeinträge ergänzt, mit deren Hilfe Client-Typen in die Schwarzen und Weißen Listen eingetragen werden können.
- Ein neuer Konfigurationsdialog Einstellungen | Nachrichten-Indexierung wurde hinzugefügt. Hier wird die Erstellung von Such-Indizes in Echtzeit und während der täglichen Wartung um Mitternacht gesteuert. Die Indizes werden durch Webmail, ActiveSync und die Remoteverwaltung genutzt.
- Für mehrere Plugins ist jetzt ein gemeinsamer Konfigurationsdialog Diagnose vorhanden.
- Die browsergestützten Hilfesysteme in der MDaemon-Remoteverwaltung und in Webmail wurden auf ein neues responsives Design umgestellt. Sie werden hierdurch besser auf unterschiedlichen Gerätetypen nutzbar.

XML-API

- Das Erscheinungsbild des Dokumentationsportals für das XMLAPI kann jetzt global und nach Domänen getrennt geändert werden. Nähere Informationen

hierzu finden Sie in englischer Sprache unter "Changes and development notes" (Änderungen und Hinweise zur Entwicklung) im Hilfe-Portal. (Sie erreichen das Hilfe-Portal über http[s]://Servername[:MDRA-Port]/MdMgmtWS) Alternativ können Sie die Datei \MDaemon\Docs\API\XML API\Help_Readme.xml im Installationsverzeichnis Ihrer MDaemon-Installation mit dem Microsoft Internet Explorer betrachten, um weitere Informationen zu erhalten. Ein Beispielsverzeichnis für die Domäne company.mail ist unter \MDaemon\Docs\API\XML API\Samples\Branding abgelegt.

- Der Vorgang Alias wurde hinzugefügt, um Verwaltung, Auflösung und Berichte für Aliasnamen zu vereinfachen.
- Die Aktion FolderOperation Search wurde hinzugefügt, um Nachrichten zu durchsuchen.
- QueryServiceState und ControlServiceState unterstützen jetzt den Cluster-Betrieb.

Archivierung 131

- Wird eine Nachricht von einem lokalen an ein lokales Benutzerkonto gesendet, so werden Archivkopien für die versendete und die empfangene Nachricht erstellt, falls sowohl die Archivierung abgehender als auch die Archivierung eingehender Nachrichten aktiv sind.
- Die Option zur Archivierung von Spam-Nachrichten, die aus Version 20.0 entfernt wurde, ist wieder verfügbar.
- Spam-Nachrichten werden archiviert, wenn sie aus der Spam-Falle freigegeben werden.

Aktualisierung verschiedener Komponenten

- MDaemon Connector wurde auf Version 7.0.0 aktualisiert.
- Der Spam-Filter wurde auf SpamAssassin 3.4.4 aktualisiert, und nicht mehr unterstützte Einstellungen wurden aus der Datei local.cf entfernt.
- AntiVirus: ClamAV wurde auf Version 0.103.0 aktualisiert. Cyren AV wurde auf Version 6.3.0.2 aktualisiert.
- XMPP-Server: Das Datenbank-Backend wurde auf SQLite 3.33.0 aktualisiert.

Versionsinformationen zu MDaemon Server

Eine Liste aller Änderungen an MDaemon finden Sie in den Versionsinformationen zu MDaemon 21.0.2.

Neuigkeiten in MDaemon 20.0

Cluster-Dienst für MDaemon 406

Die neuen Leistungsmerkmale für den Cluster-Betrieb von MDaemon ermöglichen die gemeinsame Nutzung Ihrer Konfiguration durch mehrere MDaemon-Server in Ihrem Netzwerk. Hiermit können Sie beispielsweise Lastverteilung für die Hardware- oder Software-Auslastung umsetzen und die im E-Mail-Betrieb anfallende Systemlast auf mehrere MDaemon-Server verteilen. Dies kann durch möglichst große Ausnutzung Ihrer E-Mail-Ressourcen Verarbeitungsgeschwindigkeit und Effizienz erhöhen, die

Netzwerkauslastung senken und Überlastungen verringern. Es kann außerdem die Ausfallsicherheit Ihrer E-Mail-Systeme in den Fällen erhöhen, in denen auf einem Server ein Hardware- oder Softwareausfall eintritt.Nähere Informationen über die Einrichtung eines MDaemon-Serverclusters in Ihrem Netzwerk finden Sie im Abschnitt Cluster-Dienst 406.

Neue SMTP-Erweiterungen

RequireTLS (RFC 8689) 592

Die Arbeit der IETF an RequireTLS ist abgeschlossen, und dieses Leistungsmerkmal ist jetzt verfügbar. Mithilfe von RequireTLS können Sie festlegen, welche Nachrichten **zwingend** über TLS-geschützte Verbindungen übermittelt werden **müssen**. Steht TLS für die Übermittlung einer solchen Nachricht nicht zur Verfügung, oder sind die Parameter, die während des TLS-Verbindungsaufbaus und für die beteiligten Zertifikate übermittelt werden, nicht akzeptabel, so werden die Nachrichten zurückgeleitet und nicht etwa ohne TLS zugestellt. RequireTLS ist per Voreinstellung aktiv. RequireTLS wirkt jedoch nur auf solche Nachrichten, die aufgrund der neuen Aktion des Inhaltsfilters 651 des Inhaltsfilters "*Nachricht für REQUIRETLS kennzeichnen...*" ("*Flag message for REQUIRETLS...*") besonders gekennzeichnet werden, oder die an nach dem Schema `<Postfach>+requiretls@Domäne.TLD` aufgebaute E-Mail-Adressen (z.B. `arvel+requiretls@mdaemon.com`) versandt werden. Regeln des Inhaltsfilters für die genannte Kennzeichnung müssen Sie selbst erstellen. Alle anderen Nachrichten werden so verarbeitet, als ob das Leistungsmerkmal nicht aktiv wäre. Nachrichten, für die RequireTLS aktiv ist, können nur dann erfolgreich versandt werden, wenn bestimmte Bedingungen alle erfüllt sind. Ist auch nur eine Bedingung nicht erfüllt, so werden die Nachrichten nicht etwa über eine unverschlüsselte Verbindung übermittelt sondern an den Absender zurückgeleitet. Nähere Informationen über diese Anforderungen finden Sie im Abschnitt SMTP-Erweiterungen 592. Eine vollständige Beschreibung für RequireTLS finden Sie in englischer Sprache unter RFC 8689: SMTP Require TLS Option.

SMTP MTA-STS (RFC 8461) - Strict Transport Security 593

Die Arbeit der IETF an MTA-STS ist abgeschlossen, und dieses Leistungsmerkmal ist jetzt verfügbar. Das Verfahren SMTP MTA Strict Transport Security (abgekürzt MTA-STS, Verfahren für erzwungene Transportverschlüsselung für SMTP-Mailserver) gestattet es Anbietern von E-Mail-Dienstleistungen, bekannt zu geben, dass sie durch Transport Layer Security (TLS) transportverschlüsselte SMTP-Verbindungen unterstützen. Darüber hinaus können sie festlegen, dass SMTP-Server, die Nachrichten an sie übermitteln wollen, die Übermittlung von Nachrichten an solche MX-Hosts ablehnen sollen, die TLS mit einem vertrauenswürdigen Server-Zertifikat nicht unterstützen. Nähere Informationen über die Einrichtung dieses Leistungsmerkmals finden Sie im Abschnitt SMTP-Erweiterungen 592. Sie finden eine Beschreibung dieses Leistungsmerkmals in englischer Sprache unter RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

SMTP TLS Reporting (RFC 8460) 594

Mithilfe des Leistungsmerkmals zur Berichterstellung über SMTP TLS, kurz "TLS-Berichte" genannt, können Domänen, die MTA-STS einsetzen, Benachrichtigungen erhalten, falls der Abruf der Richtliniendatei für MTA-STS oder die Herstellung einer verschlüsselten Verbindung mittels STARTTLS fehlschlagen. Wenn dieses Leistungsmerkmal aktiv ist, sendet MDaemon einmal täglich einen Bericht an alle Domänen, an die MDaemon während des zurückliegenden Tages Nachrichten versandt oder zu versenden versucht hat, und für die MTA-STS aktiv ist. Es stehen mehrere Optionen zur Konfiguration des

Inhalts dieser Berichte zur Verfügung. Nähere Informationen über die Einrichtung dieses Leistungsmerkmals finden Sie im Abschnitt SMTP-Erweiterungen[592]. Sie finden eine Beschreibung dieses Leistungsmerkmals in englischer Sprache unter RFC 8460: SMTP TLS Reporting.

Domänen-/Unternehmensweite Verschlüsselung über MDPGP mithilfe eines einzigen Schlüssels

MDPGP[631] unterstützt jetzt die Verschlüsselung von Nachrichten zwischen Domänen mithilfe eines einzigen Schlüssels für alle Benutzer. Ein Beispiel hierzu: Sollen alle zwischen "Domäne-A" und "Domäne-B" ausgetauschten Nachrichten verschlüsselt übermittelt werden, soll aber gleichzeitig vermieden werden, jeden Benutzer der Domänen mit einem eigenen Schlüsselpaar auszustatten und die Nutzung der Schlüssel entsprechend zu verwalten, so bietet das neue Leistungsmerkmal hierfür eine Lösung:

"Domäne-A" und "Domäne-B" übermitteln einander auf einem frei wählbaren Weg ihre öffentlichen Schlüssel. Sie können beispielsweise die öffentlichen Schlüssel über das Kontextmenü der Benutzeroberfläche von MDPGP exportieren und per E-Mail versenden. Sie können, falls gewünscht, neue besondere Schlüssel für diesen Zweck erstellen und dazu nach Anklicken der Schaltfläche "Schlüssel für bestimmten Benutzer erzeugen" die neue Option "Domänenschlüssel (Domäne.TLD)" verwenden. Der Erstellungsvorgang entspricht ansonsten dem Vorgang für die Erstellung benutzerindividueller Schlüssel. Sie können auch bereits bestehende Schlüssel verwenden. Sobald jede Domäne den öffentlichen Schlüssel der jeweils anderen Domäne erhalten hat, kann dieser mithilfe der Schaltfläche "Domänen-Schlüssel importieren" auf der Benutzeroberfläche von MDPGP importiert werden; hierbei wird der Domänenname der Domäne angegeben, deren Nachrichten mit diesem Schlüssel verschlüsselt werden sollen.

Falls einer Domäne bereits ein öffentlicher Schlüssel vorliegt, den sie nutzen will, und dieser Schlüssel bereits im Schlüsselbund enthalten ist, kann der Schlüssel mithilfe der neuen Option "Schlüssel als Domänen-Schlüssel festlegen" im Kontextmenü der Benutzeroberfläche von MDPGP als Domänen-Schlüssel festgelegt werden. Für diese Art der Verschlüsselung dürfen Sie keinen Schlüssel nutzen, für den Ihnen auch der zugehörige geheime Schlüssel vorliegt. Nutzen Sie einen solchen Schlüssel, dann verschlüsselt MDPGP die Nachricht zunächst, stellt dann aber sofort fest, dass der geheime Schlüssel für die Entschlüsselung bekannt ist, und entschlüsselt die Nachricht daher unmittelbar wieder.

Nach Abschluss des oben dargestellten Konfigurationsvorgangs erstellt MDPGP eine Regel des Inhaltsfilters, die bewirkt, dass alle an die betreffende Domäne gerichteten Nachrichten mit dem ausgewählten öffentlichen Schlüssel verschlüsselt werden. Sie können diesen Vorgang steuern, indem Sie die Regel im Inhaltsfilter aktivieren oder deaktivieren, und Sie können die Regel auch anpassen. Beispielsweise könnten Sie die Regel auf mehrere Domänen oder nur auf bestimmte Benutzer innerhalb der Domänen wirken lassen. Der Inhaltsfilter ermöglicht auch solche Anpassungen.

Verschlüsselung abgehender Nachrichten anhand der IP-Adresse des Empfängers

MDPGP[631] wurde um eine Option erweitert, mit deren Hilfe Sie bestimmte Schlüssel IP-Adressen zuordnen können. Wird eine abgehende SMTP-Verbindung mit einer hier zugeordneten IP-Adresse hergestellt, so werden alle abgehenden Nachrichten, die an diese IP-Adresse übermittelt werden, vor der Übermittlung mit dem der IP-Adresse zugeordneten Schlüssel verschlüsselt. Nachrichten, die bereits

verschlüsselt sind, werden nicht verändert und nicht erneut verschlüsselt. Dieses Leistungsmerkmal ist beispielsweise in Anwendungsfällen hilfreich, in denen Sie sicherstellen wollen, dass alle Nachrichten an bestimmte Gegenstellen (etwa wichtige Partner, Zulieferer, verbundene Unternehmen usw.) immer verschlüsselt werden.

Makros für Nachrichten in Mailinglisten

Der Konfigurationsdialog Editor für Mailinglisten » Routing 294 wurde um einige Optionen erweitert, mit deren Hilfe Makros im Nachrichtentext von Nachrichten genutzt werden können, die in Mailinglisten veröffentlicht werden. Beispielsweise können jetzt alle Listennachrichten personalisiert werden. In den Einleitungs- und Schlusstexten wurden Makros auch bisher schon unterstützt; neu ist die Unterstützung für Makros im Nachrichtentext selbst. Da sich die Makros auf die einzelnen Empfänger der Listennachrichten beziehen, sind sie in solchen Mailinglisten nutzbar, für die die Option "*Listennachrichten an jedes Mitglied einzeln zustellen*" aktiv ist. Da anzunehmen ist, dass nicht unbedingt beliebige Mitglieder einer Mailingliste die Makros nutzen sollen, kann die Nutzung und Umsetzung der Makros auf solche Nachrichten beschränkt werden, in denen der Absender das Listenkennwort angibt. Eine entsprechende Option steht zur Verfügung; ist sie aktiv, und wird das Listenkennwort nicht angegeben, so werden die Makros nicht umgesetzt. Das Listenkennwort gehört zu einer bereits bestehenden Option, die Sie im Abschnitt Moderation finden. Wird kein Listenkennwort festgelegt, so kann jedes Listenmitglied mit der Berechtigung zum Veröffentlichen von Nachrichten die Makros in den Nachrichtentexten nutzen. Nähere Informationen hierzu und eine Liste der unterstützten Makros finden Sie im Abschnitt Routing in Mailinglisten 294.

Verbessertes System zur Hijacking-Erkennung

Der Konfigurationsdialog Hijacking-Erkennung 569 wurde um mehrere Optionen erweitert, die verhindern sollen, dass ein Benutzerkonto zum Massenversand von Spam missbraucht wird, wenn seine Zugangsdaten kompromittiert sind. MDaemon zählt zu diesem Zweck, wie oft echtheitsbestätigte Benutzer versuchen, E-Mail-Nachrichten an ungültige Empfänger zu senden. Ein Empfänger wird dann als ungültiger Empfänger gezählt, wenn während der Übermittlung der Nachricht der Server des Empfängers auf den Befehl RCPT hin einen Fehler 5xx meldet. Treten zu viele solche Fehler binnen zu kurzer Zeit auf, so kann MDaemon das Benutzerkonto des Absenders einfrieren. Der Postmaster wird hiervon per E-Mail benachrichtigt und kann das Benutzerkonto wieder freigeben. Dieses neue Leistungsmerkmal verwirklicht eine leistungsfähige Maßnahme, um Benutzerkonten zu schützen, deren Zugangsdaten entwendet wurden, und die zum Spam-Versand in großem Umfang missbraucht werden. Dem Leistungsmerkmal liegt die Annahme zugrunde, dass beim den gängigen Versuchen, Spam zu versenden, die Fehler 5xx (Benutzer unbekannt) häufig auftreten werden. Das Leistungsmerkmal soll verhindern, dass Benutzerkonten nach einem Hijacking zu umfangreichen Schaden anrichten. **Beachte:** Im Rahmen der Umsetzung dieses Leistungsmerkmals mussten die Optionen zur Auswertung und Bearbeitung der Absenderkopfzeile From in den neuen Konfigurationsdialog From-Header-Auswertung 576 verlegt werden, um Platz für die neuen Optionen zur Hijacking-Erkennung zu schaffen.

Warteschlange für zeitversetzte Zustellung und Verbesserungen beim Zurückrufen von Nachrichten 124

MDaemon verfügt jetzt über eine eigene Warteschlange für Nachrichten, deren Zustellung verzögert oder zeitversetzt erfolgt. Die Verzögerung in der Zustellung kann aufgrund des Leistungsmerkmals Zurückrufen von Nachrichten oder aufgrund der jetzt unterstützten Kopfzeile Deferred-Delivery (zeitversetzte Zustellung)

eintreten. Vor Einführung dieser neuen Warteschlange war die Eingangs-Warteschlange bisweilen mit Nachrichten überfüllt, deren Zustellung zeitversetzt erfolgte, und die bisweilen die Zustellung normaler Nachrichten verlangsamten. Die neue Warteschlange hilft, dieses Problem zu beseitigen. Die betreffenden Nachrichten werden durch das System in die Warteschlange für zeitversetzte Zustellung aufgenommen, und Datum und Uhrzeit, zu der sie die Warteschlange verlassen sollen, sind in den Dateinamen kodiert. MDaemon prüft die Warteschlange für zeitversetzte Zustellung einmal pro Minute und verschiebt die Nachrichten, deren Zustellzeitpunkt gekommen ist, in die Eingangs-Warteschlange. Von dort aus werden sie normal weiter verarbeitet.

MDaemon protokolliert jetzt außerdem die Nachrichten-ID der jeweils letzten E-Mail-Nachricht, die lokale Benutzer nach der Anmeldung echtheitsbestätigt versenden. Hierdurch können die Benutzer die jeweils letzte versandte Nachricht (und nur diese) zurückrufen, indem sie den Begriff RECALL auf die Betreffzeile einer Nachricht setzen und diese Nachricht an das MDaemon-Systemkonto (mdaemon@) senden. Will ein Benutzer die letzte versandte Nachricht zurückrufen, so braucht er dann nicht erst die Nachrichten-ID zu recherchieren und in die Anforderung einzusetzen. Will er hingegen eine andere Nachricht zurückrufen, so muss er weiterhin entweder die Nachrichten-ID der zurückzurufenden Nachricht auf die Betreffzeile setzen oder die zurückzurufende Nachricht aus seinem Ordner für gesendete Objekte an die Anforderung als Dateianlage anfügen.

Neben der letzten jeweils durch die Benutzer versandten E-Mail-Nachricht speichert MDaemon auch die Speicherorte und Nachrichten-IDs der letzten 1000 E-Mail-Nachrichten, die durch alle echtheitsbestätigten Benutzer insgesamt gesendet wurden. Aufgrund dieser neuen Vorgehensweise können zurückgerufene Nachrichten auch nach der Zustellung noch aus den Postfächern der Benutzer entfernt werden; sie erscheinen nach dem Rückruf nicht mehr in den Mailclients und auf den mobilen Endgeräten der Benutzer. **Beachte:** Diese Vorgehensweise ist nur für solche Nachrichten möglich, die an andere lokale Benutzer gesandt wurden. Sobald MDaemon eine Nachricht an einen anderen Server übermittelt hat, steht diese Nachricht nicht mehr unter der Kontrolle von MDaemon, und sie kann daher nicht mehr zurückgerufen werden.

Protokoll für fehlgeschlagene Versuche zur Echtheitsbestätigung

There is a new Authentication Failures log file that contains a single line with details for every SMTP, IMAP, and POP logon attempt that fails. The information includes the Protocol used, the SessionID so you can search other logs, the IP of the offender, the raw Logon value they tried to use (sometimes this is an alias), and the Account that matches the logon (or 'none' if no account matches).

Es steht ein neues Protokoll für fehlgeschlagene Versuche zur Echtheitsbestätigung zur Verfügung. In diesem Protokoll wird jeder Anmeldeversuch oder Versuch zur Echtheitsbestätigung protokolliert, der für SMTP, IMAP und POP fehlschlägt. Jeder Versuch wird auf einer eigenen Zeile protokolliert. Protokolliert werden auch das genutzte Übermittlungsprotokoll, die Verbindungs-ID, nach der in anderen Protokollen gesucht werden kann, die IP-Adresse der Gegenstelle, die die Echtheitsbestätigung erfolglos versucht hat, der verwendete Anmeldename (dies kann auch ein Alias sein), und das Benutzerkonto, dem der Anmeldename zugeordnet ist (falls kein übereinstimmendes Benutzerkonto besteht, wird "none" protokolliert).

Echtheitsbestätigung bei Weiterleitung und Routing von Nachrichten

Es stehen mehrere Optionen zur Weiterleitung in MDaemon zur Verfügung, für die Sie jetzt Zugangsdaten festlegen können. Aufgrund dieser Änderungen können jetzt

mehrere Dateien im Verzeichnis \APP\ verschleierte Anmelde- und Kennwortdaten in sehr schwacher Verschlüsselung enthalten. Zu diesen Dateien gehören `forward.dat`, `gateways.dat`, `MDaemon.ini`, alle `GRP`-Dateien für Mailinglisten und weitere Dateien. Wir weisen Sie daher, wie auch sonst, darauf hin, dass Sie die Funktionen des Betriebssystems sowie weitere Maßnahmen nutzen müssen, um das System, auf dem MDaemon läuft, und die Verzeichnisstruktur von MDaemon gegen unbefugten Zugriff zu sichern. Die folgenden Konfigurationsdialoge wurden um Funktionen für die Echtheitsbestätigung erweitert: Unzustellbare Nachrichten 106, Routing in Mailinglisten 294, Gateway-Editor » Weiterleitung 263, Gateway-Editor » Freigabe wartender Nachrichten 264 und Benutzerkonten-Editor » Weiterleitung 727.

Host-bezogene Echtheitsbestätigung 127

Mithilfe des neuen Konfigurationsdialogs Host-bezogene Echtheitsbestätigung können Sie für beliebige Hosts Port, Anmeldenamen und Kennwort konfigurieren. Sendet MDaemon Nachrichten per SMTP an einen hier erfassten Host, so werden die dem Host hier zugeordneten Anmeldedaten verwendet. Bitte beachten Sie, dass diese Anmeldedaten nur dann verwendet werden, wenn für die jeweilige Aufgabe besonders konfigurierte Anmeldedaten nicht zur Verfügung stehen. Konfigurieren Sie beispielsweise Anmeldedaten mithilfe der neuen Optionen zur Weiterleitung in den Konfigurationsdialogen Benutzerkonten-Editor » Weiterleitung 727 oder Gateway-Manager » Freigabe wartender Nachrichten 264, so werden diese aufgabenspezifischen Anmeldedaten statt der hier konfigurierten Anmeldedaten verwendet. Dieses Leistungsmerkmal arbeitet nur mit Hostnamen, nicht mit IP-Adressen.

Verbesserungen für benutzerdefinierte Warteschlangen und Nachrichten-Routing 869

Sie können jetzt für jede Warteschlange für die externe Zustellung Host, Anmeldenamen, Kennwort, SMTP-Antwortpfad und Port angeben. Falls diese Daten konfiguriert sind, werden grundsätzlich alle Nachrichten in der Warteschlange unter Berücksichtigung der Daten und der neuen Einstellungen zugestellt. Nachrichten können aber auch dann unter Verwendung besonderer Einstellungen zur Zustellung zugestellt werden, wobei die Einstellungen in diesem Konfigurationsdialog übergangen werden. Sie können jetzt beliebig viele Extern-Warteschlangen einrichten, Nachrichten mithilfe des Inhaltsfilters auf die Warteschlangen verteilen und dabei alle durch den Inhaltsfilter unterstützten Bedingungen anwenden, jeder Warteschlange einen eigenen Zeitplan für die Zustellung zuweisen, und das Routine flexibel und den Anforderungen entsprechend einrichten.

Verbesserungen für die Domänen-Verteilung 117

Seit einiger Zeit wurden im Rahmen der Domänen-Verteilung Abfragen nach den Absenderdaten, die im SMTP-Befehl MAIL übermittelt wurden, nach Bedarf durchgeführt. Hierbei wurden Nachrichten oft mit der Fehlermeldung "Echtheitsbestätigung erforderlich" (Authentication Required) abgewiesen; dies war problematisch, weil der Absender dann keine Echtheitsbestätigung durchführen konnte, wenn sein Benutzerkonto auf einem anderen Server gehostet war. Dieses Problem wurde behoben; MDaemon kann jetzt Nachrichten zur Zustellung annehmen, die von Benutzerkonten versandt werden, die auf anderen Servern gehostet sind. Eine Echtheitsbestätigung wird dabei nicht verlangt. Die neue Vorgehensweise kann mithilfe einer Option im Konfigurationsdialog Echtheitsbestätigung für Absender » SMTP-Echtheitsbestätigung 524 des Sicherheits-Managers geändert werden. Falls Sie die Abfragen nach den Absenderdaten aus dem SMTP-Befehl MAIL im Rahmen der Domänen-Verteilung nicht durchführen lassen wollen, können Sie die Abfragen durch Bearbeiten einer neuen Option zur Domänen-Verteilung insgesamt abschalten.

Die Domänen-Verteilung wurde um eine Option ergänzt, mit deren Hilfe jetzt auch Mailinglisten in die Domänen-Verteilung einbezogen werden können. Geht bei aktivierter Option eine Nachricht für eine Mailingliste ein, so wird für jeden Host in der Infrastruktur der Domänen-Verteilung, bei dem ebenfalls eine Version der Mailingliste gespeichert ist (MDaemon prüft durch eine Abfrage, ob diese Voraussetzung erfüllt ist), eine Kopie erstellt. Die Kopien werden an die betreffenden Hosts übermittelt, und diese stellen die Nachrichten den Listenmitgliedern zu, deren Benutzerkonten bei Ihnen jeweils gehostet sind. Mailinglisten können somit über mehrere Server verteilt werden, ohne dass damit eine Einschränkung in der Funktionalität verbunden wäre. Diese Option arbeitet nur dann, wenn jeder Host in der Domänen-Verteilung die IP-Adressen der anderen Hosts als Vertraute IPs[521] erfasst sind.

Die Domänen-Verteilung wurde schließlich um eine Schaltfläche Erweitert ergänzt. Durch Anklicken dieser Schaltfläche können Sie eine Datei öffnen, in der die Domänennamen erfasst werden können, die die Domänen-Verteilung nutzen dürfen. Ist die Datei leer (dies entspricht der Voreinstellung), so können alle Domänen auf Ihrem System die Domänen-Verteilung nutzen. Nähere Informationen hierzu enthält der Erläuterungstext am Beginn der Datei.

Verbesserte Steuerung für die Weiterleitung von Nachrichten

Der Konfigurationsdialog Voreinstellungen » Verschiedenes[504] wurde um eine Option erweitert, mit deren Hilfe Administratoren verhindern können, dass Benutzerkonten ihre Nachrichten außerhalb ihrer eigenen Domänen weiterleiten. Konfiguriert ein von dieser Option betroffener Benutzer eine Weiterleitung an eine Zieladresse in einer externen Domäne, so wird die weitergeleitete Nachricht in die Defekt-Warteschlange verschoben. Diese Option wirkt nur auf Nachrichten, die aufgrund der für das Benutzerkonto konfigurierten Weiterleitungsoptionen weitergeleitet werden.

Der Konfigurationsdialog Benutzerkonten-Editor » Weiterleitung[727] wurde um eine Schaltfläche *Zeitplan* erweitert, mit deren Hilfe die Benutzerkonten einen Zeitplan für Beginn und Ende der Weiterleitung konfigurieren können. Eine entsprechende Option steht auch für die Vorlagen für Benutzerkonten[803] zur Verfügung. Ist diese Option aktiv, so wird die Weiterleitung nur an den ausgewählten Tagen und in dem ausgewählten Zeitraum an diesen Tagen wirksam.

Das Feld für die Zieladresse für die Weiterleitung in der Vorlage Neue Benutzerkonten[788] verarbeitet jetzt auch Makros für Benutzerkonten. Zu dem Zeitpunkt, in dem die Vorlage für die Erstellung neuer Benutzerkonten verwendet wird, sind die einzigen für das Benutzerkonto bekannten und durch Makros auswertbaren Daten der vollständige Name, die Domäne, das Postfach und das Kennwort des Benutzerkontos. Ein Beispiel hierzu: Soll jedes neue Benutzerkonto so konfiguriert werden, dass alle Nachrichten an eine E-Mail-Adresse mit demselben Postfachnamen in einer anderen Domäne weitergeleitet werden, so können Sie als Zieladresse für die Weiterleitung `$MAILBOX$@example.com` eintragen. Makros sind auch in den neuen Feldern *Senden als*, *AUTH-Anmeldename* und *AUTH-Kennwort* zulässig.

Wird eine Nachricht weitergeleitet, so wird hierbei ab jetzt auch der Zeitstempel für den letzten Zugriff auf das weiterleitende Benutzerkonto aktualisiert. Diese Änderung bewirkt, dass Benutzerkonten, die lediglich der Weiterleitung eingehender Nachrichten dienen, nicht mehr wegen Inaktivität unbeabsichtigt gelöscht werden. **Beachte:** Der Zeitstempel wird nur aktualisiert, wenn die Weiterleitung tatsächlich stattgefunden hat und nicht etwa durch bestimmte Konfigurationsoptionen verhindert wurde; dies kann beispielsweise vorkommen, wenn die Zieladresse für die Weiterleitung oder der Zeitpunkt der Weiterleitung den konfigurierten Beschränkungen nicht entsprechen. Es genügt für die Aktualisierung des

Zeitstempels nicht, dass lediglich eine Weiterleitung konfiguriert ist, sie muss auch tatsächlich wirksam sein.

Verbesserte SMTP-Echtheitsbestätigung

Der Konfigurationsdialog Echtheitsbestätigung für Absender » SMTP-Echtheitsbestätigung 524 wurde um zwei Optionen erweitert. Die Option "*Echtheitsbestätigung auf dem SMTP-Port nicht zulassen*" deaktiviert die Unterstützung für AUTH auf dem SMTP-Port vollständig. AUTH wird dann auch nicht mehr in der Antwort auf den Befehl EHLO gemeldet. Der Befehl AUTH wird als unbekannter Befehl behandelt, falls er durch einen SMTP-Client übermittelt wird. Die Option "*... IPs von Gegenstellen nach versuchter Echtheitsbestätigung in Dynamischen Filter eintragen*" fügt die IP-Adresse solcher Gegenstellen dem Dynamischen Filter 628 hinzu, die die Echtheitsbestätigung versuchen, obwohl sie deaktiviert ist. Die Verbindung wird sofort getrennt. Diese Optionen sind besonders in den Fällen hilfreich, in denen alle legitimen Benutzerkonten den MSA- oder einen anderen Port nutzen, um Nachrichten nach Echtheitsbestätigung einzuliefern. In solchen Fällen kann davon ausgegangen werden, dass Versuche, auf dem SMTP-Port eine Echtheitsbestätigung oder Anmeldung durchzuführen, von Angreifern ausgehen müssen.

Verbesserte Verwaltung der Benutzerkonten

Die gefilterte Darstellung im Benutzerkonten-Manager wurde verbessert. Sie können jetzt Benutzerkonten auswählen, die aktiv sind, die MultiPOP nutzen, oder deren Kontingente zu mindestens 70 % oder zu mindestens 90 % ausgeschöpft sind, oder für die keine Weiterleitung aktiv ist. Sie können auch das Textfeld Beschreibung nach beliebigen Texten durchsuchen und Benutzerkonten anhand der Suchergebnisse auswählen. Das Kontextmenü des Benutzerkonten-Managers wurde außerdem um einige Optionen erweitert, mit deren Hilfe Sie alle ausgewählten Benutzerkonten in Mailinglisten und Gruppen aufnehmen und aus ihnen entfernen können. Das Kontextmenü wurde außerdem um eine Option ergänzt, durch die Sie die Einstellungen eines bestehenden Benutzerkontos in ein neues Benutzerkonto kopieren können; ausgeschlossen sind dabei Vor- und Nachname, Postfach, Kennwort und Nachrichten-Verzeichnis. Schließlich wurde der Konfigurationsdialog IMAP- Filter 736 des Benutzerkonten-Editors um die Schaltfläche Veröffentlichen erweitert. Durch Anklicken dieser Schaltfläche wird die neue Regel auf alle anderen Benutzerkonten angewendet, die derselben Domäne wie das bearbeitete Benutzerkonto angehören. Hiermit soll insbesondere dann Zeit gespart werden, wenn eine Regel für alle Benutzer übernommen werden soll.

Aktivierung des Schutzes gegen Störungen für ganze Domänen 184

Der Konfigurationsdialog Hostname & IP 184 wurde um neue Optionen erweitert, mit deren Hilfe der Schutz gegen Störungen für eine Domäne insgesamt aktiviert werden kann. Solange der Schutz gegen Störungen aktiv ist, weist die Domäne alle Verbindungen von allen Benutzern für alle Dienste ab, nimmt aber von außen eingehende Nachrichten weiterhin zur Zustellung an. Sie können einen Zeitplan festlegen, nach dem der Schutz gegen Störungen beginnt und endet. Ein Beispiel hierzu: Ein Zeitplan mit den Daten 01. Mai 2020 bis 30. Juni 2020, montags bis freitags von 17:00 Uhr bis 07:00 Uhr, bewirkt, dass in dem genannten Zeitraum an den genannten Wochentagen zwischen 17:00 und 07:00 Uhr für die Benutzer keine Maildienste zur Verfügung stehen. Wenn Sie das Beginndatum löschen, dann wird der Zeitplan deaktiviert. **Dies führt dazu, dass der Schutz gegen Störungen für die Domäne dauerhaft und ohne Zeitbegrenzung aktiv ist.**

Verbesserte Archivierung

Das einfache System zur Archivierung von Nachrichten in MDaemon wurde geändert und ist jetzt effizienter und einheitlicher. Die Archivierung arbeitet jetzt wie folgt: Wird eine Nachricht aus einer lokalen Warteschlange in das Nachrichtenverzeichnis eines Benutzers zugestellt, so wird hierbei eine Archivkopie erstellt (diese Kopie wird im Ordner IN des Empfängers abgelegt, falls die Archivierung entsprechend konfiguriert ist). Wird eine Nachricht aus eine Extern-Warteschlange zur Zustellung per SMTP aufgenommen, so wird dabei eine Archivkopie erstellt, und zwar unabhängig davon, ob der Versand erfolgreich war (diese Kopie wird im Ordner OUT des Absenders abgelegt, falls die Archivierung entsprechend konfiguriert ist). In das Routing-Protokoll werden dabei Einträge nach dem Schema "ARCHIVE message: pgp5001000000172.msg" oder "* Archived: (archives) \company.test\in\frank@company.test\arc5001000000023.msg" bei Verarbeitung lokaler und externer Nachrichten eingetragen. Es wurde eine neue Warteschlange "ToArchive" (ZuArchivieren) hinzugefügt, die über die Benutzeroberfläche nicht erreichbar ist. Diese Warteschlange wird in regelmäßigen Abständen auf Nachrichten geprüft, die dort abgelegt wurden (manuell, durch ein Plugin oder in sonstiger Weise). Nachrichten, die in der Warteschlange gefunden werden, werden sofort archiviert und danach gelöscht. Werden Nachrichten gefunden, die von der Archivierung ausgeschlossen sind, so werden sie einfach gelöscht. Der Verzeichnispfad zu dieser Warteschlange lautet \MDaemon\Queues\ToArchive\. Die Protokollansicht Routing und das Protokoll Routing enthalten Einträge, die über die erfolgreiche Archivierung Aufschluss geben. Die Archivierung verschlüsselter Nachrichten wird jetzt einheitlicher gehandhabt. Per Voreinstellung werden unverschlüsselte Kopien verschlüsselter Nachrichten archiviert. Kann eine Nachricht nicht entschlüsselt werden, so wird sie verschlüsselt archiviert, da sonst keine Möglichkeit der Archivierung besteht. Mithilfe einer neuen Option können Sie bestimmen, dass verschlüsselte Nachrichten verschlüsselt archiviert werden. Die folgenden Arten von Nachrichten werden nicht archiviert: Nachrichten aus Mailinglisten, Spam (die entsprechende Option wurde abgeschafft und entfernt), mit Viren infizierte Nachrichten, Systemnachrichten und Nachrichten von Autobeantwortern.

Effizientere Protokollierung

MDaemon legt keine leeren Protokolldateien mehr an. Für Vorgänge, deren Protokollierung abgeschaltet ist, werden bereits bei Programmstart keine Protokolldateien mehr erstellt. Protokolldateien, die bei Deaktivierung einer Protokollfunktion bereits bestanden, bleiben bestehen und werden nicht etwa gelöscht. Fehlende Protokolldateien werden erstellt, sobald die Protokollierung für den zugehörigen Vorgang aktiviert wird. Diese dargestellte Änderung wirkt auf alle Protokolldateien, die das Kernmodul von MDaemon selbst verwaltet. Protokolldateien für Dynamischen Filter, Instant Messaging, XMPP, WDaemon und Webmail werden außerhalb von MDaemon selbst gepflegt und sind von der Änderung nicht betroffen; sie bestehen unverändert. Es wurden weitere Änderungen an der Protokollierung vorgenommen. ATRN-Verbindungen werden jetzt richtig dargestellt, alle Protokolle werden in einheitlicher Farbkennzeichnung dargestellt, die Darstellung der Verbindungs- und untergeordneten Child-IDs wurde vereinheitlicht, und der MultiPOP-Server protokolliert jetzt keine überschüssigen und unnötigen Daten in den Fällen mehrt, in denen das Kontingent eines Benutzerkontos überschritten ist. Das Routing-Protokoll war das einzige Protokoll, in dem die Verarbeitung von Nachrichten aus Eingangs- und lokalen Warteschlangen vermerkt war. In diesem Protokoll wird jetzt auch die Verarbeitung der Extern-Warteschlangen im Rahmen von Zustellversuchen vermerkt. Sie müssen daher nicht mehr das Routing-Protokoll und das Protokoll für abgehende SMTP-Verbindungen (SMTP[out]) durchsuchen, um die Verarbeitung einer Nachricht nachzuvollziehen.

Verbesserte Active-Directory-Integration

Sie können die Active-Directory-Integration in MDaemon jetzt so konfigurieren, dass MDaemon-Benutzerkonten dann erstellt werden, wenn Sie einen Benutzer in eine Active-Directory-Gruppe aufnehmen. Ebenso können die Benutzerkonten der Benutzer, die aus Active-Directory-Gruppen entfernt werden, gesperrt (aber nicht gelöscht) werden. Um dieses Leistungsmerkmal nutzen zu können, müssen Sie einen alternativen Suchfilter für das Active Directory erstellen. Nähere Informationen hierzu finden Sie im Abschnitt Active Directory » Echtheitsbestätigung 818.

Der Konfigurationsdialog Echtheitsbestätigung 818 für das Active Directory wurde um einen eigenen "*Suchfilter für Kontakte*" erweitert. Bislang wurde die Kontaktsuche über den Suchfilter für die Benutzer vorgenommen. Mithilfe eines neuen Steuerelements können Sie den Suchfilter testen. Die Abfragen im Active Directory wurden optimiert. Falls die Suchfilter identisch sind, wird nur eine Abfrage zur Aktualisierung aller Daten durchgeführt. Zwei getrennte Abfragen sind nur dann erforderlich, wenn sich die Suchfilter unterscheiden.

Folgende Felder wurden den Dateivorlagen ActiveDS.dat hinzugefügt, und sie werden jetzt in die Kontaktdatensätze aufgenommen, wenn durch die Active-Directory-Überwachung die Adressbücher erstellt oder aktualisiert werden: `abTitle=%personalTitle%`, `abMiddleName=%middleName%`, `abSuffix=%generationQualifier%`, `abBusPager=%pager%`, `abBusIPPhone=%ipPhone%` und `abBusFax=%FacsimileTelephoneNumber%`.

Kontakte in öffentlichen Ordnern werden jetzt per Voreinstellung gelöscht, wenn das zugehörige Benutzerkonto aus dem Active Directory gelöscht wird. Dieser Vorgang wird aber nur für solche Kontakte durchgeführt, die durch die Active-Directory-Integration erstellt wurden. Dieses Verhalten wird mithilfe einer neuen Option im Konfigurationsdialog Active Directory » Überwachung 821 gesteuert.

Erstellt oder aktualisiert die Active-Directory-Überwachung ein Benutzerkonto, und stellt MDaemon dabei fest, dass der Postfachname für das entsprechende Datenfeld in MDaemon zu lang ist, so verkürzt MDaemon den Postfachnamen; dies entspricht der bisherigen Vorgehensweise. Ab jetzt erstellt MDaemon zusätzlich einen Alias mit dem vollständigen Postfachnamen. Werden Benutzerkonten oder Aliasnamen erstellt, so werden entsprechende Vermerke in die internen Anmerkungen zu den Benutzerkonten eingetragen. Diese Anmerkungen sind im Konfigurationsdialog Administrator-Rollen 757 sichtbar und dienen der Nachvollziehbarkeit.

Der Konfigurationsdialog Active Directory 299 des Mailinglisten-Manager gestattet jetzt die Angabe eines Active-Directory-Attributs Vor- und Nachnamen der Listenmitglieder.

Änderungen an den Eigenschaften eines Benutzerkontos im Active Directory können dazu führen, dass für das Benutzerkonto in MDaemon ein Benutzerkonto erstellt wird, und zwar auch dann, wenn das Benutzerkonto in MDaemon zuvor gelöscht wurde. Um zu verhindern, dass solche gelöschten Benutzerkonten erneut erstellt werden, wurde dem Konfigurationsdialog Active Directory » Überwachung 821 eine neue Option hinzugefügt. Per Voreinstellung werden die Benutzerkonten dann nicht mehr automatisch neu erstellt, wenn sie zuvor in MDaemon gelöscht worden waren.

Verbesserte Auswertung der Absenderkopfzeile From 576

Die Funktionen zur Änderung der Absenderkopfzeile From wurden umbenannt in "*From-Header-Auswertung*" und aus dem Konfigurationsdialog Hijacking-Erkennung in einen eigenen Konfigurationsdialog From-Header-Auswertung 576 überführt. Sie wurden um einige Leistungsmerkmale erweitert. So können die Anzeigenamen in den

Absenderkopfzeilen "From:" auf Inhalte untersucht werden, die wie E-Mail-Adressen aussehen. Werden solche Inhalte gefunden, und entsprechen sie nicht der tatsächlichen E-Mail-Adresse, so werden sie durch die tatsächliche E-Mail-Adresse ersetzt. Ein Beispiel hierzu: Enthält die Absenderkopfzeile "From:" den Inhalt "`From: 'Frank Thomas <friend@friend.test>' <enemy@enemy.test>`", so wird sie geändert in "`From: 'Frank Thomas <enemy@enemy.test>' <enemy@enemy.test>`".

Prüfung auf kompromittierte Kennwörter

MDaemon kann die Kennwörter der Benutzer mit einer Liste als kompromittiert bekannter Kennwörter abgleichen, die durch einen Drittanbieter bereit gestellt wird. Der Abgleich findet statt, ohne dass das Kennwort an den Anbieter übermittelt wird. Ist das Kennwort eines Benutzers in der Liste vorhanden, so bedeutet dies nicht, dass das Benutzerkonto kompromittiert oder gehackt wurde. Es bedeutet vielmehr, dass das fragliche Kennwort bereits einmal auf einem anderen System durch einen Benutzer verwendet wurde, und dass dieses verwendete Kennwort von einer Datenpanne oder einem Datenleck betroffen war. Kennwörter, die als kompromittiert bekannt und veröffentlicht sind, können durch Angreifer für Wörterbuchangriffe verwendet werden. Kennwörter, die noch nie auf anderen Systemen verwendet wurden, sind demgegenüber sicherer. Nähere Informationen hierzu erhalten Sie in englischer Sprache unter Pwned Passwords.

Der Konfigurationsdialog Kennwörter des Sicherheits-Managers wurde um eine Option erweitert, die bewirkt, dass Kennwörter, die in der Liste kompromittierter Kennwörter gefunden werden, nicht als Kennwörter für die Benutzerkonten verwendet werden können. Mithilfe einer weiteren Option kann MDaemon die Kennwörter der Benutzerkonten in einem konfigurierbaren Intervall während der Anmeldung prüfen und dem Benutzer und dem Postmaster per E-Mail eine Warnmeldung senden, falls das Kennwort in der Liste kompromittierter Kennwörter gefunden wird. Die Warnmeldungen können mithilfe zweier Vorlagen angepasst werden, die im Verzeichnis \MDaemon\App abgelegt sind. Da die Anweisungen zum Ändern des Kennworts unter anderem davon abhängen, ob das Kennwort durch MDaemon verwaltet wird oder die Benutzerprüfung über das Active Directory erfolgt, stehen zwei Vorlagen zur Verfügung: `CompromisedPasswordMD.dat` und `CompromisedPasswordAD.dat`. Die Empfänger, Betreffzeile und Nachrichtentext können mithilfe von Makros individuell angepasst werden.

Weitere Leistungsmerkmale und Verbesserungen

MDaemon 20 enthält über 250 neue Leistungsmerkmale und Verbesserungen, von denen viele in diesem Abschnitt nicht enthalten sind. Sie finden eine vollständige Übersicht über alle neuen Leistungsmerkmale, Änderungen und Fehlerbehebungen in dieser Version in der Datei `RelNotes.html`. Sie finden diese Datei im Unterverzeichnis `\Docs\` unter dem Verzeichnis von MDaemon.

Neuigkeiten in MDaemon 19.5

Neues Webmail-Design Mobile

Das Webmail-Design Mobile wurde durch eine modernere Benutzeroberfläche ersetzt, die auch mehr Leistungsmerkmale bietet. Die Funktionen in der Nachrichtenliste umfassen jetzt auch benutzerdefinierte Kategorien, das vorübergehende Ausblenden von Nachrichten, das Sortieren nach gekennzeichneten, ungelesenen und ausgeblendeten Nachrichten, das Sortieren nach Spalten und das Zurückrufen von

Nachrichten. Die Kalenderfunktionen umfassen jetzt auch den Im- und Export von Kalendereinträgen als kommagetrennte (CSV-) Dateien und ICS-Dateien, das Hinzufügen externer Kalender, das Erstellen privater Verknüpfungen für den Zugriff auf die Kalender, das Veröffentlichen der Kalender und das gleichzeitige Betrachten mehrerer Kalender. Die Funktionen zum Verfassen von Nachrichten umfassen jetzt auch die zeitversetzte Zustellung, die Nutzung mehrerer Signaturen, Nachrichten im Format Text und HTML und die Nutzung von Vorlagen für E-Mail-Nachrichten. Zu den weiteren neuen Funktionen zählen die Verwaltung der Filter per Drag and Drop, der Editor für mehrere Signaturen, erweiterte Verwaltungsoptionen für Ordner, Benachrichtigungen, die Verwaltung der Spalten und der Kategorien per Drag and Drop, und einiges mehr. Falls Sie Webmail in die IIS eingebunden haben, sind zusätzliche Anpassungen in der Konfiguration erforderlich. Nähere Informationen hierzu erhalten Sie in englischer Sprache im Artikel 1236 in der Wissensdatenbank.

Verwaltung von Client-Signaturen

Es können jetzt Signaturen konfiguriert werden, die an Webmail und MDaemon Connector übermittelt werden können. Sie können eine Standard-Signatur für die Clients einrichten. Sie können auch mithilfe des Konfigurationsdialogs Client-Signaturen im Domänen-Manager getrennte Signaturen für jede Domäne einrichten. Mithilfe von Makros für Signaturen wie `$CONTACTFULLNAME$` und `$CONTACTEMAILADDRESS$` können Sie die Signaturen automatisch an die Benutzer anpassen. Hierzu werden Daten ausgewertet, die in den Kontaktdaten der Benutzer enthalten sind, wie sie im Ordner Öffentliche Kontakte der jeweiligen Domäne gespeichert sind. Mithilfe des Makros `$ATTACH_INLINE:Dateiname$` können Sie Grafiken nahtlos (inline) in die HTML-Signaturen einbinden. Nachdem Sie den Text für die Signatur eingegeben haben, erscheint die Signatur in Webmail unter der Bezeichnung "System"; sie ist dann die Standard-Signatur für die betreffenden Benutzer. Sie können diese Signaturen im Konfigurationsdialog Webmail-Einstellungen systemweit aktivieren und deaktivieren. Sie können die Signaturen nach Domänen getrennt im Domänen-Manager aktivieren und deaktivieren. Für den MDaemon Connector können Sie den Namen der Signatur und die zugehörigen Einstellungen im Konfigurationsdialog Signatur konfigurieren; hierzu ist der MDaemon Connector ab Version 6.5.0 erforderlich.

Kategorien

In der MDaemon-Remoteverwaltung steht jetzt im Abschnitt Webmail-Optionen die Seite Kategorien zur Verfügung. Auf dieser Seite können die Kategorien für Domänen und die voreingestellten persönlichen Kategorien konfiguriert werden.

Weitere Verbesserungen an der MDaemon-Remoteverwaltung

Zahlreiche Optionen, die bislang nur über die Benutzeroberfläche von MDaemon selbst verwaltet werden konnten, sind jetzt auch in der Remoteverwaltung verfügbar. Eine vollständige Liste hierzu enthalten die Versionsinformationen.

Weitere Leistungsmerkmale und Änderungen

MDaemon 23.0 enthält viele weitere neue Leistungsmerkmale und Änderungen. Sie finden eine vollständige Liste aller neuen Leistungsmerkmale, Änderungen und Fehlerbehebungen gegenüber der Vorversion von MDaemon in der Datei `RelNotes.html` im MDaemon-Verzeichnis `\Docs\`.

Neuigkeiten in MDaemon 19.0

Unterstützung für Server Name Identification (SNI) bei TLS 579

MDaemon unterstützt jetzt die Erweiterung Server Name Identification (SNI) für das Protokoll TLS. Das Leistungsmerkmal SNI (Identifizierung von Servernamen) ermöglicht die Nutzung eines eigenen Zertifikats für jeden einzelnen Hostnamen, der Ihrem Server zugeordnet ist. MDaemon prüft die aktiven Zertifikate und wählt das Zertifikat aus, in dessen Datenfeld Subject Alternative Names der jeweils angeforderte Hostname enthalten ist. Falls der Client keinen bestimmten Hostnamen anfordert, oder falls MDaemon kein Zertifikat mit übereinstimmendem Hostnamen findet, nutzt MDaemon das Standard-Zertifikat.

XML-API zur Verwaltung von Ordnern und Elementen

Das XML-API wurde erweitert und unterstützt jetzt die Verwaltung von Ordnern in Postfächern und von Elementen in diesen Ordnern. Ordner können mithilfe des API erstellt, gelöscht, umbenannt und verschoben werden. Das API unterstützt die Elemente E-Mail-Nachrichten, Kalender, Kontakte, Aufgaben und Notizen. Diese Elemente können mithilfe des API erstellt, gelöscht und verschoben werden. Die vollständige Dokumentation finden Sie im Verzeichnis `MDaemon\Docs\API\XML-API\`.

Verbesserungen für die Remoteverwaltung

Die Webschnittstelle für die MDaemon-Remoteverwaltung (MDRA) wurde erweitert und ermöglicht jetzt den Zugriff auf Leistungsmerkmale, die bislang nur über eine Konfigurationsverbindung mithilfe der Benutzerschnittstelle von MDaemon selbst verwaltet werden konnten. Es stehen jetzt auch einige Optionen zur Verfügung, die nur über die Remoteverwaltung erreichbar sind. Aus diesem Grund wurde auch die Arbeitsweise der Verknüpfung "MDaemon starten" im Startmenü geändert. Bei Neuinstallationen ruft diese Verknüpfung jetzt per Voreinstellung die MDaemon-Remoteverwaltung in einem Browserfenster auf. Eine Konfigurationsverbindung wird nicht mehr gestartet. Sie können dieses Verhalten ändern, indem Sie in der Datei `\MDaemon\App\MDaemon.ini` im Abschnitt `[MDLaunch]` die Einträge `OpenConfigSession=Yes/No` und `OpenRemoteAdmin=Yes/No` bearbeiten. Falls der automatisch erzeugte URL für die Remoteverwaltung nicht funktioniert, oder falls die Remoteverwaltung unter einem anderen Web-Server ausgeführt wird, können Sie den URL der Remoteverwaltung im Konfigurationsdialog Einstellungen » Web- & IM-Dienste » Remote-Verwaltung » Web-Server 352 bearbeiten. Falls ein funktionierender URL nicht festgestellt werden kann, wird beim Anklicken der Verknüpfung statt der Remoteverwaltung eine Konfigurationsverbindung gestartet. Im Startmenü für MDaemon stehen jetzt außerdem die Verknüpfungen *MDaemon-Konfigurationsverbindung aufrufen* und *MDaemon-Remoteverwaltung aufrufen* zur Verfügung.

Verbesserungen für Webmail

- Webmail-Benutzer, die die Option *Gespeicherte Suchordner anzeigen* aktiviert haben (diese Option ist erreichbar über Optionen » Ordner) werden jetzt gefragt, ob sie Suchordner für alle ungelesenen und alle gekennzeichneten Nachrichten in die Liste ihrer Suchordner aufnehmen wollen. Diese abfrage erfolgt nur einmal, und zwar bei der ersten Anmeldung. Verneinen die Benutzer die Frage, so können sie diese Suchordner später einfach im Menü Optionen » Ordner durch Anklicken der Steuerelemente *Gespeicherten Suchvorgang für alle gekennzeichneten Nachrichten erstellen* und *Gespeicherten Suchvorgang für alle ungelesenen Nachrichten erstellen* aktivieren. Die Administratoren können die Abfrage unterbinden, indem Sie

der Datei `MDaemon\WorldClient\Domains.ini` im Abschnitt `[Default:UserDefaults]` den Eintrag `DefaultSavedSearchesCheck=Yes` hinzufügen.

- Einige Symbole im Design *WorldClient* wurden geändert, um sie besser erkennbar zu machen.
- Im Titel der Registerkarte im Browser, in der eine Webmail-Verbindung besteht, erscheint jetzt der Zusatz (ABGELAUFEN), sobald die Verbindung abgelaufen ist. Benutzer, die gerade eine andere Registerkarte betrachten, können hierdurch einfacher erkennen, dass die Verbindung abgelaufen ist.
- Gemeinsame Kontakte können jetzt mithilfe eines neuen Symbols aus der Liste für die Funktion Autovervollständigen entfernt werden.

Neuigkeiten in MDaemon 18.5

Makros für Signaturen

MDaemon unterstützt in den Signaturen Makros, mit deren Hilfe Kontaktdaten des Absenders automatisch in die Signaturen eingefügt werden können. Diese Daten werden den Kontaktdaten des Absenders entnommen, die im Ordner für öffentliche Kontakte seiner Domäne gespeichert sind. Standard- und Domänen-Signaturen können hierdurch mithilfe der Daten des Absenders automatisch individuell gestaltet werden. Zwei Beispiele hierzu: `$CONTACTFULLNAME$` wird umgesetzt in den vollständigen Namen des Absenders, und `$CONTACTEMAILADDRESS$` wird umgesetzt in die E-Mail-Adresse des Absenders. Die Kontaktdaten für die öffentlichen Kontakte können mithilfe von Webmail, des MDaemon Connectors oder über ActiveSync bearbeitet werden. Falls für einen Absender keine Kontaktdaten bestehen, werden Leerstellen eingesetzt. Die verfügbaren Makros sind im Abschnitt Standard-Signaturen aufgeführt.

Die Benutzer können steuern, welche MDaemon-Signaturen wie in ihre Nachrichten eingefügt werden. Hierzu fügen sie zwei bestimmte Makros in die Nachrichten ein: Das Makro `$SYSTEMSIGNATURE$` wird ersetzt durch die Standard- oder Domänen-Signatur, und das Makro `$ACCOUNTSIGNATURE$` wird ersetzt durch die Signatur des Benutzerkontos.

MDaemon Instant Messaging in Webmail

Die Designs WorldClient und LookOut enthalten jetzt einen browsergestützten XMPP-Client, mit dessen Hilfe Benutzer Instant Messages übermitteln können, ohne dass Sie dazu die Desktop-Anwendung MDaemon Instant Messenger oder andere XMPP-Clients installieren müssen. Die Benutzer können den Client auf der Webmail-Seite Optionen | Benutzeranpassung aktivieren; es steht die Option "MDaemon Instant Messaging im Browser aktivieren" zur Verfügung. Administratoren können dieses Leistungsmerkmal mithilfe des Domänen Managers nach Domänen getrennt, mithilfe des Benutzerkonten-Managers nach Benutzerkonten getrennt und mithilfe des Gruppen-Managers nach Gruppen getrennt aktivieren und deaktivieren.

MDaemon enthält jetzt einen BOSH-Server, der das Instant Messaging direkt in Webmail unterstützt. Die Einstellungen für diesen Server können im Konfigurationsdialog XMPP bearbeitet werden **(dieses Leistungsmerkmale wurd in Version 18.5.1 hinzugefügt)**.

Ausnahmen vom Länder-Filter für Webmail

Anmeldungen an Webmail mithilfe der Zwei-Faktor-Authentifizierung können jetzt mithilfe einer neuen benutzerindividuellen Option von der Verarbeitung durch den Länder-Filter ausgenommen werden. Ist im Abschnitt `[User]` der Datei `User.ini` für einen Benutzer der Eintrag `BypassLocationScreeningTFA=Yes` enthalten, und ist für den Benutzer die Anmeldung mithilfe der Zwei-Faktor-Authentifizierung aktiv, so wird der Länder-Filter umgangen. Hiermit können sich Benutzer auch von solchen Ländern aus ab Webmail anmelden, die sonst durch den Länder-Filter gesperrt sind.

Verbesserte Active-Directory-Integration

Benutzer, deren Benutzerkonten für die Echtheitsbestätigung über das Active Directory eingerichtet sind, können jetzt ihre Active-Directory-Kennwörter von Webmail aus ändern. Hierzu muss der Eintrag `AllowADPasswordChange` in der Datei \MDaemon\WorldClient\Domains.ini aktiv sein. Der Eintrag ist per Voreinstellung nicht aktiv.

Erweiterung für die MDaemon-Remoteverwaltung

Die Webschnittstelle der MDaemon-Remoteverwaltung wurde erweitert. Sie ermöglicht jetzt den Zugriff auf viele Leistungsmerkmale, die bislang nur mithilfe der grafischen Benutzeroberfläche von MDaemon selbst verwaltet werden konnten.

Neuigkeiten in MDaemon 18.0

DNSSEC 595

Mithilfe der Option DNSSEC (DNS Security Extensions, Sicherheitserweiterungen für DNS) kann MDaemon als nicht-validierender, sicherheitsbewusster Stub-Resolver ("Non-Validating Security-Aware Stub Resolver") arbeiten. Die RFCs 4033 und 4035 definieren einen solchen Resolver als eine Einheit, die DNS-Abfragen übermittelt, DNS-Antworten empfängt, und einen angemessen gesicherten Kanal zu einem sicherheitsbewussten rekursiv arbeitenden Nameserver aufbauen kann, der diese Dienste für den sicherheitsbewussten Stub-Resolver erbringt". Dies bedeutet, dass MDaemon in den DNS-Abfragen den DNSSEC-Dienst von Ihren DNS-Servern anfordern kann, das Kennzeichen für echtheitsbestätigte Daten (AD, Authentic Data) in den Abfragen setzen und die Antworten auf sein Vorhandensein prüfen kann. Hierdurch wird während der Verarbeitung von DNS-Daten zusätzliche Sicherheit geschaffen; da aber noch nicht alle DNS-Server und Top-Level-Domänen DNSSEC unterstützen, kann diese zusätzliche Sicherheit nur für einen Teil der anfallenden Nachrichten wirksam werden.

DNSSEC wirkt auch nach der Aktivierung nur auf Nachrichten, die den festgelegten Auswahlkriterien entsprechen. Sie können daher flexibel bestimmen, in welchem Umfang DNSSEC genutzt werden soll. Auf diesem Konfigurationsdialog können Sie Kombinationen aus "`Kopfzeile` und `Inhalt`" bestimmen. MDaemon fordert dann bei der DNS-Abfrage DNSSEC für alle Nachrichten an, die den hierdurch bestimmten Kriterien entsprechen. Enthalten die DNS-Antworten keine echtheitsbestätigten Daten, so führt dies grundsätzlich nicht zu negativen Folgen, und MDaemon fällt nur auf normalen DNS-Betrieb zurück. Hiervon abweichend können Sie DNSSEC für bestimmte Nachrichten *zwingend erforderlich* machen, indem Sie der Kombination aus Kopfzeile und Inhalt das Schlüsselwort "SECURE" hinzusetzen (etwa `To *@example.net SECURE`). Enthalten bei Nachrichten, die solchen Kriterien entsprechen, die DNS-Antworten keine echtheitsbestätigten Daten, so werden diese

Nachrichten an die Absender zurückgeleitet. **Beachte:** DNSSEC-Abfragen nehmen mehr Zeit in Anspruch und sind ressourcenintensiver als normale DNS-Abfragen, außerdem wird DNSSEC noch nicht durch alle Server unterstützt. MDaemon ist daher per Voreinstellung nicht darauf konfiguriert, für alle Nachrichten DNSSEC zu verwenden. Falls Sie DNSSEC für jede Nachricht verwenden wollen, fügen Sie in diesem Konfigurationsdialog den Eintrag "`To *`" hinzu.

AntiVirus-Prüfung für die Postfächer

Im Konfigurationsdialog Sicherheit » AntiVirus[671] steht die neue Option *Alle Postfächer alle x Tage prüfen* zur Verfügung. Diese Option bewirkt, dass alle gespeicherten Nachrichten in regelmäßigen Zeitabständen auf Viren geprüft werden. Mithilfe einer solchen turnusgemäßen Prüfung können auch infizierte Nachrichten entdeckt werden, die zum Zeitpunkt ihrer ursprünglichen Zustellung noch nicht als infiziert erkannt werden konnten, etwa, weil eine die passende Signatur enthaltende Virendefinition erst nach der Zustellung verfügbar wurde. Infizierte Nachrichten werden in Quarantäne gegeben, und ihnen wird die Kopfzeile `X-MDBadQueue-Reason` hinzugefügt. Anhand des Inhalts dieser Kopfzeile können Sie in MDaemon weitere Erklärungen erhalten. Nachrichten, die nicht geprüft werden können, werden auch nicht in Quarantäne gegeben. Sie können neben der turnusgemäßen Prüfung auch jederzeit eine sofortige Prüfung veranlassen.

Ausnahmen vom Länder-Filter für bekannte ActiveSync-Endgeräte

In den ActiveSync-Einstellungen für die Clients steht die neue Option Vom Länder-Filter ausnehmen[464] zur Verfügung. Wenn Sie diese Option in den Einstellungen eines ActiveSync-Clients aktivieren, kann das Endgerät den Länder-Filter[574] umgehen. Hierdurch kann ein berechtigter Benutzer auf sein Benutzerkonto über ActiveSync beispielsweise auch dann zugreifen, wenn er sich in einem Land befindet, für das Versuche zur Echtheitsbestätigung ansonsten durch den Länder-Filter unterbunden werden. Ein Endgerät kann nur dann vom Länder-Filter ausgenommen sein, wenn es innerhalb des durch die Option Inaktive Clients entfernen nach [x] Tagen[418] im Abschnitt Anpassung bestimmten Zeitraums eine echtheitsbestätigte Verbindung über ActiveSync erfolgreich hergestellt hat.

Neue Leistungsmerkmale für Webmail und die MDaemon-Remoteverwaltung

Speichern und Beibehalten von Anmeldungen zulassen

In den Konfigurationsdialogen Einstellungen[345] für Webmail sowie Web-Server[352] für die MDaemon-Remoteverwaltung stehen neue Optionen zur Verfügung, mit deren Hilfe Anmeldungen gespeichert und beibehalten werden können. Diese Optionen ermöglichen es den Benutzern, ihre Anmeldungen für eine bestimmte Zeit zu speichern. Sind sie aktiv, und stellen die Benutzer eine Verbindung über den https[327]-Port her, so erscheint auf der Anmeldeseite die Option *Anmeldung beibehalten*. Aktivieren die Benutzer diese Option vor der Anmeldung, dann wird ihre Anmeldung auf dem gerade genutzten Endgerät gespeichert. Rufen die Benutzer danach Webmail oder die Remoteverwaltung erneut von demselben Endgerät aus auf, so werden sie automatisch angemeldet und müssen Benutzernamen und Kennwort nicht eingeben. Diese Anmeldung wird beibehalten, bis sie sich manuell von Webmail oder der Remoteverwaltung abmelden oder der Token für die Speicherung der Anmeldung verfällt. Die Option *Speichern von Anmeldungen zulassen* ist per Voreinstellung abgeschaltet. Sie wirkt auf alle Ihre Domänen. Falls Sie diese Einstellung für einzelne Webmail-Domänen abweichend konfigurieren

wollen, können Sie hierzu im Abschnitt Webmail[194] des Domänen-Managers auf der Desktop-Benutzeroberfläche von MDaemon die Einstellung *Speichern von Anmeldungen zulassen* für die betreffenden Domänen konfigurieren.

Per Voreinstellung werden Anmeldungen für 30 Tage gespeichert, und danach müssen sich die Benutzer erneut anmelden. Mithilfe der Option *Token für gespeicherte Anmeldungen laufen nach folgender Anzahl Tagen ab* in der MDaemon-Remoteverwaltung können Sie den Zeitraum auf höchstens 365 Tage setzen. **Beachte**: Für die Zwei-Faktor-Authentifizierung[720] besteht eine eigene Einstellung. Sie finden diese Einstellung, den Eintrag `TwoFactorAuthRememberUserExpiration=30` im Abschnitt `[Default:Settings]` der Datei `Domains.ini`. Sie finden diese Datei im Verzeichnis `\MDaemon\WorldClient\`. Sobald der Zeitraum für die Zwei-Faktor-Authentifizierung abgelaufen ist, müssen sich die Benutzer erneut mithilfe der Zwei-Faktor-Authentifizierung anmelden, und zwar auch dann, wenn die Speicherdauer für die Anmeldung zu diesem Zeitpunkt noch nicht abgelaufen ist.

In der MDaemon-Remoteverwaltung steht darüber hinaus die Schaltfläche *Speichern von Anmeldungen zurücksetzen* zur Verfügung, die Sie nutzen können, falls der Verdacht auf einen unerlaubten Zugriff auf ein Benutzerkonto besteht. Durch Anklicken dieser Schaltfläche werden die Token für alle gespeicherten Anmeldungen sofort ungültig, und alle Benutzer müssen sich erneut anmelden.

E-Mail-Nachrichten vorübergehend ausblenden

MDaemon Webmail wurde um eine Option erweitert, mit deren Hilfe die Benutzer E-Mail-Nachrichten vorübergehend ausblenden können. Hat ein Benutzer eine Nachricht vorübergehend ausgeblendet, so wird die Nachricht für den gewählten Zeitraum vor dem Benutzer verborgen. Um eine Nachricht auszublenden, führen Sie auf der Nachricht einen Rechtsklick aus, und klicken Sie im Kontextmenü auf "Ausblenden für...". Sie können dann auswählen, für welchen Zeitraum die Nachricht ausgeblendet werden soll. Die Auswahl von Datum und Uhrzeit ist nur in Browsern möglich, die Auswahlfelder für Datum und Uhrzeit unterstützen. Im Design LookOut können Sie sich ausgeblendete Nachrichten anzeigen lassen, indem Sie das Symbol "Ausgeblendete Nachrichten anzeigen" in der Symbolleiste anklicken. Im Design WorldClient können Sie sich ausgeblendete Nachrichten anzeigen lassen, indem Sie den Eintrag "Ausgeblendete Nachrichten anzeigen" im Menü "Ansicht" anklicken. Das Leistungsmerkmal ist per Voreinstellung aktiv. Um das Leistungsmerkmal zu deaktivieren, rufen Sie die Seite Optionen | Benutzeranpassung auf, und deaktivieren Sie im Abschnitt für die Einstellungen für den Posteingang die Option "Ausblenden von Nachrichten aktivieren". In den Designs Lite und Mobile stehen keine Steuerelemente für das Ausblenden von Nachrichten zur Verfügung; bereits ausgeblendete Nachrichten werden aber auch in diesen Designs nicht angezeigt.

Öffentlich freigegebene Kalender

Benutzer von MDaemon Webmail können einen Kalender unter einem öffentlich zugänglichen URL freigeben. Sie können dabei den freigegebenen Kalender auch mit einem Kennwort schützen. Um einen Kalender öffentlich verfügbar zu machen, rufen Sie in den Designs LookOut oder WorldClient die Seite Optionen | Ordner auf, und klicken Sie neben dem zu veröffentlichenden Kalender auf "Ordner freigeben". Es öffnet sich ein Konfigurationsdialog; wechseln Sie dort die Registerkarte Öffentlicher Zugriff, tragen Sie, falls gewünscht, einen für den Kalender anzuzeigenden Namen und ein Kennwort ein, und klicken Sie dann auf "Kalender öffentlich freigeben". Es erscheint eine Sicherheitsabfrage, die den Benutzer auf die Wirkungen der öffentlichen Freigabe hinweist. Nachdem der Benutzer diese Abfrage bestätigt hat, erscheint in einem Hinweis der URL, unter dem der Kalender erreichbar ist.

Anschließend erscheint auch auf der Seite selbst eine entsprechende Verknüpfung. Um die öffentliche Freigabe des Kalenders zu beenden, klicken Sie auf "Öffentliche Kalenderfreigabe beenden". Um das Kennwort oder den Anzeigenamen zu ändern, klicken Sie auf "Aktualisieren".

Um dieses Leistungsmerkmal systemweit zu deaktivieren, setzen Sie im Abschnitt `[Default:Settings]` der Datei `Domains.ini` den Eintrag `EnablePublicCalendars` auf **No**. Um dieses Leistungsmerkmal für einzelne Benutzer zu deaktivieren, fügen Sie den Dateien `User.ini` der betroffenen Benutzer den Eintrag `CanPublishCalendars=No` hinzu.

Neuigkeiten in MDaemon 17.5

Länder-Filter 574

Der Länder-Filter ist ein auf geographische Daten gestütztes Filtersystem. Mit seiner Hilfe können Sie SMTP-, POP- und IMAP-Verbindungsversuche abweisen, falls diese Verbindungsversuche von bestimmten geographischen Regionen ausgehen, die Sie als nicht zugelassen definiert haben. MDaemon stellt fest, mit welchem Land die IP-Adressen in Verbindung stehen, von denen eingehende Verbindungen ausgehen. Verbindungen, die von gesperrten Regionen ausgehen, werden abgewiesen, und dieser Vorgang wird im Protokoll Screening vermerkt. Bei SMTP-Verbindungen kann der Länder-Filter wahlweise nur solche Verbindungen abweisen, in denen eine Echtheitsbestätigung über AUTH versucht wird. Diese Vorgehensweise ist beispielsweise dann sinnvoll, wenn Sie in einem bestimmten Land keine Benutzer haben, gleichwohl aber von dort aus Nachrichten empfangen wollen. Es werden dann nur Verbindungen abgewiesen, in denen eine Anmeldung an einem Benutzerkonto Ihres Servers versucht wird.

Das Verzeichnis `\MDaemon\Geo\` enthält Datenbankdateien, die als Hauptdatenbanken für die Zuordnung von IP-Adressbereichen zu Ländern dienen. Diese Datenbanken wurden durch MaxMind (http://www.maxmind.com) bereit gestellt. Aktualisierungen sind bei Bedarf auf der genannten Website erhältlich.

Dynamischer Filter für alle Protokolle und Dienste 612

Der dynamische Filter von MDaemon wurde erheblich erweitert und arbeitet nun für die Protokolle und Dienste SMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery, XML-API, Remoteverwaltung, CalDAV/CardDAV, XMPP und Minger. Fehlgeschlagene Versuche zur Echtheitsbestätigung werden für alle genannten Protokolle und Dienste erfasst, und es können IP-Adressen für alle genannten Protokolle und Dienste gesperrt werden. Die entsprechenden Einstellungen legen Sie in einem neu gestalteten, in mehrere Registerkarten unterteilten Konfigurationsdialog fest, den Sie über das Menü Sicherheit erreichen.

Dateianlagen in PIM-Elementen

PIM-Elemente (Kalendereinträge, Kontakte, Aufgaben und Notizen) unterstützen jetzt Dateianlagen. Sie können die Dateianlagen den PIM-Elementen über Webmail, den Outlook Connector und CalDAV/CardDAV hinzufügen. Dateianlagen in Besprechungsanfragen werden an alle eingeladenen Besprechungsteilnehmer übermittelt.

Austausch von PGP-Schlüsseln über SMTP 631

Der Konfigurationsdialog MDPGP wurde um ein Leistungsmerkmal erweitert, mit dessen Hilfe öffentliche Schlüssel während der Übermittlung von Nachrichten über SMTP ausgetauscht werden können. Hierfür steht eine neue Option im Konfigurationsdialog MDPGP zur Verfügung. Ist sie aktiv, so befolgt der SMTP-Server von MDaemon den SMTP-Befehl RKEY. Übermittelt MDaemon eine E-Mail-Nachricht an eine Gegenstelle, die RKEY unterstützt, so bietet MDaemon dieser Gegenstelle an, den aktuellen und bevorzugten öffentlichen Schlüssel des Absenders der Nachricht zusätzlich zu der Nachricht selbst ebenfalls zu übermitteln. Die Gegenstelle antwortet dann entweder, dass der Schlüssel bereits bekannt ist und nicht erneut benötigt wird (Meldung "250 2.7.0 Key already known", Schlüssel schon bekannt), oder dass der Schlüssel benötigt wird. Im zweiten Fall übermittelt MDaemon den Schlüssel sofort im ASCII-Armored-Format (auf Meldung der Gegenstelle "354 Enter key, end with CRLF.CRLF", Schlüssel übermitteln, beenden mit CRLF.CRLF). Die Übermittlung entspricht dabei technisch der Übermittlung einer E-Mail-Nachricht. Schlüssel mit abgelaufener Gültigkeit und widerrufene Schlüssel werden keinesfalls übermittelt. Verfügt MDaemon über mehrere Schlüssel für den Absender, so bietet MDaemon immer den als bevorzugt gekennzeichneten Schlüssel an. Ist kein Schlüssel als bevorzugt gekennzeichnet, so bietet MDaemon den ersten gefundenen Schlüssel an. Sind keine gültigen Schlüssel verfügbar, so wird keine Übermittlung durchgeführt. Es werden nur Schlüssel angeboten, die lokalen Benutzern zugeordnet sind.

Die Übermittlung der öffentlichen Schlüssel erfolgt während der SMTP-Verbindung, über die auch die zugehörige Nachricht übermittelt wird. Öffentliche Schlüssel, die auf diesem Weg übermittelt werden, werden nur akzeptiert, falls die zugehörige Nachricht alle folgenden Voraussetzungen erfüllt: Die Nachricht muss mit einer gültigen DKIM -Signatur 533 der Domäne versehen sein, zu der der Schlüsselinhaber gehört. Der Tag i= muss dabei die Adresse des Schlüsselinhabers enthalten, und diese Adresse muss genau der Adresse aus der Absenderkopfzeile From: entsprechen. Es darf nur eine Absenderkopfzeile From: vorhanden sein. Der Schlüsselinhaber wird dem Schlüssel selbst entnommen. Die Nachricht muss durch einen Host zugestellt werden, der in den SPF-Einträgen 527 der Absenderdomäne enthalten ist. Der Schlüsselinhaber muss zur Nutzung von RKEY berechtigt sein. Hierzu müssen in der Regeldatei von MDPGP entsprechende Einträge entweder für den Schlüsselinhaber selbst oder für die gesamte Domäne enthalten sein (Anweisungen hierzu enthält die Datei selbst), die bestimmen, dass die Domäne für Zwecke des Schlüsselaustauschs vertrauenswürdig ist. Die Prüfung, ob die Voraussetzungen erfüllt sind, laufen automatisch ab, und hierzu müssen die DKIM 529 und die SPF-Prüfung 527 zwingend aktiv sein.

Das Protokoll für MDPGP weist die Ergebnisse und die Einzelheiten für alle Schlüssel aus, die importiert und gelöscht werden, und zwar auch für die während der SMTP-Verbindung übermittelten Schlüssel. Die eigentliche Übermittlung der Schlüssel während der SMTP-Verbindung wird im Protokoll für SMTP vermerkt.

Verwaltung von Add-Ins für Microsoft Outlook für Benutzer des Outlook Connectors 405

Mithilfe des neuen Abschnitts Add-Ins im Konfigurationsdialog OC-Client-Einstellungen können Sie die Nutzung von Add-Ins für Microsoft Outlook durch Ihre Outlook-Connector-Benutzer steuern. Sie können die Nutzung einzelner oder aller Add-Ins freigeben, und Sie können einzelne Add-Ins wahlweise deaktivieren. Dieses Leistungsmerkmal ist insbesondere dann nützlich, wenn bekannt ist, dass bestimmte Add-Ins einen Konflikt mit dem Outlook-Connector-Client verursachen; Sie können

solche Add-Ins deaktivieren, um Problemen vorzubeugen. Das Leistungsmerkmal Add-Ins erfordert den Outlook Connector ab Version 5.0.

Änderungen an Webmail

Import und Export von Gruppen und Verteilerlisten
In den Designs LookOut und WorldClient können Gruppen und Verteilerlisten mithilfe einer neuen Option jetzt in Webmail-Kontaktordner importiert und aus Webmail-Kontaktordnern exportiert werden. Das Format ist hierbei Webmail-spezifisch, da Microsoft Outlook den Export und den Import von Gruppen nicht unterstützt. Das Format ist folgendermaßen aufgebaut:

> Spalten: **Gruppen-GUID**, **Gruppen-Name**, **GUID**, **Vor- und Nachname**, **E-Mail-Adresse**
>
> Jede Zeile, die entweder einen Gruppen-Namen oder eine Gruppen-GUID enthält, wird als Beginn einer neuen Gruppe betrachtet. GUID, Vor- und Nachname und E-Mail-Adresse auf derselben Zeile werden als erstes Mitglied der Gruppe oder Liste betrachtet.
>
> Ein aus Microsoft Excel entnommenes Beispiel:

Gruppen-GUID	Gruppen-Name	GUID	Vor- und Nachname	E-Mail-Adresse
	The Jedis		Anakin Skywalker	ani@jedi.mail
			Leia Organa	leia.organa@jedi.mail
			Luke Skywalker	luke.skywalker@jedi.mail
			Yoda	yoda@jedi.mail
	The Siths		Darth Maul	darth.maul@sith.mail
			Darth Vader	darth.vader@sith.mail
			Emperor Palpatine	emperor.palpatine@sith.mail

Während des Imports wird die Gruppen-GUID durch eine neu erstellte GUID ersetzt. Ist kein Gruppen-Name angegeben, wird der Name nach dem Schema "ImportedFromCSV_%GUID%" angegeben, wobei %GUID% durch die ersten fünf Zeichen der GUID ersetzt wird. Bleiben die Zellen rechts von einem Gruppen-Namen leer, so wird die folgende Zeile als erstes Mitglied in die Gruppe oder Liste aufgenommen. Mitglieder können nur hinzugefügt werden, wenn für sie das Feld E-Mail mit einer Adresse belegt ist.

Sprachaufzeichnung
Den Designs LookOut und WorldClient wurde ein Leistungsmerkmal für Sprachaufzeichnung hinzugefügt. Dieses Leistungsmerkmal erfordert ein Mikrofon und ist nur in bestimmten Browsern verfügbar. Der Administrator kann das Leistungsmerkmal nach Benutzern getrennt deaktivieren, indem er der Datei `User.ini` für die betreffenden Benutzer den Eintrag `EnableVoiceRecorder=No` hinzufügt. Jeder Benutzer kann höchstens fünf Aufzeichnungen zu je fünf Minuten Länge speichern. Nimmt er danach eine weitere Aufzeichnung vor, so wird der Benutzer aufgefordert, zu entscheiden, ob er die ausgewählte Aufzeichnung oder die erste Aufzeichnung überschreiben will. Nach Ende der Aufzeichnung - entweder, weil der Benutzer sie beendet, oder weil die Höchstdauer erreicht ist, wird die

Aufzeichnung in das Format MP3 umgewandelt und an den Server übermittelt. Den Benutzern stehen für jede Sprachaufzeichnung vier Optionen zur Verfügung:

- Auf dem Desktop speichern.
- Im Standard-Dokumentenordner von Webmail speichern.
- Per E-Mail versenden, wobei ein vereinfachter Versanddialog mit nur den Feldern An, CC, BCC, Betreff und Nachrichtentext verwendet wird.

  Hierbei muss nur der Empfänger zwingend angegeben werden. Für Betreff und Nachrichtentext stehen vorbereitete Texte zur Verfügung, die verwendet werden, falls der Benutzer keinen Betreff und/oder keinen Nachrichtentext eingibt.
- Neues Editorfenster zum Verfassen einer Nachricht öffnen und Sprachaufzeichnung als Dateianlage anfügen.

Mithilfe dieser Optionen können die Benutzer nur jeweils mit einer Sprachaufzeichnung gleichzeitig arbeiten. Ein Beispiel hierzu: Mithilfe der Optionen kann nur eine Sprachaufzeichnung an eine Nachricht als Dateianlage angefügt werden. Will der Benutzer mehrere Sprachaufzeichnungen anfügen, so muss er zunächst alle Sprachaufzeichnungen in den Standard-Dokumentenordner speichern und sie danach von dort aus als Dateianlagen anfügen.

Neue Leistungsmerkmale zur Ordnerverwaltung
In den Designs LookOut und WorldClient stehen unter Optionen » Ordner und in der Haupt-Ordnerliste neue Verwaltungsfunktionen für die Ordner zur Verfügung.

In der Ordnerliste (linker Bereich):

- Benutzer können Unterordner durch Ziehen und Ablegen zwischen unterschiedlichen übergeordneten Ordnern verschieben.
- Benutzer können Ordner umbenennen und für Favoriten Kurznamen vergeben, indem sie die Ordner kurz hintereinander zweimal anklicken (einmal zur Auswahl, danach ein weiteres Mal nach der Auswahl).
- Im Design LookOut können jetzt Ordner nach Typ angezeigt werden.
- Benutzer können Ordner den Favoriten hinzufügen, indem sie die gewünschten Ordner in die Favoritenliste ziehen und dort ablegen. Dies funktioniert jedoch nur, wenn bereits Favoriten bestehen, da sonst die Favoritenliste nicht angezeigt wird. Das Herausziehen von Ordnern aus den Favoriten hat keine Wirkung.
- Das Design LookOut wurde um neue Dialoge zum Erstellen und Umbenennen von Ordnern erweitert.

In der Übersicht Optionen » Ordner ist die Baumdarstellung der Ordner jetzt einklappbar, und der Dialog zum Erstellen neuer Ordner wurde - wie bereits im Design WorldClient - in ein eigenes Fenster ausgelagert.

Neuigkeiten in MDaemon 17.0

Unterstützung für XMPP[372] im WorldClient Instant Messenger[318] (WCIM)

WCIM nutzt ab jetzt statt des eigenen, proprietären WorldClient-Protokolls das Protokoll XMPP für das Instant Messaging. Aufgrund dieser Änderung kann der WCIM-Desktop-Client ab jetzt nicht nur mit anderen WCIM-Clients sondern mit allen XMPP-Clients von Drittanbietern kommunizieren, die mit dem XMPP-Server von MDaemon verbunden sind. Hierzu gehören auch Clients für mobile Endgeräte. WCIM nutzt jetzt zwei Arten von Verbindungen: "WCMailCheck" - über diese Verbindung mit WorldClient werden die Benachrichtigungen über neue Nachrichten und die Nachrichtenzähler übermittelt, und "WCIMXMPP" - über diese Verbindung mit dem XMPP-Server wird das Instant Messaging abgewickelt. Während der Aktualisierung auf Version 17 stellt WCIM die IM-Kontakte automatisch vom bisherigen System auf XMPP um und erstellt eine WCIMXMPP-Verbindung, die zur bestehenden WCMailCheck-Verbindung gehört. Aussehen und Handhabung des neuen WCIM-Clients entsprechen im wesentlichen den bisherigen Versionen; es bestehen aber einige Unterschiede, etwa in der Verwaltung von Kontakten und Gruppenunterhaltungen. Nähere Informationen über die Änderungen können Sie dem Hilfesystem des WCIM-Clients entnehmen.

Integration von Dropbox in WorldClient[336]

WorldClient unterstützt Dropbox direkt. Die Benutzer können daher Dateianlagen in ihren Dropbox-Benutzerkonten speichert, und sie können direkte Verknüpfungen mit Dateien, die in Dropbox-Benutzerkonten gespeichert sind, in abgehende Nachrichten einfügen. Um den Benutzern diese Leistungsmerkmale bereit zu stellen, müssen Sie Ihre WorldClient-Installation auf der DBX-Plattform als Dropbox-App registrieren. Diese Registrierung ist unkompliziert; Sie müssen sich lediglich an einem Dropbox-Benutzerkonto anmelden, einen eindeutigen Namen für eine App mit Vollzugriff auf Dropbox ("Full Dropbox") erstellen, den URI für die Umleitung nach WorldClient angeben ("Redirect URI") und eine Standardeinstellung ändern. Anschließend müssen Sie den App Key und das App Secret der Dropbox in die entsprechenden Felder des Dropbox-Konfigurationsdialogs in MDaemon kopieren. Ihre Benutzer können dann bei der nächsten Anmeldung an WorldClient ihre Dropbox-Benutzerkonten mit WorldClient verknüpfen. Eine genaue Anleitung für die Erstellung Ihrer Dropbox-App und die Verknüpfung mit WorldClient finden Sie im Abschnitt Erstellen und Verknüpfen Ihrer Dropbox-App[338] weiter unten.

Nachdem Sie Ihre Dropbox-App erstellt haben, hat die App zunächst den Status "Entwicklung" ("Development"). In diesem Status können 500 WorldClient-Benutzer ihre Dropbox-Benutzerkonten mit der App verknüpfen. Dropbox verlangt jedoch, dass Sie den Status "Wirkbetrieb" ("Production") binnen zwei Wochen beantragen und erteilt erhalten, nachdem sich 50 Benutzer mit Ihrer Dropbox-App verknüpft haben. Ist dieser Status nach Ablauf der genannten Frist nicht erteilt, dann wird die Verknüpfung weiterer Benutzer mit Ihrer App unterbunden, und zwar unabhängig davon, wie viele Benutzer (0 bis 500) mit Ihrer App verknüpft sind. Solange der Status "Wirkbetrieb" nicht erteilt wurde, funktioniert die Dropbox-Integration zwar weiterhin, aber es können keine weiteren Benutzer ihre Benutzerkonten mit der Dropbox-App verknüpfen. Die Erteilung der Freigabe für den Wirkbetrieb ist ein unkomplizierter Prozess, der sicherstellen soll, dass Ihre App den Richtlinien und Nutzungsbedingungen von Dropbox entspricht. Nähere Informationen hierzu erhalten Sie in englischer Sprache im Abschnitt Production Approval ("Freigabe für den Wirkbetrieb") der Entwicklerrichtlinien für die DBX-Plattform.

Sobald Ihre WorldClient-App erstellt und richtig konfiguriert ist, erhalten alle WorldClient-Benutzer bei der Anmeldung an WorldClient die Möglichkeit, ihre Benutzerkonten mit ihren eigenen Dropbox-Konten zu verknüpfen. Die Benutzer müssen sich dazu an Dropbox anmelden und der App die Berechtigung für den Zugriff auf das Dropbox-Benutzerkonto erteilen. Die Benutzer werden dann mithilfe eines Umleitungs-URIs, der während des Anmeldeverfahrens an Dropbox übermittelt wurde, wieder zu WorldClient zurückgeleitet. Aus Sicherheitsgründen muss dieser URI einem der Umleitungs-URIs ("Redirect URIs") entsprechen, die Sie auf der Info-Seite Ihrer App auf Dropbox.com angegeben haben. Nähere Informationen hierzu finden Sie weiter unten. Abschließend tauschen WorldClient und Dropbox einen Zugriffskode und einen Zugriffstoken aus, mit deren Hilfe WorldClient eine Verbindung zum Dropbox-Benutzerkonto herstellen kann. Diese Verbindung ermöglicht es den Benutzern, Dateianlagen in ihren Dropbox-Benutzerkonten zu speichern. Der Zugriffstoken läuft nach jeweils sieben Tagen ab; die Benutzer müssen daher die Berechtigung zur Nutzung ihrer Dropbox-Benutzerkonten immer wieder neu erteilen. Die Benutzer können auf der Seite Cloud-Apps in WorldClient auch die Verknüpfung ihres Benutzerkontos mit ihrer Dropbox manuell trennen, und sie können die Berechtigung manuell neu erteilen.

Integration von Let's Encrypt 596 über ein PowerShell-Skript

Um SSL/TLS und HTTPS 577 für MDaemon 579, WorldClient 582 und die Remoteverwaltung 586 nutzen zu können, benötigen Sie ein SSL/TLS-Zertifikat. Zertifikate sind kleine Dateien, die durch eine Zertifizierungsstelle (nach der englischen Bezeichnung Certificate Authority auch als CA abgekürzt) ausgestellt werden. Sie dienen einem Client oder Browser zur Prüfung, ob er wirklich mit der gewünschten Gegenstelle verbunden ist, und sie ermöglichen die Transportverschlüsselung (SSL/TLS/HTTPS), um die Verbindung mit dieser Gegenstelle zu sichern. Let's Encrypt ist eine Zertifizierungsstelle, und sie stellt Zertifikate unentgeltlich über einen automatisch ablaufenden Vorgang zur Verfügung, der den ansonsten noch komplexen Vorgang manueller Erstellung, Prüfung, Signatur, Installation und Erneuerung von Zertifikaten für sichere Websites ersetzen soll.

MDaemon unterstützt den automatisierten Vorgang zur Verwaltung von Let's-Encrypt-Zertifikaten mithilfe eines PowerShell-Skripts, das im Verzeichnis "`MDaemon\LetsEncrypt`" abgelegt ist. Eine Abhängigkeit dieses Skripts ist das Modul ACMESharp v2, das PowerShell 5.1 und das .Net Framework 4.7.2 erfordert. Aus diesem Grund kann das Skript nicht auf Microsoft Windows Server 2003 eingesetzt werden. Damit das Skript richtig arbeiten werden kann, muss außerdem WorldClient auf Port 80 arbeiten, da sonst die HTTP-Anforderung (Challenge) nicht erfolgreich abgeschlossen werden kann. Um das Skript auszuführen, müssen Sie die PowerShell-Ausführungsrichtlinie richtig setzen. Wird das Skript ausgeführt, so werden alle Vorbereitungen für die Nutzung von Let's Encrypt automatisch getroffen, insbesondere werden auch die erforderlichen Dateien im WorldClient-Verzeichnis HTTP gespeichert, damit die Anforderung http-01 erfolgreich abgeschlossen werden kann. Das Skript nutzt den SMTP-Hostnamen 184 der Standard-Domäne 181 als Domäne für das Zertifikat, ruft das Zertifikat ab, importiert es in Windows, und konfiguriert MDaemon so, dass das Zertifikat für MDaemon, WorldClient und die Remoteverwaltung genutzt wird.

Falls Sie für Ihre Standard-Domäne einen voll qualifizierten Domänennamen (FQDN 184) eingerichtet haben, der nicht auf den MDaemon-Server verweist, kann das Skript nicht arbeiten. Falls Sie in das Zertifikat weitere Domänennamen eintragen lassen wollen, können Sie hierzu die gewünschten weiteren Hostnamen auf der Befehlszeile übergeben.

Ein Beispiel für eine solche Nutzung:

```
..\LetsEncrypt.ps1 -AlternateHostNames
   mail.domain.com,wc.domain.com -IISSiteName MeineSite -To
   "admin@ihredomaene.com"
```

Sie müssen den FQDN für die Standard-Domäne nicht in die Liste für den Parameter `AlternateHostNames` eintragen. Ist beispielsweise für Ihre Standard-Domäne "`example.com`" der FQDN "`mail.example.com`" konfiguriert, und wollen Sie als weiteren Domänennamen "`imap.example.com`" nutzen, so müssen Sie bei Ausführung des Skripts nur den wert "`imap.example.com`" als weiteren Domänennamen übergeben. Übergeben Sie solche weiteren Domänennamen, so muss für jeden Domänennamen eine eigene Anforderung (Challenge) erfolgreich ausgeführt werden. Falls nicht alle Anforderungen erfolgreich ausgeführt werden können, wird der Vorgang nicht erfolgreich abgeschlossen werden. Falls Sie keine weiteren Domänennamen nutzen wollen, dürfen Sie den Parameter `-AlternateHostNames` auf der Befehlszeile nicht übergeben.

Falls Sie WorldClient über die IIS ausführen, müssen Sie an das Skript den Namen der genutzten Site übergeben. Hierzu dient der Parameter `-IISSiteName`. Um das Zertifikat automatisch in die IIS einzutragen, müssen Sie die Web Scripting Tools von Microsoft installiert haben.

Das Skript erstellt im Verzeichnis "`MDaemon\Logs\`" eine Protokolldatei namens `LetsEncrypt.log`. Bei jeder Ausführung des Skripts wird die Protokolldatei gelöscht und neu erstellt. Die Protokolldatei enthält Datum und Uhrzeit, zu denen die Ausführung des Skripts beginnt, aber keine Zeitstempel für die einzelnen Aktionen, die das Skript ausführt. Falls Fehler auftreten, können E-Mails mit entsprechenden Benachrichtigungen versandt werden. Hierzu dient die Variable `$error`, die durch PowerShell automatisch erstellt und gesetzt wird. Falls Sie bei Fehlern keine Benachrichtigung über E-Mail erhalten wollen, lassen Sie den Parameter `-To` auf der Befehlszeile weg.

Speicherung von Postfach-Kennwörtern mit nicht-umkehrbarer Verschlüsselung

Es steht eine neue Kennwort-Option 847 zur Verfügung. Diese Option bewirkt, dass MDaemon die Kennwörter mithilfe eines Verfahrens speichert, dessen Verschlüsselung nicht umkehrbar ist. Hierdurch werden die Kennwörter gegen Entschlüsselung und Offenlegung im Klartext durch MDaemon, die Administratoren und mögliche Angreifer geschützt. MDaemon nutzt, wenn diese Option aktiv ist, die Funktion bcrypt zur Erstellung von Kennworthashes. Hiermit werden längere Kennwörter von bis zu 72 Zeichen möglich. Die Kennwörter müssen außerdem bei Export und Import von Benutzerkonten nicht mehr offengelegt werden, bleiben aber dennoch erhalten. Einige Leistungsmerkmale sind zu dieser Verschlüsselung nicht kompatibel, insbesondere die Erkennung schwacher Kennwörter und die Leistungsmerkmale APOP und CRAM-MD5 für die Echtheitsbestätigung. Diese Leistungsmerkmale setzen voraus, dass MDaemon die Kennwörter entschlüsseln kann. Die nicht-umkehrbare Verschlüsselung ist per Voreinstellung aktiv.

Freigabe von ActiveSync-Clients durch Administratoren

Es steht eine neue ActiveSync-Einstellung "Synchronisierung für neue Clients erst nach Freigabe durch Administrator zulassen" zur Verfügung. Diese Option bewirkt, dass neue Clients sich erst dann mit Benutzerkonten synchronisieren können, wenn sie zunächst durch einen Administrator freigegeben wurden. In der Liste der Clients 464 sind alle Clients aufgeführt, die noch die Freigabe erwarten, und die

Administratoren können sie über diese Liste freigeben. Diese Option steht in den Konfigurationsdialogen für globale 422 und benutzerkontenbezogene 764 Optionen zur Verfügung. Die globale Option ist per Voreinstellung abgeschaltet, und die benutzerkontenbezogene Option wird per Voreinstellung geerbt.

ActiveSync-Benachrichtigungen

Für ActiveSync stehen zwei neue Arten von Benachrichtigungen für Administratoren zur Verfügung: Rollback-Benachrichtigungen für ActiveSync-Synchronisierungen und Benachrichtigungen über beschädigte Nachrichten.

Rollback-Benachrichtigungen für ActiveSync-Synchronisierungen

Der ActiveSync-Dienst kann die Administratoren benachrichtigen, falls ein Client im Rahmen von Synchronisierungsvorgängen wiederholt oder öfter abgelaufene Sync-Schlüssel übermittelt.

Diese Benachrichtigungen teilen dem Administrator mit, dass der Server für eine bestimmte Sammlung einen Rollback veranlasst hat, weil der Client eine Sync-Anforderung mit dem zuletzt gültigen, zwischenzeitlich aber abgelaufenen Sync-Schlüssel angefordert hat. Die Betreffzeile enthält den Hinweis, dass ein ActiveSync-Client einen abgelaufenen Sync-Schlüssel verwendet. Gründe hierfür können Netzwerkprobleme oder Probleme mit Inhalten sein, die dem Client aus der betroffenen Sammlung früher übermittelt wurden. In manchen Fällen wird eine Element-ID aufgeführt. Ob dies der Fall ist, hängt davon ab, ob dem Client in der vorangegangenen Synchronisierung der Sammlung Elemente übermittelt wurden.

Rollback-Benachrichtigungen bedeuten nicht, dass der betroffene Client nicht mehr synchronisiert ist, sondern dass der Client die Synchronisierung verlieren könnte, und dass das System dies erkannt hat. Rollback-Benachrichtigungen werden je Sammlung nur einmal alle 24 Stunden übermittelt. Sie können mithilfe der folgenden Einträge im Abschnitt `[System]` der Datei `\MDaemon\Data\AirSync.ini` konfiguriert werden:

- [System] SendRollbackNotifications=[0|1|Yes|No|True|False]: Diese Option bestimmt, ob Rollback-Benachrichtigungen gesendet werden. Sie ist per Voreinstellung abgeschaltet.
- [System] RollbackNotificationThreshhold=[1-254]: Dies ist die Anzahl der Rollbacks, die für eine bestimmte Sammlung erreicht sein muss, bevor der Administrator eine Rollback-Benachrichtigung erhält. Da auch vorübergehende kleinere Einschränkungen im Netzbetrieb zu Rollbacks führen können, empfiehlt sich ein Schwellwert von mindestens 5. Die Voreinstellung beträgt 10.
- [System] RollbackNotificationCCUser=[0|1|Yes|No|True|False]: Diese Option bestimmt, dass der betroffene Benutzer, dessen Client einen abgelaufenen Sync-Schlüssel übermittelt hat, eine Kopie der Benachrichtigung an den Administrator erhält. Diese Option ist per Voreinstellung abgeschaltet.

ActiveSync-Benachrichtigungen über beschädigte Nachrichten

Der ActiveSync-Dienst kann die Administratoren benachrichtigen, falls eine bestimmte Nachricht nicht verarbeitet werden kann. Solche Benachrichtigungen werden in Echtzeit versandt und informieren den Administrator darüber, dass ein Nachrichten-Element nicht verarbeitet werden konnte und weitere Vorgänge für dieses Element nicht möglich sind. Die Betreffzeile enthält den Hinweis, dass eine

beschädigte Nachricht vorliegt. Solche beschädigten Elemente konnten in früheren Versionen zum Programmabsturz führen. In den meisten solchen Fällen enthält die MSG-Datei keine MIME-Daten. Falls sie MIME-Daten enthält, sind diese Daten wahrscheinlich beschädigt. Mithilfe des Eintrags `CMNCCUser` können Sie dem betroffenen Benutzer eine Kopie der Benachrichtigung senden lassen, damit der Benutzer darauf aufmerksam wird, dass eine Nachricht in seinem Postfach eingegangen ist, die nicht verarbeitet werden konnte. Die richtige Vorgehensweise für solche Nachrichten ist es, sie aus dem Postfach des Benutzers zu entfernen und zu analysieren. So kann festgestellt werden, warum sie nicht verarbeitet werden konnte, und wie es zu diesem Zustand gekommen ist. Diese Benachrichtigungen können mithilfe der folgenden Einträge im Abschnitt `[System]` der Datei `\MDaemon\Data\AirSync.ini` konfiguriert werden:

- [System] SendCorruptMessageNotifications=[Yes|No|1|0|True|False]: Versand der Benachrichtigung. Diese Option ist per Voreinstellung aktiv.
- [System] CMNCCUser==[0|1|Yes|No|True|False]: Versand der Benachrichtigung in Kopie an den betroffenen Benutzer. Diese Option ist per Voreinstellung aktiv.

Neuigkeiten in MDaemon 16.5

Verbesserungen für MDPGP 631

Unterstützung für Schlüssel-Server

WorldClient

WorldClient ist jetzt als einfacher Server für öffentliche Schlüssel nutzbar. Wenn Sie die neue Option "*Öffentliche Schlüssel über HTTP senden (WorldClient)*" aktivieren, beantworter WorldClient Anforderungen nach den öffentlichen Schlüsseln Ihrer lokalen Benutzer. Um eine solche Anforderung zu senden, muss ein URL nach folgendem Muster verwendet werden: "`http://<WorldClient-URL>/WorldClient.dll?View=MDPGP&k=<Schlüssel-ID>`". Dabei muss für den Platzhalter `<WorldClient-URL>` der Pfad zu Ihrem WorldClient-Server eingesetzt werden (beispielsweise "`http://worldclient.example.com`"). Für den Platzhalter `<Schlüssel-ID>` muss die 16 Zeichen lange Schlüssel-ID des gewünschten Schlüssels eingesetzt werden (beispielsweise "`0A1B3C4D5E6F7G8H`"). Die Schlüssel-ID besteht aus den letzten 8 Byte des Fingerabdrucks des Schlüssels und enthält insgesamt 16 Zeichen.

DNS (PKA1)

Mithilfe der neuen MDPGP-Option "*Öffentliche Schlüssel aus DNS (pka1) abrufen und zwischenspeichern für [xx] Stunden*" kann MDPGP DNS-Abfragen nach den öffentlichen Schlüsseln von Nachrichten-Empfängern durchführen. Solche öffentlichen Schlüssel können in TXT-Einträgen des Formats PKA1 im DNS veröffentlicht sein. Diese Option erleichtert die Arbeit, weil sie den Abruf öffentlicher Schlüssel, die zum Verschlüsseln von Nachrichten benötigt werden, automatisiert. Ihre Benutzer müssen dann nicht zunächst die öffentlichen Schlüssel ihrer Kommunikationspartner selbst beschaffen und in den Schlüsselbund importieren, damit sie den Kommunikationspartnern verschlüsselte Nachrichten senden können. Alle Schlüssel-URIs, die im Rahmen der PKA1-Abfragen gefunden werden, werden sofort ausgewertet. Die entsprechenden Schlüssel werden abgerufen, geprüft und in

den Schlüsselbund aufgenommen. Schlüssel, die in dieser Weise erfolgreich abgerufen wurden, bbleiben nur für die in dieser Option angegebene Dauer gültig. Ist für den PKA1-Eintrag selbst im Feld TTL (time to live, Gültigkeitsdauer) eine Gültigkeitsdauer bestimmt, so wird diese Gültigkeitsdauer ausgewertet. Unterscheiden sich die Gültigkeitsdauer aus dieser Option und die aus dem PKA1-Eintrag, so gilt die längere Gültigkeitsdauer.

Behandlung und Verarbeitung von Schlüsseln

Nachverfolgung von Schlüsseln

MDPGP verfolgt die Schlüssel jetzt immer anhand ihrer primären Schlüssel-IDs nach und identifiziert sie auch so. Bislang wurde hierzu eine Kombination aus verschiedenen Datenelementen verwendet, wobei bisweilen die Schlüssel-ID und Schlüssel-Sub-IDs verwendet werden. Die Benutzeroberfläche wurde bereinigt, und es wurden zwei unnötige Spalten aus der Übersicht über die Schlüssel entfernt, in denen für die eigentliche Übersicht nicht erforderliche Schlüssel-IDs erschienen. Die beschriebenen Änderungen zwangen auch zu einer genaueren Kontrolle der Inhalte des MDPGP-Verzeichnisses "exports". Aufgrund der hiermit im Zusammenhang stehenden Anpassungen finden Sie jetzt in diesem Verzeichnis immer die exportierten Kopien der Schlüssel lokaler Benutzer. Sie müssen dieses Verzeichnis - und die gesamte PEM-Verzeichnisstruktur - mithilfe des Betriebssystems gegen unzulässige Zugriffe schützen, da dort auch die geheimen Schlüssel der Benutzer, wenngleich in verschlüsselter Form, gespeichert sind.

Bevorzugte Schlüssel

MDPGP verwendete, wenn auf dem Schlüsselbund mehrere Schlüssel für dieselbe E-Mail-Adresse erfasst waren, bisher einfach den ersten gefundenen Schlüssel. Sie können ab jetzt auf jedem Schlüsseleintrag einen Rechtsklick ausführen und den Schlüssel im Kontextmenü als bevorzugten Schlüssel kennzeichnen. Bevorzugte Schlüssel werden immer dann genutzt, wenn mehrere Schlüssel zur Auswahl stehen. Stehen mehrere Schlüssel zur Verfügung, und ist keiner davon als bevorzugter Schlüssel gekennzeichnet, so wird auch weiterhin der erste gefundene Schlüssel genutzt. Beim Entschlüsseln von Nachrichten versucht MDaemon jeden verfügbaren Schlüssel.

Gesperrte und deaktivierte Schlüssel

Gesperrte und deaktivierte Schlüssen werden ab jetzt in der neuen Datei `oldkeys.txt` erfasst. Bislang wurden gesperrte und deaktivierte Schlüssel in der Datei `plugins.dat` erfasst.

Signaturprüfung durch MDPGP

MDPGP kann jetzt Signaturen auch in unverschlüsselten Nachrichten prüfen. Bislang konnten Signaturen nur geprüft werden, wenn die signierte Nachricht zugleich verschlüsselt war. Beim Betrachten einer Nachricht mit erfolgreich geprüfter Signatur in WorldClient erscheint ein neues Symbol, das dem Benutzer mitteilt, dass die Signatur geprüft ist. Die Signaturprüfung ist per Voreinstellung für alle externen Benutzer aktiv. Sie können wahlweise auch im Einzelnen festlegen, welche Nachrichten dieses Leistungsmerkmal nutzen dürfen (siehe auch "*Berechtigungen für die Nutzung von MDPGP im Einzelnen festlegen*" im Konfigurationsdialog für MDPGP 631).

Instant-Messaging-Server XMPP 372

MDaemon ist mit einem Server für das Extensible Messaging and Presence Protocol (XMPP) ausgestattet; solche Server werden bisweilen auch als Jabber-Server bezeichnet. Über diesen Server können die Benutzer mithilfe von XMPP-Clients, die Drittanbieter bereit stellen, Instant Messages senden und empfangen. Zu diesen Clients gehören Pidgin, Gajim, Swift und viele andere. Solche Clients sind für die meisten Betriebssysteme und Plattformen für mobile Endgeräte verfügbar. Das in MDaemon integrierte XMPP-System ist von dem Chat-System WorldClient Instant Messenger unabhängig. Beide Systeme können nicht miteinander kommunizieren und ihre Kontaktlisten nicht austauschen oder gemeinsam nutzen.

Der XMPP-Server wird als Windows-Dienst installiert. Per Voreinstellung nutzt er die Ports 5222 (SSL über STARTTLS) und 5223 (gesonderter SSL-Port). Der XMPP-Server nutzt die SSL-Konfiguration von MDaemon, falls SSL in MDaemon aktiv ist. Manche XMPP-Clients nutzen DNS-Einträge des Typs SRV, um die Hostnamen der Server automatisch zu ermitteln. Nähere Informationen hierzu finden Sie in englischer Sprache unter http://wiki.xmpp.org/web/SRV_Records.

Die Benutzer melden sich in ihren XMPP-Clients mit Ihrer E-Mail-Adressen und Kennwörtern an. Bei manchen Clients ist es erforderlich, die E-Mail-Adresse für die Anmeldung in ihre Bestandteile zu zerlegen. Ein Beispiel hierzu: Bei Nutzung einer E-Mail-Adresse wie "`frank@example.com`" ist es bei manchen Clients erforderlich, "`frank`" als Anmeldenamen oder Benutzernamen und "`example.com`" als Domäne einzutragen.

Für Chats, an denen mehrere Benutzer oder Gruppen von Benutzern beteiligt sind, stellen die Clients üblicherweise "Chaträume" oder "Konferenzräume" zur Verfügung. Um einen Chat mit einer Benutzergruppe zu beginnen, erstellen Sie einen Chatraum oder Konferenzraum und geben Sie diesem Raum einen Namen. Danach laden sie die gewünschten Benutzer in den Raum ein. Die meisten Clients verlangen keine Servernamen für solche Räume; es genügt vielmehr, den Räumen einen Namen zuzuweisen. Sollte aber ein Servername für einen Raum erforderlich sein, können Sie hierfür das Muster "`conference.<Ihre Domäne>`" nutzen (beispielsweise `conference.example.com`). Einige wenige Clients verlangen, dass der Name des Raums und der Servername in einem Eintrag zusammengefasst werden. Hierfür können Sie das Muster "`konferenzraum@conference.<Ihre Domäneyour domain>`" nutzen (beispielsweise `Raum01@conference.example.com`).

Manche Clients, wie etwa Pidgin, unterstützen die Suche nach Benutzern. Hiermit können die Benutzer auf dem Server anhand von Namen und E-Mail-Adressen nach anderen Benutzern suchen und sie dann einfach in die Kontaktlisten aufnehmen. Üblicherweise muss hierfür kein Servername oder eine besondere Information, wo die Suche durchgeführt werden soll, angegeben werden. Falls der verwendete Client für die Suche einen Servernamen verlangt, können Sie das Muster "`search.<Ihre Domäne>`" nutzen (beispielsweise `search.example.com`). Bei der Suche ist das Zeichen % als Jokerzeichen zulässig. So können Sie beispielsweise in das Feld für die E-Mail-Adresse "%@example.com" eintragen, und Sie erhalten eine Liste aller Benutzer, deren E-Mail-Adressen auf "@example.com" enden.

Zentralisierte Verwaltung der OC-Client-Einstellungen 388

Mithilfe des Konfigurationsdialog OC-Client-Einstellungen können Sie die Client-Einstellungen für die Benutzer des Outlook Connectors verwalten. Die Client-Einstellungen, die Sie in den zugehörigen Konfigurationsdialogen festlegen, übermittelt MDaemon jedes Mal dann an die betroffenen Clients, wenn diese eine Verbindung mit dem Server herstellen. Die Einstellungen werden dann in die

zugehörigen Konfigurationsdialoge des Outlook Connectors übernommen. Die OC-Client-Einstellungen werden dabei nur dann an die Clients übermittelt, wenn sie sich seit der letzten Übermittlung der Einstellungen an die Clients geändert haben. Mithilfe der Option "*Lokale Änderungen an übermittelten Einstellungen durch OC-Benutzer zulassen*" bestimmen Sie, ob die Benutzer die zentral verwalteten und übermittelten Einstellungen auf ihren Clients ändern dürfen. Ist die Option aktiv, so können die Benutzer die Einstellungen in den Konfigurationsdialogen lokal ändern. Ist die Option nicht aktiv, so sind die Konfigurationsdialoge im Outlook Connector gegen Änderungen durch die Benutzer gesperrt, und die Benutzer können die zentral verwalteten und übermittelten Einstellungen nicht ändern.

Bestimmte Einstellungen müssen zwangsläufig für die Benutzer oder für Domänen einzeln unterschiedlich getroffen werden. In den OC-Client-Einstellungen sind daher Makros, wie etwa `$USERNAME$`, `$EMAIL$` und `$DOMAIN$` zugelassen. Diese Makros werden bei der Übermittlung der Einstellungen an die Clients durch Daten ersetzt, die sich auf Benutzer oder Domänen einzeln beziehen. Die Festlegung statischer Einstellungen in solchen Feldern, die dynamisch belegt sein müssen, ist zu vermeiden. Wird beispielsweise der Name "Frank Thomas" in der Einstellung "Ihr Name" festgelegt, so wird der Name jedes Benutzers des Outlook Connectors in "Frank Thomas" geändert, sobald er eine Verbindung mit MDaemon herstellt. Der Abschnitt Allgemeines 391 enthält zur Vereinfachung eine Schaltfläche "*Makro-Übersicht*", mit deren Hilfe Sie eine einfache Liste der unterstützten Makros aufrufen können.

Bei Nutzung von MDaemon Private Cloud steht im Domänen-Manager 181 ein weiterer Konfigurationsdialog OC-Client-Einstellungen zur Verfügung, in dem die Client-Einstellungen für den Outlook Connector nach Domänen getrennt verwaltet werden können.

Dieses Leistungsmerkmal ist per Voreinstellung abgeschaltet. Es erfordert den Outlook Connector ab der Client-Version 4.0.0.

Änderung der Absenderkopfzeile "From:" als Schutz gegen Missbrauch 569

Dieses Leistungsmerkmal ändert die Absenderkopfzeile "From:" eingehender Nachrichten aus Sicherheitsgründen so, dass im Namensfeld der Absenderkopfzeile, das üblicherweise nur den Namen enthält, sowohl der Name als auch die E-Mail-Adresse erscheinen. Das Leistungsmerkmal will verhindern, dass Benutzer über die Absender eingehender Nachrichten getäuscht werden und meinen, dass eine Nachricht von einer bestimmten Person stammt, wohingegen sie tatsächlich beispielsweise von einem Angreifer gesandt wurde. Eine solche Täuschung wird durch den Umstand begünstigt, dass viele E-Mail-Clients nur den Namen des Absenders und nicht auch seine E-Mail-Adresse anzeigen. Der Empfänger sieht die eigentliche E-Mail-Adresse üblicherweise erst, wenn er die Nachricht geöffnet oder einen sonstigen Vorgang durchgeführt hat, etwa, das Kontextmenü zu öffnen, oder den Mauszeiger auf dem Eintrag stehen zu lassen. Aus diesem Grund erstellen Angreifer E-Mail-Nachrichten oft so, dass in dem sichtbaren Feld der Absenderkopfzeile "From:" ein legitim erscheinender Name einer Person oder eines Unternehmens erscheint, wohingegen die E-Mail-Adresse, die Hinweise auf eine missbräuchliche Verwendung gibt, nicht angezeigt wird. So kann beispielsweise die Absenderkopfzeile "From:" einer Nachricht `"Ehrenwerte Bank und Treuhand" <langfinger.klepto@example.com>` lauten, woraufhin der E-Mail-Client nur den Teil `"Ehrenwerte Bank und Treuhand"` als Absender anzeigt. Dieses Leistungsmerkmal ändert daher den sichtbaren Teil der Absenderkopfzeile, um eine solche Täuschung offenzulegen. Hierzu wird die E-Mail-Adresse zuerst angezeigt. In dem genannten Beispiel erscheint dann der Absender beim Empfänger als

"langfinger.klepto@example.com -- Ehrenwerte Bank und Treuhand" und zeigt damit dem Empfänger an, dass die Nachricht missbräuchlich versandt wurde. Diese Option wirkt nur auf Nachrichten an lokale Benutzerkonten und ist per Voreinstellung abgeschaltet.

Verbesserter IP-Filter

Mithilfe einer neuen Schaltfläche im Konfigurationsdialog des IP-Filters können Sie IP-Adressdaten aus APF- und .htaccess-Dateien importieren. Wählen Sie dazu die gewünschte IP-Adresse aus, und klicken Sie auf die Schaltfläche. Der Import der IP-Adressdaten durch MDaemon aus solchen Dateien unterliegt folgenden Einschränkungen:

- Einträge der Typen "deny from" und "allow from" werden unterstützt.
- Es werden nur IP-Adressen, nicht jedoch Domänennamen importiert.
- Die CIDR-Schreibweise ist zulässig. Unvollständige IP-Adressen sind nicht zulässig.
- Auf jeder Zeile sind beliebig viele durch Leerzeichen oder Kommata getrennte IP-Adressen zulässig. Ein Beispiel hierzu: "deny from 1.1.1.1 2.2.2.2/16", ""3.3.3.3, 4.4.4.4, 5.5.5.5".
- Zeilen, die mit # beginnen, werden ignoriert.

Automatische Installation neuer Programmversionen

Mithilfe der Leistungsmerkmale zur automatischen Aktualisierung kann MDaemon den Postmaster benachrichtigen, sobald für ein installiertes Produkt eine neue Version verfügbar ist. MDaemon kann wahlweise auch die neuen Versionen automatisch abrufen und installieren. Diese Leistungsmerkmale umfassen MDaemon, SecurityPlus und den Outlook Connector. Die automatische Installation neuer Versionen kann für jedes Produkt getrennt gesteuert werden. Nach jeder automatischen Installation einer neuen Version muss das System neu gestartet werden. Die Installationsdateien werden abgerufen, sobald eine neue Version gefunden wird, und die Installation und der Neustart des Systems können zeitgesteuert zu einem vorbestimmten Zeitpunkt erfolgen. Alle Installationen werden im Systemprotokoll von MDaemon protokolliert, und der Postmaster wird informiert, sobald eine Aktualisierung durchgeführt wurde. Nähere Informationen finden Sie im Abschnitt Aktualisierungen.

Änderungen bei WorldClient

Kategorien

WorldClient unterstützt in den Designs LookOut und WorldClient Kategorien für E-Mail-Nachrichten. Benutzer können der Nachrichten-Übersicht die Spalte Kategorien hinzufügen. Sie müssen hierzu auf der Seite "Optionen » Spalten" den Eintrag "Kategorien" aktivieren. Um Nachrichten den Kategorien zuzuweisen, werden zunächst die betroffenen Nachrichten in der Nachrichtenliste ausgewählt. Danach wird per Rechtsklick auf den ausgewählten Nachrichten das Kontextmenü aufgerufen, und hier werden die Kategorien ausgewählt.

- Die Administratoren können benutzerdefinierte Kategorien erstellen. Hierfür stehen die Dateien `DomainCategories.json` und `PersonalCategories.json` zur Verfügung.
- Domänen-Kategorien sind per Voreinstellung aktiv. Um diese Kategorien zu deaktivieren, öffnen Sie die Datei `MDaemon\WorldClient\Domains.ini`, und

ändern Sie im Abschnitt `[Default:Settings]` den Eintrag "`DomainCategoriesEnabled=`" von "`Yes`" in "`No`".

- Die Benutzer können per Voreinstellung eigene Kategorien hinzufügen und bearbeiten. Sie können dies für einzelne Benutzer und systemweit unterbinden. Hierzu ändern Sie den Eintrag "`CanEditPersonalCategories=`" von "`Yes`" in "`No`". Um diese Einstellung für einzelne Benutzer zu ändern, bearbeiten Sie den entsprechenden Eintrag im Abschnitt `[User]` der Dateien `User.ini` für die betroffenen Benutzer. Um diese Einstellung systemweit zu ändern, bearbeiten Sie den entsprechenden Eintrag im Abschnitt `[Default:UserDefaults]` der Datei `Domains.ini`.
- Falls Domänen-Kategorien aktiv sind und ein Benutzer nicht zur Bearbeitung persönlicher Kategorien berechtigt ist, stehen dem Benutzer nur die Kategorien aus der Datei `DomainCategories.json` zur Verfügung.
- Falls Domänen-Kategorien nicht aktiv sind und ein Benutzer nicht zur Bearbeitung persönlicher Kategorien berechtigt ist, stehen dem Benutzer nur die Kategorien aus der Datei `PersonalCategories.json` zur Verfügung.
- Mithilfe der Datei `CustomCategoriesTranslations.json` können Sie für benutzerdefinierte Namen für Kategorien in mehreren Sprachen festlegen. Sie können dieser Datei alle erforderlichen Übersetzungen für die Namen der Kategorien hinzufügen. WorldClient stellt mithilfe dieser Datei sicher, dass Kategorien den Terminen, Notizen und Aufgaben in jeweils verschiedenen Sprachfassungen unter der jeweils für die lokale Sprachfassung zutreffenden Bezeichnung zugewiesen werden können, und dass diese Zuweisung jeweils derselben Kategorie folgt und damit über alle Sprachfassungen konsistent bleibt.

Nähere Informationen über die hier aufgeführten Dateien finden Sie in der Datei `MDaemon\WorldClient\CustomCategories.txt`.

Weiße und Schwarze Listen 350

Sie können die Ordner für Weiße und Schwarze Listen per Voreinstellung vor den Benutzern von WorldClient verbergen. Hierzu öffnen Sie die Datei `MDaemon\WorldClient\Domains.ini`, und ändern Sie im Abschnitt `[Default:UserDefaults]` die Einträge "`HideWhiteListFolder=`" oder "`HideBlackListFolder=`" von "`No`" in "`Yes`". Sie können diese Ordner auch vor einzelnen Benutzern verbergen, indem Sie die gleich lautenden Einträge im Abschnitt `[User]` der Dateien `User.ini` für die betroffenen Benutzer bearbeiten.

Warnung bei möglicherweise fehlenden Dateianlagen

In den Designs LookOut und WorldClient kann WorldClient beim Verfassen von Nachrichten vor dem Versand jetzt prüfen, ob der Entwurf Dateianlagen enthält, falls sich der Nachrichtentext oder die Betreffzeile auf Dateianlagen beziehen. Dieses Leistungsmerkmal kann helfen, zu verhindern, dass Benutzer Dateianlagen mit einer Nachricht versenden wollen, sie dann aber beim Verfassen der Nachricht vergessen und die Nachrichten irrtümlich ohne Dateianlagen senden.

Zwei-Faktor Authentifizierung 720

Sie können jetzt bestimmen, ob Benutzerkonten die Zwei-Faktor-Authentifizierung nutzen dürfen oder nutzen müssen. Es stehen zwei neue Optionen in der Vorlage Neue Benutzerkonten 795 zur Verfügung, die die Voreinstellung für neue Benutzerkonten steuern. Es stehen entsprechende Optionen im Abschnitt Web-Dienste 720 des Benutzerkonten-Editors zur Verfügung, mit deren Hilfe die

Einstellungen zur Zwei-Faktor-Authentifizierung für einzelne Benutzerkonten geändert werden können.

Neuigkeiten in MDaemon 16.0

Aktualisierung für die Benutzeroberfläche der MDaemon-Remoteverwaltung

Die Benutzeroberfläche der Remoteverwaltung verwendet keine Frames mehr und wurde auf ein reaktionsfähiges Design umgestellt, das in erster Linie von einer mobilen Nutzung ausgeht. Das zugrundeliegende Konzept wird auch als Mobile First Responsive Design bezeichnet. Es werden der Internet Explorer ab Version 10, die neuesten Versionen von Chrome und Firefox, sowie unter MacOS und iOS die neuesten Versionen von Safari unterstützt. Die Standard-Browser auf Android-Geräten zeigen bekannte Probleme beim Scrollen; Chrome funktioniert auf Android-Geräten jedoch gut.

Das neue Design stützt sich ausschließlich auf die Größe des jeweils genutzten Fensters. Das Aussehen ist für gleiche Fenstergrößen immer gleich, und zwar unabhängig davon, ob der Benutzer ein Mobiltelefon, ein Tablet oder einen PC nutzt. Die wichtigste Änderung betrifft dabei das Menü. Bei einer Fensterbreite von 1024 Bildpunkten oder weniger ist das Menü auf der linken Seite des Browserfensters ausgeblendet. Es bestehen zwei Möglichkeiten, das Menü anzuzeigen. Falls ein Bildschirm mit Berührungseingabe (Touchscreen) genutzt wird, kann das sekundäre Menü durch eine Wischgeste nach rechts eingeblendet werden. Außerdem kann durch Antippen des Steuerelements Menü in der oberen rechten Fensterecke das sekundäre Menü aufgerufen werden. Durch Antippen oder Anklicken des Menütitels am oberen Rand des Menüs, neben dem ein Pfeil nach links erscheint, erscheint das primäre Menü. Das Menü Hilfe, Informationen und Abmelden in der oberen rechten Fensterecke ändert sich ebenfalls mit der Fensterbreite. Zwischen 481 und 767 Bildpunkten erscheinen nur die Symbole, und bei 480 Bildpunkten oder weniger erscheint ein Zahnrad-Symbol, unter dem nach dem Antippen oder Anklicken ein Menü mit den Einträgen Hilfe, Informationen und Abmelden erscheint. Listenansichten mit mehr als einer Spalte erhalten Steuerelemente, mit denen die einzelnen Spalten ein- und ausgeblendet werden können. Sie sind erreichbar durch Anklicken oder Antippen des grauen Rechtspfeils am rechten Rand des Containers für die Symbolleiten. Die Konfigurationsdialoge sind nicht mehr als genaue Kopien der Konfigurationsdialoge aus der Benutzeroberfläche von MDaemon angelegt; sie ändern ihre Position und Größe jetzt in Abhängigkeit von der Breite und Höhe des Browserfensters.

Spambot-Erkennung 572

MDaemon wurde um ein neues Leistungsmerkmal namens Spambot-Erkennung erweitert. Dieses Leistungsmerkmal protokolliert IP-Adressen aus eingehenden SMTP-Verbindungen und gleicht sie mit den Antwortpfaden ab, die im Rahmen der SMTP-Befehle MAIL übermittelt werden. Ergibt dieser Abgleich, dass derselbe Antwortpfad von zahlreichen verschiedenen IP-Adressen verwendet wird, und gehen die entsprechenden Nachrichten innerhalb eines verhältnismäßig kurzen Zeitraums ein, so kann dies darauf hindeuten, dass die Nachrichten von einem Netz aus Spambots übermittelt wurden. Dies gilt insbesondere, wenn derselbe Antwortpfad von mehr verschiedenen IP-Adressen genutzt wird, als es bei Benutzern normalerweise zu erwarten wäre, wenn sie mehrere Geräte oder Zugänge nutzen. Feststehende Kriterien für die Erkennung von Spambots allgemein bestehen

allerdings nicht, und es kann auch legitime Gründe für die genannten Erscheinungen geben. Versuche haben aber gezeigt, dass sich anhand der gezeigten Kriterien Spambot-Netze zumindest dann recht zuverlässig erkennen lassen, wenn sie denselben Antwortpfad nutzen. Wird während einer Verbindung erkannt, dass die Gegenstelle möglicherweise ein Spambot ist, dann wird die Verbindung sofort getrennt, und der Antwortpfad kann wahlweise für eine bestimmte Zeit in eine Schwarze Liste aufgenommen werden. Sie können wahlweise auch alle IP-Adressen, von denen vermutet wird, dass sie zu dem betreffenden Spambot-Netzwerk gehören, für eine bestimmte Zeit in die Schwarze Liste aufnehmen lassen.

CardDAV

MDaemon unterstützt jetzt die Synchronisierung von Kontakten über das Protokoll CardDAV. Der CardDAV-Server von MDaemon gestattet echtheitsbestätigten CardDAV-Clients den Zugriff auf die in MDaemon gespeicherten Kontaktdaten. Bekannte CardDAV-Clients sind beispielsweise Apple Contacts (Mac OS X), Apple iOS (iPhone) und Mozilla Thunderbird mithilfe des Plugins SOGO. Nähere Informationen über CardDAV und die Konfiguration der CardDAV-Clients finden Sie im Abschnitt CalDAV & CardDAV.

Zwei-Faktor-Authentifizierung für WorldClient und die Remoteverwaltung

MDaemon unterstützt jetzt die Zwei-Faktor-Authentifizierung (also die Anmeldung mithilfe zweier Sicherungsmittel) für Anmeldungen an WorldClient und der MDaemon-Remoteverwaltung. Benutzer, die sich über eine verschlüsselte Verbindung (HTTPS) an WorldClient anmelden, können über den Konfigurationsdialog **Optionen » Sicherheit** die Zwei-Faktor-Authentifizierung aktivieren. Sie müssen dann bei jeder Anmeldung an WorldClient oder der Remoteverwaltung einen Bestätigungskode eingeben. Sie erhalten diesen Kode von einer Authenticator-App, die auf den mobilen Endgeräten der Benutzer installiert ist. Das Leistungsmerkmal ist für jeden Client nutzbar, der den Google Authenticator unterstützt.

Migrationsclient auf Basis des Protokolls ActiveSync

MDaemon wird jetzt mit einem Migrationsclient auf Basis des Protokolls ActiveSync ausgeliefert (`ASMC.exe`). Dieser Client unterstützt die Migration von Nachrichten, Kalendern, Aufgaben, Notizen und Kontakten von ActiveSync-Servern, die die Protokollversion 14.1 unterstützen. Sie finden eine Dokumentation über die Nutzung dieses Clients im Verzeichnis `\MDaemon\Docs`.

XML-basiertes API für Verwaltungsaufgaben

MDaemon enthält jetzt ein API auf Basis von XML via http(s). Aufgrund dieser Änderung können jetzt Verwaltungsclients für MDaemon in jeder Sprache und auf jeder Plattform programmiert werden, die http(s)-post-Anforderungen an den Server übermitteln kann. In MDaemon stehen die entsprechenden Funktionen nur angemeldeten Globalen Administratoren zur Verfügung. In MDaemon Private Cloud steht ein Teil der verfügbaren Funktionen auch angemeldeten Domänen-Administratoren zur Verfügung. Das API erstellt auch eine Website, auf der die Spezifikation für das API dokumentiert ist. Per Voreinstellung lautet der URL dieser Website `http://Servername/MdMgmtWS/`, er kann aber geändert werden, insbesondere auch, um die Sicherheit zu erhöhen.

Insbesondere folgende Funktionen sind verfügbar:

- Help (Hilfe)
- CreateDomain (Domäne erstellen)
- DeleteDomain (Domäne löschen)
- GetDomainInfo (Domäneninformation abrufen)
- UpdateDomain (Domäne aktualisieren)
- CreateUser (Benutzer erstellen)
- DeleteUser (Benutzer löschen)
- GetUserInfo (Benutzerinformation abrufen)
- UpdateUser (Benutzer aktualisieren)
- CreateList (Mailingliste erstellen)
- DeleteList (Mailingliste löschen)
- GetListInfo (Mailinglisteninformation abrufen)
- UpdateList (Mailingliste aktualisieren)
- AddDomainAdministrator (Domänen-Administrator hinzufügen)
- DeleteDomainUsers (Domänenbenutzer löschen)
- GetDomainList (Domänenliste abrufen)
- GetVersionInfo (Versionsinformation abrufen)
- GetQueueState (Warteschlangenstatus abrufen)
- GetServiceState (Dienststatus abrufen)
- SetAddressRestriction (Adresssperre einrichten)
- GetAddressRestriction (Adresssperre abrufen)

Derzeit sind Befehlszeilen-Clients in Javascript, Powershell, VBScript, C, C++ und Visual Basic programmiert und getestet worden. Eine einfache Test-Site für HTML und Javascript wurde als Machbarkeitsnachweis für eine webgestützte Managementkonsole erstellt und arbeitet in mehreren allgemein verbreiteten Browsern. Es wird erwartet, dass das API auch auf Webservern, die PHP, Perl und andere Entwicklungsplattformen einsetzen, einwandfrei funktioniert, jedoch ist noch keine Erprobung durchgeführt worden.

Siehe auch:

Einleitung 12
Die Umstellung auf MDaemon 23.0.0 65
Die Haupt-Benutzeroberfläche von MDaemon 74

1.4 Die Umstellung auf MDaemon 23.0.0

Die nachfolgende Aufstellung enthält einige Hinweise zur besonderen Beachtung, die bei der Umstellung von älteren Programmversionen auf MDaemon 23.0.0 besonders wichtig sind.

Version 23.0.0

- Für die Umstellung von Version 22.0.0 auf 23.0.0 sind keine besonderen Anweisungen erforderlich. Falls Sie eine frühere Version aktualisieren, beachten Sie bitte die folgenden Hinweise.

Version 22.0.0

- Die 32-Bit-Version von MDaemon wurde eingestellt. Ab MDaemon 22.0 ist MDaemon nur noch in der 64-Bit-Version verfügbar. Falls Sie derzeit eine 32-Bit-Version auf einem unterstützten 64-Bit-Betriebssystem einsetzen, können Sie die 64-Bit-Version herunterladen und einfach über die bestehende Installation installieren.
- Die Mindestlänge für starke Kennwörter[847] beträgt jetzt mindestens 8 Zeichen. Falls auf Ihrem System vor der Aktualisierung auf MDaemon 22 eine Mindestlänge von weniger als 8 Zeichen konfiguriert war, so wird die Mindestlänge während der Installation auf 8 Zeichen erhöht. Die Voreinstellung für die Mindestlänge starker Kennwörter bei Neuinstallationen beträgt jetzt 10 Zeichen.
- In MDaemon wurden die Begriffe "Schwarze Liste" und "Weiße Liste" durch andere Begriffe ersetzt. In vielen Fällen lauten die jetzt verwendeten Begriffe "Freigabeliste" und "Sperrliste". Leistungsmerkmale, in denen "Weiße Listen" vorgesehen waren, um IP-Adressen, E-Mail-Adressen und andere Daten von der Bearbeitung durch die Leistungsmerkmale auszuschließen, enthalten jetzt "Ausnahmelisten". Die benutzerindividuellen Kontaktordner, die der Spam-Filter nutzt, tragen jetzt die Bezeichnungen "Zugelassene Absender" und "Gesperrte Absender". Die Ordner aller Benutzerkonten werden entsprechend umbenannt, während MDaemon 22 zum ersten Mal gestartet wird.

Version 21.5.0

- Die Kopfzeile "`X-MDOrigin-Country`", die der Länder-Filter[574] in die Nachrichten einfügen kann, enthält jetzt nicht mehr die vollständigen Namen der Länder und Kontinente sondern stattdessen die aus zwei Buchstaben bestehenden geografischen Kodes, wie sie in der Kodierliste zu ISO 3166 definiert sind. Falls Sie Filter verwenden, die die genannte Kopfzeile auswerten, müssen Sie diese Filter daher anpassen, sodass die Kodes nach ISO 3166 ausgewertet werden.
- Die Umbenennung des Webmail-Designs Mobile in Pro kann unter Umständen zu einem Fehler bei solchen Benutzern führen, die das Design Mobile nutzen und ihre Anmeldung gespeichert haben. Diese Benutzer können unter Umständen keine Dateianlagen mehr speichern. Um diesen Fehler zu beheben, genügt es, dass sich die Benutzer ab- und danach wieder anmelden.

Version 21.0.2

- Die Einstellungen im Konfigurationsdialog Einstellungen » Voreinstellungen » Verschiedenes, mit denen Systemnachrichten an den Postmaster auch an globale und Domänen-Administratoren versandt werden, wirken sich jetzt auf weitere Benachrichtigungen aus. Hierzu gehören Benachrichtigungen über das Einfrieren und Sperren von Benutzerkonten, Meldungen über unbekannte Benutzer, Fehler auf den Datenträgern, unzureichender Speicherplatz, und

Hinweis auf das bevorstehende Ende der Gültigkeit von Beta-Versionen und AntiVirus-Abonnements. Falls Sie nicht wünschen, dass Ihre Administratoren diese Nachrichten erhalten, müssen Sie die entsprechenden Einstellungen deaktivieren.

Version 20.0.3

- MDaemon deaktiviert in der ClamAV-Datei `clamd.conf` den Eintrag "`AlertExceedsMax yes`", da dieser Eintrag übermäßig viele Fehler "`Heuristics.Limits.Exceeded`" in der AntiVirus-Prüfung verursachte.

Version 20.0.1

- Mithilfe der Einstellungen für den Zugriff auf Netzwerkressourcen im Konfigurationsdialog Einstellungen » Voreinstellungen » Windows-Dienst können Sie jetzt ein Benutzerkonto festlegen, unter dem die Windows-Dienste MDaemon, MDaemon-Remoteverwaltung und XMPP ausgeführt werden. Bislang wurden diese Dienste und die Prozesse und Threads, die durch diese Dienste gestartet wurden, im Sicherheitskontext des Benutzerkontos SYSTEM ausgeführt. Die Installationsroutine ändert während der Aktualisierung auf die vorliegende Version die Konfiguration der betroffenen Windows-Dienste so, dass sie unter dem angegebenen Benutzerkonto ausgeführt werden.
- In der Datei `clamd.conf` haben sich Änderungen ergeben, und viele Einstellungen werden nicht mehr unterstützt. Die Installationsroutine überschreibt daher eine bestehende Datei `clamd.conf`. Falls Sie Ihre Datei `clamd.conf` angepasst haben, müssen Sie die Datei `clamd.conf` nach der Installation überprüfen und möglicherweise anpassen.

Version 20.0.0

- Bitte lesen Sie in den vollständigen Versionsinformationen den Abschnitt [8930] besonders sorgfältig durch. Dieser Abschnitt enthält Informationen über Änderungen an der Integration des Active Directory, und Sie bemerken unter Umständen eine Änderung in der Funktionsweise, wobei bislang nicht funktionierende Vorgänge jetzt funktionieren. Um einen Überblick über die einzelnen Änderungen und ihre Wirkung zu erhalten, müssen Sie den genannten Abschnitt vollständig und sorgfältig durcharbeiten.
- MDaemon 20.0 erfordert Microsoft Windows 7, Server 2008 R2 oder eine neuere Version der genannten Betriebssysteme.
- Der Konfigurationsdialog Voreinstellungen » Verschiedenes 504 wurde um zwei Optionen erweitert. Sie bestimmen, ob die durch das System erstellten Benachrichtigungen, die an den Postmaster gesandt werden, auch an die Globalen und Domänen-Administratoren gesandt werden sollen. Per Voreinstellung sind beide Optionen aktiv. Domänen-Administratoren erhalten hierbei nur Nachrichten, die sich auf ihre Domänen beziehen, sowie die Versionsinformationen. Globale Administratoren erhalten alle Nachrichten sowie die Berichte über Inhalte der Warteschlangen, Statistiken, Versionsinformationen, Meldungen, dass Benutzer nicht gefunden wurden (für alle Domänen), Meldungen über Datenträgerfehler, Meldungen über eingefrorene und gesperrte Benutzerkonten für alle Domänen (sie und die Domänen-Administratoren können die Benutzerkonten wieder freigeben), Warnmeldungen über Lizenzen und den bevorstehenden Ablauf der Funktionsdauer von Betaversionen, Übersichten über Spam und weitere

Nachrichten. Falls Sie nicht wünschen, dass die Administratoren diese Nachrichten erhalten, müssen Sie die neuen Optionen deaktivieren.

- Autobeantworter werden ab jetzt anders als bisher gespeichert. Der Text des Autobeantworters für ein Benutzerkonto wird jetzt als Datei `OOF.MRK` in den Verzeichnissen DATA der Benutzerkonten gespeichert. Dieses Verzeichnis ist ein neues Unterverzeichnis unter dem Hauptverzeichnis des Postfachs. Die Skriptdateien für die Autobeantworter werden nicht mehr im Verzeichnis APP gespeichert, und sie werden auch nicht mehr durch mehrere Benutzerkonten gemeinsam genutzt. Beim ersten Programmstart überführt MDaemon alle Dateien und Einstellungen der bestehenden Autobeantworter an die neuen Speicherorte für die betreffenden Benutzerkonten. Die Datei `AUTORESP.DAT` wird nicht mehr verwendet. Sie und die `RSP`-Dateien der einzelnen Benutzerkonten werden gelöscht. Die Datei `OutOfOffice.RSP` und Dateien, die sich nicht auf einzelne Benutzerkonten beziehen, bleiben als Standard-Referenzskript und Beispieldateien erhalten. Falls Sie eine bestimmte Autobeantworter-Konfiguration mehreren Benutzerkonten gleichzeitig zuweisen wollen, können Sie dies mithilfe der neuen Schaltfläche Veröffentlichen im Konfigurationsdialog Benutzerkonten-Einstellungen » Autobeantworter 724 erreichen. Durch Anklicken dieser Schaltfläche werden der bestehende Text des Skripts für den Autobeantworter und alle Einstellungen aus dem gerade bearbeiteten Benutzerkonto in die anderen Benutzerkonten kopiert, die Sie auswählen. Es steht außerdem eine neue Schaltfläche Skript für den Autobeantworter bearbeiten 724 zur Verfügung, mit deren Hilfe Sie das Standard-Skript für die Autobeantworter (`OutOfOffice.rsp`) bearbeiten können. Die so bearbeitete Datei wird in die Datei `OOF.MRK` der Benutzerkonten kopiert, in denen die Datei `OOF.MRK` fehlt oder leer ist.
- Die Signaturen für Benutzerkonten werden ab jetzt anders als bisher gespeichert. Die Signaturdateien werden jetzt als Dateien `SIGNATURE.MRK` in den Verzeichnissen DATA der Benutzerkonten gespeichert. Dieses Verzeichnis ist ein neues Unterverzeichnis unter dem Hauptverzeichnis des Postfachs. Beim ersten Programmstart überführt MDaemon alle Dateien der bestehenden Signaturen an die neuen Speicherorte für die betreffenden Benutzerkonten. Im Verzeichnis Signatures unter dem Hauptverzeichnis von MDaemon sind danach keine benutzerspezifischen Signaturdateien mehr gespeichert. Das Verzeichnis selbst bleibt aber bestehen, da es noch Elemente enthalten kann, die durch die MDaemon-Remoteverwaltung und den Inhaltsfilter benötigt werden. Der ursprüngliche Inhalt des Verzeichnisses Signatures wurde vor der Umstellung in das Verzeichnis `\Backup\20.0.0\Signatures\` gesichert. Auch die Dateien `ADMINNOTES.MRK` für die einzelnen Benutzerkonten wurden in das neue Unterverzeichnis DATA verschoben.
- Im Konfigurationsdialog Spam-Filter » Weiße Liste (automatisch) 692 wurde die Voreinstellung für die Option "*... nur über DKIM echtheitsbestätigte Adressen in die Weiße Liste eintragen*" geändert; die Option ist jetzt per Voreinstellung deaktiviert. Die Option hat sich für mehrere Anwendungszwecke als zu stark einschränkend erwiesen. Sie verhindert auch die Nutzung des Adressbuchs als Weiße Liste für Nachrichten, die über MultiPOP und DomainPOP abgerufen wurden. Falls die Option bislang aktiv war und so beibehalten werden soll, müssen Sie die Option nunmehr erneut aktivieren.
- Im Konfigurationsdialog Voreinstellungen » Benutzeroberfläche 492 wurde die Option "*Alle Konfigurationsdialoge der Benutzeroberfläche zentrieren*" für alle Installationen auf die Voreinstellung gesetzt und damit aktiviert. Falls dies

nicht Ihren Anforderungen entspricht, müssen Sie die Option deaktivieren. Die Option verhindert, dass Konfigurationsdialoge teilweise außerhalb des darstellbaren Bildschirmbereichs erstellt werden (was für die meisten Anwendungszwecke wünschenswert sein dürfte), sie erschwert aber bisweilen die Anwahl eines von mehreren überlappenden Fenstern.

- Im Konfigurationsdialog Sicherheits-Manager » Filter » Länder-Filter[574] ist der Länder-Filter ab jetzt per Voreinstellung aktiv. Bei aktiviertem Länder-Filter werden das Land oder die Region, aus dem oder der eine eingehende Verbindung hergestellt wird, immer protokolliert, soweit sie sich feststellen lassen. Die Protokollierung erfolgt auch, wenn das betreffende Land oder die betreffende Region nicht durch den Länder-Filter gesperrt sind. Sie können daher den Länder-Filter auch dann aktivieren, wenn Sie keine zu sperrenden Länder auswählen, und die Informationen über Land oder Region werden danach angezeigt und protokolliert. Da sich die Voreinstellung für diese Option geändert hat, sollten Sie nach einer Aktualisierung von MDaemon die Konfiguration des Länder-Filters darauf hin überprüfen, ob sie Ihren Anforderungen weiterhin entspricht. MDaemon fügt in die Nachrichten die Kopfzeile "`X-MDOrigin-Country`" ein; in ihr erscheinen Land oder Region. Sie können diese Kopfzeile zur Bearbeitung durch den Inhaltsfilter oder für andere Verarbeitungszwecke nutzen.
- Die bislang fest kodierte Größenbegrenzung von 2 MB, oberhalb derer Nachrichten nicht mehr durch den Spam-Filter ausgewertet wurden, wurde entfernt. Es besteht jetzt theoretisch keine höchstzulässige Größe mehr, ab der Nachrichten nicht mehr durch den Spam-Filter geprüft werden können. Sie können, falls die neue Vorgehensweise zu Problemen führt, auch weiterhin eine höchstzulässige Größe konfigurieren. Der Wert 0 (null) in der Konfiguration bewirkt ab jetzt aber, dass keine Größenbegrenzung mehr gilt. Der Wert der höchstzulässigen Größe wird ab jetzt nicht mehr in KB sondern in MB angegeben. Eine etwa bestehende Größenbegrenzung wurde entsprechend umgerechnet. Falls keine Größenbegrenzung konfiguriert war, wurde der Wert 0 gesetzt. Sie sollten im Konfigurationsdialog Spam-Filter » Einstellungen[701] den Wert daraufhin prüfen, ob er Ihren Anforderungen entspricht.
- Die Übersichten über die Warteschlangen auf der Haupt-Benutzeroberfläche wurden um die Spalten "Domäne des Absenders" und "Domäne des Empfängers" erweitert. Aufgrund dieser Erweiterung mussten einmalig die etwa zuvor gespeicherten Spaltenbreiten auf die Voreinstellungen zurückgesetzt werden. Wenn Sie die Spaltenbreiten nunmehr erneut anpassen, werden die angepassten Spaltenbreiten wieder gespeichert werden.
- Der Host-Filter wird per Voreinstellung jetzt auch auf MSA-Verbindungen angewendet. Falls gewünscht, können Sie die entsprechende Option im Konfigurationsdialog Sicherheits-Manager » Filter » Host-Filter[565] deaktivieren.
- Per Voreinstellung gestatten die MDaemon-Dienste IMAP, Webmail und ActiveSync den Zugriff auf freigegebene gemeinsam genutzte Ordner gesperrter Benutzerkonten ab jetzt nicht mehr. Sie können dieses Verhalten mithilfe neuer Einstellungen im Konfigurationsdialog Server-Einstellungen » Öffentliche & Freigegebene Ordner[122] anpassen.

Version 19.5.2

- Die Optionen "Höchstzahl der RSET-Befehle" im Konfigurationsdialog F2 » Server-Einstellungen » Server wurden entfernt. Sie stellten im Ergebnis lediglich weniger flexible Doppelungen vergleichbarer Optionen im Konfigurationsdialog Strg+S » Filter » SMTP-Filter dar. Die Optionen im Konfigurationsdialog SMTP-Filter gehören systematisch zum Dynamischen Filter, und der Dynamische Filter wertet mehr Kriterien aus und berücksichtigt mehr Gegebenheiten (so verfügt er über eine Weiße Liste, wertet den Status der Echtheitsbestätigung und vieles mehr aus). Die bisher im Konfigurationsdialog F2 » Server-Einstellungen » Server getroffenen Einstellungen wurden in den SMTP-Filter übernommen. Bitte prüfen Sie die Einstellungen unter Strg+S » Filter » SMTP-Filter, und stellen Sie sicher, dass die dort jetzt eingestellten Werte Ihren Anforderungen entsprechen. Zutreffende und empfohlene Voreinstellungen sind 20 höchstens zulässige RSET-Befehle, und die Option "SMTP-Verbindung nach Sperren der IP trennen" sollte aktiv sein.

Version 19.5.1

- Die Leistungsmerkmale für LetsEncrypt[596] wurden aktualisiert und nutzen jetzt ACME v2. Diese Aktualisierung wurde notwendig, da LetsEncrypt die Unterstützung für ACME v1 einstellt. Für die Nutzung von LetsEncrypt sind ab jetzt PowerShell 5.1 und das .Net Framework 4.7.2 erforderlich.

Version 19.5.0

- Einige Einstellungen (etwa die Lizenzschlüssel) wurden von `\MDaemon\App\MDaemon.ini` nach `\MDaemon\LocalData\LocalData.ini` verschoben. Falls Sie eine frühere Programmversion wieder herstellen müssen, ergibt sich aus dieser Änderung das Problem, dass die Installationsroutinen älterer Programmversionen die Einstellungen nicht an den neuen Speicherorten finden können. Sie fordern daher zur Eingabe eines Lizenzschlüssels auf. Sie können dies vermeiden, indem Sie die Einstellungen zuvor in die Datei `MDaemon.ini` zurück kopieren, oder indem Sie eine Sicherheitskopie der Datei `MDaemon.ini` wieder herstellen.

Version 19.0.0

- Die Webschnittstelle für die MDaemon-Remoteverwaltung (MDRA) wurde erweitert und ermöglicht jetzt den Zugriff auf Leistungsmerkmale, die bislang nur über eine Konfigurationsverbindung mithilfe der Benutzerschnittstelle von MDaemon selbst verwaltet werden konnten. Es stehen jetzt auch einige Optionen zur Verfügung, die nur über die Remoteverwaltung erreichbar sind. Aus diesem Grund wurde auch die Arbeitsweise der Verknüpfung "MDaemon starten" im Startmenü geändert. Bei Neuinstallationen ruft diese Verknüpfung jetzt per Voreinstellung die MDaemon-Remoteverwaltung in einem Browserfenster auf. Eine Konfigurationsverbindung wird nicht mehr gestartet. Sie können dieses Verhalten ändern, indem Sie in der Datei `\MDaemon\App\MDaemon.ini` im Abschnitt `[MDLaunch]` die Einträge `OpenConfigSession=Yes/No` und `OpenRemoteAdmin=Yes/No` bearbeiten. Falls der automatisch erzeugte URL für die Remoteverwaltung nicht funktioniert, oder falls die Remoteverwaltung unter einem anderen Web-Server ausgeführt wird, können Sie den URL der Remoteverwaltung im Konfigurationsdialog Einstellungen » Web- & IM-Dienste » Remote-Verwaltung » Web-Server[352] bearbeiten. Falls ein funktionierender URL nicht festgestellt werden kann, wird beim Anklicken der

Verknüpfung statt der Remoteverwaltung eine Konfigurationsverbindung gestartet. Im Startmenü für MDaemon stehen jetzt außerdem die Verknüpfungen *MDaemon-Konfigurationsverbindung aufrufen* und *MDaemon-Remoteverwaltung aufrufen* zur Verfügung.

- SyncML wurde abgeschafft und aus MDaemon entfernt.
- MDaemon führte bisher die Berechnung für Speicherplatz nicht immer in allen betroffenen Leistungsmerkmalen konsistent durch. So wurde 1 kByte in manchen Bereichen als 1.000, in anderen als 1.024 Byte berechnet. Diese Berechnungsmethoden sind vereinheitlicht worden; sie legen jetzt stets 1.024 Byte zugrunde. Aufgrund dieser Änderung können sich die Speicherplatz-Kontingente der Benutzerkonten gegenüber den bisherigen Programmversionen geringfügig geändert haben. Bitte prüfen Sie die Kontingent-Einstellung, und nehmen Sie nötigenfalls entsprechende Anpassungen vor.
- Die Option "Benachrichtigungen über AntiVirus-Aktualisierungen nur im Fehlerfall senden" 667 ist jetzt per Voreinstellung aktiv. Nach der Aktualisierung auf MDaemon 19 wird die Option beim ersten Start von MDaemon aktiviert.

Siehe auch:

Einführung 12
Neuigkeiten MDaemon 23.0 15
Die Haupt-Benutzeroberfläche von MDaemon 74

1.5 So erhalten Sie Hilfe

Angebote für Support und technische Unterstützung

Der technische Support ist ein wesentlicher Bestandteil der Leistungen von MDaemon Technologies für unsere Kunden. Wir wollen, dass Sie auch lange nach dem Erwerb der Lizenz und der Installation unsere Produkte diese noch in vollem Leistungsumfang nutzen können, und wir arbeiten dafür, dass etwaige Probleme zu Ihrer Zufriedenheit gelöst werden. Die neuesten Informationen für unsere Kunden, Angebote für technischen Support, Ressourcen, mit denen Sie sich selbst helfen können, Produktinformationen und vieles mehr erhalten Sie auf der Support-Website von MDaemon Technologies unter www.mdaemon.com/support/.

MDaemon im Betatest

MDaemon Technologies unterhält aktive Teams für den Betatest der Produkte. Falls Sie Informationen über die Teilnahme am Beta-Team für MDaemon erhalten wollen, senden Sie bitte eine entsprechende Nachricht an MDaemonBeta@mdaemon.com.

Das Beta-Team steht Interessenten offen, die Software von MDaemon Technologies bereits vor der allgemeinen Verfügbarkeit erhalten und sich an der Erprobung beteiligen wollen. Es stellt keine Alternative zum technischen Support dar. Technischer Support für MDaemon wird nur im Rahmen der Angebote geleistet, die unter www.mdaemon.com/support/ dargestellt sind.

So erreichen Sie uns

Geschäftszeiten
Mo-Fr 08.30 - 17.30 US Central Standard Time
An Wochenenden und Feiertagen geschlossen.
Kundendienst und Vertrieb
Gebührenfrei in den USA: +1 866 601-ALTN (2586)
International: +1 817 601-3222
sales@helpdesk.mdaemon.com

Technischer Support
www.mdaemon.com/support/

Training
training@mdaemon.com

Business Development/Vertriebspartnerschaften
alliance@mdaemon.com

Medien/Analysten
press@mdaemon.com

Anfragen für Channel- und Reseller-Vertrieb
Sie erhalten nähere Informationen auf unserer Seite für Channel-Partner.

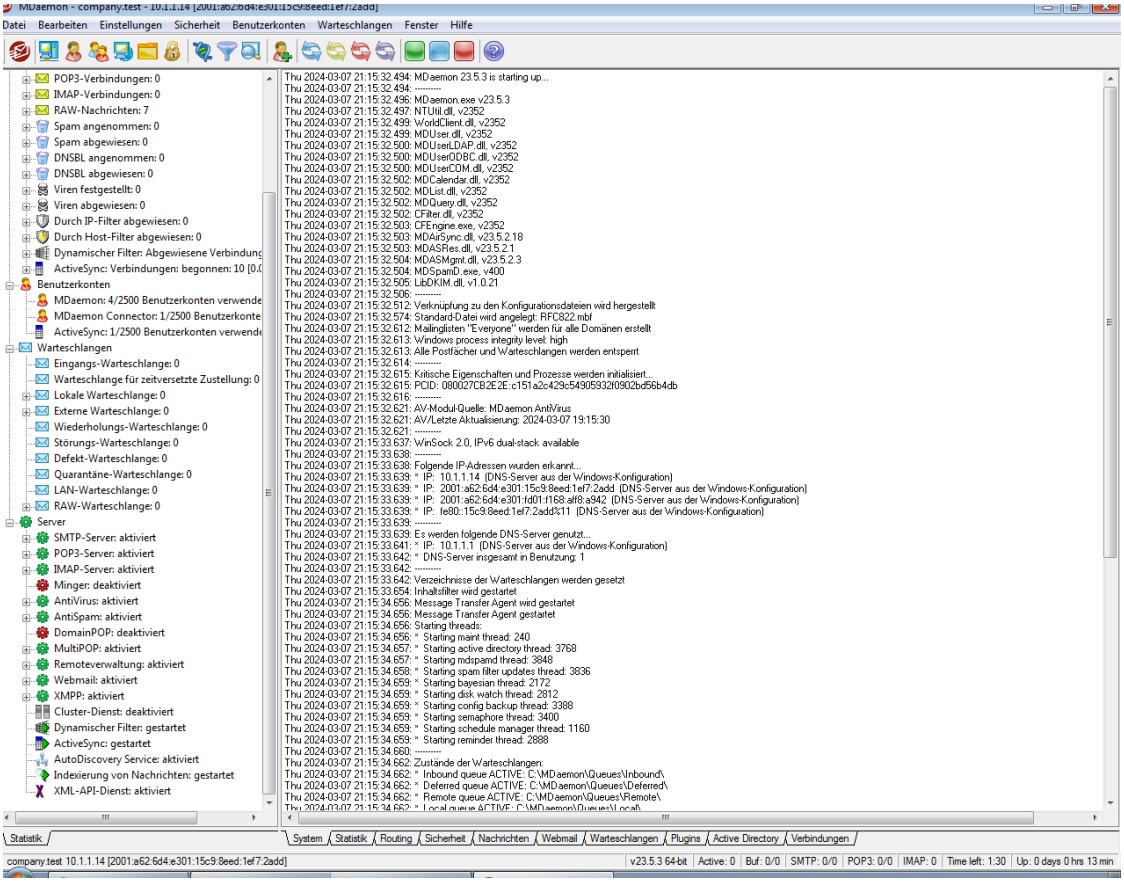
Sitz der Gesellschaft

MDaemon Technologies
4550 State Highway 360, Suite 100
Grapevine, Texas 76051
USA
Gebührenfrei in den USA: +1 866 601-ALTN (2586)
International: +1 817 601-3222
Fax: +1 817 601-3223

Marken

Kapitel II

2 Die Haupt-Benutzeroberfläche von MDaemon



Die Haupt-Benutzeroberfläche von MDaemon (englisch kurz "GUI" für "Graphical User Interface", d.h. grafische Benutzeroberfläche) stellt wichtige Informationen zu Ressourcen, Statistik, den aktiven Verbindungen und den Nachrichten in den Warteschlangen dar. Sie enthält auch Menüpunkte, mit denen die einzelnen Serverdienste von MDaemon leicht aktiviert und deaktiviert werden können. Die in Registerkarten unterteilte Anzeige der Benutzeroberfläche gibt Auskunft über den Leistungszustand der Servers sowie der ankommenden und abgehenden Verbindungen.

Statistik

Der Abschnitt *Statistik* enthält Statistikdaten über die Anzahl der Nachrichten, die MDaemon versendet und empfangen hat, über die Anzahl der POP- und IMAP-Verbindungen, der Spam-Nachrichten, die angenommen und abgewiesen wurden, der festgestellten Viren und andere Informationen. Alle hier aufgeführten Daten werden jeweils seit dem letzten Programmstart von MDaemon gezählt. Im Kontextmenü, das durch Rechtsklick aufgerufen werden kann, steht ein Befehl zur Verfügung, um die Zähler zurückzusetzen.

Der Befehl zum Zurücksetzen der Zähler im Kontextmenü setzt alle Zähler zurück, nicht etwa nur den Zähler, von dem aus das Kontextmenü durch Rechtsklick aufgerufen wurde. Im Konfigurationsdialog Einstellungen »

> Voreinstellungen » Benutzeroberfläche steht die Option "*Nachrichtenzähler oberster Ebene nach Neustart nicht zurücksetzen*" zur Verfügung. Sie bewirkt, dass die Zählerstände nach einem Neustart nicht zurückgesetzt sondern fortgeschrieben werden. Ist diese Option nicht aktiv, werden die Zähler bei jedem Neustart des Servers zurückgesetzt.

Der Abschnitt *Benutzerkonten* enthält Einträge für MDaemon, den MDaemon Connector und ActiveSync. Jeder Eintrag zeigt die Anzahl der Benutzerkonten, die bereits in Gebrauch sind, und die Anzahl der Benutzerkonten, die noch zur Verfügung stehen. Diese letzte Zahl hängt von dem Umfang Ihrer Lizenz für die jeweiligen Produkte ab.

Der Abschnitt *Warteschlangen* enthält pro Warteschlange einen Eintrag und zeigt die Anzahl der Nachrichten in den einzelnen Warteschlangen. Jeder Warteschlange ist ein Kontextmenü zugeordnet, das über einen Rechtsklick auf den Eintrag der Warteschlange erreicht werden kann. Je nach Art der Warteschlange kann es folgende Menüpunkte enthalten:

Warteschlange anzeigen — Diese Option schaltet das Hauptfenster auf die Registerkarte Warteschlangen um und zeigt die ausgewählte Warteschlange an. Es erscheint eine Liste aller Nachrichten in der Warteschlange, und jeder Nachricht ist ein Kontextmenü mit zahlreichen Menüpunkten zugeordnet. Sie sind den Optionen aus dem Warteschlangen- und Statistik-Manager nachgebildet, und zu ihnen gehören Kopieren, Verschieben, Bearbeiten und so weiter.

Warteschlangen- und Statistik-Manager — Hierdurch wird der Warteschlangen- und Statistik-Manager aufgerufen; die ausgewählte Warteschlange wird in den Manager geladen und angezeigt.

Jetzt verarbeiten — Diese Option leitet alle Nachrichten aus der Warteschlange in den normalen Verarbeitungsdurchlauf für Nachrichten. Falls Nachrichten in den Störungs- oder Defekt-Warteschlangen verarbeitet werden sollen, ist zu beachten, dass möglicherweise dieselben Fehler, wegen derer die Nachrichten in diesen Warteschlangen abgelegt wurden, erneut auftreten. Die Nachrichten werden, falls dieser Fall eintritt, wiederum in der Störungs- oder Defekt-Warteschlange abgelegt werden.

Warteschlange anhalten/wieder starten — Diese Option unterbricht vorübergehend die Verarbeitung der ausgewählten Warteschlange. Ist die Warteschlange bereits angehalten, wird ihre Verarbeitung durch erneute Auswahl der Option wieder aufgenommen.

Freigeben — Diese Option gibt die Nachrichten aus der Störungs-Warteschlange zur Zustellung frei. MDaemon versucht, die Nachrichten ohne Rücksicht auf etwa auftretende Fehler zuzustellen. Die Nachrichten werden auch dann nicht mehr in die Störungs-Warteschlange verschoben, wenn dieselben Fehler, aufgrund derer sie zuvor in die Störungs-Warteschlange verschoben worden waren, erneut auftreten.

Erneut in die Warteschlange — Dieser Menüpunkt steht nur für die Störungs-Warteschlange zur Verfügung, und er bewirkt dasselbe wie der Menüpunkt *Jetzt verarbeiten* weiter oben.

Warteschlange aktivieren/deaktivieren — Diese Option aktiviert und deaktiviert die Störungs-Warteschlange. So lange diese Warteschlange

deaktiviert ist, werden Nachrichten ohne Rücksicht auf die bei der Verarbeitung aufgetretenen Fehler nicht in die Störungs-Warteschlange verschoben.

Der Abschnitt *Server* enthält für jeden Server-Dienst von MDaemon einen Eintrag, der seinen Zustand als "aktiv" oder "nicht aktiv" anzeigt. Unter dem Eintrag jedes Dienstes ist - soweit zutreffend - ein Eintrag für jede Domäne aufgeführt, und es erscheinen der Port (die Anschlussnummer) und die IP-Adresse, die der Dienst oder die Domäne belegen. Das Kontextmenü erlaubt es, die Server-Dienste ein- und auszuschalten. Ist ein Server nicht aktiv, so wird sein Symbol rot dargestellt.

Überwachung und Protokollierung von Ereignissen

In der rechten Fensterhälfte der Benutzeroberfläche erscheinen standardmäßig mehrere Registerkarten. Sie zeigen den Zustand der verschiedenen Serverdienste und sonstigen Ressourcen an und werden daher sehr oft aktualisiert, um den aktuellen Betriebszustand wiederzugeben. Alle aktiven Verbindungen sowie alle sonstige Aktivität des Servers werden in den entsprechenden Registerkarten aufgezeichnet, sobald sie abgeschlossen sind. Die Informationen aus diesen Registerkarten werden in der Protokolldatei im Verzeichnis Logs gespeichert, falls das Systemprotokoll für die Speicherung der entsprechenden Ereignisse konfiguriert ist.

Der Hauptbereich der GUI von MDaemon enthält die folgenden Registerkarten:

System — Beim Programmstart zeigt die Registerkarte System ein Protokoll des Initialisierungsvorgangs an, das auf mögliche Probleme mit der Konfiguration oder dem Zustand von MDaemon aufmerksam macht. Auch Ereignisse wie das Ein- und Ausschalten von Serverdiensten werden hier vermerkt.

Statistik — Auf dieser Registerkarte werden Statistikdaten zu den einzelnen Zählerständen auf der Registerkarte Statistik im Fensterbereich für Statistiken angezeigt. Schriftart und –größe für diese Ansicht können durch Bearbeiten der folgenden Einträge in der Datei `MDaemon.ini` angepasst werden:

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

Jede Nacht um Mitternacht erhalten der Postmaster und alle übrigen E-Mail-Adressen, die im Abschnitt Empfänger[667] im Konfigurationsdialog für den Inhaltsfilter erfasst sind, eine Ausfertigung dieses Berichts per E-Mail. Der Bericht entspricht dem Bericht, den MDaemon bei Empfang des Befehls "Status" erstellt; dieser Befehl ist im Kapitel über die Steuerung allgemeiner E-Mail-Dienste[890] genauer beschrieben. Soll dieser Bericht nicht automatisch versandt werden, so wird dies durch Abschalten der Option "*Statistik-Bericht um Mitternacht an den Postmaster senden*" im Abschnitt Verschiedenes[504] im Konfigurationsdialog Voreinstellungen erreicht.

Routing — Zeigt die Routinginformationen für jede Nachricht an, die durch MDaemon ausgewertet wird (Von, An, Nachrichten-ID, u.s.w.).

Sicherheit — Ein Klick auf diese Registerkarte blendet mehrere andere Registerkarten mit Informationen zu den Sicherheitsfunktionen auf der darüber liegenden Zeile ein.

Inhaltsfilter — Auf dieser Registerkarte werden die Aktionen des Inhaltsfilters[649] von MDaemon angezeigt. Stimmt eine Nachricht mit einer

Regel des Inhaltsfilters überein, so werden die dafür maßgeblichen Informationen über diese Nachricht und die Aktion, die der Inhaltsfilter ausgelöst hat, hier angezeigt.

AntiVirus — Auf dieser Registerkarte werden alle AntiVirus 648-Vorgänge angezeigt. Nach der Prüfung einer Nachricht auf Viren werden die maßgeblichen Informationen über die Nachricht und etwa ausgelöste Aktionen hier aufgeführt.

AntiSpam — Hier werden die Aktionen des Spam-Filters 678 und Informationen über die Abwehrmaßnahmen gegen Spam angezeigt.

MDSpamD — Hier wird die Aktivität des Spam-Daemons von MDaemon 689 angezeigt.

SPF — Hier werden die Aktivitäten des Sender-Policy-Frameworks 527 angezeigt.

DKIM — Hier werden die Aktivitäten der Funktionen DomainKeys Identified Mail 529 angezeigt.

DMARC — Hier werden die Aktivitäten der Funktion DMARC 538 angezeigt.

VBR — Hier werden die Aktivitäten der VBR-Zertifizierung von Nachrichten 554 angezeigt.

MDPGP — Hier werden die Aktivitäten von MDPGP 631 angezeigt.

Filter — Diese Registerkarte zeigt die Aktivität von Teergrube 604 und Dynamischem Filter 567 an.

Fehlgeschlagene Echtheitsbestätigungen — Auf dieser Registerkarte und in der zugehörigen Protokolldatei sind detaillierte Einträge für alle Anmeldeversuche in SMTP-, IMAP- und POP-Verbindungen sichtbar, bei denen die Echtheitsbestätigung fehlschlägt. Es werden jeweils folgende Informationen vermerkt: das verwendete Protokoll, die Verbindungs-ID (sie ist zur Suche in anderen Protokollen hilfreich), die IP-Adresse der Gegenstelle, der unveränderte Anmeldename, den die Gegenstelle übermittelt hat (dies kann auch ein Alias sein) und das Benutzerkonto, das zu dem Anmeldenamen gehört (falls dem Anmeldenamen kein Benutzerkonto zugeordnet werden kann, erscheint hier "keines"). Sie können aus dieser Übersicht durch Rechtsklick auf einen Eintrag ein Kontextmenü aufrufen, über das Sie die IP-Adresse der Gegenstelle, die die fehlgeschlagene Echtheitsbestätigung versucht hat, unmittelbar in die Sperrlisten eintragen können.

MTA-STS — Hier werden die Aktivitäten zu dem SMTP-Verfahren MTA Strict Transport Security (MTA-STS) angezeigt.

Nachrichten — Ein Klick auf diese Registerkarte blendet mehrere andere Registerkarten mit Informationen zur Zustellung von Nachrichten auf der darüber liegenden Zeile ein.

SMTP (eing.) — Alle ankommenden SMTP-Verbindungen werden hier angezeigt.

SMTP (abg.) — Alle abgehenden SMTP-Verbindungen werden hier angezeigt.

IMAP — Verbindungen mit dem IMAP-Protokoll werden auf dieser Registerkarte vermerkt.

POP3 — Das Abrufen von Post durch die Benutzer über das POP3-Protokoll wird hier vermerkt.

MultiPOP — Diese Registerkarte gibt Auskunft über die MultiPOP-Verbindungen.

DomainPOP — Diese Registerkarte zeigt die DomainPOP-Vorgänge an.

LDAP — Diese Registerkarte zeigt die Aktivität das LDAP-Servers LDaemon.

Minger — Diese Registerkarte zeigt die Aktivität des Minger 855-Servers.

RAW — Hier wird die Aktivität für RAW- und Systemnachrichten angezeigt.

MDaemon Connector — Hier wird die Aktivität des MDaemon Connectors angezeigt.

Webmail

Webmail — Auf dieser Registerkarte werden die Verbindungen von Webmail angezeigt.

ActiveSync — Auf dieser Registerkarte wird die Aktivität von ActiveSync angezeigt.

Warteschlangen — Diese Registerkarte eröffnet den Zugriff auf eine Reihe weiterer Registerkarten. Jede dieser Registerkarten gehört zu einer Warteschlange, wie etwa lokal, extern, Störung, Quarantäne, Bayes/Spam usw.

Plugins — Hier wird die Aktivität der installierten Plugins für MDaemon angezeigt.

Active Directory — Hier wird alle Aktivität in Bezug auf das Active Directory angezeigt.

Verbindungen — Nach Anklicken dieser Registerkarte erscheinen mehrere weitere Registerkarten auf der darüber liegenden Zeile. Sie enthalten Einträge mit weiteren Informationen für jede aktive Verbindung mit MDaemon - unabhängig davon, ob es sich dabei um eingehende oder abgehende SMTP-, POP-, IMAP-, Webmail- oder ActiveSync-Verbindungen handelt. Durch Doppelklick auf eine aktive Verbindung kann ein Verbindungsfenster 91 aufgerufen werden; in ihm erscheint ein Mitschnitt der SMTP-Verbindung, der laufend aktualisiert wird.

Die Informationen, die auf diesen Registerkarten angezeigt werden, wirken sich nicht auf die Datenmenge aus, die tatsächlich in den Protokolldateien gespeichert wird. MDaemon ist, was Menge und Art der in den Protokolldateien zu speichernden Informationen angeht, sehr flexibel. Im Kapitel über das Systemprotokoll 167 sind zu diesen Optionen ausführliche Informationen verfügbar.

Das Kontextmenü für die Ereignisanzeigen

Ein Rechtsklick in einen Teil des Fensters, in dem die Protokolle und Ereignisanzeigen dargestellt werden, öffnet ein Kontextmenü. Dieses Menü enthält verschiedene Befehle, mit denen die Inhalte der jeweils aktiven Registerkarte ausgewählt, kopiert, gelöscht und gespeichert werden können. Der Menüpunkt *Drucken/Kopieren* öffnet Notepad und überträgt den gerade markierten Text in das Editor-Fenster. Von dort aus kann der Text dann gedruckt oder in eine Datei gespeichert werden. Der Menüpunkt *Löschen* löscht den markierten Text. Der Menüpunkt *Suchen* öffnet ein neues Fenster, in dem die Protokolle nach Wörtern und Texten durchsucht werden können. MDaemon durchsucht dabei alle Protokolldateien und fasst alle Verbindungsmitschnitte, die den gesuchten Text enthalten, in einer Datei zusammen. Diese Datei wird im Editor geöffnet. Ein Anwendungsbeispiel aus der

Praxis ist die Suche nach einer bestimmten Nachrichten-ID, deren Ergebnis eine Zusammenfassung aller Verbindungsmitschnitte für diese Nachrichten-ID ist. Einige Registerkarten enthalten auch Optionen, mit deren Hilfe Nachrichten an MDaemon.com gemeldet werden können. Diese Optionen sind für Fälle gedacht, in denen Nachrichten irrtümlich als Spam oder als vireninfiziert erkannt wurden, oder in denen Spam-Nachrichten und Viren irrtümlich nicht erkannt wurden (sog. falsche Positive und falsche Negative). Nachrichten, die mithilfe dieser Optionen gemeldet werden, werden analysiert und an Drittanbieter weitergeleitet, damit Korrekturmaßnahmen ergriffen werden können.

Die Darstellung der Protokolle und Ereignisanzeigen beschränkt sich nicht auf die vorgegebene Fensteraufteilung, wie sie oben beschrieben. Sie können durch Auswahl des Menüpunktes Fenster » Ansichten umschalten in der Menüleiste ein anderes Erscheinungsbild einstellen.

Das Verbundprotokoll

Im Menü Fenster befindet sich der Eintrag Verbundprotokoll betrachten. Die Auswahl dieses Menüpunktes blendet in die Benutzeroberfläche einen Abschnitt ein, in dem sich die Informationen aus einem oder mehreren Registerkarten des Hauptfensters gemeinsam anzeigen lassen. Die Menüpunkte im Abschnitt Verbundprotokoll 169 des Konfigurationsdialogs Protokollierung legen fest, welche Informationen in dem Fenster zusammengefasst werden sollen.

Windows-Leistungszähler (Windows Performance Counter)

MDaemon unterstützt die Windows-Leistungszähler ("Windows Performance Counter"), die es Softwarelösungen zur Überwachung und zum Monitoring gestatten, den Status von MDaemon in Echtzeit zu überwachen. Es stehen Zähler für die Anzahl der aktiven Verbindungen für die einzelnen Protokolle, die Zahl der Nachrichten in den Warteschlangen, die Zustände aktiv und inaktiv für die einzelnen Dienste, die Laufzeit von MDaemon und die Statistiken über Verbindungen und Nachrichten zur Verfügung.

Um die Performance Counter zu nutzen, starten Sie den Systemmonitor über Systemsteuerung | Verwaltungs-Tools | Systemmonitor, oder führen Sie den Befehl "perfmon" aus. Bei den Performance Countern handelt es sich um 32-Bit-Leistungszähler. Auf 64-Bit-Systemen müssen Sie daher "mmc /32 perfmon.msc" ausführen. Klicken Sie auf Counter hinzufügen, wählen Sie das Performance-Objekt MDaemon aus, wählen Sie die gewünschten Counter aus, und klicken Sie auf Hinzufügen. Um die Performance Counter einer MDaemon-Installation zu überwachen, die auf einem anderen System ausgeführt wird, muss der Dienst "Remoteregistrierung" aktiv und in der Lage sein, durch etwaige Firewalls zu kommunizieren.

Siehe auch:

Das Verbindungsfenster 91
Das Symbol im Systray 88
Das Kontextmenü 89
Das Verbundprotokoll 169

2. .1 AutoDiscovery-Dienst

MDaemon unterstützt den Dienst AutoDiscovery. Mithilfe dieses Dienstes können die Benutzer ihre E-Mail-Clients für die Nutzung ihrer Benutzerkonten einrichten, und sie müssen dafür nur ihre E-Mail-Adresse und ihr Kennwort angeben. Sie müssen die weiteren Einzelheiten der Konfiguration - insbesondere Servernamen und Ports der Mailserver - nicht kennen. Die meisten Clients unterstützen diesen Dienst, bei einigen Clients kann die Unterstützung aber eingeschränkt sein. Der Dienst AutoDiscovery ist per Voreinstellung aktiv. Sie können ihn über die Haupt-Benutzeroberfläche von MDaemon manuell aktivieren und deaktivieren. Führen Sie hierzu Abschnitt **Server** des Bereichs Statistik einen Rechtsklick auf dem Eintrag **Auto-Discovery-Dienst** einen Rechtsklick aus, und klicken Sie in dem sich öffnenden Kontextmenü auf **Auto-Discovery-Dienst aktivieren/deaktivieren.**

Clients, die den Dienst AutoDiscovery vollständig unterstützen, führen für den Domänennamen aus der E-Mail-Adresse des Benutzers zunächst eine DNS-Abfrage nach einem Eintrag des Typs SRV ("Diensteintrag") für den Diensttyp ("Service Type") _autodiscover._tcp aus. Sie stellen dann eine Verbindung mit dem Server her, dessen Hostnamen sie auf die Abfrage erhalten haben, und beziehen von diesem weitere Informationen. Um AutoDiscovery zu unterstützen, müssen Sie daher im DNS Einträge des Typs SRV für AutoDiscovery selbst und für die Dienste erstellen, die unterstützt werden. Die Implementation von AutoDiscover, die MDaemon enthält, unterstützt die folgenden Dienste: ActiveSync 416 (AirSync), IMAP, POP, SMTP, DAV und XMPP.

```
_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.
```

Beachte: Einige Clients fragen immer zuerst den Eintrag `autodiscover.{Domäne}.{TLD}` ab. Es kann in diesen Fällen hilfreich sein, den SRV-Eintrag für AutoDiscovery auf einen Server mit dem Hostnamen `autodiscover.{Domäne}.{TLD}` verweisen zu lassen. Im nachfolgend dargestellten Beispiel lautet der Hostname des AutoDiscovery-Servers jedoch `adsc.example.com`.

Ein Beispiel hierzu:

Domänenname: example.com

Der Administrator sollte einen SRV-Eintrag _tcp für den Service Type _autodiscover erstellen.

```
_autodiscover._tcp SRV 0 0 443 adsc.example.com.
```

Der Eintrag verweist in diesem Fall auf `adsc.example.com`. Der A-Eintrag dieses Hostnamens verweist auf `192.168.0.101`.

Der Client stellt dann eine Verbindung mit diesem Server her und fragt nach verbindungsspezifischen Konfigurationsdaten für mehrere Protokolle: ActiveSync, IMAP, XMPP, SMTP, DAV usw.

Der AutoDiscovery-Server sucht dann nach Konfigurationsdaten für die angeforderten Protokolle und übermittelt für jedes Protokoll den zutreffenden

Hostnamen. Ein Beispiel hierzu: Für ActiveSync übermittelt der Server den Hostnamen, der im _tcp-Serviceeintrag _airsync definiert ist. Im Beispiel oben ist das eas.{Domäne}.{TLD}.

Falls Microsoft Outlook die AutoDiscovery durchführt, übermittelt der AutoDiscovery-Server die Hostnamen für die IMAP- und SMTP-Server. Diese sind in den _tcp-Serviceeinträgen _imap und _msa definiert. Im Beispiel oben werden daher die Hostnamen imap4.example.com und msa.example.com übermittelt.

Es folgt ein Beispiel dafür, wie die AutoDiscovery-Dienste richtig eingerichtet werden. Das Beispiel geht davon aus, dass Sie für jedes Protokoll einen eigenen Hostnamen nutzen wollen. Es lässt sich leicht an Fälle anpassen, in denen ein gemeinsamer Hostname verwendet werden soll, wie etwa mail.example.com.

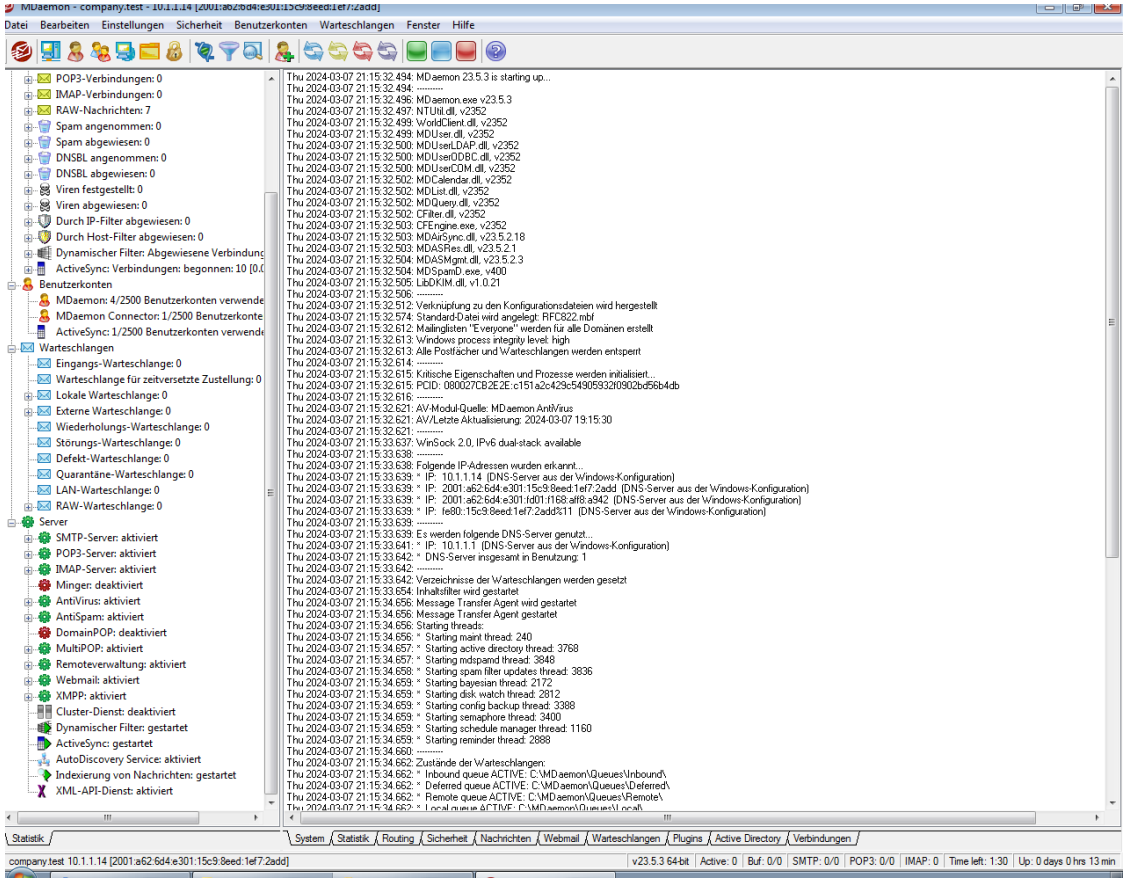
```
;
;  Datenbankdatei example.com.dns für die Zone example.com.
;

@ IN  SOA dns.meindnsprovider.org. hostmaster.meindnsprovider.org. (
        4            ; Seriennummer
        900          ; Aktualisierungsintervall
        600          ; Intervall für Wiederholungen
        86400        ; Gültigkeitsdauer
        3600       ) ; Standard-Gültigkeit für Einträge (TTL)

;
;  Nameserver-Einträge für die Zone
;

@       NS dns.meindnsprovider.org

;
;  Einträge für die Zone
;

@             A 192.168.0.100
adsc                A 192.168.0.101
www                 A 192.168.0.102
imap4               A 192.168.0.103
pop3                A 192.168.0.104
msa                 A 192.168.0.105
eas                 A 192.168.0.106
api                 A 192.168.0.107
autodiscover        A 192.168.0.108
dav                 A 192.168.0.109
chat                A 192.168.0.110
inbound       A 192.168.0.111

              MX 10 inbound.example.com.
;
;  Serviceeinträge
;

_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.
```

Siehe auch:

Allgemeine Informationen über AutoDiscover finden Sie in dem Microsoft-Dokument Autodiscover für Exchange.

2.2 Überwachung und Protokollierung von Ereignissen



Die Haupt-Benutzeroberfläche von MDaemon (englisch kurz "GUI" für "Graphical User Interface", d.h. grafische Benutzeroberfläche) stellt wichtige Informationen zu Ressourcen, Statistik, den aktiven Verbindungen und den Nachrichten in den Warteschlangen dar. Sie enthält auch Menüpunkte, mit denen die einzelnen Serverdienste von MDaemon leicht aktiviert und deaktiviert werden können. Die in Registerkarten unterteilte Anzeige der Benutzeroberfläche gibt Auskunft über den Leistungszustand der Servers sowie der ankommenden und abgehenden Verbindungen.

Statistik

Der Abschnitt *Statistik* enthält Statistikdaten über die Anzahl der Nachrichten, die MDaemon versendet und empfangen hat, über die Anzahl der POP- und IMAP-Verbindungen, der Spam-Nachrichten, die angenommen und abgewiesen wurden, der festgestellten Viren und andere Informationen. Alle hier aufgeführten Daten werden

jeweils seit dem letzten Programmstart von MDaemon gezählt. Im Kontextmenü, das durch Rechtsklick aufgerufen werden kann, steht ein Befehl zur Verfügung, um die Zähler zurückzusetzen.

Der Befehl zum Zurücksetzen der Zähler im Kontextmenü setzt alle Zähler zurück, nicht etwa nur den Zähler, von dem aus das Kontextmenü durch Rechtsklick aufgerufen wurde. Im Konfigurationsdialog Einstellungen » Voreinstellungen » Benutzeroberfläche steht die Option "*Nachrichtenzähler oberster Ebene nach Neustart nicht zurücksetzen*" zur Verfügung. Sie bewirkt, dass die Zählerstände nach einem Neustart nicht zurückgesetzt sondern fortgeschrieben werden. Ist diese Option nicht aktiv, werden die Zähler bei jedem Neustart des Servers zurückgesetzt.

Der Abschnitt *Benutzerkonten* enthält Einträge für MDaemon, den MDaemon Connector und ActiveSync. Jeder Eintrag zeigt die Anzahl der Benutzerkonten, die bereits in Gebrauch sind, und die Anzahl der Benutzerkonten, die noch zur Verfügung stehen. Diese letzte Zahl hängt von dem Umfang Ihrer Lizenz für die jeweiligen Produkte ab.

Der Abschnitt *Warteschlangen* enthält pro Warteschlange einen Eintrag und zeigt die Anzahl der Nachrichten in den einzelnen Warteschlangen. Jeder Warteschlange ist ein Kontextmenü zugeordnet, das über einen Rechtsklick auf den Eintrag der Warteschlange erreicht werden kann. Je nach Art der Warteschlange kann es folgende Menüpunkte enthalten:

Warteschlange anzeigen — Diese Option schaltet das Hauptfenster auf die Registerkarte Warteschlangen um und zeigt die ausgewählte Warteschlange an. Es erscheint eine Liste aller Nachrichten in der Warteschlange, und jeder Nachricht ist ein Kontextmenü mit zahlreichen Menüpunkten zugeordnet. Sie sind den Optionen aus dem Warteschlangen- und Statistik-Manager nachgebildet, und zu ihnen gehören Kopieren, Verschieben, Bearbeiten und so weiter.

Warteschlangen- und Statistik-Manager — Hierdurch wird der Warteschlangen- und Statistik-Manager aufgerufen; die ausgewählte Warteschlange wird in den Manager geladen und angezeigt.

Jetzt verarbeiten — Diese Option leitet alle Nachrichten aus der Warteschlange in den normalen Verarbeitungsdurchlauf für Nachrichten. Falls Nachrichten in den Störungs- oder Defekt-Warteschlangen verarbeitet werden sollen, ist zu beachten, dass möglicherweise dieselben Fehler, wegen derer die Nachrichten in diesen Warteschlangen abgelegt wurden, erneut auftreten. Die Nachrichten werden, falls dieser Fall eintritt, wiederum in der Störungs- oder Defekt-Warteschlange abgelegt werden.

Warteschlange anhalten/wieder starten — Diese Option unterbricht vorübergehend die Verarbeitung der ausgewählten Warteschlange. Ist die Warteschlange bereits angehalten, wird ihre Verarbeitung durch erneute Auswahl der Option wieder aufgenommen.

Freigeben — Diese Option gibt die Nachrichten aus der Störungs-Warteschlange zur Zustellung frei. MDaemon versucht, die Nachrichten ohne Rücksicht auf etwa auftretende Fehler zuzustellen. Die Nachrichten werden auch dann nicht mehr in die Störungs-Warteschlange verschoben, wenn dieselben

Fehler, aufgrund derer sie zuvor in die Störungs-Warteschlange verschoben worden waren, erneut auftreten.

Erneut in die Warteschlange — Dieser Menüpunkt steht nur für die Störungs-Warteschlange zur Verfügung, und er bewirkt dasselbe wie der Menüpunkt *Jetzt verarbeiten* weiter oben.

Warteschlange aktivieren/deaktivieren — Diese Option aktiviert und deaktiviert die Störungs-Warteschlange. So lange diese Warteschlange deaktiviert ist, werden Nachrichten ohne Rücksicht auf die bei der Verarbeitung aufgetretenen Fehler nicht in die Störungs-Warteschlange verschoben.

Der Abschnitt *Server* enthält für jeden Server-Dienst von MDaemon einen Eintrag, der seinen Zustand als "aktiv" oder "nicht aktiv" anzeigt. Unter dem Eintrag jedes Dienstes ist - soweit zutreffend - ein Eintrag für jede Domäne aufgeführt, und es erscheinen der Port (die Anschlussnummer) und die IP-Adresse, die der Dienst oder die Domäne belegen. Das Kontextmenü erlaubt es, die Server-Dienste ein- und auszuschalten. Ist ein Server nicht aktiv, so wird sein Symbol rot dargestellt.

Überwachung und Protokollierung von Ereignissen

In der rechten Fensterhälfte der Benutzeroberfläche erscheinen standardmäßig mehrere Registerkarten. Sie zeigen den Zustand der verschiedenen Serverdienste und sonstigen Ressourcen an und werden daher sehr oft aktualisiert, um den aktuellen Betriebszustand wiederzugeben. Alle aktiven Verbindungen sowie alle sonstige Aktivität des Servers werden in den entsprechenden Registerkarten aufgezeichnet, sobald sie abgeschlossen sind. Die Informationen aus diesen Registerkarten werden in der Protokolldatei im Verzeichnis Logs gespeichert, falls das Systemprotokoll für die Speicherung der entsprechenden Ereignisse konfiguriert ist.

Der Hauptbereich der GUI von MDaemon enthält die folgenden Registerkarten:

System — Beim Programmstart zeigt die Registerkarte System ein Protokoll des Initialisierungsvorgangs an, das auf mögliche Probleme mit der Konfiguration oder dem Zustand von MDaemon aufmerksam macht. Auch Ereignisse wie das Ein- und Ausschalten von Serverdiensten werden hier vermerkt.

Statistik — Auf dieser Registerkarte werden Statistikdaten zu den einzelnen Zählerständen auf der Registerkarte Statistik im Fensterbereich für Statistiken angezeigt. Schriftart und –größe für diese Ansicht können durch Bearbeiten der folgenden Einträge in der Datei `MDaemon.ini` angepasst werden:

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

Jede Nacht um Mitternacht erhalten der Postmaster und alle übrigen E-Mail-Adressen, die im Abschnitt Empfänger 667 im Konfigurationsdialog für den Inhaltsfilter erfasst sind, eine Ausfertigung dieses Berichts per E-Mail. Der Bericht entspricht dem Bericht, den MDaemon bei Empfang des Befehls "Status" erstellt; dieser Befehl ist im Kapitel über die Steuerung allgemeiner E-Mail-Dienste 890 genauer beschrieben. Soll dieser Bericht nicht automatisch versandt werden, so wird dies durch Abschalten der Option "*Statistik-Bericht um Mitternacht an den Postmaster senden*" im Abschnitt Verschiedenes 504 im Konfigurationsdialog Voreinstellungen erreicht.

Routing — Zeigt die Routinginformationen für jede Nachricht an, die durch MDaemon ausgewertet wird (Von, An, Nachrichten-ID, u.s.w.).

Sicherheit — Ein Klick auf diese Registerkarte blendet mehrere andere Registerkarten mit Informationen zu den Sicherheitsfunktionen auf der darüber liegenden Zeile ein.

Inhaltsfilter — Auf dieser Registerkarte werden die Aktionen des Inhaltsfilters 649 von MDaemon angezeigt. Stimmt eine Nachricht mit einer Regel des Inhaltsfilters überein, so werden die dafür maßgeblichen Informationen über diese Nachricht und die Aktion, die der Inhaltsfilter ausgelöst hat, hier angezeigt.

AntiVirus — Auf dieser Registerkarte werden alle AntiVirus 648-Vorgänge angezeigt. Nach der Prüfung einer Nachricht auf Viren werden die maßgeblichen Informationen über die Nachricht und etwa ausgelöste Aktionen hier aufgeführt.

AntiSpam — Hier werden die Aktionen des Spam-Filters 678 und Informationen über die Abwehrmaßnahmen gegen Spam angezeigt.

MDSpamD — Hier wird die Aktivität des Spam-Daemons von MDaemon 689 angezeigt.

SPF — Hier werden die Aktivitäten des Sender-Policy-Frameworks 527 angezeigt.

DKIM — Hier werden die Aktivitäten der Funktionen DomainKeys Identified Mail 529 angezeigt.

DMARC — Hier werden die Aktivitäten der Funktion DMARC 538 angezeigt.

VBR — Hier werden die Aktivitäten der VBR-Zertifizierung von Nachrichten 554 angezeigt.

MDPGP — Hier werden die Aktivitäten von MDPGP 631 angezeigt.

Filter — Diese Registerkarte zeigt die Aktivität von Teergrube 604 und Dynamischem Filter 567 an.

Fehlgeschlagene Echtheitsbestätigungen — Auf dieser Registerkarte und in der zugehörigen Protokolldatei sind detaillierte Einträge für alle Anmeldeversuche in SMTP-, IMAP- und POP-Verbindungen sichtbar, bei denen die Echtheitsbestätigung fehlschlägt. Es werden jeweils folgende Informationen vermerkt: das verwendete Protokoll, die Verbindungs-ID (sie ist zur Suche in anderen Protokollen hilfreich), die IP-Adresse der Gegenstelle, der unveränderte Anmeldename, den die Gegenstelle übermittelt hat (dies kann auch ein Alias sein) und das Benutzerkonto, das zu dem Anmeldenamen gehört (falls dem Anmeldenamen kein Benutzerkonto zugeordnet werden kann, erscheint hier "keines"). Sie können aus dieser Übersicht durch Rechtsklick auf einen Eintrag ein Kontextmenü aufrufen, über das Sie die IP-Adresse der Gegenstelle, die die fehlgeschlagene Echtheitsbestätigung versucht hat, unmittelbar in die Sperrlisten eintragen können.

MTA-STS — Hier werden die Aktivitäten zu dem SMTP-Verfahren MTA Strict Transport Security (MTA-STS) angezeigt.

Nachrichten — Ein Klick auf diese Registerkarte blendet mehrere andere Registerkarten mit Informationen zur Zustellung von Nachrichten auf der darüber liegenden Zeile ein.

SMTP (eing.) — Alle ankommenden SMTP-Verbindungen werden hier angezeigt.

SMTP (abg.) — Alle abgehenden SMTP-Verbindungen werden hier angezeigt.

IMAP — Verbindungen mit dem IMAP-Protokoll werden auf dieser Registerkarte vermerkt.

POP3 — Das Abrufen von Post durch die Benutzer über das POP3-Protokoll wird hier vermerkt.

MultiPOP — Diese Registerkarte gibt Auskunft über die MultiPOP-Verbindungen.

DomainPOP — Diese Registerkarte zeigt die DomainPOP-Vorgänge an.

LDAP — Diese Registerkarte zeigt die Aktivität das LDAP-Servers LDaemon.

Minger — Diese Registerkarte zeigt die Aktivität des Minger 855-Servers.

RAW — Hier wird die Aktivität für RAW- und Systemnachrichten angezeigt.

MDaemon Connector — Hier wird die Aktivität des MDaemon Connectors angezeigt.

Webmail

Webmail — Auf dieser Registerkarte werden die Verbindungen von Webmail angezeigt.

ActiveSync — Auf dieser Registerkarte wird die Aktivität von ActiveSync angezeigt.

Warteschlangen — Diese Registerkarte eröffnet den Zugriff auf eine Reihe weiterer Registerkarten. Jede dieser Registerkarten gehört zu einer Warteschlange, wie etwa lokal, extern, Störung, Quarantäne, Bayes/Spam usw.

Plugins — Hier wird die Aktivität der installierten Plugins für MDaemon angezeigt.

Active Directory — Hier wird alle Aktivität in Bezug auf das Active Directory angezeigt.

Verbindungen — Nach Anklicken dieser Registerkarte erscheinen mehrere weitere Registerkarten auf der darüber liegenden Zeile. Sie enthalten Einträge mit weiteren Informationen für jede aktive Verbindung mit MDaemon - unabhängig davon, ob es sich dabei um eingehende oder abgehende SMTP-, POP-, IMAP-, Webmail- oder ActiveSync-Verbindungen handelt. Durch Doppelklick auf eine aktive Verbindung kann ein Verbindungsfenster 91 aufgerufen werden; in ihm erscheint ein Mitschnitt der SMTP-Verbindung, der laufend aktualisiert wird.

Die Informationen, die auf diesen Registerkarten angezeigt werden, wirken sich nicht auf die Datenmenge aus, die tatsächlich in den Protokolldateien gespeichert wird. MDaemon ist, was Menge und Art der in den Protokolldateien zu speichernden Informationen angeht, sehr flexibel. Im Kapitel über das Systemprotokoll 167 sind zu diesen Optionen ausführliche Informationen verfügbar.

Das Kontextmenü für die Ereignisanzeigen

Ein Rechtsklick in einen Teil des Fensters, in dem die Protokolle und Ereignisanzeigen dargestellt werden, öffnet ein Kontextmenü. Dieses Menü enthält verschiedene Befehle, mit denen die Inhalte der jeweils aktiven Registerkarte ausgewählt, kopiert, gelöscht und gespeichert werden können. Der Menüpunkt *Drucken/Kopieren* öffnet Notepad und überträgt den gerade markierten Text in das Editor-Fenster. Von dort aus kann der Text dann gedruckt oder in eine Datei gespeichert werden. Der Menüpunkt *Löschen* löscht den markierten Text. Der Menüpunkt *Suchen* öffnet ein neues Fenster, in dem die Protokolle nach Wörtern und Texten durchsucht werden können. MDaemon durchsucht dabei alle Protokolldateien und fasst alle Verbindungsmitschnitte, die den gesuchten Text enthalten, in einer Datei zusammen. Diese Datei wird im Editor geöffnet. Ein Anwendungsbeispiel aus der Praxis ist die Suche nach einer bestimmten Nachrichten-ID, deren Ergebnis eine Zusammenfassung aller Verbindungsmitschnitte für diese Nachrichten-ID ist. Einige Registerkarten enthalten auch Optionen, mit deren Hilfe Nachrichten an MDaemon.com gemeldet werden können. Diese Optionen sind für Fälle gedacht, in denen Nachrichten irrtümlich als Spam oder als vireninfiziert erkannt wurden, oder in denen Spam-Nachrichten und Viren irrtümlich nicht erkannt wurden (sog. falsche Positive und falsche Negative). Nachrichten, die mithilfe dieser Optionen gemeldet werden, werden analysiert und an Drittanbieter weitergeleitet, damit Korrekturmaßnahmen ergriffen werden können.

Die Darstellung der Protokolle und Ereignisanzeigen beschränkt sich nicht auf die vorgegebene Fensteraufteilung, wie sie oben beschrieben. Sie können durch Auswahl des Menüpunktes Fenster » Ansichten umschalten in der Menüleiste ein anderes Erscheinungsbild einstellen.

Das Verbundprotokoll

Im Menü Fenster befindet sich der Eintrag Verbundprotokoll betrachten. Die Auswahl dieses Menüpunktes blendet in die Benutzeroberfläche einen Abschnitt ein, in dem sich die Informationen aus einem oder mehreren Registerkarten des Hauptfensters gemeinsam anzeigen lassen. Die Menüpunkte im Abschnitt Verbundprotokoll 169 des Konfigurationsdialogs Protokollierung legen fest, welche Informationen in dem Fenster zusammengefasst werden sollen.

Windows-Leistungszähler (Windows Performance Counter)

MDaemon unterstützt die Windows-Leistungszähler ("Windows Performance Counter"), die es Softwarelösungen zur Überwachung und zum Monitoring gestatten, den Status von MDaemon in Echtzeit zu überwachen. Es stehen Zähler für die Anzahl der aktiven Verbindungen für die einzelnen Protokolle, die Zahl der Nachrichten in den Warteschlangen, die Zustände aktiv und inaktiv für die einzelnen Dienste, die Laufzeit von MDaemon und die Statistiken über Verbindungen und Nachrichten zur Verfügung.

Um die Performance Counter zu nutzen, starten Sie den Systemmonitor über Systemsteuerung | Verwaltungs-Tools | Systemmonitor, oder führen Sie den Befehl "perfmon" aus. Bei den Performance Countern handelt es sich um 32-Bit-Leistungszähler. Auf 64-Bit-Systemen müssen Sie daher "mmc /32 perfmon.msc" ausführen. Klicken Sie auf Counter hinzufügen, wählen Sie das Performance-Objekt MDaemon aus, wählen Sie die gewünschten Counter aus, und klicken Sie auf

Hinzufügen. Um die Performance Counter einer MDaemon-Installation zu überwachen, die auf einem anderen System ausgeführt wird, muss der Dienst "Remoteregistrierung" aktiv und in der Lage sein, durch etwaige Firewalls zu kommunizieren.

Siehe auch:

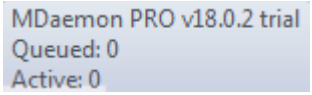
Das Verbindungsfenster 91
Das Symbol im Systray 88
Das Kontextmenü 89
Das Verbundprotokoll 169

2.4 Das Symbol im Systray

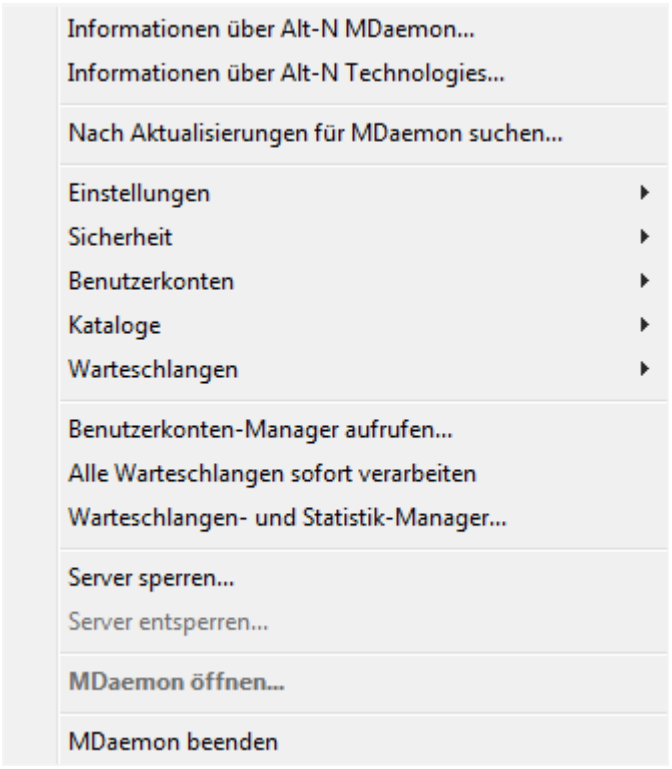
Solange MDaemon ausgeführt wird, bleibt sein Symbol im Systray sichtbar. Das Symbol zeigt jedoch nicht nur an, dass der Server gerade läuft; es ist vielmehr veränderlich und wird, abhängig vom Zustand des Servers, in verschiedenen Farben angezeigt. Die folgende Liste zeigt die möglichen Zustandsanzeigen:

	Alles in Ordnung. In den lokalen und externen Warteschlangen stehen keine Nachrichten.
	Alles in Ordnung. In den lokalen oder externen Warteschlangen stehen Nachrichten.
	Verfügbarer Speicherplatz unter dem Schwellwert (vgl. Einstellungen » Voreinstellungen » Speicherplatz 497).
	Netzwerk ausgefallen, Verbindungsaufbau über DFÜ-Netzwerk fehlgeschlagen oder Festplatte voll.
Symbol blinkt	Eine neuere Version von MDaemon ist verfügbar.

Sie erhalten weitere Informationen zum Zustand des Servers über den Tooltipp, den Sie über das Symbol angezeigt erhalten können. Lassen Sie den Mauszeiger über dem Symbol im Systray stehen, so erscheint der Tooltipp und gibt Auskunft über die Zahl der Nachrichten in den Warteschlangen ("Queued") und die Zahl der aktiven Verbindungen ("Active").



Das Kontextmenü



Ein Rechtsklick auf das Symbol für MDaemon im Systray öffnet das Kontextmenü. Durch dieses Menü erhalten Sie einen schnellen Zugriff auf nahezu alle Menüs und Funktionen von MDaemon, ohne die Haupt-Benutzerschnittstelle öffnen zu müssen.

Durch einen Klick auf "Informationen über MDaemon..." im obersten Abschnitt des Kontextmenüs erhalten Sie weitere Informationen über MDaemon und MDaemon Technologies.

Im folgenden Abschnitt können Sie durch einen Klick auf "Nach Aktualisierungen für MDaemon suchen..." prüfen, ob eine neuere Version von MDaemon zum Herunterladen bereit steht.

Im dritten Abschnitt erreichen Sie die folgenden Menüs von MDaemon: Einstellungen, Sicherheit, Benutzerkonten und Warteschlangen. Jedes dieser in Menübäume aufgeteilten Menüs ist mit dem gleichnamigen Menü in der Menüzeile der Haupt-Benutzeroberfläche identisch.

Der vierte Abschnitt enthält Menüpunkte, um den Benutzerkonten-Manager und den

Warteschlangen- und Statistik-Manager zu öffnen, und um alle Warteschlangen sofort zu verarbeiten.

Im folgenden Abschnitt finden sich Menüpunkte, um die Benutzeroberfläche zu sperren und zu entsperren (vgl. "Sperren und Entsperren der Benutzeroberfläche von MDaemon" weiter unten) sowie der Menüpunkt "MDaemon öffnen...", mit dessen Hilfe die Benutzeroberfläche von MDaemon geöffnet und angezeigt werden kann, falls MDaemon in den Systray ausgeblendet ist.

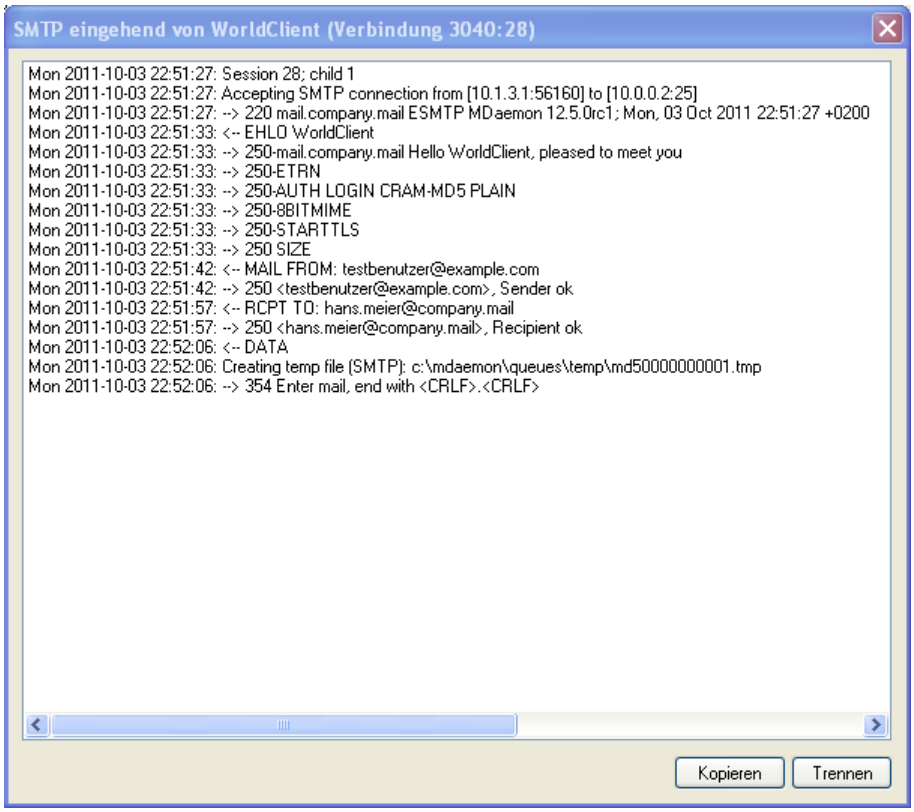
Der Menüpunkt "Konfigurationsverbindung beenden" beendet die Benutzeroberfläche von MDaemon. Der Windows-Dienst MDaemon wird auch nach dem Beenden der Benutzeroberfläche weiterhin ausgeführt.

Sperren und Entsperren der Benutzeroberfläche von MDaemon

Um die Benutzeroberfläche zu sperren, muss MDaemon zunächst minimiert werden. Danach wird die Sperre durch Auswahl des Menüpunktes "Server sperren..." eingeleitet und durch Eingabe und Bestätigung eines Kennworts im folgenden Dialog abgeschlossen. Danach ist die Benutzeroberfläche gegen Zugriffe gesperrt und kann weder geöffnet noch sonst eingesehen werden, MDaemon arbeitet jedoch weiterhin normal. Es kann auch weiterhin durch Auswahl des Menüpunktes "Alle Warteschlangen sofort verarbeiten" ein Verarbeitungsdurchlauf für alle Warteschlangen manuell ausgelöst werden. Um MDaemon zu entsperren, muss durch Doppelklick auf das Symbol im Systray oder durch Rechtsklick auf das Symbol und Auswahl des Menüpunktes "Server entsperren..." der Entsperrdialog aufgerufen werden. Nach Eingabe des vorher gewählten Kennworts ist die Benutzeroberfläche wieder zugänglich.

2.5 Das Verbindungsfenster

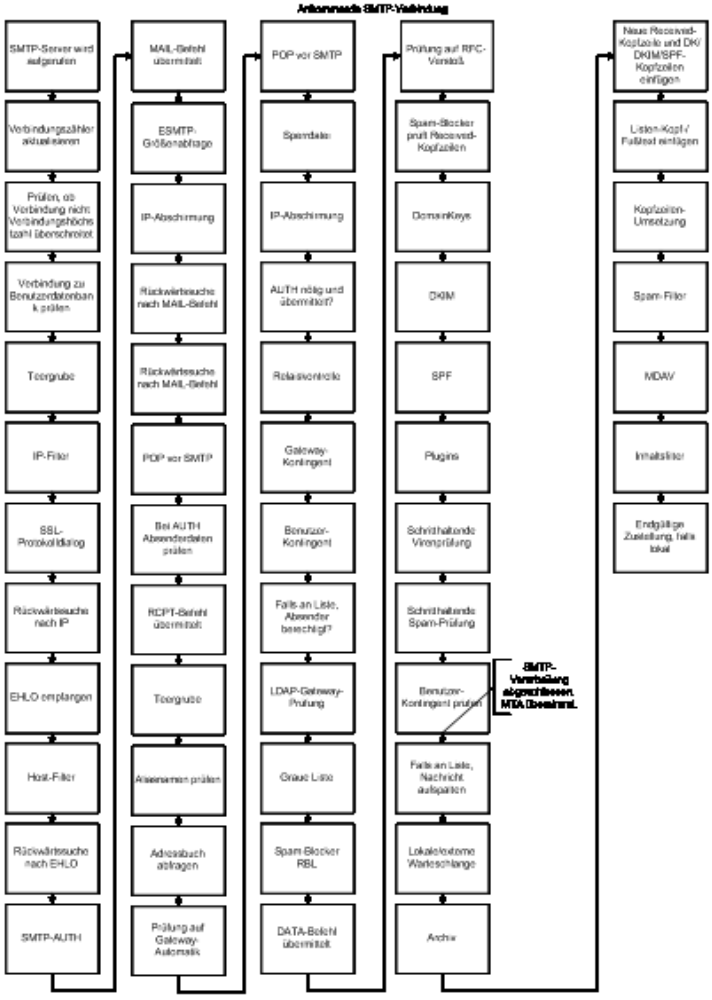
Sie können durch Doppelklick auf den Eintrag einer aktiven Verbindung auf einer der Registerkarten der Gruppe Verbindungen[76] auf der Benutzeroberfläche ein Verbindungsfenster für diese Verbindung öffnen. Das Verbindungsfenster zeigt einen Mitschnitt der SMTP-Verbindung, der laufend aktualisiert wird. Sie können in diesem Fenster auf das Steuerelement "Trennen" klicken, um die laufende Verbindung zu unterbrechen und zu trennen.



2.6 Der SMTP-Arbeitsablauf von MDaemon

Nachdem eine eingehende SMTP-Verbindung hergestellt wurde, durchläuft MDaemon einen komplexen Prozess, um festzustellen, ob die Nachricht zur Zustellung angenommen werden kann, und wie sie danach weiterzuverarbeiten ist. Die folgende Übersicht soll diesen Arbeitsablauf bei eingehenden SMTP-Verbindungen grafisch darstellen.

Ob alle dargestellten Schritte im Einzelfall auch durchlaufen werden, hängt von der genauen Konfiguration des jeweils verwendeten Systems ab. Sind in der Konfiguration einzelne Funktionen abgeschaltet, so werden u.U. Schritte übersprungen.



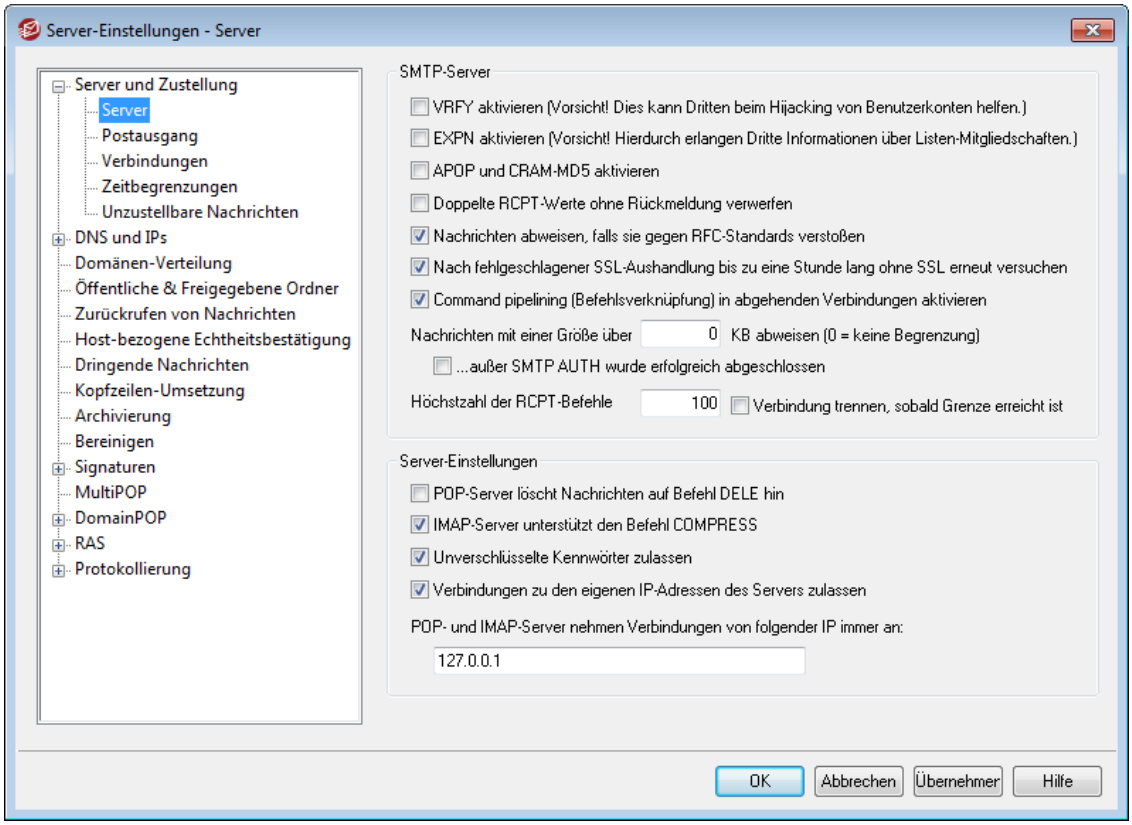
Kapitel III

3 Das Menü Einstellungen

3.1 Server-Einstellungen

3.1.1 Server und Zustellung

3.1.1.1 Server



SMTP-Server

VRFY aktivieren
Diese Option bewirkt, dass ESMTP-Befehle VRFY befolgt werden. Manche Server, die vorwärtsgerichtete SMTP-Prüfungen oder Rückrufprüfungen nutzen, um die Echtheit von E-Mail-Adressen auf Ihrem Server zu prüfen, nutzen diesen Befehl bisweilen. Diese Option ist per Voreinstellung abgeschaltet.

EXPN aktivieren
Diese Option bewirkt, dass ESMTP-Befehle EXPN befolgt werden.

APOP und CRAM-MD5 aktivieren
Per Voreinstellung unterstützen die Serverdienste von MDaemon (POP, IMAP usw.) die Echtheitsbestätigungsverfahren APOP und CRAM-MD5 nicht. Diese Verfahren setzen voraus, dass die Kennwörter mit umkehrbarer Verschlüsselung gespeichert werden. Diese Art der Speicherung ist aus Sicherheitsgründen nicht zu empfehlen, da sie nicht verhindert, dass Kennwörter durch MDaemon, die Administratoren oder mögliche Angreifer entschlüsselt werden. Aus diesen Gründen sind die genannten Verfahren nicht mit der Option *"Kennwörter der Benutzerkonten mit nicht-umkehrbarer Verschlüsselung speichern"* im Abschnitt Kennwörter 847 kompatibel, und sie können nicht bei Echtheitsbestätigung über

das Active Directory genutzt werden. Falls Sie allerdings SSL/TLS nicht einsetzen, dann können APOP und CRAM-MD5 möglicherweise die Sicherheit erhöhen, da sie die Echtheitsbestätigung ermöglichen, ohne dass die Benutzer die Kennwörter im Klartext übermitteln müssen.

Doppelte RCPT-Werte ohne Rückmeldung verwerfen
Diese Option verhindert, dass der SMTP-Server die Mehrfachnennung solcher Empfänger ignoriert, die innerhalb derselben SMTP-Verbindung mehrfach übermittelt werden. Die entsprechenden Nachrichten werden angenommen, an mehrfach genannte Empfänger aber nur einmal zugestellt. Diese Option ist per Voreinstellung abgeschaltet.

Nachrichten abweisen, falls sie gegen RFC-Standards verstoßen
Mithilfe dieser Option können Sie Nachrichten während der SMTP-Verbindung abweisen lassen, falls diese Nachrichten die in den RFC-Internet-Standards niedergelegten Anforderungen nicht erfüllen. Um die Prüfung auf Übereinstimmung mit diesen Anforderungen erfolgreich zu bestehen, müssen Nachrichten folgenden Kriterien entsprechen:

1. Ihre Größe muss 32 Byte überschreiten (dies ist die Mindestgröße, die alle nötigen Bestandteile noch enthalten kann).
2. Sie müssen entweder eine Absenderkopfzeile FROM: oder eine Kopfzeile SENDER: enthalten.
3. Sie dürfen nur höchstens eine Absenderkopfzeile FROM: enthalten.
4. Sie dürfen nur höchstens eine Betreffzeile (SUBJECT:) enthalten, jedoch muss eine Betreffzeile nicht zwingend vorhanden sein.

Nachrichten, die in Verbindungen mit Echtheitsbestätigung oder durch vertraute Domänen oder IP-Adressen übermittelt werden, sind von dieser Anforderung ausgenommen.

Nach fehlgeschlagener SSL-Aushandlung bis zu eine Stunde lang ohne SSL erneut versuchen
Diese Option bewirkt nach SSL-Fehlern in abgehenden SMTP-Verbindungen, dass der Verbindungsaufbau zur IP-Adresse des betreffenden Hosts eine Stunde lang ohne SSL erneut versucht wird. Nach Ablauf dieser Stunde kehrt MDaemon zur normalen Vorgehensweise zurück.

Command pipelining (Befehlsverknüpfung) in abgehenden Verbindungen aktivieren
Per Voreinstellung unterstützt MDaemon die SMTP-Diensterweiterung "Command Pipelining" (siehe RFC 2920) zur Verknüpfung von Befehlen. Bei Nutzung dieser Erweiterung werden die Befehle MAIL, RCPT und DATA nicht einzeln sondern stapelweise übermittelt. Hierdurch wird die Leistung bei Netzwerkverbindungen mit hoher Latenz erhöht. Die Befehlsverknüpfung wird in eingehenden Verbindungen immer genutzt. Sie ist in abgehenden Verbindungen per Voreinstellung aktiv. Falls Sie die Befehlsverknüpfung in abgehenden Verbindungen nicht nutzen wollen, deaktivieren Sie dieses Kontrollkästchen.

Nachrichten mit einer Größe über [xx] KB abweisen (0=keine Begrenzung)
Wird hier ein Wert eingetragen, so nimmt MDaemon keine Nachrichten über dieser Größe an. MDaemon versucht dann, den ESMTP-Befehl SIZE gemäß RFC-1870 zu benutzen. Unterstützt das Absendersystem diesen Befehl, so erkennt MDaemon vor dem Versand die Größe der Nachricht und weist sie ggf. sofort ab. Andernfalls kann MDaemon die Nachricht nur während der Übertragung überwachen und erst

abweisen, sobald während des Empfangs die festgesetzte Größe überschritten wird. Der Wert 0 bewirkt, dass per SMTP Nachrichten ohne Größenbegrenzung übermittelt werden können. Falls Sie solche Verbindungen von den SIZE-Prüfungen ausnehmen wollen, die echtheitsbestätigt sind, können Sie hierzu die Option "*...außer SMTP AUTH wurde erfolgreich abgeschlossen*" nutzen.

...außer SMTP AUTH wurde erfolgreich abgeschlossen
Mithilfe dieser Option nehmen Sie solche Nachrichten von der Größenbegrenzung aus, die über echtheitsbestätigte SMTP-Verbindungen übermittelt werden.

Höchstzahl der RCPT-Befehle
Mit dieser Option wird die Zahl der RCPT-Befehle für jede einzelne Nachricht begrenzt. Falls Sie keine Begrenzung setzen wollen, tragen Sie hier den Wert "0" ein.

Verbindung trennen, sobald Grenze erreicht ist
Diese Option bewirkt, dass die Verbindung sofort getrennt wird, sobald die Höchstzahl der zulässigen RCPT-Befehle erreicht ist.

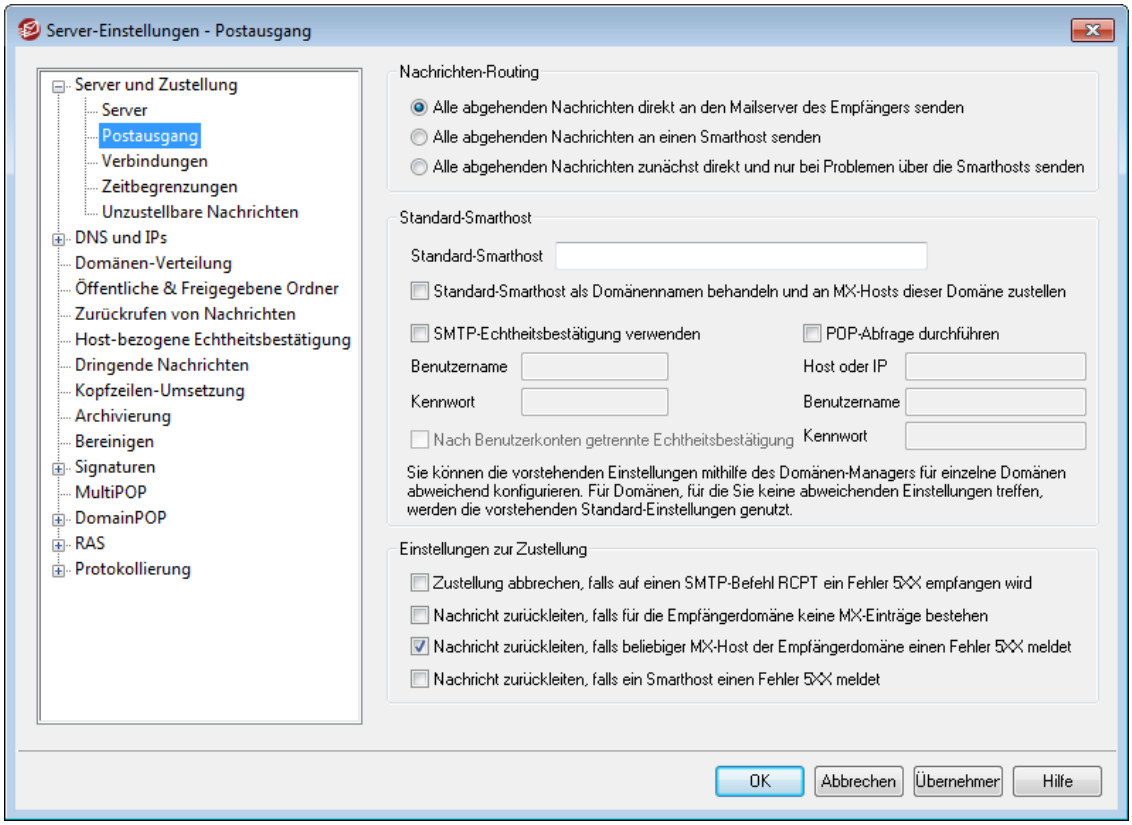
Server-Einstellungen

POP-Server löscht Nachrichten auf den Befehl DELE hin
Diese Option bewirkt, dass MDaemon abgerufene Nachrichten sofort aus dem Nachrichtenverzeichnis des Benutzers löscht, selbst wenn die POP-Verbindung unerwartet abbricht oder nicht ordnungsgemäß beendet wird.

Unverschlüsselte Kennwörter zulassen
Diese Option bestimmt, ob MDaemon für die Serverdienste SMTP, IMAP und POP3 Kennwörter im Klartext zulässt. Ist diese Option abgeschaltet, so gibt der Server auf die Befehle `POP3-USER`, `POP3-PASS`, `IMAP-LOGIN`, `IMAP-AUTH-LOGIN` und `SMTP-AUTH-LOGIN` Fehlermeldungen aus, falls die Verbindung nicht über SSL hergestellt wird.

Verbindungen zu den eigenen IP-Adressen des Servers zulassen
Ist diese Option aktiv, so kann MDaemon Verbindungen zu sich selbst herstellen.

3.1.1.2 Postausgang



Nachrichten-Routing

Alle abgehenden Nachrichten direkt an den Mailserver des Empfängers senden
Wird diese Einstellung gewählt, versucht MDaemon, Nachrichten direkt zuzustellen, und bedient sich nicht eines anderen Servers, der die Zustellung übernimmt. Unzustellbare Nachrichten werden für die erneute Zustellung vorgemerkt, bis die in der Konfiguration der Wiederholungs-Warteschlange 864 vorgegebenen Grenzen für erneute Zustellversuche erreicht sind.

Alle abgehenden Nachrichten an einen Smarthost senden
Wählen Sie diese Option, um abgehende Nachrichten, unabhängig von ihren Empfängerdomänen, an einen anderen Host oder Server zu senden, damit dieser Host sie zustellt. Ist diese Option aktiv, so werden abgehende Nachrichten über den weiter unten in diesem Konfigurationsdialog angegebenen *Standard-Smarthost* genutzt. Diese Funktion ist üblicherweise in Spitzenlastzeiten hilfreich, wenn eine direkte Zustellung abgehender Nachrichten den Server übermäßig stark auslasten würde. Kann eine Nachricht nicht an den Mailserver übermittelt werden, so wird sie in die Wiederholungs-Warteschlange verschoben, und MDaemon versucht weiterhin, die Nachricht in Übereinstimmung mit den Einstellungen für die Wiederholungs-Warteschlange 864 zuzustellen.

Alle abgehenden Nachrichten zunächst direkt und nur bei Problemen über die Smarthosts senden
Diese Option vereinigt Leistungsmerkmale aus den beiden vorherigen Optionen über die Zustellung. MDaemon versucht jeweils zunächst, die abgehenden Nachrichten direkt an den Server des Empfängers zuzustellen. Schlägt diese direkte Zustellung fehl, dann sendet MDaemon die Nachrichten über den *Standard-Smarthost*, der weiter unten angegeben wird. MDaemon betrachtet die

direkte Zustellung als fehlgeschlagen, wenn die Zustellung an einen Host erfolgen sollte, der zwar erfolgreich aufgelöst, mit dem aber keine direkte Verbindung hergestellt werden konnte, oder der direkte Verbindungen abgelehnt hat. Ist diese Option aktiv, so leitet MDaemon die Nachrichten nicht direkt zurück sondern versucht die Zustellung über einen Smarthost, dem mutmaßlich weiter gehende Möglichkeiten zur Zustellung zur Verfügung stehen. Insbesondere wenn der Mailserver des ISP als Smarthost genutzt wird, stehen diesem oft Möglichkeiten zur Zustellung zur Verfügung, auf die der lokale Server sonst keinen Zugriff hätte. Kann allerdings die Nachricht auch nicht über den Smarthost zugestellt werden, so wendet MDaemon die Funktionen zur wiederholten Zustellung an, die Sie im Abschnitt Wiederholungs-Warteschlange 864 des Konfigurationsdialogs für die Nachrichten-Warteschlangen festlegen können. Bei jedem weiteren Zustellversuch sendet MDaemon zunächst die Nachricht wieder direkt an den Server des Empfängers und dann nötigenfalls an den Smarthost.

Standard-Smarthost

Standard-Smarthost
Hier wird der Hostname oder die IP-Adresse des E-Mail-Hosts eingetragen, der als Gateway oder Smarthost genutzt werden soll. Dieser Smarthost ist normalerweise der SMTP-Server bei dem verwendeten ISP.

Der Name oder die IP-Adresse der Standard-Domäne von MDaemon dürfen hier nicht eingetragen werden. Dieser Eintrag sollte einen ISP oder anderen Mailserver bezeichnen, über den E-Mail versandt werden kann.

Standard-Smarthost als Domänennamen behandeln und an MX-Hosts dieser Domäne zustellen
Diese Option bewirkt, dass MDaemon den *Standard-Smarthost* als Namen einer Domäne behandelt, die DNS-Einträge für diese Domäne abfragt und die Nachrichten an die MX-Hosts dieser Domäne zustellt.

SMTP-Echtheitsbestätigung verwenden
Diese Option muss aktiv sein, falls der *Standard-Smarthost* eine Echtheitsbestätigung erfordert. Benutzername und Kennwort müssen dann in die folgenden Felder eingetragen werden. Die hier eingetragenen Anmeldedaten werden für alle abgehenden SMTP-Verbindungen zu dem angegebenen Server genutzt. Wird hingegen die Option *Echtheitsbestätigung nach Benutzerkonten getrennt durchführen* weiter unten aktiviert, so führt MDaemon für jede einzelne Nachricht eine eigene Echtheitsbestätigung durch und übermittelt dazu die E-Mail-Adresse und das Kennwort für den Smarthost, die im Feld *Benutzername/Kennwort für Smarthost* für das Benutzerkonto des jeweiligen Absenders eingetragen sind. Dieses Feld ist über den Abschnitt Mail-Dienste 718 des Benutzerkonten-Editors erreichbar.

Benutzername
Geben Sie hier den Benutzernamen oder Anmeldenamen ein.

Kennwort
Geben Sie hier das Kennwort für die Anmeldung beim Smarthost ein.

POP-Abfrage durchführen
Falls der verwendete Smarthost die Abfrage eines lokalen Postfachs über POP verlangt, bevor er Nachrichten zur Zustellung entgegen nimmt, muss diese Option aktiviert werden. Die nötigen Anmeldedaten für das Postfach können dann in die folgenden Felder eingetragen werden.

Host oder IP
Geben Sie den Hostnamen oder die IP-Adresse ein, mit denen die Verbindung hergestellt werden soll.

Benutzername
Geben Sie hier den Benutzernamen oder den Anmeldenamen für das POP-Benutzerkonto ein.

Kennwort
Geben Sie hier das Kennwort für das POP-Benutzerkonto ein.

Nach Benutzerkonten getrennte Echtheitsbestätigung
Diese Option bewirkt, dass beim Versand von Nachrichten über SMTP für jede Nachricht eigene Anmeldedaten für die Echtheitsbestätigung an den oben konfigurierten *Standard-Smarthost* gesendet werden. Die hier unter *Benutzername* und *Kennwort* eingetragenen Anmeldedaten werden nicht genutzt. Stattdessen werden für jedes Benutzerkonto die E-Mail-Adresse und das Kennwort für den Smarthost (die beide im Abschnitt Mail-Dienste 718 des Benutzerkonten-Editors eingetragen werden) übermittelt. Sind für ein Benutzerkonto dort kein Benutzername und kein Kennwort für den Smarthost eingetragen, so werden die oben angegebenen Anmeldedaten für das Benutzerkonto verwendet.

Soll für die nach Benutzerkonten getrennte Echtheitsbestätigung nicht das *Kennwort für den Smarthost* sondern das *E-Mail-Kennwort* des Benutzerkontos verwendet werden, so wird dies durch Bearbeiten des folgenden Eintrags in der Datei `MDaemon.ini` erreicht:

```
[AUTH]
ISPAUTHUsePasswords=Yes (Ja, Voreinstellung ist "No", Nein)
```

Wird die Option `ISPAUTHUsePasswords=Yes` aktiviert, so führt dies dazu, dass mit der Zeit alle Kennwörter der lokalen Benutzerkonten an den Smarthost übermittelt werden. Hieraus kann sich ein Risiko für die Sicherheit des Mailservers ergeben, da die Kennwörter Teil der Zugriffskontrolle sind. Diese Option sollte daher nur genutzt werden, wenn der Smarthost absolut vertrauenswürdig ist. Dürfen die Benutzer ihre *E-Mail-Kennwörter* über Webmail oder auf andere Weise selbst ändern, so ändern sie damit auch ihre *Kennwörter für den Smarthost*. Die Echtheitsbestätigung beim Smarthost kann dann fehlschlagen, wenn ein *E-Mail-Kennwort* lokal geändert wird, der Smarthost aber von der Änderung keine Kenntnis hat.

Zustellung abbrechen, falls auf einen SMTP-Befehl RCPT ein Fehler 5XX empfangen wird
Diese Option bewirkt, dass MDaemon den Versuch, eine Nachricht zuzustellen abbricht, falls als Antwort auf den SMTP-Befehl RCPT ein Fehler 5xx (endgültiger Fehler) empfangen wird. Diese Option ist per Voreinstellung abgeschaltet.

Nachricht zurückleiten, falls für die Empfängerdomäne keine MX-Einträge bestehen
MDaemon sucht während der Prüfung der DNS-Einträge für eine Empfängerdomäne üblicherweise zuerst nach MX-Einträgen und dann, falls keine MX-Einträge gefunden werden, nach A-Einträgen. Falls weder MX- noch A-Einträge gefunden werden, leitet MDaemon die Nachricht als unzustellbar an den Absender zurück. Diese Option veranlasst MDaemon, nicht noch nach A-Einträgen zu suchen, sondern die Nachricht sofort zurückzuleiten, falls keine MX-Einträge gefunden werden. Die Option ist per Voreinstellung abgeschaltet.

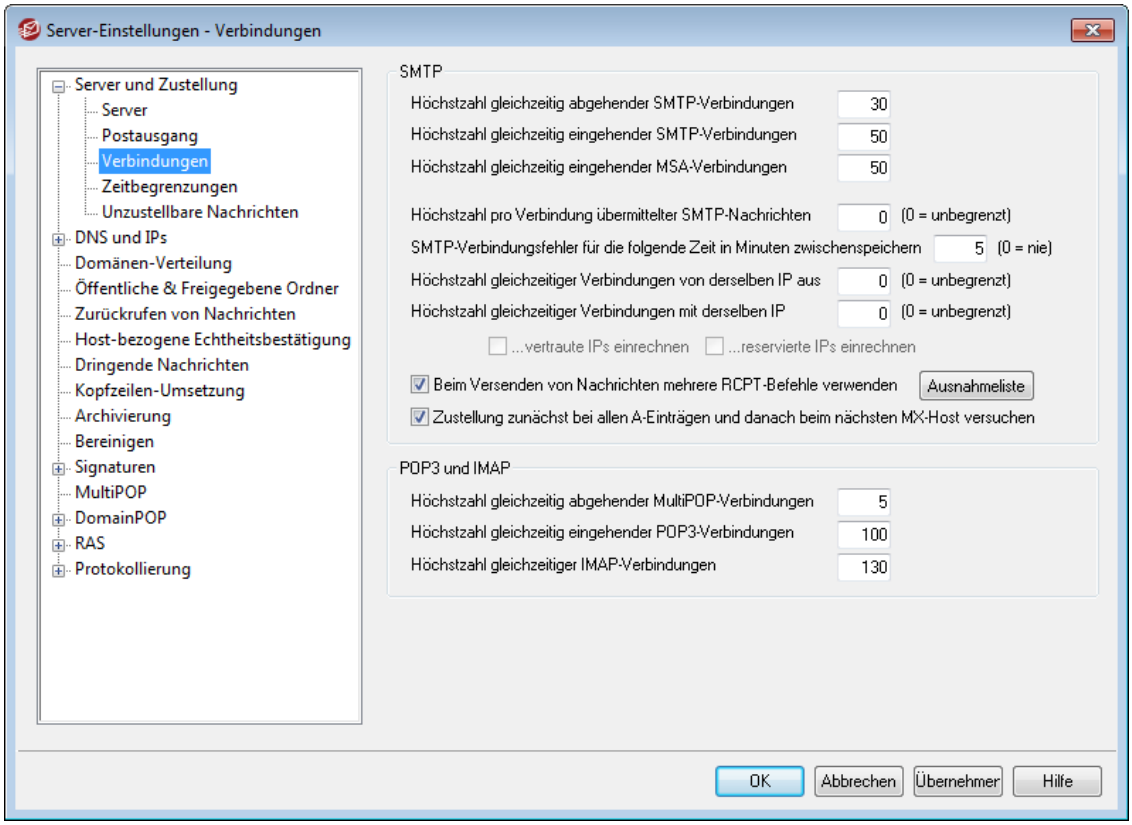
Nachricht zurückleiten, falls beliebiger MX-Host der Empfängerdomäne einen Fehler 5XX meldet
Ist diese Option aktiv, so leitet MDaemon eine Nachricht immer bereits dann an den Absender zurück, wenn ein MX-Host einen Fehler 5xx und damit eine endgültig fehlgeschlagene Zustellung meldet. Auch wenn für die Empfängerdomäne mehrere MX-Hosts eingetragen sind, versucht MDaemon die Zustellung über die weiteren MX-Hosts nicht mehr. Ist die Option nicht aktiv, so versucht MDaemon weiterhin, die Nachricht zuzustellen, falls wenigstens einer der MX-Server einen nur vorübergehenden Fehler 4xx meldet. Diese Option ist per Voreinstellung aktiv.

Nachricht zurückleiten, falls ein Smarthost einen Fehler 5XX meldet
Diese Option bewirkt, dass eine Nachricht zurückgeleitet wird, sobald ein Smarthost einen endgültigen Fehler 5xx meldet.

Siehe auch:

Wiederholungs-Warteschlange 864
Mail-Dienste 718

3.1.1.3 Verbindungen



SMTP

Höchstzahl gleichzeitig abgehender SMTP-Verbindungen
Dieses Feld legt fest, wie viele abgehende SMTP-Verbindungen gleichzeitig bestehen dürfen, wenn abgehende Nachrichten versandt werden. In jeder Verbindung werden abgehende Nachrichten so lange versandt, bis entweder die Post-Warteschlange leer oder die *Höchstzahl pro Verbindung übermittelter SMTP-Nachrichten* erreicht ist. Stehen also z.B. in der Warteschlange für externe Nachrichten 20 Nachrichten zum Versand, und liegt diese Höchstzahl pro Verbindung bei 5, so werden 5 Verbindungen gleichzeitig aufgebaut, und in jeder der Reihe nach 4 Nachrichten versandt.

Die Voreinstellung für diese Option beträgt 30. In der Praxis sollte erprobt werden, wie viele Verbindungen die beste Leistung bei der jeweils zur Verfügung stehenden Bandbreite ergeben. Es dürfen nicht so viele Verbindungen aufgebaut werden, dass die Bandbreite nicht mehr ausreicht oder die Systemlast auf dem Rechner zu groß wird, da dann die Zustellung ineffizient ist. Jede SMTP-Verbindung versendet, wie erwähnt, mehrere Nachrichten hintereinander. Daher können 4 Verbindungen mit je zwei Nachrichten effizienter sein als 8 Verbindungen mit je einer Nachricht. Angemessene Richtwerte sind 5 – 10 Verbindungen bei Übermittlung über ein Modem mit 56 KBit/s und 20 – 30 Verbindungen bei Breitband-Anbindungen.

Höchstzahl gleichzeitig eingehender SMTP-Verbindungen
Die Anzahl gleichzeitig eingehender SMTP-Verbindungen, die der Server annimmt, bevor er weitere Verbindungen mit der Fehlermeldung "Server überlastet" abweist, kann hier eingestellt werden. Die Voreinstellung beträgt 50.

Höchstzahl gleichzeitig eingehender MSA-Verbindungen
Diese Option bestimmt die Höchstzahl gleichzeitig eingehender Verbindungen von Mail Submission Agents (MSAs), die auf dem Server zugelassen ist.

Höchstzahl pro Verbindung übermittelter SMTP-Nachrichten (0 = unbegrenzt)
Diese Einstellung legt die Höchstzahl an Nachrichten fest, die jede Verbindung sendet, bevor sie beendet wird. Normalerweise sollte der Wert 0 eingestellt sein, damit auf allen Verbindungen so lange Nachrichten übertragen werden, bis die Warteschlange leer ist.

SMTP-Verbindungsfehler für die folgende Zeit in Minuten zwischenspeichern (0 = nie)
Bricht eine SMTP-Verbindung mit einer bestimmten Gegenstelle ab, so unterlässt MDaemon während der hier in Minuten angegebenen Zeit alle weiteren Versuche, zu dieser Gegenstelle eine Verbindung herzustellen. Dies kann verhindern, dass MDaemon unnötig versucht, eine Gegenstelle zu erreichen, bei der technische Probleme auftreten, besonders, wenn mehrere Nachrichten für die Gegenstelle vorliegen, MDaemon aber bereits beim ersten Zustellversuch feststellt, dass eine Verbindung zur Gegenstelle nicht möglich ist. Die Voreinstellung beträgt 5 Minuten. Sollen die SMTP-Verbindungsfehler nicht zwischengespeichert werden, so muss der Wert 0 eingetragen werden.

Höchstzahl gleichzeitiger Verbindungen von derselben IP aus [xx] (0 = keine Begrenzung)
Diese Einstellung legt die Höchstzahl gleichzeitiger Verbindungen fest, die von derselben IP-Adresse ausgehen dürfen. Weitere Verbindungen von derselben IP-Adresse, die diese Begrenzung überschreiten, werden abgewiesen. Der Wert 0 bewirkt, dass unbegrenzt viele gleichzeitige Verbindungen von derselben IP-Adresse gleichzeitig ausgehen dürfen.

Höchstzahl gleichzeitiger Verbindungen mit derselben IP (0 = unbegrenzt)
Diese Option begrenzt die Anzahl der Verbindungen, die zur Übermittlung von Nachrichten gleichzeitig mit derselben IP-Adresse hergestellt werden dürfen. Der Wert 0 setzt die Begrenzung außer Kraft.

Diese Option verhindert, dass zu viele Verbindungen mit bestimmten IP-Adressen gleichzeitig aufgebaut werden können. Liegt während der Nachrichtenzustellung eine Nachricht für eine bestimmte Gegenstelle vor, und würde eine weitere Verbindung mit der IP-Adresse der Gegenstelle die Beschränkung überschreiten, so wird diese Verbindung nicht hergestellt, und MDaemon geht zum nächsten MX- oder Smarthost über. Stehen keine weiteren Hosts zur Verfügung, wird die Zustellung der Nachricht bis zum nächsten Verarbeitungsdurchlauf aufgeschoben. Die Option ist per Voreinstellung abgeschaltet, sodass das bisherige Verhalten beibehalten wird.

...vertraute IPs einrechnen
Per Voreinstellung werden Verbindungen mit vertrauten IP-Adressen nicht in die *Höchstzahl gleichzeitiger Verbindungen mit derselben IP* eingerechnet. Falls Sie Verbindungen mit solchen IP-Adressen ebenfalls auf die angegebene Höchstzahl beschränken wollen, aktivieren Sie diese Option.

...reservierte IPs einrechnen
Per Voreinstellung sind außerdem Verbindungen mit reservierten IP-Adressen, die für die Nutzung im Intranet vorgesehen sind, von dieser Begrenzung ausgenommen. Diese IP-Adressen sind `127.0.0.*`, `192.168.*.*`, `10.*.*.*` und `172.16.0.0/12`. Falls Sie Verbindungen mit solchen IP-Adressen

ebenfalls auf die angegebene Höchstzahl beschränken wollen, aktivieren Sie diese Option.

Beim Versenden von Nachrichten mehrere RCPT-Befehle verwenden
Diese Option ist per Voreinstellung aktiv. Sie bewirkt, dass MDaemon die Übermittlung von Nachrichten optimiert und dazu innerhalb derselben Verbindung mehrere RCPT-Befehle übermittelt, soweit das möglich und sinnvoll ist. Falls Sie in jeder Verbindung nur einen RCPT-Befehl übermitteln lassen wollen, deaktivieren Sie diese Option.

Ausnahmeliste
Dieses Steuerelement ruft die Ausnahmeliste für die Optimierung der Übermittlung von Nachrichten auf. MDaemon optimiert die Übermittlung von Nachrichten an Domänen, die in dieser Liste erfasst sind, nicht. Stattdessen übermittelt MDaemon nur einen RCPT-Befehl je Verbindung.

Zustellung zunächst bei allen A-Einträgen und danach beim nächsten MX-Host versuchen
MDaemon versucht nach Fehlern in der Zustellung sowie nach endgültig fehlgeschlagener Zustellung zunächst die Zustellung an alle anderen A-Einträge eines MX-Hosts, bevor die Zustellversuche mit dem nächsten MX-Host fortgesetzt werden. Falls MDaemon nach einem Fehler in der Zustellung nicht zunächst die anderen A-Einträge versuchen, sondern direkt zum nächsten MX-Host wechseln soll, aktivieren Sie diese Option.

POP3 und IMAP

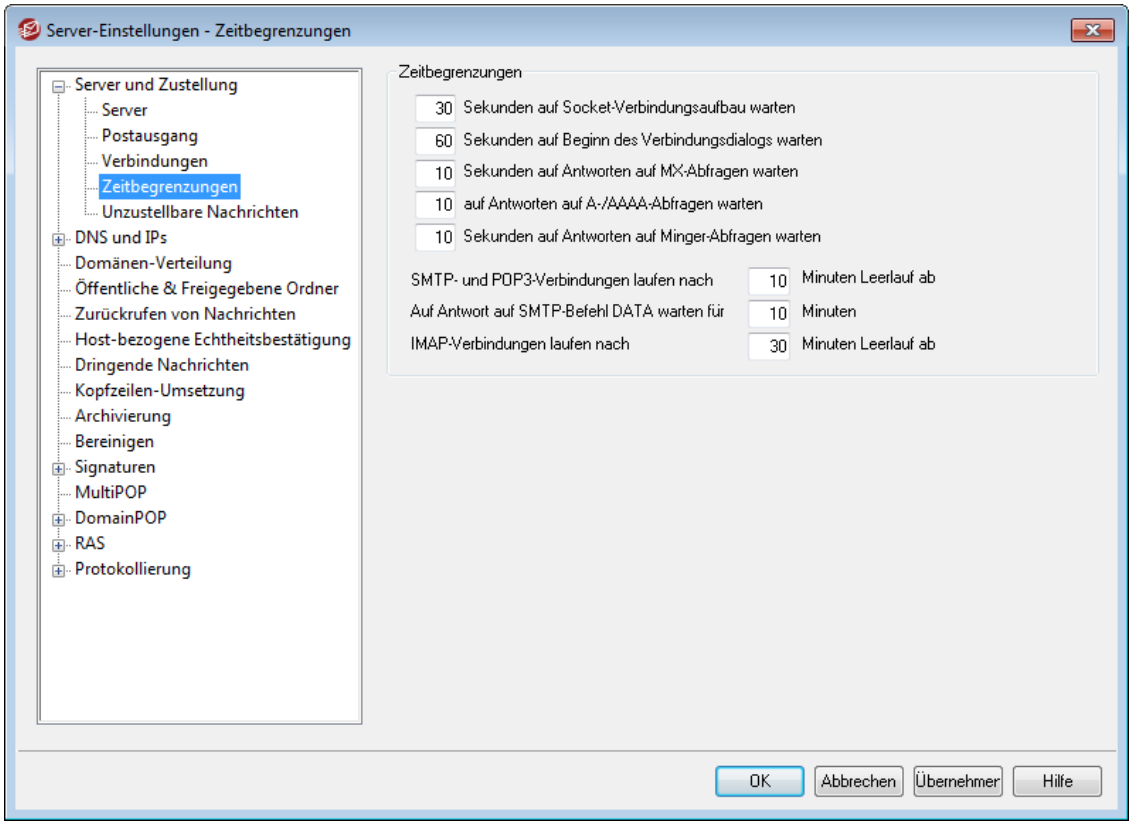
Höchstzahl gleichzeitig abgehender MultiPOP-Verbindungen
Dieser Wert legt die Höchstzahl der abgehenden POP-Verbindungen fest, die beim Abruf von Nachrichten über MultiPOP gleichzeitig bestehen dürfen. In jeder Verbindung werden so lange Nachrichten abgerufen, bis alle MultiPOP-Gegenstellen abgearbeitet und alle Nachrichten abgerufen sind. Sind also z.B. in der Benutzerdatenbank 15 MultiPOP-Server konfiguriert, und liegt die Höchstzahl der abgehenden POP-Verbindungen bei 3, so werden in jeder Verbindung Nachrichten von 5 MultiPOP-Gegenstellen abgerufen.

In der Praxis sollte erprobt werden, wie viele Verbindungen die beste Leistung bei der jeweils zur Verfügung stehenden Bandbreite ergeben. Es dürfen nicht so viele Verbindungen aufgebaut werden, dass die Bandbreite nicht mehr ausreicht oder die Systemlast auf dem Rechner zu groß wird, da dann die Zustellung ineffizient ist. Jede POP-Verbindung ruft, wie erwähnt, so lange Nachrichten ab, bis alle Gegenstellen abgearbeitet sind. Daher können 4 Verbindungen, die jeweils zwanzig Gegenstellen abrufen, effizienter sein als 20 Verbindungen, die alle dieselbe Gegenstelle abrufen.

Höchstzahl gleichzeitig eingehender POP3-Verbindungen
Diese Einstellung legt die Höchstzahl gleichzeitig eingehender POP-Verbindungen fest, die der Server annimmt, bevor er weitere Verbindungen mit der Fehlermeldung "Server überlastet" abweist.

Höchstzahl gleichzeitiger IMAP-Verbindungen
Dieser Wert legt die Höchstzahl gleichzeitiger IMAP-Verbindungen fest, die der Server zulässt, bevor er weitere Verbindungen mit der Fehlermeldung "Server überlastet" abweist.

3.1.1.4 Zeitbegrenzungen



Zeitbegrenzungen

[xx] Sekunden auf Socket-Verbindungsaufbau warten
Beim Aufbau einer abgehenden Verbindung wartet MDaemon nach dem Absetzen der Anfrage so lange, wie hier konfiguriert, darauf, dass die Gegenstelle die Verbindung annimmt. Antwortet die Gegenstelle nicht innerhalb dieser Zeit, sendet MDaemon die Nachricht entweder an einen *Smarthost*, falls dieser festgelegt ist, oder leitet weitere Zustellversuche ein, je nach der Einstellung im Abschnitt Postausgang 97 des Konfigurationsdialogs Server-Einstellungen.

[xx] Sekunden auf Beginn des Verbindungsdialogs warten
Sobald eine Verbindung zu einer Gegenstelle besteht, wartet MDaemon so lange, wie hier konfiguriert, darauf, dass die Gegenstelle den SMTP- oder POP3-Verbindungsdialog beginnt. Beginnt die Gegenstelle nicht innerhalb dieser Zeit mit dem Verbindungsdialog, sendet MDaemon die Nachricht entweder an einen Smarthost, falls dieser festgelegt ist, oder leitet weitere Zustellversuche ein, je nach der Einstellung im Abschnitt Postausgang 97 des Konfigurationsdialogs Server-Einstellungen.

[xx] Sekunden auf Antworten auf MX-Abfragen warten
Während DNS-Abfragen nach "MX"-Einträgen durchgeführt werden, wartet MDaemon auf die Antwort so lange, wie hier konfiguriert. Antwortet der DNS-Server nicht innerhalb dieser Zeit, so versucht MDaemon, die Nachricht an die IP-Adresse aus dem "A"-Eintrag des Zielsystems zuzustellen. Schlägt dieser Versuch fehl, sendet MDaemon die Nachricht entweder an einen Smarthost, falls dieser festgelegt ist, oder leitet weitere Zustellversuche ein, je nach der Einstellung im Bereich Postausgang 97 des Konfigurationsdialogs Server-Einstellungen.

[xx] Sekunden auf Antworten auf A-/AAAA-Abfragen warten
Dieser Timer legt fest, wie lange MDaemon während der Auflösung einer IP-Adresse anhand des "A"-Eintrags einer Gegenstelle warten soll. Schlägt der Versuch fehl, sendet MDaemon die Nachricht entweder an den *Smarthost* oder leitet weitere Zustellversuche ein, je nach der Einstellung im Bereich Postausgang 97 des Konfigurationsdialogs Server-Einstellungen.

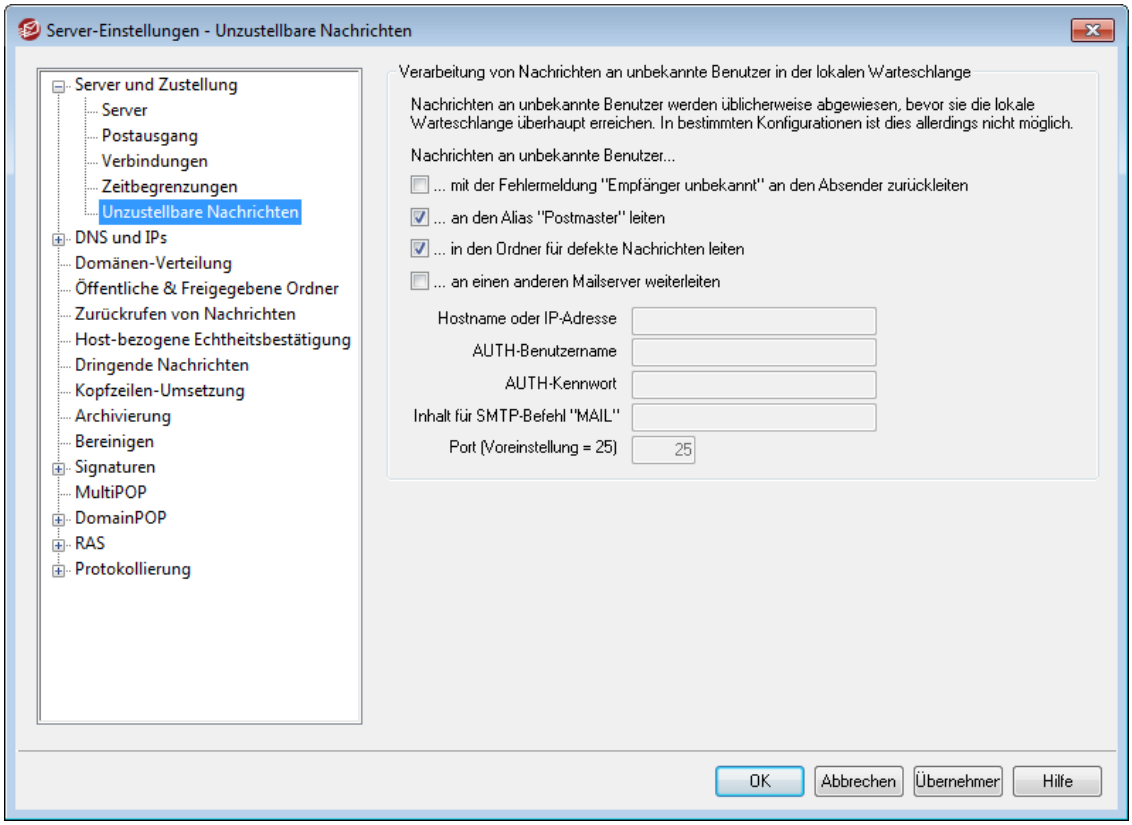
[xx] Sekunden auf Antworten auf Minger-Abfragen warten
Dieser Timer legt fest, wie lange (in Sekunden) MDaemon auf eine Antwort eines Minger 855-Servers wartet.

SMTP- und POP3-Verbindungen laufen nach [xx] Minuten Leerlauf ab
Befindet sich eine ordnungsgemäß hergestellte funktionsfähige Verbindung für die hier angegebene Dauer im Leerlauf, werden also keine Daten über sie ausgetauscht, bricht MDaemon die Verbindung ab. MDaemon versucht bei der nächsten planmäßigen Verarbeitung von Nachrichten wieder, die Verbindung herzustellen.

Auf Antwort auf SMTP-Befehl DATA warten für [xx] Minuten
Diese Option bestimmt, wie lange MDaemon während einer SMTP-Verbindung nach Senden des Befehls DATA auf die Antwort „250 Ok" warten soll. Manche Empfängergegenstellen führen zeitaufwändige Prüfungen zur Spam-Abwehr, Virenprüfungen und sonstige Vorgänge durch, und diese Option dient dazu, für solche Vorgänge ausreichend Zeit zu lassen. Der Vorgabewert beträgt 10 Minuten.

IMAP-Verbindungen laufen nach [xx] Minuten Leerlauf ab
Befindet sich eine IMAP-Verbindung für die hier angegebene Dauer im Leerlauf, bricht MDaemon die Verbindung ab.

3.1.1.5 Unzustellbare Nachrichten



Nachrichten an unbekannte Benutzer...

...mit der Fehlermeldung "Empfänger unbekannt" an den Absender zurückleiten
Nachrichten an vermeintliche Benutzer des Systems, für die jedoch kein Benutzerkonto besteht, werden an den Absender zurück geleitet, wenn diese Option aktiv ist. Sie können den Inhalt der Warnnachricht anpassen, die mit der Fehlermeldung "Empfänger unbekannt" versandt wird. Erstellen Sie hierzu eine Textdatei des Dateinamens "`NoShUser.dat`", und legen Sie diese Datei im Verzeichnis "`MDaemon\app\`" ab.

...an den Alias "Postmaster" leiten
Nachrichten an vermeintliche Benutzer des Systems, für die jedoch kein Benutzerkonto besteht, werden an den Benutzer weitergeleitet, auf dessen Benutzerkonto der Adress-Aliasname Postmaster verweist. Falls Sie solche Nachrichten nicht an den Postmaster weiterleiten werden, deaktivieren Sie diese Option.

...in den Ordner für defekte Nachrichten leiten
Nachrichten an vermeintliche Benutzer des Systems, für die jedoch kein Benutzerkonto besteht, werden per Voreinstellung in das Verzeichnis für defekte Post verschoben. Falls Sie solche Nachrichten nicht in die Defekt-Warteschlange verschieben wollen, deaktivieren Sie diese Option.

...an einen anderen Mailserver weiterleiten
Mithilfe dieser Option können Sie Nachrichten, die an unbekannte lokale Benutzer gerichtet sind, an einen anderen Mailserver weiterleiten.

Hostname oder IP-Adresse
Geben Sie hier den Hostnamen oder die IP-Adresse des Mailservers an, an den Sie die Nachrichten weiterleiten lassen wollen.

Der nachfolgende Hinweis trifft auf alle Fälle zu, in denen bei MDaemon ein Host angegeben werden kann, an den Nachrichten weitergeleitet, kopiert oder gesendet werden. Wird in diesen Fällen der Hostname in eckige Klammern gesetzt (z.B. `[example.com]`), so überspringt MDaemon die Abfrage von MX-Einträgen bei der Zustellung an diesen Host. Wird in das Textfeld "`example.com`" eingetragen, so werden die MX-Abfragen wie gewohnt durchgeführt, wird dort hingegen "`[example.com]`" eingetragen, so wird nur die Abfrage nach A-Einträgen durchgeführt.

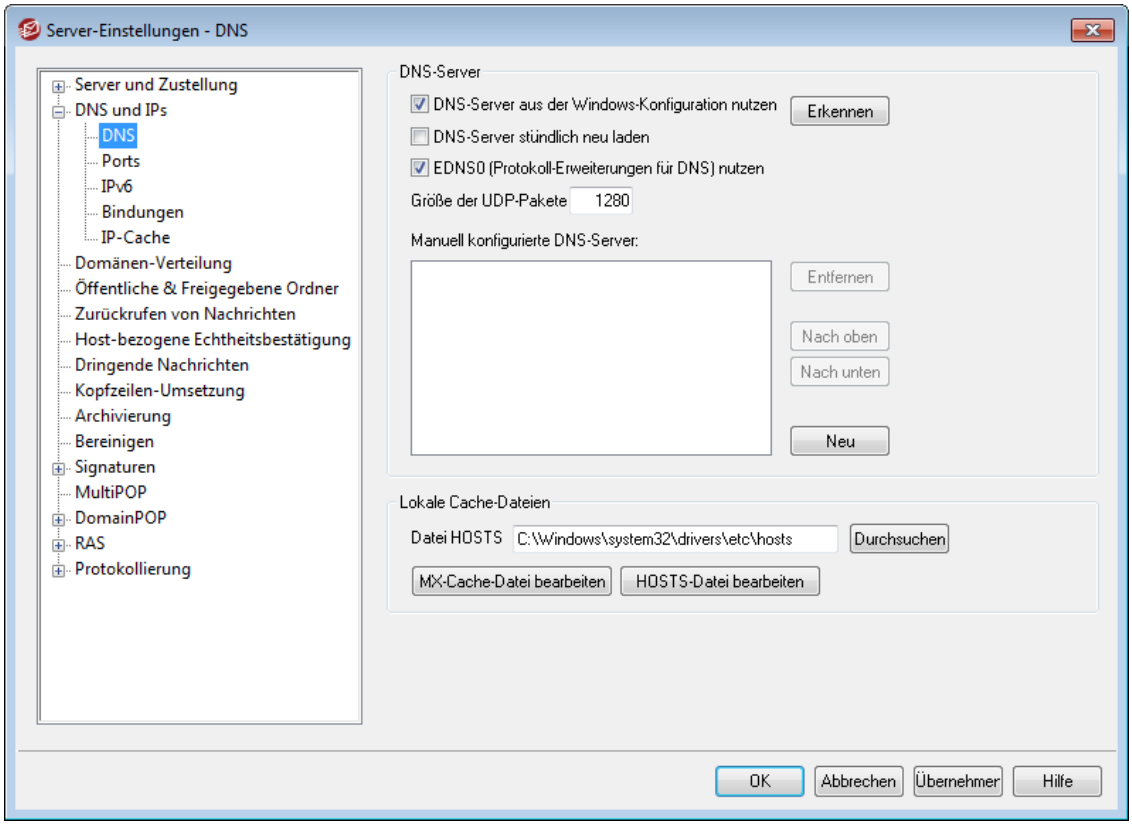
AUTH Benutzername/Kennwort
Falls der oben angegebene Mailserver eine Echtheitsbestätigung verlangt, geben Sie die Anmeldedaten - Benutzername und Kennwort - in diese Felder ein.

Inhalt für SMTP-Befehl "MAIL"
Die hier angegebene Adresse wird in dem SMTP-Befehl "`Mail From:`" während des Verbindungsdialogs mit dem oben angegebenen Mailserver verwendet. Üblicherweise steht hier der Name des Absenders. Falls jedoch dieser Name und das Feld leer bleiben müssen (`MAIL FROM <>`), so geben Sie in diesem Eingabefeld "`[trash]`" ein.

Port (Voreinstellung = 25)
MDaemon verwendet für den Versand der Nachricht den hier angegebenen TCP-Port. Die Voreinstellung ist Port 25.

3.1.2 DNS & IPs

3.1.2.1 DNS



DNS-Server

DNS-Server aus der Windows-Konfiguration nutzen
Ist diese Option aktiv, so fragt MDaemon alle DNS-Server ab, die MDaemon in der TCP/IP-Konfiguration von Windows findet. MDaemon fragt jeden DNS-Server bei jeder Abfrage in der Reihenfolge der Konfiguration ab, bis entweder ein DNS-Server geantwortet hat oder alle DNS-Server abgefragt sind. Falls Sie in das folgende Feld *Manuell konfigurierte DNS-Server* weitere DNS-Server eintragen, fragt MDaemon auch diese Server ab. Beim Programmstart werden in das System-Protokoll alle DNS-Server eingetragen, und es wird dazu vermerkt, aus welcher Quelle sie entnommen wurden (manuell eingetragen oder aus der Windows-Konfiguration).

DNS-Server stündlich neu laden
Diese Option bewirkt, dass MDaemon die DNS-Server jede Stunde neu lädt. Diese Option ist per Voreinstellung abgeschaltet.

UEDNS0 (Protokoll-Erweiterungen für DNS) nutzen
MDaemon unterstützt per Voreinstellung die Protokoll-Erweiterungen für DNS (Extension Mechanisms for DNS, siehe RFC 2671). Falls Sie die Nutzung der Protokoll-Erweiterungen nicht wünschen, deaktivieren Sie dieses Kontrollkästchen.

Größe der UDP-Pakete
Diese Option steuert die Größe der UDP-Pakete. Die Voreinstellung beträgt 1280 Byte.

Manuell konfigurierte DNS-Server
MDaemon nutzt bei DNS-Abfragen alle hier angegebenen DNS-Server (falls Sie mehrere Server eintragen, trennen Sie die IP-Adressen durch Leerzeichen). MDaemon fragt bei jeder Abfrage jeden Server in der hier angegebenen Reihenfolge ab, bis ein DNS-Server antwortet oder alle DNS-Server abgefragt sind. Falls Sie die Option *DNS-Server aus der Windows-Konfiguration nutzen* weiter oben aktivieren, fragt MDaemon auch alle DNS-Server ab, die in der TCP/IP-Konfiguration von Windows erfasst sind. Beim Programmstart werden in das System-Protokoll alle DNS-Server eingetragen, und es wird dazu vermerkt, aus welcher Quelle sie entnommen wurden (manuell eingetragen oder aus der Windows-Konfiguration).

Lokale Cache-Dateien

Datei HOSTS...
MDaemon versucht zuerst, eine Adresse durch Auswertung der HOSTS-Datei von Windows aufzulösen, bevor DNS-Server abgefragt werden. Falls in dieser Datei eine IP-Adresse zur betreffenden Domäne gefunden wird, so führt MDaemon keine DNS-Serverabfrage durch.

Sie müssen immer den kompletten Pfad und den Dateinamen angeben; der Dateiname allein genügt nicht. MDaemon versucht, folgenden Pfadnamen als Voreinstellung zu verwenden:

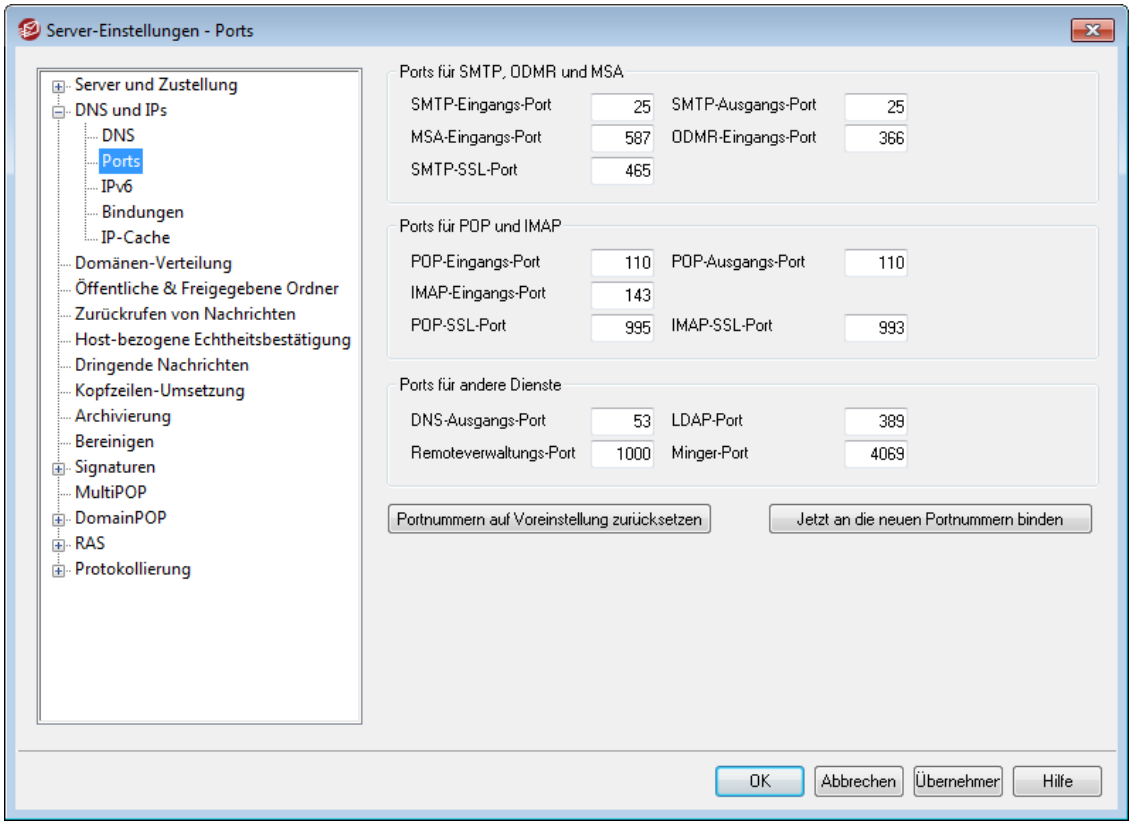
[Laufwerk]:\windows\system32\drivers\etc\hosts

Die Windows-Datei HOSTS enthält die A-Einträge, also die primären IP-Adressen für Domänennamen. Zusätzlich können in der Datei MXCACHE.DAT, speziell für MDaemon, die IP-Adressen für MX-Einträge zu den Domänennamen abgelegt werden. Diese Datei befindet sich im Unterverzeichnis MDaemon\APP\. Nähere Informationen über die Struktur der Datei können Sie der Datei selbst entnehmen. Klicken Sie auf **MX-Cache-Datei bearbeiten**, und lesen Sie die Kommentare am Beginn der Datei, um diese Informationen zu erhalten.

MX-Cache-Datei bearbeiten
Klicken Sie auf dieses Steuerelement, um die Datei MXCACHE.DAT einzusehen und zu bearbeiten.

HOSTS-Datei bearbeiten
Klicken Sie auf dieses Steuerelement, um die Datei HOSTS einzusehen und zu bearbeiten.

3.1.2.2 Ports



Ports für SMTP, ODMR und MSA

SMTP-Eingangs-Port
MDaemon überwacht diesen TCP-Port auf ankommende Verbindungen von SMTP-Clients. Dieser Port ist der Standard-Port für SMTP-Verbindungen, der für die meisten Anwendungsfälle auf den Vorgabewert 25 eingestellt bleiben soll.

SMTP-Ausgangs-Port
Dieser Port wird beim Versand von Nachrichten an andere SMTP-Servern verwendet.

MSA-Eingangs-Post
Dieser Port ist ein Ausweichport für die Nachrichtenzustellung (Software, die solche Ports zur Anlieferung von Nachrichten nutzt, wird im Englischen auch als Message Submission Agent, kurz MSA, bezeichnet). Dieser Port kann als Alternative zu dem *SMTP-Eingangs-Port* weiter oben genutzt werden. Die Übertragung über diesen Port erfordert AUTH, daher müssen die Benutzer bei Nutzung dieses Ports durch Konfiguration ihrer Mailclients sicher stellen, dass eine Echtheitsbestätigung durchgeführt wird. Der Ausweichport kann außen liegenden Benutzern auch helfen, falls der ISP, der diese versorgt, den Port 25 sperrt. Durch Nutzung des MSA- anstelle des SMTP-Ports können solche Benutzer die Sperre umgehen, falls nicht auch der MSA-Port gesperrt ist. Falls der Ausweichport nicht zur Verfügung gestellt werden soll, kann er durch Eintragen des Wertes "0" abgeschaltet werden.

Verbindungen, die über den MSA-Port hergestellt werden, sind von PTR- und Rückwärtssuche, Host- und IP-Filter, IP-Abschirmung und Teergrube ausgenommen. Bei Verbindungen über den MSA-Port wird aber durch bestimmte Prüfmechanismen und Beschränkungen für die zulässigen Verbindungen sicher gestellt, dass sie nicht durch Wörterbuchangriffe beeinträchtigt werden können.

ODMR-Eingangs-Port
MDaemon überwacht diesen Port auf eingehende ODMR-Verbindungen, etwa `ATRN`–Befehle von Gateway-Domänen.

SMTP-SSL-Port
Dieser Port wird für SMTP-Verbindungen reserviert, die das Secure-Sockets-Layer-Protokoll (SSL) verwenden. Weitere Informationen hierzu finden Sie unter SSL & TLS 577.

Ports für POP und IMAP

POP-Eingangs-Port
MDaemon überwacht diesen Port auf eingehende POP-Verbindungen von externen POP-Clients.

POP-Ausgangs-Port
Dieser Port wird zum Abrufen bereit liegender Nachrichten von anderen Servern durch MDaemon verwendet.

IMAP-Eingangs-Port
MDaemon überwacht diesen Port auf eingehende IMAP-Verbindungen.

POP-SSL-Port
Dieser Port wird für Verbindungen von POP3-Mailclients reserviert, die das Secure-Sockets-Layer-Protokoll (SSL) verwenden. Weitere Informationen hierzu finden Sie unter SSL & Zertifikate 577.

IMAP-SSL-Port
Dieser Port wird für Verbindungen von IMAP-Mailclients reserviert, die das Secure-Sockets-Layer-Protokoll (SSL) verwenden. Weitere Informationen hierzu finden Sie unter SSL & Zertifikate 577.

Ports für andere Dienste

DNS-Ausgangs-Port
Diese Portnummer verwendet MDaemon, um Datagramme an DNS-Server zu übermitteln und von ihnen zu empfangen.

LDAP-Port
MDaemon verwendet diese Portnummer, um Datenbank-Informationen und Adressbücher mit dem verwendeten LDAP-Server auszutauschen.

Siehe auch: Unterstützung für LDAP-Adressbücher 824

Remoteverwaltungs-Port
MDaemon überwacht diesen Port auf eingehende Verbindungen für die Remoteverwaltung 350.

Minger-Port
Der Minger 855-Server überwacht diesen Port auf eingehende Verbindungen.

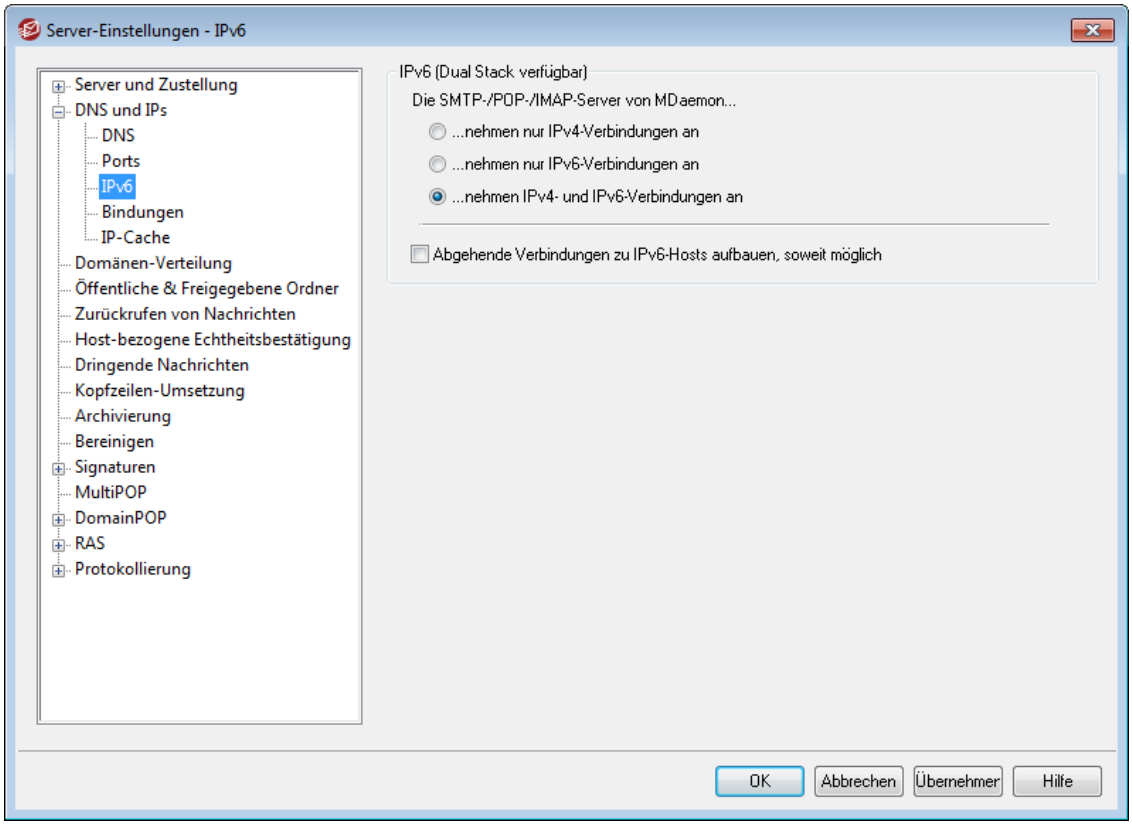
Portnummern auf Voreinstellung zurücksetzen
Mit dieser Schaltfläche werden alle Port-Nummern auf die Voreinstellung zurückgesetzt.

Jetzt an die neuen Portnummern binden
Nach einer Änderung an den Portnummern werden die neuen Einstellungen nur dann sofort wirksam, wenn diese Schaltfläche betätigt wird. Ansonsten werden die Änderungen beim nächsten Neustart von MDaemon wirksam.

Für den störungsfreien Betrieb des Servers sind diese Port-Einstellungen entscheidend. Sie sollten daher nur geändert werden, wenn es zwingend erforderlich ist. Die Portnummern müssen u.a. dann umkonfiguriert werden, wenn MDaemon mit bestimmten Proxy-Servern oder anderer Software zusammenarbeiten soll, die ihrerseits bestimmte Portnummern verwenden müssen.

Bei jeder IP-Adresse, also grundsätzlich bei jedem Rechner, ist jeder Port nur genau einmal vorhanden. Wenn ein Programm versucht, einen schon anderweit belegten Port selbst zu nützen, wird der Benutzer durch eine Fehlermeldung davon informiert, dass die gewünschte Adresse (IP:PORT) bereits verwendet wird.

3.1.2.3 IPv6



MDaemon erkennt per Voreinstellung, in welchem Umfang das verwendete Betriebssystem IPv6 unterstützt, und arbeitet im Dual-Stack-Betrieb, soweit das möglich ist. Ist der Dual-Stack-Betrieb nicht möglich, so überwacht MDaemon die IPv4- und IPv6-Adressen unabhängig voneinander.

IPv6

Die SMTP-/POP-/IMAP-Server von MDaemon...

... nehmen nur IPv4-Verbindungen an
Diese Option bewirkt, dass MDaemon nur IPv4-Verbindungen annimmt,

... nehmen nur IPv6-Verbindungen an
Diese Option bewirkt, dass MDaemon nur IPv6-Verbindungen annimmt,

... nehmen IPv4- und IPv6-Verbindungen an
Diese Option bewirkt, dass MDaemon sowohl IPv4- als auch IPv6-Verbindungen annimmt. MDaemon gibt hierbei den IPv6-Verbindungen den Vorzug vor IPv4-Verbindungen, soweit dies möglich ist. Diese Option ist per Voreinstellung aktiv.

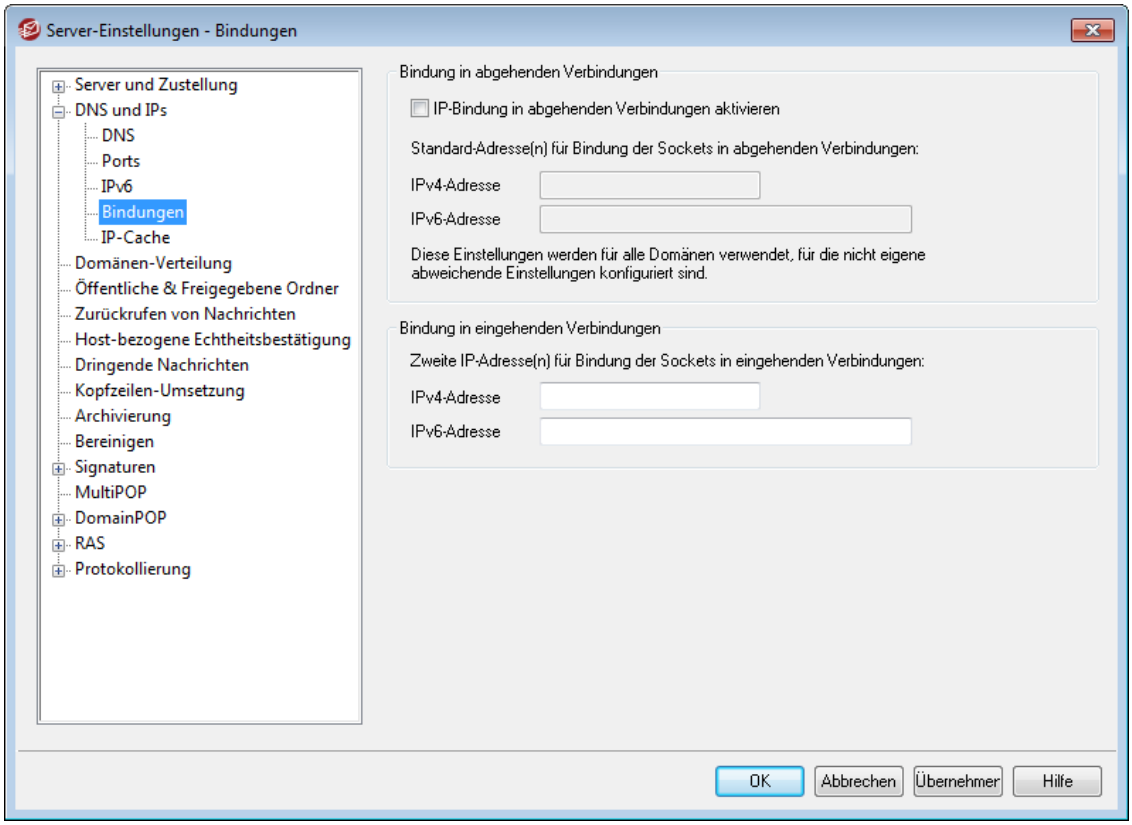
Abgehende Verbindungen zu IPv6-Hosts aufbauen, soweit möglich
Diese Option bewirkt, dass MDaemon abgehende Verbindungen, soweit möglich, zu IPv6-Hosts aufbaut.

Stellt MDaemon eine Verbindung zu einem IPv6-Host her, so muss MDaemon hierfür eine eigene lokale IPv6-Adresse nutzen. Diese IPv6-Adresse wird im Konfigurationsdialog Domänen-Manager » Hostname & IP 184 festgelegt. Falls erforderlich, können Sie eine Adresse für die Bindung abgehender Sockets im Konfigurationsdialog Bindungen 114 festlegen.

Siehe auch:

Bindungen 114
Domänen-Manager » Hostname & IP 184

3.1.2.4 Bindungen



Bindung in abgehenden Verbindungen

IP-Bindung in abgehenden Verbindungen aktivieren
Diese Option bewirkt, dass MDaemon bei abgehenden Verbindungen die Sockets immer an bestimmte IP-Adressen bindet. Bei Domänen, für die im Konfigurationsdialog Hostname & IP 184 die Option *Diese Domäne akzeptiert nur Verbindungen mit den oben angegebenen IP-Adressen* 184 aktiv ist, nutzt MDaemon die dort angegebenen IP-Adressen. Andernfalls nutzt MDaemon die *Standard-Adresse(n) für die Bindung der Sockets in abgehenden Verbindungen*, die in der folgenden Option konfiguriert werden können.

Standard-Adresse(n) für die Bindung der Sockets in abgehenden Verbindungen: IPv4-/IPv6-Adresse
An die hier angegebenen IP-Adressen werden die Sockets in abgehenden Verbindungen aller Domänen gebunden, für die nicht bereits im Konfigurationsdialog Hostname & IP 184 des Domänen-Managers abweichende Adressen angegeben sind.

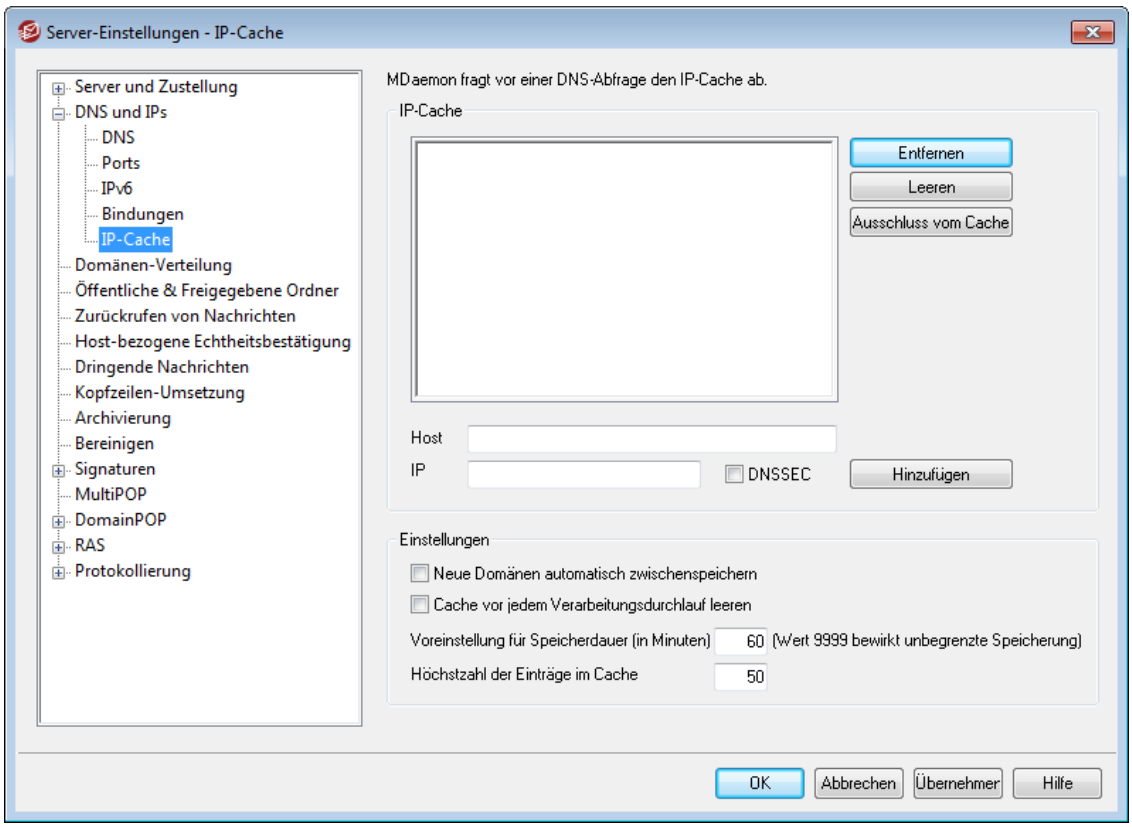
Bindung in eingehenden Verbindungen

Zweite IP-Adresse(n) für Bindung der Sockets in eingehenden Verbindungen
Mithilfe dieser Option können Sie einen zweiten Satz IP-Adressen für die Bindung von Sockets in eingehenden Verbindungen 184 angeben.

Siehe auch:

Domänen-Manager » Hostname & IP 184
IPv6 113

3.1.2.5 IP-Cache



Um den Nachrichtenversand zu beschleunigen und die Verarbeitungszeit zu verringern, speichert ("cacht") MDaemon die IP-Adressen aller Gegenstellen zwischen, mit denen schon einmal eine Verbindung bestanden hat. Vor DNS-Abfragen wird zuerst der Zwischenspeicher ("Cache") durchsucht. Findet sich dort die gesuchte IP-Adresse zur fraglichen Domäne, so wird die DNS-Abfrage übersprungen, was erstaunliche Zeitersparnis bringen kann. Die Einstellungen dieses Konfigurationsdialogs steuern die Arbeitsweise des Zwischenspeichers. Sie können von hier aus auch Einträge hinzufügen und entfernen, die Nutzung von DNSSEC festlegen, eine Größenbegrenzung für den Zwischenspeicher festlegen und

bestimmen, wie lange die Einträge gespeichert bleiben. Sie erreichen diesen Konfigurationsdialog über den Menüeintrag "Einstellungen » Server-Einstellungen » IP-Cache".

IP-Cache

Host
Hier wird der Host angegeben, der dem IP-Cache hinzugefügt werden soll.

IP-Adresse
Hier wird die IP-Adresse zum soeben angegebenen Domänennamen angegeben.

DNSSEC
Um DNSSEC zu nutzen, aktivieren Sie diese Option.

Hinzufügen
Eine von Hand eingegebene Kombination aus Host und IP-Adresse wird mit einem Klick auf dieses Steuerelement in den Cache übernommen.

Entfernen
Um einen Eintrag aus dem Cache zu löschen, wählen Sie den Eintrag in der Liste aus, und klicken Sie dann auf dieses Steuerelement.

Leeren
Ein Klick auf dieses Steuerelement leert den Cache.

Ausschluss vom Cache
Durch Anklicken dieses Steuerelements wird eine Liste von Domänennamen und IP-Adressen aufgerufen, die MDaemon niemals in den Cache übernehmen soll.

Optionen

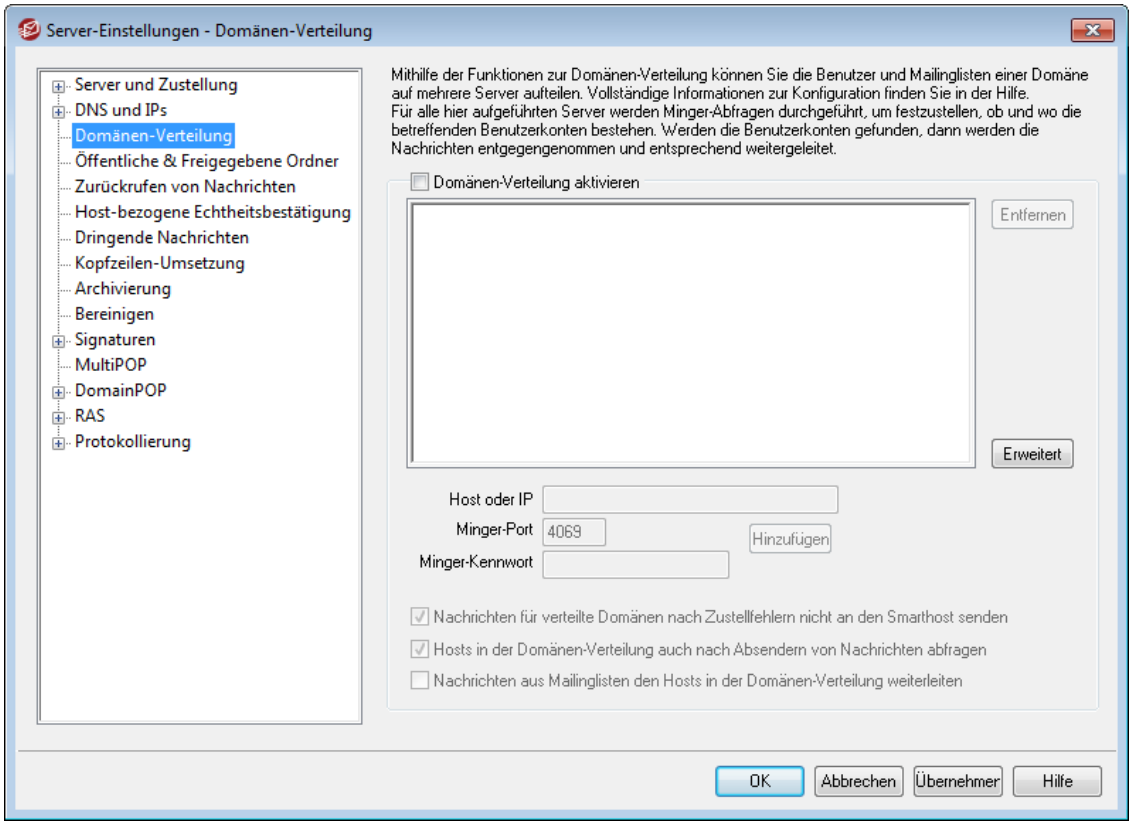
Neue Domänen automatisch zwischenspeichern
Diese Option legt fest, ob MDaemon den Cache automatisch beschicken soll. Wenn alle Domänen automatisch zwischengespeichert werden sollen, muss diese Option aktiv sein. Wenn der Systemverwalter die Einträge im Cache selbst bestimmen will, muss sie inaktiv sein.

Cache vor jedem Verarbeitungsdurchlauf leeren
Wenn diese Option aktiv ist, leert MDaemon den Cache beim Beginn eines jeden Verarbeitungsdurchlaufs. Damit beginnt jede Mail-Verbindung mit einem leeren Cache.

Voreinstellung für die Speicherdauer (in Minuten)
Hier wird vorgegeben, wie lange ein Eintrag im IP-Cache gehalten wird. Sobald der Eintrag die Speicherdauer überschritten hat, wird er durch MDaemon gelöscht. Wenn ein Eintrag unbegrenzt lang im Cache verbleiben soll, muss seine *Speicherdauer* auf 9999 eingestellt werden.

Höchstzahl der Cache-Einträge
Dieser Wert legt fest, wie groß der Cache werden darf. Sobald diese Grenze erreicht ist, fällt beim nächsten Neueintrag der älteste Eintrag aus dem Cache.

3.1.3 Domänen-Verteilung



Mithilfe der neuen Funktion Verteilte Domänen können die Nutzer einer Domäne beliebig über verschiedene Server verteilt werden. Dies ermöglicht die Nutzung von MDaemon-Servern an mehreren Standorten, an denen dieselben Domänennamen genutzt werden, aber unterschiedliche Nutzer aktiv sein sollen. Mithilfe der Funktion kann ein Teil der Benutzerkonten auf einem Server, ein anderer auf einem anderen Server oder mehreren anderen Servern angelegt werden. Die Server, auf die eine Domäne verteilt wird, lassen sich in einem neuen Konfigurationsdialog einrichten. Geht eine Nachricht für einen Nutzer einer solchen Domäne ein, und hat dieser Nutzer auf dem empfangenden Server kein Benutzerkonto, so werden die anderen hier konfigurierten Server per Minger 855 abgefragt, ob dort ein Benutzerkonto für den Empfänger besteht. Wird ein entsprechender Server gefunden, so wird die Nachricht entgegengenommen und weitergeleitet.

Sie können beispielsweise Niederlassungen an verschiedenen Orten so einrichten, dass alle Mitarbeiter eine E-Mail-Adresse haben, die auf "`@example.com`" endet. An jeder Niederlassung ist ein MDaemon-Server vorhanden, der nur einen Teil der E-Mail-Adressen für `example.com` bereit stellt und unmittelbar nur die Mitarbeiter versorgt, die ihren Dienstsitz an dieser Niederlassung haben. Jede Niederlassung wird dann für die Nutzung der Verteilten Domänen konfiguriert, so dass alle Nachrichten an die richtige Niederlassung geleitet werden.

Die Domänen-Verteilung stützt sich zur Prüfung von Adressen auf Minger 855; Minger muss daher auf allen beteiligten Servern richtig konfiguriert sein und die Abfragen ordnungsgemäß bearbeiten. Tritt während einer Minger-Abfrage dennoch ein Fehler auf, etwa, weil einer der angesprochenen Server vorübergehend nicht erreichbar ist, meldet MDaemon einen vorübergehenden Fehler 451, sodass der Server des Absenders später noch einmal versuchen kann, die Nachricht zuzustellen. Wurde eine Adresse erfolgreich überprüft, so wird das Ergebnis dieser Prüfung fünf Tage lang zwischengespeichert. MDaemon kann weitere Nachrichten an dieselbe Adresse

in diesem Zeitraum direkt annehmen und an den zuständigen Server leiten, ohne die Abfrage wiederholen zu müssen.

Falls dasselbe Benutzerkonto auf mehreren Servern angelegt wird, kann es zu Problemen kommen. MDaemon fragt daher vor der Erstellung eines jeden neuen Benutzerkontos alle anderen Server für die verteilten Domänen ab, ob dort ein entsprechendes Benutzerkonto bereits besteht.

Im Bereich Optionen[268] des Gateway-Editors steht die Einstellung "*Abfragen zur Minger-Prüfung lösen auch Abfragen in verteilten Domänen aus*" zur Verfügung. Mithilfe dieser Option können Sie MDaemon veranlassen, bei jeder durch einen Gateway ausgeführten Minger-Prüfung[259] auch alle Server abzufragen, auf denen verteilte Domänen liegen.

Domänen-Verteilung aktivieren
Diese Option aktiviert die Funktionen zur Domänen-Verteilung. Nach dem Aktivieren dieser Option müssen Sie weiter unten alle Hosts oder IP-Adressen eintragen, auf die sich die verteilten Domänen erstrecken. Sie müssen dann auch sicher stellen, dass Minger[855] aktiv und richtig konfiguriert ist, sodass alle Anfragen der Hosts zur Prüfung lokaler Adressen richtig beantwortet werden können.

Entfernen
Um einen Eintrag aus der Domänen-Verteilung zu entfernen, wählen Sie den Eintrag in der Liste aus, und klicken Sie auf dieses Steuerelement.

Erweitert
Durch Anklicken dieses Steuerelements können Sie eine Datei zur Bearbeitung öffnen. In dieser Datei können Sie die Domänennamen erfassen, die zur Nutzung der Domänen-Verteilung berechtigt sind. Falls diese Datei leer ist (dies entspricht der Voreinstellung), dann können alle Ihre Domänen die Domänen-Verteilung nutzen. Nähere Informationen können Sie den Anweisungen am Beginn der Datei entnehmen.

Host oder IP
Geben Sie in dieses Textfeld den Hostnamen oder die IP-Adresse ein, die für eine oder mehrere Ihrer Domänen in die Domänen-Verteilung einbezogen werden soll. You can append a colon and port (e.g. `mail.example.com:2525`) if you wish to use a specific, non-default port when sending SMTP messages to the host (this is not the same as the Minger port below).

Minger-Port
Hier wird der Port angegeben, auf dem der Minger-Server für diesen Host abgefragt werden soll. Die Voreinstellung ist 4069.

Minger-Kennwort (nicht zwingend erforderlich)
Falls der Host, den Sie gerade hinzufügen, für die Minger-Abfrage auch ein Kennwort verlangt, geben Sie dieses Kennwort hier ein. Minger-Dienste müssen zwar nicht unbedingt kennwortgeschützt sein, es empfiehlt sich aber, die Abfragen nur gegen Kennwort zuzulassen. Das Minger-Kennwort wird auch als Shared Secret für Minger bezeichnet.

Hinzufügen
Nachdem Sie Host oder IP, und ggf. das Kennwort, eingegeben haben, klicken Sie auf dieses Steuerelement, um den Eintrag der Liste der Hosts für die Domänen-Verteilung hinzuzufügen.

Eingehende Minger-Abfragen lösen Abfragen in verteilten Domänen aus
Diese Option bewirkt, dass eingehende Minger-Abfragen mit TRUE beantwortet werden, falls ein anderer Server im Netz der verteilten Domänen bestätigt, dass er die Nachricht annehmen wird. Der andere Server kann dies unter Umständen auch dann bestätigen, wenn er nicht selbst das lokale Postfach unterhält. Diese Option ist per Voreinstellung abgeschaltet.

Nachrichten für verteilte Domänen nach Zustellfehlern nicht an den Smarthost senden
Ist diese Option aktiv, und stellt MDaemon bei dem Versuch, eine Nachricht für eine verteilte Domäne zuzustellen, einen Fehler fest (etwa, weil der angesprochene Server in der Infrastruktur verteilter Domänen nicht erreichbar ist), so wird die E-Mail-Nachricht nicht an den Smarthost 97 gesendet, sondern sie verbleibt in der Warteschlange 864. Das Versenden solcher Nachrichten an einen Smarthost führt oft zu Endlosschleifen in der Nachrichtenzustellung. Diese Option ist per Voreinstellung aktiv.

Hosts in der Domänen-Verteilung auch nach Absendern von Nachrichten abfragen
Per Voreinstellung akzeptiert MDaemon Nachrichten von Benutzerkonten, die auf anderen Hosts in der Struktur der verteilten Domänen bestehen, wenn bestätigt ist, dass diese Benutzerkonten dort bestehen. Falls Sie für die Absender aus den SMTP-Befehlen MAIL keine Abfragen in den verteilten Domänen durchführen möchten, deaktivieren Sie diese Option.

Nachrichten aus Mailinglisten den Hosts in der Domänen-Verteilung weiterleiten
Diese Option ermöglicht es Ihnen, die Mailinglisten mit den Hosts in den verteilten Domänen zu teilen. Geht eine Nachricht für eine Mailingliste ein, so wird für jeden Host in den verteilten Domänen, der die Mailingliste ebenfalls unterhält, eine Kopie der Nachricht erstellt. Welche Hosts die Mailingliste allenfalls unterhalten, wird durch eine Abfrage festgestellt. Sobald die Mailserver ihre Kopien der Listennachrichten erhalten, stellen Sie diese an alle Listenmitglieder zu, die bei ihnen bestehen. Mailinglisten können so auf mehrere Server aufgeteilt werden, ohne dass hierbei der Funktionsumfang beeinträchtigt wird. Dieses Leistungsmerkmal ist nur nutzbar, wenn jeder Host in den verteilten Domänen in seiner Liste vertrauter IP-Adressen 521 die IP-Adressen der anderen Hosts führt. Ist dies nicht der Fall, so werden die Nachrichten unter Umständen mit der Meldung abgewiesen, dass der Absender nicht Mitglied der Mailingliste ist.

Siehe auch:

Minger 855
Domänen-Manager 181

3.1.4 Öffentliche & Freigegebene Ordner

MDaemon unterstützt die gemeinsame Nutzung ("Freigabe") sowohl von öffentlichen als auch von persönlichen IMAP-Ordnern. Öffentliche Ordner sind zusätzliche Ordner, die keinem bestimmten Benutzerkonto zugeordnet sind und daher mehreren IMAP-Benutzern zur Verfügung stehen können. Sie werden über den Konfigurationsdialog Verwaltung für öffentliche Ordner 309 verwaltet. Persönliche Ordner sind IMAP-

Ordner, die zu bestimmten MDaemon-Benutzerkonten gehören. Jedem freigegebenen IMAP-Ordner, egal ob öffentlich oder persönlich, muss eine Liste von MDaemon-Benutzern zugeordnet sein, und nur die Benutzer in dieser Zugriffsliste können durch MDaemon Webmail oder einen IMAP-Client auf den jeweiligen Ordner zugreifen.

IMAP-Benutzer sehen in der Liste ihrer persönlichen Ordner gleichzeitig die freigegebenen öffentlichen und persönlichen Ordner anderer Benutzer, auf die sie Zugriff erhalten haben. Mehrere Benutzer können sich so bestimmte Ordner teilen, wobei diese Ordner immer noch durch die individuellen Zugangsdaten geschützt sind. Außerdem bedeutet der Zugriff auf einen Ordner nicht notwendig, dass der Benutzer vollen Schreib-/Lesezugriff oder Administratorrechte hat. Einzelnen Benutzern können vielmehr individuelle Benutzerrechte zugewiesen werden, die sich in verschiedene Stufen gliedern. Einigen Benutzern kann beispielsweise gestattet werden, Nachrichten zu löschen, anderen wiederum nicht.

Sobald ein öffentlicher oder persönlicher IMAP-Ordner angelegt wurde, können im Inhaltsfilter Kriterien definiert werden, nach welchen bestimmte Nachrichten in diesem Ordner abgelegt werden. Es kann beispielsweise nützlich sein, eine Regel zu definieren, nach der Nachrichten mit der Adresse `support@example.com` in der Kopfzeile `TO:` in den öffentlichen Ordner Support verschoben werden. Die Aktionen des Inhaltsfilters 651 "`Nachricht in öffentliche Ordner verschieben...`" und "`Nachricht in Ordner kopieren...`" ermöglichen diese Vorgehensweise. Bei freigegebenen persönlichen Ordnern können die persönlichen IMAP-Filter 736 des Benutzers dazu verwendet werden, um bestimmte Nachrichten in die Ordner zu verschieben. Zusätzlich zu Inhaltsfilter und IMAP-Filtern kann ein bestimmtes Benutzerkonto mit einem freigegebenen Ordner verknüpft werden, sodass Nachrichten an die "Adresse für Veröffentlichung" automatisch in dem freigegebenen Ordner abgelegt werden. An die "Adresse für Veröffentlichung", die zu diesem Benutzerkonto gehört, dürfen aber nur zum Veröffentlichen ("post") berechtigte Benutzer Nachrichten senden.

Zusätzlichen Komfort bietet eine Erweiterung des Editors für Mailinglisten. Er enthält einen Konfigurationsdialog für Öffentliche Ordner 298, der es erlaubt, einer Mailingliste einen bestimmten öffentlichen Ordner zuzuweisen. Diese Funktion bewirkt, dass eine Kopie aller Listennachrichten in dem angegebenen öffentlichen Ordner abgelegt wird. Alle öffentlichen Ordner werden im Verzeichnis `\Public Folders\` innerhalb der Verzeichnisstruktur von MDaemon abgelegt.

Dokumentenordner für Webmail

Die Webmail-Designs unterstützen jetzt die Freigabe und gemeinsame Nutzung von Dokumenten mithilfe von Dokumentenordnern. Die Dokumentenordner verfügen, wie andere freigegebene Ordner auch, über vollständige Unterstützung für Zugriffskontrolllisten (ACL) 311, mit deren Hilfe die Berechtigungen und Freigabeeinstellungen konfiguriert werden können. Das System kann zur Freigabe beliebiger Dateien genutzt werden. Benutzer von Webmail können mithilfe der in Webmail integrierten Hilfsmittel die Dokumente in ihre Dokumentenordner hochladen. Wird das Design LookOut in Browsern genutzt, die das Drag-and-Drop-API aus HTML5 unterstützen, wie etwa Chrome und Firefox, so können die Dateien vom Desktop in das Browserfenster gezogen werden, um sie als Dokumente hochzuladen. Die Dateinamen der Dokumente können durchsucht werden. An neu erstellte Nachrichten können ausgewählte Dokumente angehängt werden.

Sie können die Leistungsmerkmale für Dokumentenordner, wie auch andere gemeinsam genutzte und freigegebene Ordner, nach Domänen und nach Benutzern getrennt aktivieren und deaktivieren. Sie müssen hierzu für Einstellungen auf Domänen-Ebene die Datei `\WorldClient\Domains.ini` und für Einstellungen auf

Benutzerebene die betreffende Datei `\Users\..\WC\user.ini` mit einem Texteditor bearbeiten. Sie können Standard-Einstellungen festlegen; Sie können ferner auch benutzerdefinierte Einstellungen festlegen, die die Standard-Einstellungen überschreiben. Ein Beispiel hierzu:

```
[Default:UserDefaults]
DocumentsFolderName=Dokumente
EnableDocuments=Yes ("Ja")

[example.com:UserDefaults]
DocumentsFolderName=Beispiel-Dokumente
EnableDocuments=Yes ("Ja")

[superControllingDomain.gov:UserDefaults]
EnableDocuments=No ("Nein")
EnableCalendar=No ("Nein")
EnableNotes=No ("Nein")
EnableTasks=No ("Nein")
```

Festlegen der höchstzulässigen Dateigröße

Sie können die zulässige Größe für die einzelnen Dateien begrenzen, die die Benutzer in die Dokumentenordner hochladen können. Fügen Sie hierzu der Datei `domains.ini` den Eintrag `MaxAttachmentSize=<Größe in KB>` hinzu. Per Voreinstellung beträgt der Wert 0; hierdurch ist die Größe unbegrenzt.

Sperren und Zulassen bestimmter Dateitypen

Um zu verhindern, dass bestimmte Dateitypen in die Dokumentenordner hochgeladen werden, fügen Sie der Datei `domains.ini` den Eintrag `BlockFileTypes=` hinzu. In diesem Eintrag führen Sie die gesperrten Dateiendungen auf, und trennen Sie mehrere Endungen durch Kommata oder Leerzeichen. Ein Beispiel hierzu: "`BlockFileTypes=exe dll js`".

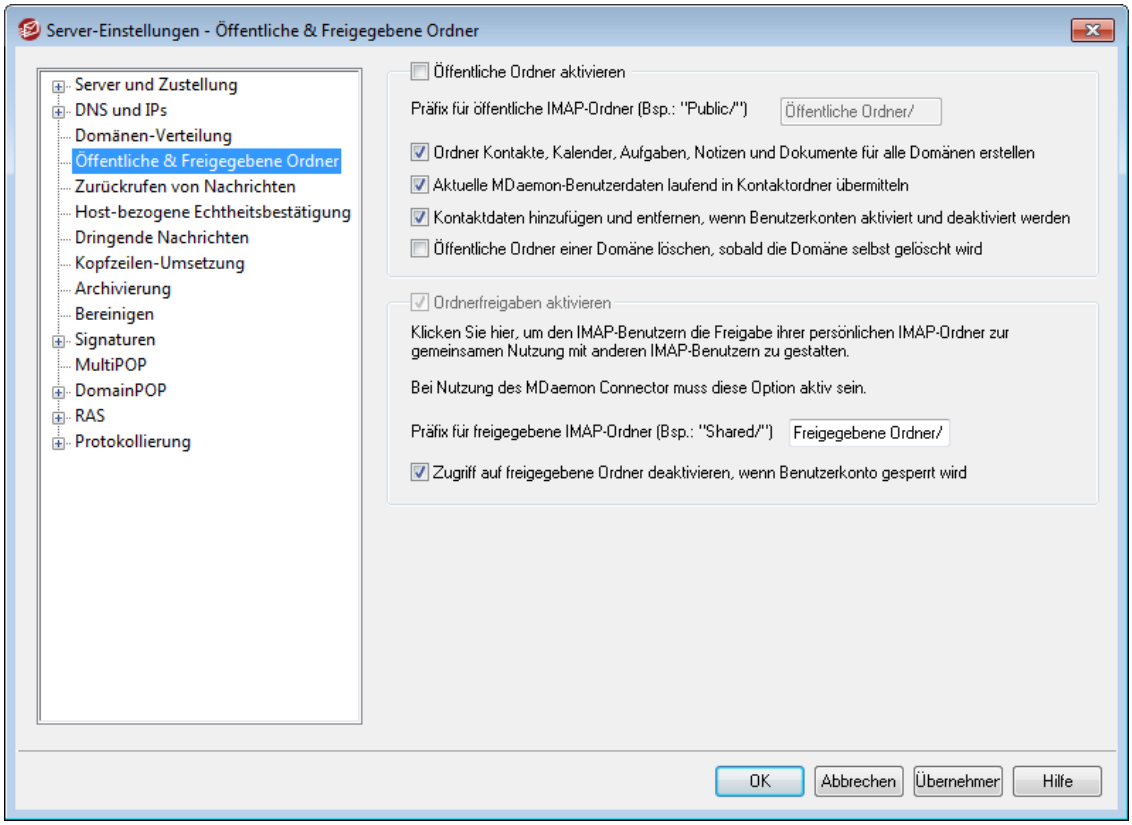
Um nur bestimmte Dateitypen zum Hochladen in die Dokumentenordner zuzulassen und alle anderen Dateiendungen zu sperren, fügen Sie der Datei `domains.ini` den Eintrag `AllowFileTypes=` hinzu. In diesem Eintrag führen Sie die zugelassenen Dateiendungen auf, und trennen Sie mehrere Endungen durch Kommata oder Leerzeichen. Ein Beispiel hierzu: "`AllowFileTypes=jpg png doc docx xls xlsx`".

Sind beide Einträge vorhanden, so gehen die gesperrten Dateiendungen der zugelassenen Dateiendungen vor. Eine Dateiendung, die in beiden Listen eingetragen ist, wird daher gesperrt. Ist ein Eintrag vorhanden, der keine Dateiendungen enthält (Leereintrag), so wird dieser Eintrag nicht berücksichtigt. Den Dateiendungen kann ein Punkt vorangestellt werden (z.B. `.exe .dll`); dies ist aber nicht erforderlich.

Siehe auch:

Öffentliche & Freigegebene Ordner 122
Verwaltung für öffentliche Ordner 309
Zugriffskontrollliste (ACL) 311
Benutzerkonten-Editor » Freigegebene Ordner 742
Mailingliste » Öffentlicher Ordner 298

3.1.4.1 Öffentliche & Freigegebene Ordner



Sie erreichen den Konfigurationsdialog Öffentliche & Freigegebene Ordner durch Anklicken von "Einstellungen » Server-Einstellungen » Öffentliche & Freigegebene Ordner".

Öffentliche Ordner aktivieren

Mit dieser Option wird IMAP-Benutzern der Zugriff auf die öffentlichen Ordner gestattet. Die Benutzer können auf diese Ordner nach Maßgabe der Rechte zugreifen, die für jeden Ordner im Konfigurationsdialog Verwaltung für öffentliche Ordner 309 festgelegt wurden. So lange diese Option nicht aktiv ist, werden die öffentlichen Ordner den Benutzern nicht angezeigt.

Präfix für öffentliche IMAP-Ordner (Bsp.: "Public/")
Die Namen öffentlicher Ordner beginnen mit einem Vorspanntext ("Präfix") von bis zu zwanzig Zeichen Länge, beispielsweise "#" oder "Public/". Die Benutzer können so in ihrem E-Mail-Client die öffentlichen Ordner leicht von den persönlichen unterscheiden. Hier wird der Text angegeben, mit dem öffentliche Ordner gekennzeichnet werden.

Ordner Kontakte, Kalender, Aufgaben, Journal und Notizen für alle Domänen erstellen
Diese Option stellt sicher, dass die genannten Ordner für alle Domänen existieren. Wird in MDaemon eine Domäne 181 hinzugefügt, so werden diese Ordner ebenfalls automatisch angelegt.

Aktuelle MDaemon-Benutzerdaten laufend in Kontaktordner übermitteln
Diese Option bewirkt, dass MDaemon die Kontaktordner immer mit den aktuellen Daten der MDaemon-Benutzer abgleicht.

Kontaktdaten hinzufügen und entfernen, wenn Benutzerkonten aktiviert und deaktiviert werden
Per Voreinstellung werden Benutzerkonten aus dem Ordner öffentliche Kontakte der jeweiligen Domäne entfernt, wenn sie deaktiviert werden. Werden die Benutzerkonten wieder aktiviert, so werden sie den Kontakten wieder hinzugefügt. Diese Option ist per Voreinstellung aktiv. Sie verhindert, dass deaktivierte Benutzerkonten in der Funktion Autovervollständigen von Webmail erscheinen.

Öffentliche Ordner einer Domäne löschen, sobald die Domäne selbst gelöscht wird
Diese Option bewirkt, dass MDaemon die öffentlichen Ordner einer Domäne löscht, sobald auch die Domäne selbst gelöscht wird.

Ordnerfreigaben aktivieren

Diese Option gestattet es den IMAP-Benutzern, ihre IMAP-Ordner zur gemeinsamen Nutzung freizugeben. Die Benutzer, die auf die Ordner Zugriff haben sollen, und ihre Rechte, werden für jeden Ordner im Konfigurationsdialog Freigegebene Ordner 742 des Benutzerkonten-Editors festgelegt (Benutzerkonten » Benutzerkonten-Manager » [Benutzerkonto] » Freigegebene Ordner). So lange diese Option nicht aktiv ist, dürfen die Benutzer ihre Ordner nicht zur gemeinsamen Nutzung freigeben. Der Konfigurationsdialog für freigegebene Ordner erscheint dann auch nicht im Benutzerkonten-Editor.

Bei Nutzung des MDaemon Connectors 385 ist diese Option stets aktiv und kann nicht abgeschaltet werden. Die Option lässt sich nicht abschalten, weil die Freigabe von Ordnern zur gemeinsamen Nutzung für die Funktion des Outlook Connectors erforderlich ist.

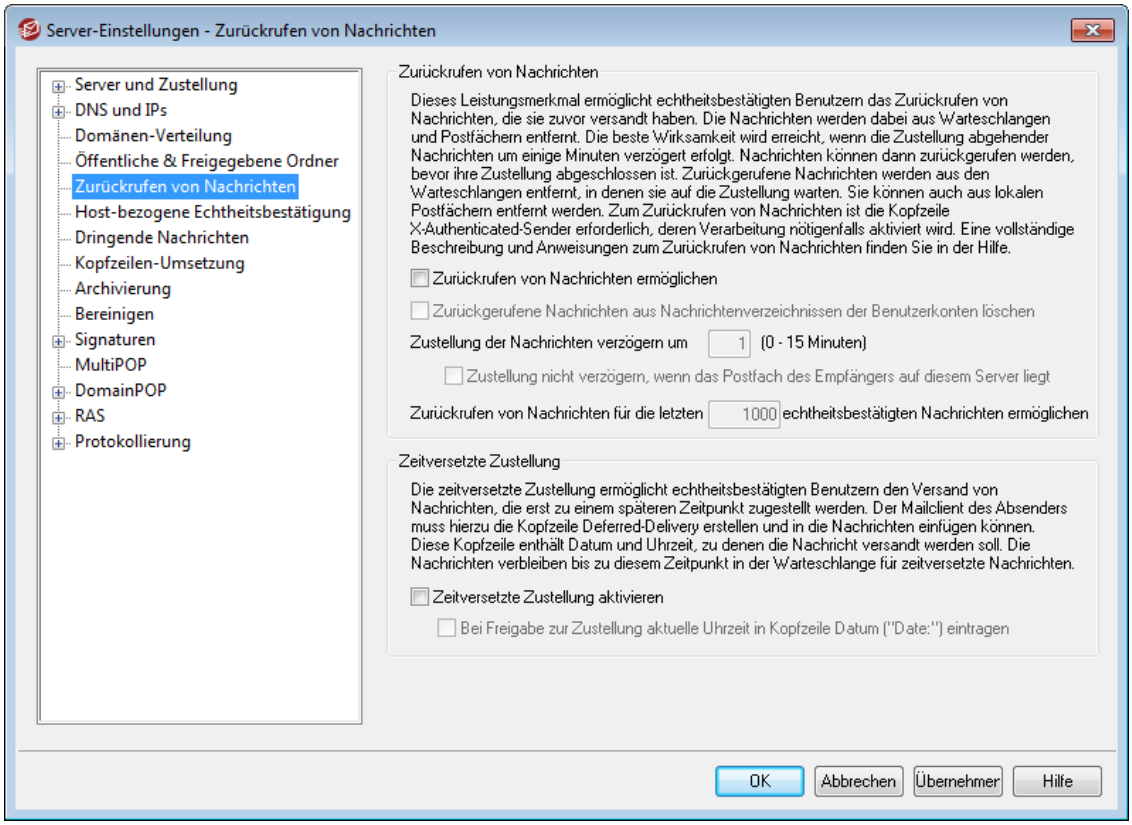
Präfix für freigegebene IMAP-Ordner (Bsp.: "Shared/")
Die Namen freigegebener persönlicher Ordner beginnen mit einem Vorspanntext ("Präfix") von bis zu zwanzig Zeichen Länge, beispielsweise "#" oder "Shared/". Die Benutzer können so in ihrem E-Mail-Client die freigegebenen Ordner leicht von ihren eigenen unterscheiden. Hier wird der Text angegeben, mit dem freigegebene persönliche Ordner gekennzeichnet werden.

Zugriff auf freigegebene Ordner deaktivieren, wenn Benutzerkonto gesperrt wird
Per Voreinstellung gestatten die MDaemon-Serverdienste IMAP, Webmail und ActiveSync keinen Zugriff auf freigegebene Ordner gesperrter Benutzerkonten. Falls Sie den Zugriff auf die freigegebenen Ordner auch für die Freigaben gesperrter Benutzerkonten gestatten wollen, aktivieren Sie diese Option..

Siehe auch:

Öffentliche Ordner - Übersicht 119
Verwaltung für öffentliche Ordner 309
Zugriffskontrollliste (ACL) 311
Benutzerkonten-Editor » Freigegebene Ordner 742
Mailinglisten » Öffentlicher Ordner 298

3.1.5 Zurückrufen von Nachrichten



Zurückrufen von Nachrichten

MDaemon verfügt über Leistungsmerkmale, mit deren Hilfe die Zustellung solcher Nachrichten, die durch echtheitsbestätigte lokale Benutzer versandt werden, um eine Zeitspanne zwischen 0 und 15 Minuten verzögert werden kann. Während dieser Zeitspanne können die Absender versuchen, die Zustellung einer durch sie versandten Nachricht noch zu verhindern. Während dieser Zeitspanne werden die Nachrichten in eine besondere Warteschlange für zeitversetzte Zustellung eingestellt. Sie erreichen nicht direkt die Eingangs-Warteschlange. Die Dateinamen der Nachrichten in der Warteschlange für zeitversetzte Zustellung enthalten das Datum und den Zeitpunkt, zu dem die Nachrichten die Warteschlange verlassen. MDaemon prüft diese Warteschlange im Minutentakt und verschiebt die Nachrichten, für die der genannte Zeitpunkt erreicht ist, in die Eingangs-Warteschlange. Von dort aus werden die Nachrichten normal verarbeitet und zugestellt, und hierfür gelten die allgemein konfigurierten Regeln. Die Aktivität wird auf der Registerkarte und im Protokoll Routing protokolliert.

Sie können die Verzögerung auf den Wert "0" setzen. Diese Vorgehensweise erhöht aber die Wahrscheinlichkeit, dass Nachrichten bereits zugestellt sind, wenn sie die Benutzer zurückrufen wollen. Empfehlenswert ist daher ein Wert von mindestens 1 oder 2 Minuten. Solche Werte lassen den Benutzern genügend Zeit dafür, festzustellen, dass sie eine Nachricht zurückrufen wollen, und die entsprechende Anforderung zu senden, und sie lassen MDaemon genügend Zeit, um die Anforderung zu verarbeiten. MDaemon kann zurückgerufenen Nachrichten aus den Extern-Warteschlangen entfernen. Da bei der Verarbeitung dieser Extern-Warteschlangen ohnehin Verzögerungen auftreten können, halten manche Administratoren eine zusätzliche Verzögerung unter Umständen für überflüssig.

Zurückrufen einer Nachricht

Den Benutzern stehen mehrere Möglichkeiten für das Zurückrufen einer Nachricht zur Verfügung.

1. Um eine Nachricht zurückzurufen, kann sich der Benutzer an Webmail anmelden und das Steuerelement *Zurückrufen* anklicken. Dieses Steuerelement erscheint, wenn der Benutzer eine kürzlich versandte Nachricht im Ordner für gesendete Objekte betrachtet. Klickt der Benutzer dieses Steuerelement an, bevor die Zeitspanne abgelaufen ist, dann sendet Webmail eine Steuernachricht ("RECALL-Nachricht") an MDaemon.
2. Der Benutzer kann eine Nachricht an das MDaemon-Systemkonto senden und das Wort `RECALL` in die Betreffzeile setzen. Hierdurch wird jeweils die letzte versandte Nachricht zurückgerufen. Andere Nachrichten sind davon nicht betroffen.
3. Der Benutzer kann die gesendete und zurückzurufende Nachricht in einem verwendeten Mailclient aufsuchen und sie als Dateianlage an das Systemkonto (z.B. `mdaemon@example.com`) weiterleiten, wobei er in die Betreffzeile der Weiterleitungsnachricht `RECALL` eintragen muss.
4. Der Benutzer kann die Kopfzeilen der zurückzurufenden Nachricht betrachten und den Inhalt der Kopfzeile für die Nachrichten-ID ("`Message-ID: <Wert der Nachrichten-ID>`") kopieren. Der Benutzer erstellt dann eine neue Nachricht und setzt "`RECALL Message-ID: <Wert der Nachrichten-ID>`" (ohne Anführungs- und Schlusszeichen) in die Betreffzeile.

In allen Fällen sendet MDaemon dem Absender eine Information darüber per E-Mail zu, ob die Nachricht erfolgreich zurückgerufen wurde. Sobald eine Nachricht erfolgreich zurückgerufen wurde, löscht MDaemon die Nachricht aus der Eingangs-Warteschlange und behandelt sie damit so, wie wenn sie nie versandt worden wäre. Ist die Option *Zurückgerufene Nachrichten aus Nachrichtenverzeichnissen der Benutzerkonten löschen* aktiv, so versucht MDaemon auch, die Nachricht aus den Nachrichten-Ordnern der lokalen Benutzer zu löschen, denen die Nachricht vielleicht bereits zugestellt wurde. Nachrichten, die an mehrere Empfänger versandt wurden, werden gesammelt durch dieselbe Anforderung zurückgerufen. Um die Sicherheit zu erhöhen und zu verhindern, dass Benutzer Nachrichten zurückrufen, die sie selbst gar nicht versandt haben, ist das Zurückrufen von Nachrichten nur möglich, wenn die Kopfzeile `X-Authenticated-Sender` vorhanden ist. Die Option zum Deaktivieren dieser Kopfzeile 500 bleibt daher wirkungslos, wenn die Leistungsmerkmale zum Zurückrufen von Nachrichten aktiv sind.

Zurückrufen von Nachrichten

Zurückrufen von Nachrichten ermöglichen
Diese Option ermöglicht das Zurückrufen von Nachrichten. Sie ist per Voreinstellung abgeschaltet.

Zurückgerufene Nachrichten aus Nachrichtenverzeichnissen der Benutzerkonten löschen
Diese Option bewirkt, dass zurückgerufene Nachrichten aus den Nachrichtenverzeichnissen der lokalen MDaemon-Benutzerkonten gelöscht werden, falls die Nachrichten bereits zugestellt waren, bevor sie zurückgerufen wurden. Diese Option kann dazu führen, dass Nachrichten aus

den lokalen Mailclients und den mobilen Endgeräten verschwinden. Diese Option ist per Voreinstellung aktiv.

Zustellung der Nachrichten verzögern um XX (0-15 Minuten)
Diese Option bestimmt die Zeitdauer, für die MDaemon Nachrichten von echtheitsbestätigten lokalen Benutzern in der Warteschlange für zeitversetzte Zustellung hält. Geht während dieser Zeit eine RECALL-Nachricht ein, so löscht MDaemon die dadurch zurückgerufene Nachricht, bevor Zustellversuche unternommen werden. Die Zeitdauer kann 0 bis 15 Minuten betragen. Per Voreinstellung beträgt sie 1 Minute.

Zustellung nicht verzögern, wenn das Postfach des Empfängers auf diesem Server liegt
Diese Option bewirkt, dass die Zustellung dann nicht verzögert wird, wenn die Benutzerkonten und Postfächer von Absender und Empfänger auf demselben MDaemon-Server bestehen. Beachte: Wenn die Option "*Zurückgerufene Nachrichten aus Nachrichtenverzeichnissen der Benutzerkonten löschen*" weiter oben aktiv ist, dann können Nachrichten auch dann noch zurückgerufen und aus den Postfächern der Empfänger gelöscht werden, wenn sie bereits zugestellt sind.

Zurückrufen von Nachrichten für die letzten [xx] echtheitsbestätigten Nachrichten ermöglichen
Diese Option bestimmt die Anzahl der letzten Nachrichten echtheitsbestätigter lokaler Benutzer, deren Nachrichten-IDs und Speicherorte MDaemon speichert. Das Zurückrufen von Nachrichten ist nur für solche Nachrichten möglich, die hierdurch erfasst sind. Für Nachrichten, die nicht mehr durch diese Option erfasst sind, ist ein Zurückrufen nicht möglich. Bei Nutzung der Option "*Zurückgerufene Nachrichten aus Nachrichtenverzeichnissen der Benutzerkonten löschen*" weiter oben ist es in Verbindung mit dieser Option möglich, Nachrichten direkt aus den Postfächern der Benutzer zurückzurufen, auch wenn sie schon zugestellt wurden. Per Voreinstellung beträgt der Wert für diese Option 1000 Nachrichten.

Zeitversetzte Zustellung

Das Leistungsmerkmal zeitversetzte Zustellung ermöglicht echtheitsbestätigten Clients den Versand von Nachrichten, die erst zu einem späteren Zeitpunkt zugestellt werden. Das Leistungsmerkmal ist über Webmail nutzbar; der Benutzer kann hier auf "Später senden" klicken und Datum und Uhrzeit für den Versand der Nachricht festlegen. Nachrichten, für die die zeitversetzte Zustellung aktiv ist, enthalten die Kopfzeile `Deferred-Delivery`, in der Datum und Uhrzeit für den Versand erfasst sind. Ist die Option zum Zurückrufen von Nachrichten aktiv, und geht eine Anforderung ein, eine noch nicht zugestellte Nachricht mit zeitversetzter Zustellung zurückzurufen, so versucht MDaemon, die zurückgerufene Nachricht aus den Warteschlangen zu entfernen.

Zeitversetzte Zustellung aktivieren
Diese Option gestattet es echtheitsbestätigten Clients, die Kopfzeile `Deferred-Delivery` zu nutzen, um den Zeitpunkt des Versands für Nachrichten festzulegen. Ist diese Option aktiv, so können Webmail-Benutzer in den Designs WorldClient und LookOut die Option **Später senden** nutzen. Diese Option ist per Voreinstellung abgeschaltet.

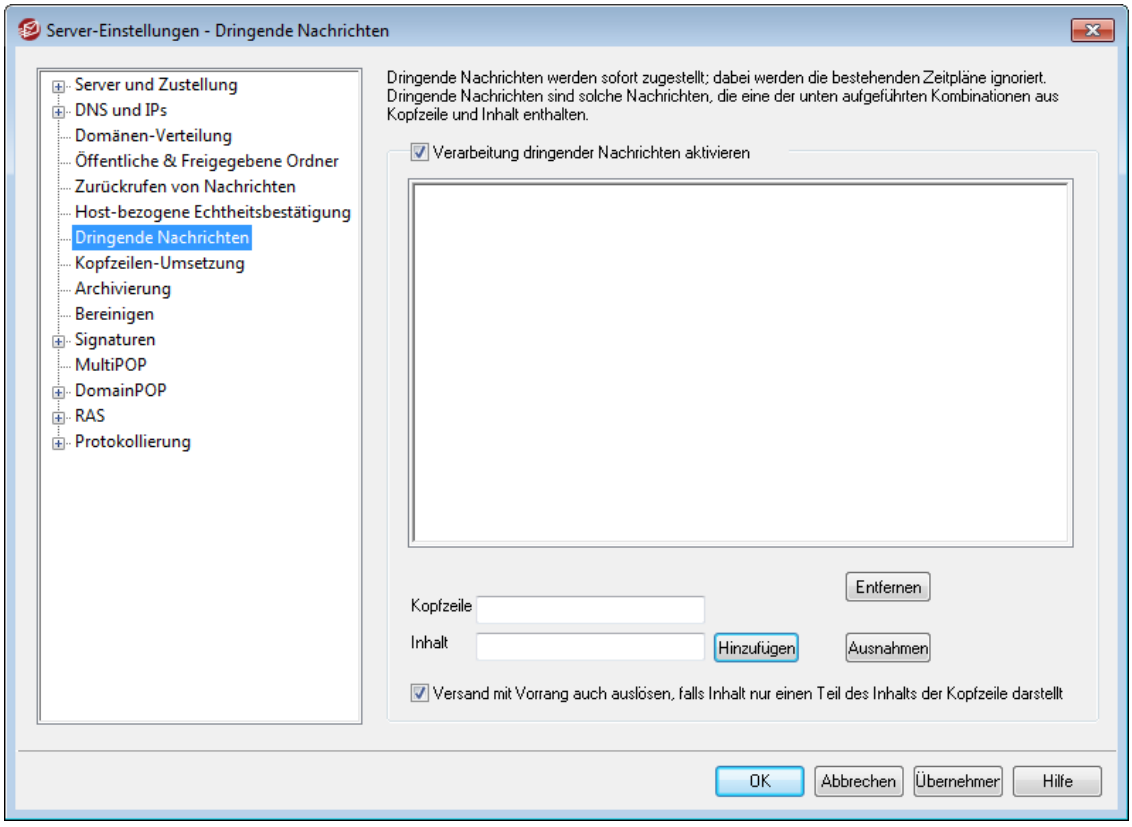
Bei Freigabe zur Zustellung aktuelle Uhrzeit in Kopfzeile Datum ("Date:") eintragen
Diese Option bewirkt, dass bei Freigabe einer Nachricht aus der Warteschlange für zeitversetzte Zustellung der Inhalt der Kopfzeile "Date": (Datum/Uhrzeit) durch das jeweils aktuelle Datum und die jeweils aktuelle Uhrzeit ersetzt wird. Diese Option ist per Voreinstellung aktiv.

3.1.6 Host-bezogene Echtheitsbestätigung

Host-bezogene Echtheitsbestätigung

Mithilfe dieses Konfigurationsdialogs können Sie Benutzernamen, Kennwörter und Ports für beliebige Hosts konfigurieren. Sendet MDaemon Nachrichten über SMTP an einen hier erfassten Host, so nutzt MDaemon die für den Host gespeicherten Zugangsdaten zur Echtheitsbestätigung. Diese Zugangsdaten dienen als Ausweichdaten und werden nur dann verwendet, wenn für den jeweiligen Vorgang keine besonders konfigurierten Zugangsdaten zur Verfügung stehen. Ein Beispiel hierzu: Wenn Sie Anmeldenamen und Kennwort in der Konfiguration für die Weiterleitung von Nachrichten im Benutzerkonten-Editor konfigurieren,dann werden für Weiterleitungen die dort konfigurierten Anmeldedaten genutzt. Sie gehen den hier etwa konfigurierten Anmeldedaten vor. Dieses Leistungsmerkmal arbeitet nur mit Hostnamen, nicht aber mit IP-Adressen.

3.1.7 Dringende Nachrichten



Sie erreichen den Konfigurationsdialog für dringende Nachrichten über den Menüeintrag "Einstellungen » Server-Einstellungen » Dringende Nachrichten". Die folgenden Einstellungen bestimmen, welche Nachrichten auf Ihrem System als dringend behandelt werden sollen. Dringende Nachrichten werden unabhängig vom

Zeitplan und den Verarbeitungsintervallen sofort zugestellt. MDaemon untersucht die neu eintreffenden Nachrichten auf Kombinationen aus bestimmten Kopfzeilen und Inhalten, die hier angegeben werden. Nachrichten mit solchen Kopfzeilen werden als dringend behandelt und sofort zugestellt.

Verarbeitung dringender Nachrichten aktivieren

Verarbeitung dringender Nachrichten aktivieren
Um die sofortige Zustellung dringender Nachrichten zu aktivieren und MDaemon nach dringenden Nachrichten suchen zu lassen, muss diese Option aktiv sein.

Kopfzeile
Der zu suchende Name der Kopfzeile wird ohne den abschließenden Doppelpunkt hier angegeben.

Inhalt
Hier muss der Inhalt der soeben angegebenen Kopfzeile angegeben werden. Nur, wenn beide Texte gefunden werden, wird die Nachricht als dringend behandelt.

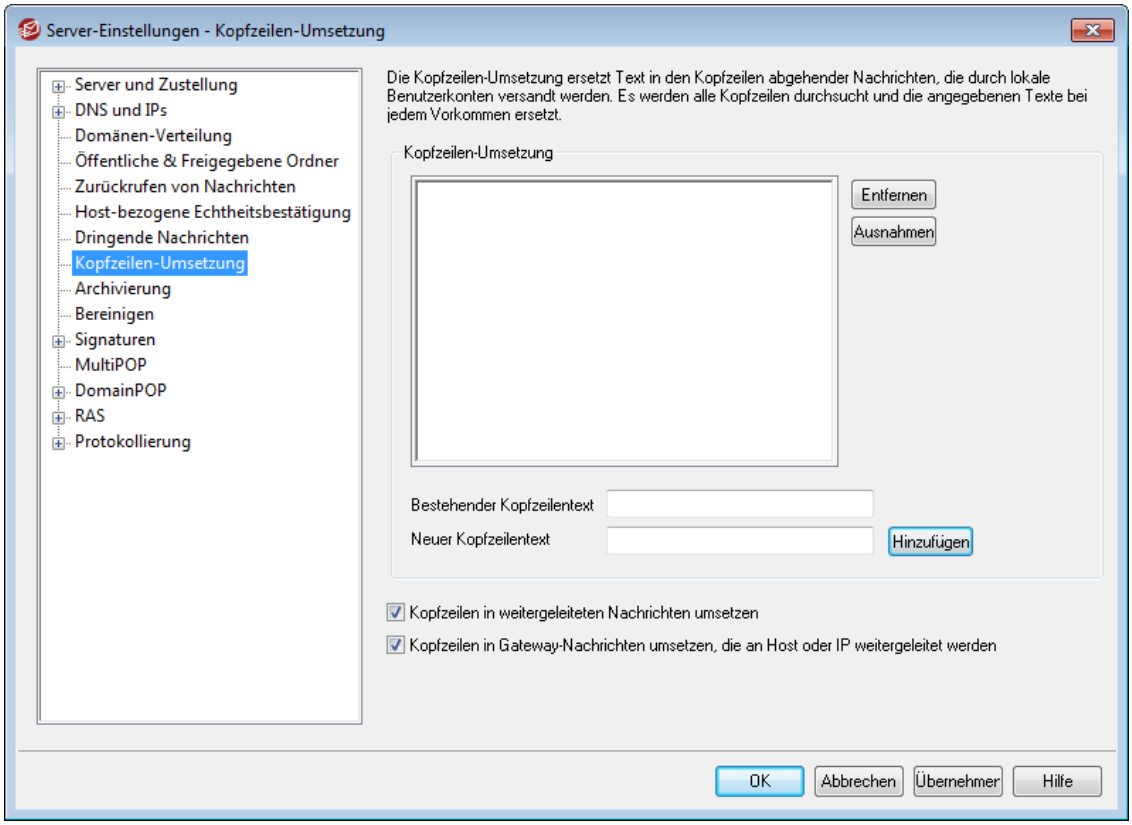
Versand mit Vorrang auch auslösen, falls Inhalt nur einen Teil des Inhalts der Kopfzeile darstellt
Diese Funktion kann aktiviert werden, wenn es für den Versand als dringend genügen soll, dass der im Feld "Inhalt" angegebene Text nur ein Teil des tatsächlichen Inhalts der Kopfzeile ist. Beispielsweise kann ein Eintrag für die Kopfzeile "`To`" mit dem Inhalt "`Chef`" angelegt werden. Dann würde jede Nachricht, die "`Chef@irgendwo`" enthält, als dringend behandelt werden. Wird der Eintrag ohne diese Option angelegt, muss der Inhalt der Kopfzeile dem vorgegebenen Text genau entsprechen, nur teilweise Übereinstimmung reicht nicht.

Hinzufügen
Nachdem die Informationen zu Kopfzeile und Inhalt angegeben und, falls gewünscht, die Option für Teilübereinstimmung ausgewählt ist, wird der neue Eintrag hiermit der Liste hinzugefügt.

Entfernen
Hiermit wird der jeweils gewählte Eintrag aus der Liste der Kopfzeilen-/Inhaltspaare für dringende Nachrichten gelöscht.

Ausnahmen
Um noch größere Flexibilität zu erreichen, können hier Kombinationen aus Kopfzeile und Inhalt angegeben werden, die als Ausnahme zu den übrigen Einstellungen für die Verarbeitung dringender Nachrichten behandelt werden sollen.

3.1.8 Kopfzeilen-Umsetzung



Die Kopfzeilen-Umsetzung kann Zeichenketten in den Kopfzeilen solcher Nachrichten ändern, die von einer lokalen Domäne an einen externen Empfänger versandt werden. Sie geben hierzu den Text an, nach dem gesucht werden soll, und Sie bestimmen, wie er zu ändern ist. MDaemon prüft dann alle Kopfzeilen der jeweiligen Nachricht und führt die Änderungen durch. Sie können auch Kopfzeilen angeben, die MDaemon **nicht** ändern darf (etwa die Betreffzeile oder "Received:"-Kopfzeilen). Sie können solche Ausnahmen durch Anklicken des Steuerelements *Ausnahmen* in diesem Konfigurationsdialog eintragen.

Die Kopfzeilen-Umsetzung wird für Konfigurationen benötigt, bei denen der lokale Domänenname frei erfunden ist, also etwa nicht registriert ist, oder sich sonst von dem Domänennamen unterscheidet, der in abgehenden Nachrichten erscheinen muss. In solchen Fällen kann die Kopfzeilen-Umsetzung beispielsweise dazu genutzt werden, den Text "`@lokaledomaene`" to "`@externedomaene`" zu ändern.

Kopfzeilen-Umsetzung

Diese Liste zeigt alle Textblöcke, nach denen MDaemon in abgehenden Nachrichten sucht, und die Textblöcke, durch welche sie ersetzt werden, falls eine Übereinstimmung gefunden wird.

Entfernen

Um einen Umsetzer aus der Liste zu entfernen, wählen Sie den Umsetzer in der Liste aus, und klicken Sie dann auf dieses Steuerelement.

Ausnahmen

Durch Anklicken dieses Steuerelements rufen Sie den Editor für die Ausnahmen von der Kopfzeilen-Umsetzung 130 auf. Dort werden Kopfzeilen angegeben, bei der Umsetzung nicht bearbeitet werden sollen.

Bestehender Kopfzeilentext
Hier muss der zu suchende und zu ersetzende Text, der bei allen abgehenden Nachrichten ersetzt werden soll, eingetragen werden.

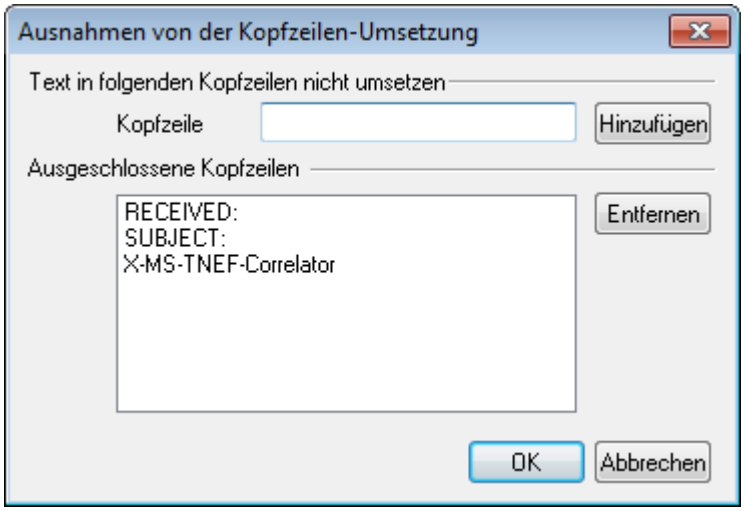
Neuer Kopfzeilentext
Dieser Text wird anstelle des im Feld *Bestehender Kopftext* eingetragenen Textes eingesetzt.

Hinzufügen
Durch Anklicken dieses Steuerelements fügen Sie die beiden Texte der Liste der Kopfzeilen-Umsetzer hinzu.

Kopfzeilen in weitergeleiteten Nachrichten umsetzen
Falls die Kopfzeilen-Umsetzung auch bei solchen Nachrichten gewünscht wird, die aus einer lokalen Domäne automatisch an eine externe Domäne weitergeleitet werden, muss diese Option gesetzt werden.

Kopfzeilen in Gateway-Nachrichten umsetzen, die an Host oder IP weitergeleitet werden
Diese Option bewirkt, dass die Kopfzeilen durch Domänen-Gateways weitergeleiteten Nachrichten ebenfalls umgesetzt werden. Weitere Informationen hierzu finden Sie in der Beschreibung des Abschnitts Weiterleitung 263 für den Gateway-Editor.

3.1.8.1 Ausnahmen von der Kopfzeilen-Umsetzung



Text in folgenden Kopfzeilen nicht umsetzen

Kopfzeile
Geben Sie hier die Kopfzeilen an, die von den Funktionen zur Kopfzeilen-Umsetzung 129 ausgenommen sein sollen.

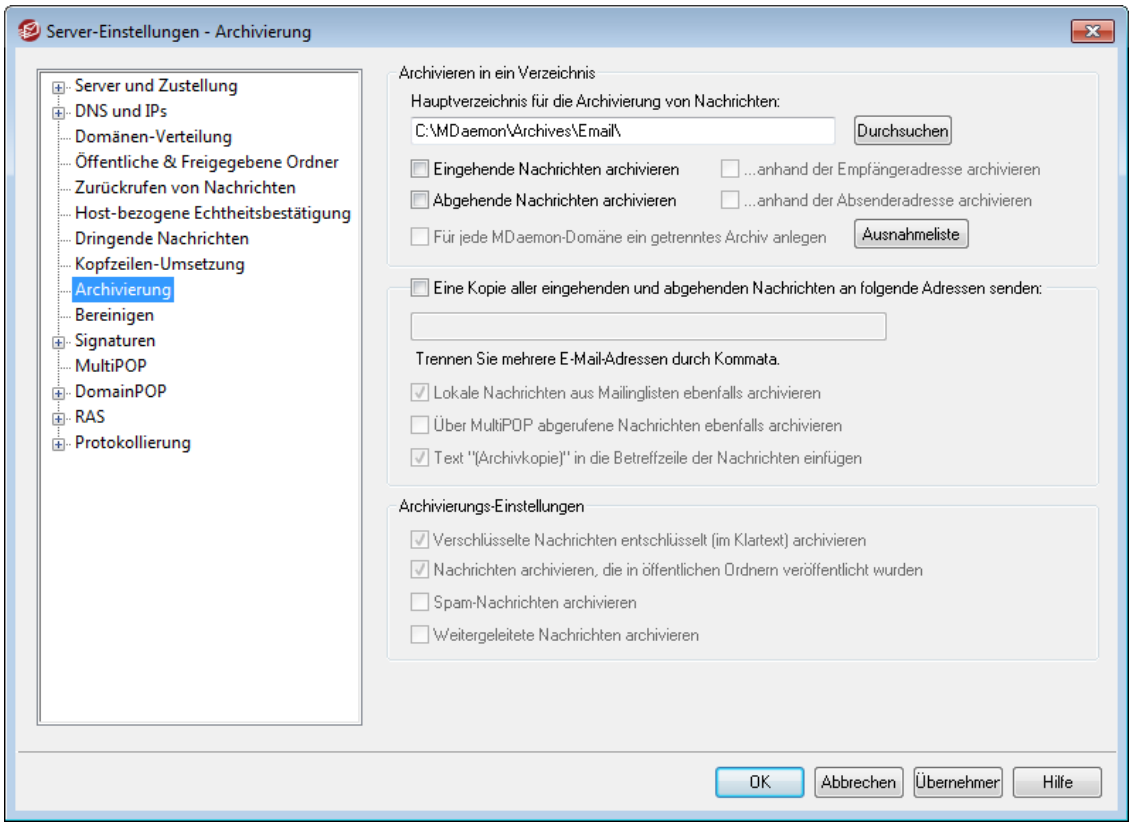
Hinzufügen
Klicken Sie auf dieses Steuerelement, um die Kopfzeile in die Liste einzutragen.

Ausgeschlossene Kopfzeilen

MDaemon wertet die folgenden Kopfzeilen für die Umsetzung von Texten in Kopfzeilen nicht aus.

Entfernen
Um eine Kopfzeile aus der Liste zu entfernen, wählen Sie die Kopfzeile aus, und klicken Sie dann auf dieses Steuerelement.

3.1.9 Archivierung



Mithilfe der Leistungsmerkmale zur Archivierung können Sie alle abgehenden und eingehenden Nachrichten in ein bestimmtes Verzeichnis archivieren lassen. Per Voreinstellung nutzt MDaemon hierzu das Verzeichnis `C:\MDaemon\Archives\Email\`; Sie können aber auch ein beliebiges anderes Verzeichnis nutzen. Sie können eingehende, an lokale Benutzer gerichtete Nachrichten sowie abgehende Nachrichten der lokalen Benutzer archivieren, und Sie können beide Nachrichtenkategorien gemeinsam archivieren. Nachrichten aus Mailinglisten, Nachrichten, die im Relaisbetrieb übermittelt werden, Systemnachrichten, Autobeantworter, Spam-Nachrichten und durch Viren infizierte Nachrichten werden nicht archiviert.

Eingehende Nachrichten werden in das Unterverzeichnis `\In\`, abgehende Nachrichten werden in das Unterverzeichnis `\Out\` des Archiv-Verzeichnisses archiviert. Sie können die Nachrichten für die Archivierung mit Hilfe der nachfolgend beschriebenen Optionen *...anhand der Empfängeradresse archivieren* und *...anhand der Absenderadresse archivieren* noch weiter unterteilen. Mithilfe der Option *Für jede MDaemon-Domäne ein getrenntes Archiv anlegen* können Sie die Nachrichten auch nach Domänen getrennt archivieren.

Eingehende Nachrichten werden so archiviert, wie sie in das Postfach des Benutzers eingestellt werden. Abgehende Nachrichten werden so archiviert, wie sie zur Übermittlung in die Warteschlange für externe Nachrichten eingestellt werden. Werden bei der Verarbeitung eingehender und abgehender Nachrichten Änderungen an ihnen vorgenommen, etwa durch Hinzufügen von Kopfzeilen mithilfe des

Inhaltsfilters, so enthalten die Archivkopien der Nachrichten diese Änderungen ebenfalls.

Um das Archivverzeichnis zu durchsuchen und zugänglich zu machen, erstellen Sie ein neues oder nutzen Sie ein bestehendes Benutzerkonto. In beiden Fällen ändern Sie das Nachrichten-Verzeichnis[717] so, dass es auf das Archiv-Verzeichnis verweist. Falls mehrere Benutzer Zugriff auf das Archiv benötigen, melden Sie sich an dem Benutzerkonto an, und erstellen Sie die erforderlichen Ordnerfreigaben[742] mithilfe des Konfigurationsdialogs für die Zugriffskontrollliste[311].

Es besteht eine verdeckte Systemwarteschlange im Verzeichnis "`\MDaemon\Queues\ToArchive\`". Diese Warteschlange wird regelmäßig auf Nachrichten geprüft, die dort manuell, durch ein Plugin, oder in sonstiger Weise abgelegt werden. Nachrichten, die in der Warteschlange gefunden werden, werden sofort archiviert und gelöscht. Nachrichten, die in der Warteschlange gefunden werden und von der Archivierung ausgeschlossen sind, werden jedoch ohne weiteres gelöscht. Die Registerkarte und das Protokoll Routing zeigen genaue Informationen über die erfolgreiche Archivierung von Nachrichten.

Archivieren in ein Verzeichnis

In dieses Feld tragen Sie den Verzeichnispfad zum gewünschten Archiv-Verzeichnis ein. Per Voreinstellung ist der Verzeichnispfad auf `C:\MDaemon\Archives\Email\` gesetzt; Sie können aber ein beliebiges Verzeichnis nutzen.

Eingehende Nachrichten archivieren
Diese Option bewirkt, dass eine Kopie aller eingehenden Nachrichten, die an lokale Benutzer gerichtet sind, archiviert wird. Nachrichten aus Mailinglisten und Nachrichten, die mit Viren infiziert sind, werden nicht archiviert.

...anhand der Empfängeradresse archivieren
Diese Option bewirkt, dass die archivierten eingehenden Nachrichten nach den E-Mail-Adressen ihrer Empfänger gruppiert werden.

Abgehende Nachrichten archivieren
Diese Option bewirkt, dass eine Kopie aller abgehenden Nachrichten lokaler Benutzer archiviert wird. Nachrichten aus Mailinglisten und Nachrichten, die mit Viren infiziert sind, werden nicht archiviert.

...anhand der Absenderadresse archivieren
Diese Option bewirkt, dass die archivierten eingehenden Nachrichten nach den E-Mail-Adressen ihrer Absender gruppiert werden.

Für jede MDaemon-Domäne ein getrenntes Archiv anlegen
Diese Option bewirkt, dass MDaemon für jede Domäne ein eigenes Archiv unterhält.

Ausnahmeliste
Dieses Steuerelement ruft die Ausnahmeliste für die Archivierung auf. In dieser Liste können Sie Empfänger- und Absenderadressen erfassen, die von der Archivierung ausgenommen sind.

Eine Kopie aller eingehenden und abgehenden Nachrichten an folgende Adressen senden

Mithilfe dieser Option können Sie Kopien aller archivierten Nachrichten an die hier angegebenen Empfänger senden. Trennen Sie mehrere Adressen durch Kommata. Als Empfänger sind lokale und externe E-Mail-Adressen sowie Adress-Aliasnamen zugelassen.

Lokale Nachrichten aus Mailinglisten ebenfalls archivieren
Diese Option bewirkt, dass auch Kopien lokaler Nachrichten aus Mailinglisten an die angegebenen Adressen gesendet werden.

Über MultiPOP abgerufene Nachrichten ebenfalls archivieren
Diese Option bewirkt, dass auch die über das MDaemon-Leistungsmerkmal MultiPOP 739 abgerufenen Nachrichten an die angegebenen Adressen übermittelt werden.

Text "(Archivkopie)" in die Betreffzeile der Nachrichten einfügen
Diese Option bewirkt, dass der Text "(Archivkopie)" in die Betreffzeile der übermittelten Nachrichten eingefügt wird.

Archivierungs-Einstellungen

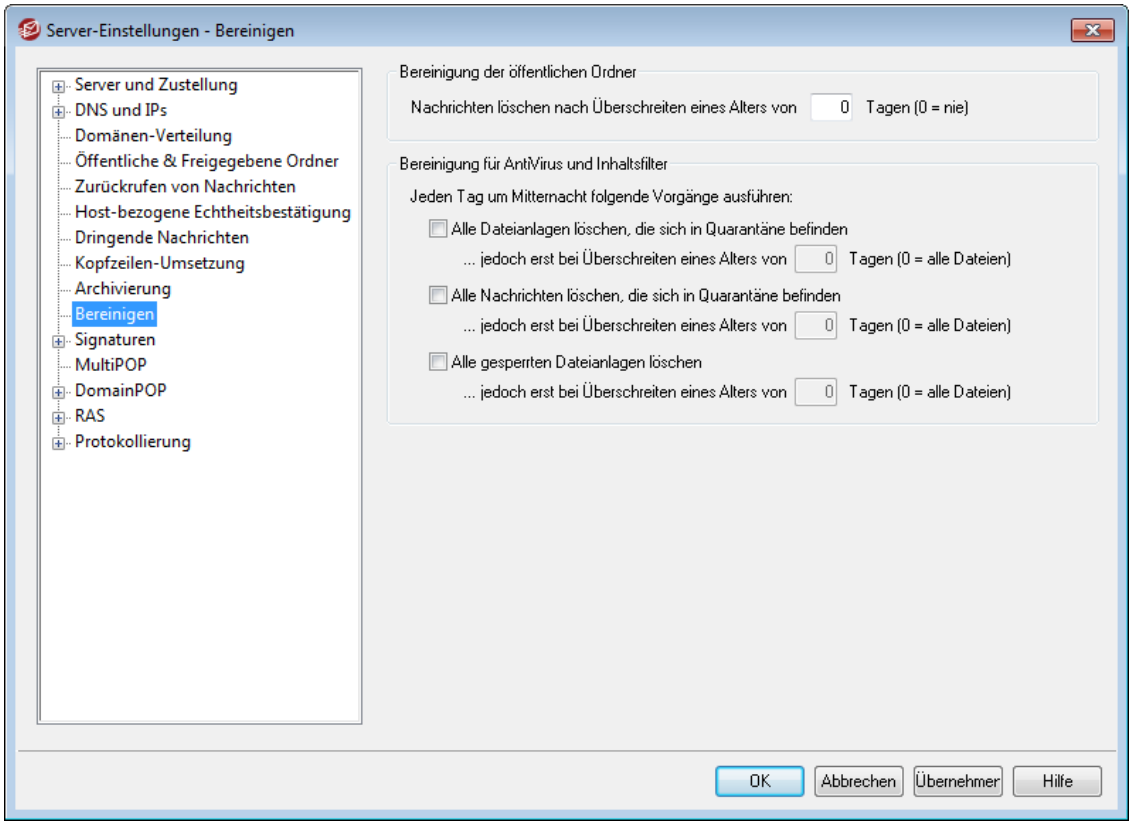
Verschlüsselte Nachrichten entschlüsselt (im Klartext) archivieren
Per Voreinstellung werden entschlüsselte Kopien verschlüsselter Nachrichten im Klartext archiviert. Kann eine Nachricht nicht entschlüsselt werden, so wird jedoch die verschlüsselte Nachricht archiviert. Falls Sie Nachrichten, die entschlüsselt werden können, trotzdem in verschlüsselter Form archivieren wollen, deaktivieren Sie diese Option.

Nachrichten archivieren, die in öffentlichen Ordnern veröffentlicht wurden
Per Voreinstellung werden Nachrichten archiviert, die an die Adresse zur Veröffentlichung in öffentlichen Ordnern gesandt werden. Falls Sie solche Nachrichten nicht archivieren wollen, deaktivieren Sie diese Option.

Spam-Nachrichten archivieren
Per Voreinstellung werden als Spam erkannte Nachrichten nicht archiviert. Falls Sie solche Nachrichten ebenfalls archivieren wollen, aktivieren Sie diese Option.

Weitergeleitete Nachrichten archivieren (dies erfordert eine Verarbeitung durch den Inhaltsfilter)
Diese Option bewirkt, dass auch weitergeleitete Nachrichten archiviert und per E-Mail an die angegebenen Empfänger übermittelt werden. Diese Nachrichten werden per Voreinstellung nicht archiviert.

3.1.10 Bereinigen



Bereinigung der öffentlichen Ordner

Nachrichten löschen nach Überschreiten eines Alters von [xx] Tagen (0 = nie)
Nachrichten in den öffentlichen Ordnern werden gelöscht, sobald sie das hier in Tagen angegebene Alter überschritten haben.

Bereinigung für AntiVirus und Inhaltsfilter

Alle Dateien löschen, die sich in Quarantäne befinden
Diese Einstellung bewirkt, dass jeden Tag um Mitternacht alle in Quarantäne gegebenen Dateien gelöscht werden.

... jedoch erst bei Überschreiten eines Alters von [xx] Tagen (0 = alle Dateien)
Per Voreinstellung werden jeweils alle in Quarantäne gegebenen Dateien gelöscht. Falls Sie nur Dateien löschen wollen, die ein bestimmtes Alter überschritten haben, aktivieren Sie diese Option, und tragen Sie das gewünschte Alter in Tagen hier ein.

Alle Nachrichten löschen, die sich in Quarantäne befinden
Diese Einstellung bewirkt, dass jeden Tag um Mitternacht alle in Quarantäne gegebenen Nachrichten gelöscht werden.

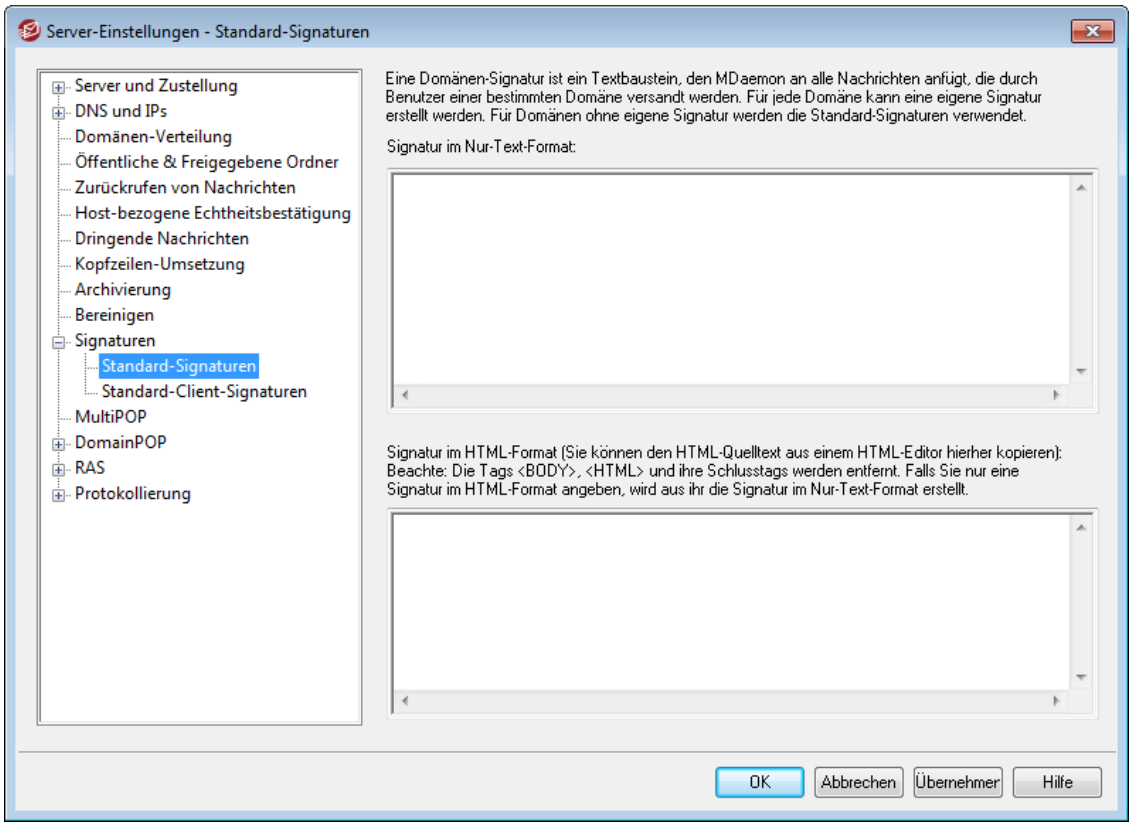
... jedoch erst bei Überschreiten eines Alters von [xx] Tagen (0 = alle Dateien)
Per Voreinstellung werden jeweils alle in Quarantäne gegebenen Nachrichten gelöscht. Falls Sie nur Dateien löschen wollen, die ein bestimmtes Alter überschritten haben, aktivieren Sie diese Option, und tragen Sie das gewünschte Alter in Tagen hier ein.

Alle gesperrten Dateianlagen löschen
Diese Einstellung bewirkt, dass jeden Tag um Mitternacht alle als gesperrt abgefangenen Dateianlagen gelöscht werden.

... jedoch erst bei Überschreiten eines Alters von [xx] Tagen (0 = alle Dateien)
Per Voreinstellung werden jeweils alle gesperrten Dateianlagen gelöscht. Falls Sie nur Dateien löschen wollen, die ein bestimmtes Alter überschritten haben, aktivieren Sie diese Option, und tragen Sie das gewünschte Alter in Tagen hier ein.

3.1.11 Signaturen

3.1.11.1 Standard-Signaturen



Mithilfe dieses Konfigurationsdialogs können Sie eine Signatur definieren, die allen abgehenden Nachrichten Ihrer MDaemon-Benutzer hinzugefügt wird. Mithilfe des Konfigurationsdialogs Signaturen 202 im Domänen-Manager können Sie für die Benutzer einzelner Domänen eigene getrennte Signaturen festlegen. Besteht für eine Domäne eine solche eigene Signatur, so wird sie für diese Domäne statt der Standard-Signatur verwendet. Signaturen werden werden am Ende des Nachrichtentextes eingefügt. Eine Ausnahme hiervon bilden Nachrichten in Mailinglisten, für die ein Schlusstext 296 definiert ist; bei solchen Nachrichten wird der Schlusstext nach der Signatur eingefügt. Im Abschnitt Signatur 753 des Benutzerkonten-Editors können Sie zusätzlich eigene getrennte Signaturen für jedes Benutzerkonto festlegen. Signaturen der Benutzerkonten werden unmittelbar vor den Standard- oder Domänen-Signaturen eingefügt.

Signatur im Nur-Text-Format

In dieses Textfeld können Sie eine Signatur im Nur-Text-Format eintragen. Falls Sie für die Verwendung im Teil "text/html" von Multipart-Nachrichten eine hierzu passende HTML-Signatur festlegen wollen, tragen Sie deren HTML-Quellkode in das Textfeld *Signatur im HTML-Format* weiter unten ein. MDaemon nutzt dann für jeden Teil der Multipart-Nachricht die passende Signatur. Ist keine HTML-Signatur festgelegt, so wird die Signatur im Nur-Text-Format in beide Teile der Nachricht eingefügt.

Signatur im HTML-Format (Sie können den HTML-Quelltext aus einem HTML-Editor hierher kopieren)

In dieses Textfeld können Sie eine Signatur im HTML-Format eintragen. Diese Signatur wird in den Teil "text/html" von Multipart-Nachrichten eingefügt. Falls Sie sowohl in dieses Textfeld wie auch in das Textfeld *Signatur im Nur-Text-Format* weiter oben je eine Signatur eintragen, nutzt MDaemon für jeden Teil der Multipart-Nachricht die passende Signatur. Ist keine HTML-Signatur festgelegt, so wird die Signatur im Nur-Text-Format in beide Teile der Nachricht eingefügt. Ist keine Signatur im Nur-Text-Format festgelegt, so wird die Signatur aus der Signatur im HTML-Format erstellt.

Sie können eine Signatur im HTML-Format erstellen, indem Sie den HTML-Kode unmittelbar in dieses Textfeld eintragen, oder indem Sie den HTML-Kode in einem HTML-Editor erstellen und dann über die Zwischenablage in dieses Textfeld kopieren. Sie können in eine Signatur im HTML-Format auch Grafikdateien unmittelbar (inline) einbetten; hierzu steht das Makro `$ATTACH_INLINE:Pfad_zur_Grafikdatei$` zur Verfügung.

Ein Anwendungsbeispiel stellt der nachfolgend dargestellte HTML-Kode dar:

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \grafiken\mr_t_and_arnold.jpg$">
```

Sie können Grafiken auch mithilfe der MDaemon-Remoteverwaltung 350 in die Signaturen einfügen. Hierzu stehen Ihnen folgende Vorgehensweisen zur Verfügung:

- Klicken Sie in der Remoteverwaltung im Abschnitt Standard-Signaturen auf das Steuerelement "Grafik" in der Symbolleiste des HTML-Editors, und wählen Sie dann die Registerkarte Upload aus.
- Klicken Sie in der Remoteverwaltung im Abschnitt Standard-Signaturen auf das Steuerelement "Grafik hinzufügen" in der Symbolleiste des HTML-Editors.
- Falls Sie Chrome, FireFox, Safari oder den MS Internet Explorer ab Version 10 nutzen, ziehen Sie eine Grafikdatei in den HTML-Editor im Abschnitt Standard-Signaturen, und legen Sie sie dort ab.
- Falls Sie Chrome, FireFox oder den MS Internet Explorer ab Version 11 nutzen, können Sie die Grafik aus der Zwischenablage direkt in den HTML-Editor im Abschnitt Standard-Signaturen kopieren.

Die Tags <body></body> und <html></html> sind in Signaturen nicht zugelassen. Falls sie in Signaturen enthalten sind, werden sie entfernt.

Makros für Signaturen

MDaemon unterstützt in den Signaturen Makros, mit deren Hilfe Kontaktdaten des Absenders automatisch in die Signaturen eingefügt werden können. Diese Daten werden den Kontaktdaten des Absenders entnommen, die im Ordner für öffentliche Kontakte seiner Domäne gespeichert sind. Standard- und Domänen-Signaturen können hierdurch mithilfe der Daten des Absenders automatisch individuell gestaltet werden. Zwei Beispiele hierzu: `$CONTACTFULLNAME$` wird umgesetzt in den vollständigen Namen des Absenders, und `$CONTACTEMAILADDRESS$` wird umgesetzt in die E-Mail-Adresse des Absenders. Die Kontaktdaten für die öffentlichen Kontakte können mithilfe von Webmail, des MDaemon Connectors oder über ActiveSync bearbeitet werden. Falls für einen Absender keine Kontaktdaten bestehen, werden Leerstellen eingesetzt. Die verfügbaren Makros sind unten aufgeführt.

Die Benutzer können steuern, welche MDaemon-Signaturen wie in ihre Nachrichten eingefügt werden. Hierzu fügen sie zwei bestimmte Makros in die Nachrichten ein: Das Makro `$SYSTEMSIGNATURE$` wird ersetzt durch die Standard- oder Domänen-Signatur, und das Makro `$ACCOUNTSIGNATURE$` wird ersetzt durch die Signatur des Benutzerkontos.

Namen und IDs	
Vollständiger Name	**$CONTACTFULLNAME$**
Vorname	**$CONTACTFIRSTNAME$**
Zweiter Vorname	**$CONTACTMIDDLENAME$**
Nachname	**$CONTACTLASTNAME$**
Titel	**$CONTACTTITLE$**
Namenszusatz	**$CONTACTSUFFIX$**
Spitzname	**$CONTACTNICKNAME$**
Vorname (Yomi)	**$CONTACTYOMIFIRSTNAME$**
Nachname (Yomi)	**$CONTACTYOMILASTNAME$**
Name des Benutzerkontos	**$CONTACTACCOUNTNAME$**
Kunden-ID	**$CONTACTCUSTOMERID$**
Verwaltungs-ID	**$CONTACTGOVERNMENTID$**
Speichern unter	**$CONTACTFILEAS$**
E-Mail-Adressen	
E-Mail-Adresse	**$CONTACTEMAILADDRESS$**
E-Mail-Adresse 2	**$CONTACTEMAILADDRESS2$**
E-Mail-Adresse 3	**$CONTACTEMAILADDRESS3$**
Telefon- und Faxnummern	
Mobiltelefon	**$CONTACTHOMEMOBILE$**

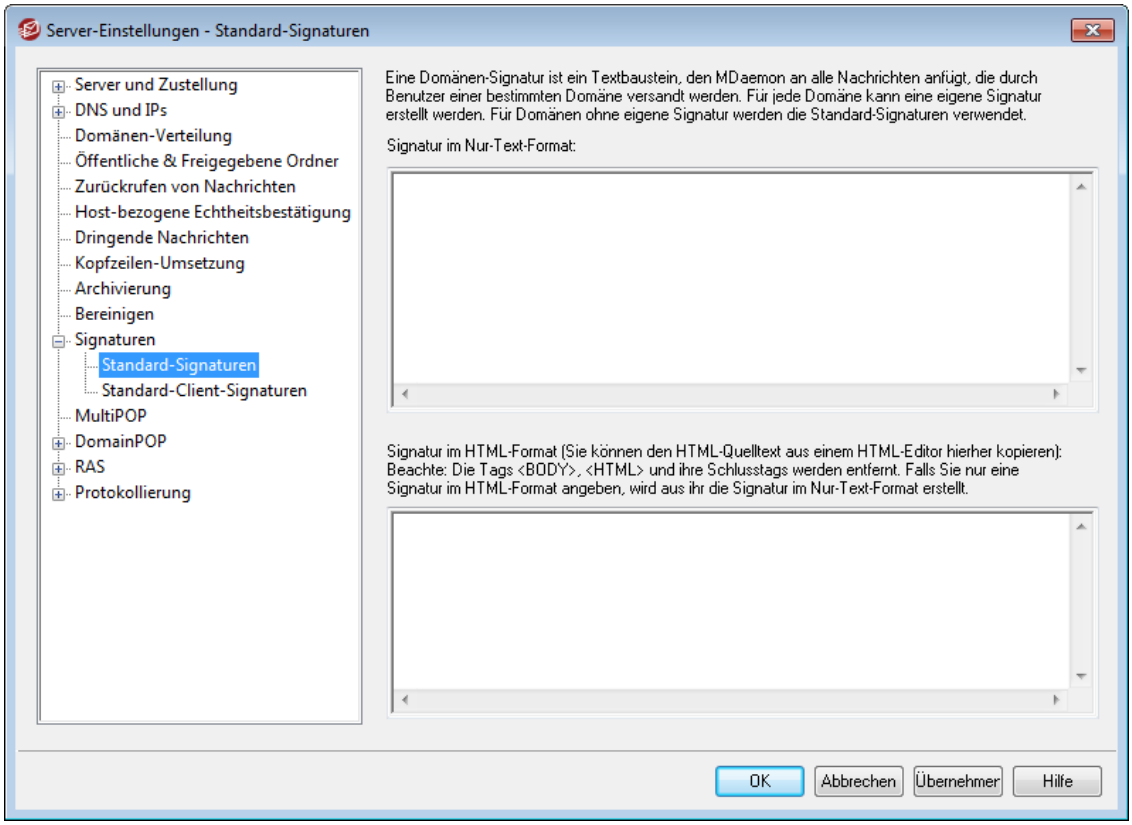
Mobiltelefon 2	**$CONTACTMOBILE2$**
Autotelefon	**$CONTACTCARPHONENUMBER$**
Telefon privat	**$CONTACTHOMEPHONE$**
Telefon privat 2	**$CONTACTHOMEPHONE2$**
Telefax privat	**$CONTACTHOMEFAX$**
Anderes Telefon	**$CONTACTOTHERPHONE$**
Instant Messaging und Web	
IM-Adresse	**$CONTACTIMADDRESS$**
IM-Adresse 2	**$CONTACTIMADDRESS2$**
IM-Adresse 3	**$CONTACTIMADDRESS3$**
MMS-Adresse	**$CONTACTMMSADDRESS$**
Web-Adresse privat	**$CONTACTHOMEWEBADDRESS$**
Adresse	
Adresse privat	**$CONTACTHOMEADDRESS$**
Stadt privat	**$CONTACTHOMECITY$**
Bundesland/Kanton privat	**$CONTACTHOMESTATE$**
PLZ privat	**$CONTACTHOMEZIPCODE$**
Land privat	**$CONTACTHOMECOUNTRY$**
Andere Adresse	**$CONTACTOTHERADDRESS$**
Andere Stadt	**$CONTACTOTHERCITY$**
Anderes Bundesland/ anderer Kanton	**$CONTACTOTHERSTATE$**
Andere PLZ	**$CONTACTOTHERZIPCODE$**
Anderes Land	**$CONTACTOTHERCOUNTRY$**
Geschäftsbezogene Daten	
Firma	**$CONTACTBUSINESSCOMPANY$**
Firma (Yomi)	**$CONTACTYOMICOMPANYNAME$**
Titel/Berufsbezeichnung	**$CONTACTBUSINESSTITLE$**
Büro geschäftlich	**$CONTACTBUSINESSOFFICE$**
Abteilung geschäftlich	**$CONTACTBUSINESSDEPARTMENT$**
Manager geschäftlich	**$CONTACTBUSINESSMANAGER$**
Assistenz geschäftlich	**$CONTACTBUSINESSASSISTANT$**

Telefon Assistenz geschäftlich	$CONTACTBUSINESSASSISTANTPHONE$
Telefon zentral geschäftlich	$CONTACTBUSINESSMAINPHONE$
Telefon geschäftlich	$CONTACTBUSINESSPHONE$
Telefon geschäftlich 2	$CONTACTBUSINESSPHONE2$
IP-Telefon geschäftlich	$CONTACTBUSINESSIPPHONE$
Fax geschäftlich	$CONTACTBUSINESSFAX$
Pager geschäftlich	$CONTACTBUSINESSPAGER$
Funkdienst geschäftlich	$CONTACTBUSINESSRADIO$
Adresse geschäftlich	$CONTACTBUSINESSADDRESS$
Stadt geschäftlich	$CONTACTBUSINESSCITY$
Bundesland/Kanton geschäftlich	$CONTACTBUSINESSSTATE$
PLZ geschäftlich	$CONTACTBUSINESSZIPCODE$
Land geschäftlich	$CONTACTBUSINESSCOUNTRY$
Web-Adresse geschäftlich	$CONTACTBUSINESSWEBADDRESS$
Weitere Daten	
Ehegatte	$CONTACTSPOUSE$
Kinder	$CONTACTCHILDREN$
Kategorien	$CONTACTCATEGORIES$
Kommentar	$CONTACTCOMMENT$

Siehe auch:

Domänen-Manager » Signaturen 202
Benutzerkonten-Editor » Signatur 753

3.1.11.2 Standard-Client-Signaturen



Mithilfe dieses Konfigurationsdialogs können Sie eine Standard-Signatur für Clients definieren, die Sie dann an MDaemon Webmail[345] und an den MDaemon Connector[404] übermitteln können. Die Signatur kann durch Ihre Benutzer beim Verfassen von E-Mail-Nachrichten eingesetzt werden. Sie können die nachfolgend aufgeführten Makros[142] nutzen, um die Signatur benutzerindividuell zu gestalten. Die Signatur kann Elemente enthalten, die sich für jeden Benutzer unterscheiden, insbesondere Vor- und Nachname, E-Mail-Adresse, Telefonnummer und weiteres. Mithilfe des Konfigurationsdialogs Client-Signaturen[206] im Domänen-Manager können Sie für die Benutzer einzelner Domänen eigene getrennte Signaturen festlegen. Besteht für eine Domäne eine solche eigene Signatur, so wird sie für diese Domäne statt der Standard-Signatur verwendet. Signaturen werden werden am Ende des Nachrichtentextes eingefügt. Mithilfe der Option *Signatur an Clients übermitteln*[345] können Sie die Client-Signatur an Webmail übermitteln. Mithilfe der Option *Client-Signatur an Microsoft Outlook übermitteln*[404] können Sie die Client-Signatur an den MDaemon Connector übermitteln. In den Webmail-Optionen zum Verfassen von Nachrichten trägt die so übermittelte Client-Signatur die Bezeichnung "System". Für den MDaemon Connector können Sie eine Bezeichnung für die Signatur festlegen, die in Microsoft Outlook erscheint.

Signatur im Nur-Text-Format

In dieses Textfeld können Sie eine Signatur im Nur-Text-Format eintragen. Falls Sie für die Verwendung im Teil "text/html" von Multipart-Nachrichten eine hierzu passende HTML-Signatur festlegen wollen, tragen Sie deren HTML-Quellkode in das Textfeld *Signatur im HTML-Format* weiter unten ein. MDaemon nutzt dann für jeden Teil der Multipart-Nachricht die passende Signatur. Ist keine HTML-Signatur

festgelegt, so wird die Signatur im Nur-Text-Format in beide Teile der Nachricht eingefügt.

Signatur im HTML-Format (Sie können den HTML-Quelltext aus einem HTML-Editor hierher kopieren)

In dieses Textfeld können Sie eine Signatur im HTML-Format eintragen. Diese Signatur wird in den Teil "text/html" von Multipart-Nachrichten eingefügt. Falls Sie sowohl in dieses Textfeld wie auch in das Textfeld *Signatur im Nur-Text-Format* weiter oben je eine Signatur eintragen, nutzt MDaemon für jeden Teil der Multipart-Nachricht die passende Signatur. Ist keine HTML-Signatur festgelegt, so wird die Signatur im Nur-Text-Format in beide Teile der Nachricht eingefügt. Ist keine Signatur im Nur-Text-Format festgelegt, so wird die Signatur aus der Signatur im HTML-Format erstellt.

Sie können eine Signatur im HTML-Format erstellen, indem Sie den HTML-Kode unmittelbar in dieses Textfeld eintragen, oder indem Sie den HTML-Kode in einem HTML-Editor erstellen und dann über die Zwischenablage in dieses Textfeld kopieren. Sie können in eine Signatur im HTML-Format auch Grafikdateien unmittelbar (inline) einbetten; hierzu steht das Makro `$ATTACH_INLINE:Pfad_zur_Grafikdatei$` zur Verfügung.

Ein Anwendungsbeispiel stellt der nachfolgend dargestellte HTML-Kode dar:

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \grafiken\mr_t_and_arnold.jpg$">
```

Sie können Grafiken auch mithilfe der MDaemon-Remoteverwaltung 350 in die Signaturen einfügen. Hierzu stehen Ihnen folgende Vorgehensweisen zur Verfügung:

- Klicken Sie in der Remoteverwaltung im Abschnitt Standard-Signaturen auf das Steuerelement "Grafik" in der Symbolleiste des HTML-Editors, und wählen Sie dann die Registerkarte Upload aus.
- Klicken Sie in der Remoteverwaltung im Abschnitt Standard-Signaturen auf das Steuerelement "Grafik hinzufügen" in der Symbolleiste des HTML-Editors.
- Falls Sie Chrome, FireFox, Safari oder den MS Internet Explorer ab Version 10 nutzen, ziehen Sie eine Grafikdatei in den HTML-Editor im Abschnitt Standard-Signaturen, und legen Sie sie dort ab.
- Falls Sie Chrome, FireFox oder den MS Internet Explorer ab Version 11 nutzen, können Sie die Grafik aus der Zwischenablage direkt in den HTML-Editor im Abschnitt Standard-Signaturen kopieren.

Vorgehensweise zum Einfügen von Grafiken

Sie können Grafiken in Signaturen einfügen. Hierzu stehen die folgenden Vorgehensweisen zur Verfügung:

- Klicken Sie in der Symbolleiste des HTML-Editors auf das Symbol "Grafik", und geben Sie den URL der gewünschten Grafikdatei ein. Sie können auch mithilfe des Steuerelements "Hochladen" eine Grafikdatei hochladen.
- Klicken Sie in der Symbolleiste des HTML-Editors auf das Symbol "Grafik hinzufügen", um eine Grafikdatei hochzuladen.
- Ziehen Sie eine Grafikdatei in das Eingabefeld für den Signaturtext, und legen Sie sie dort ab. Diese Vorgehensweise funktioniert bei Nutzung von Google Chrome, Mozilla FireFox, Apple Safari und dem Microsoft Internet Explorer ab Version 10.

- Kopieren Sie eine Grafikdatei aus der Zwischenablage in das Eingabefeld für den Signaturtext. Diese Vorgehensweise funktioniert bei Nutzung von Google Chrome, Mozilla FireFox und dem Microsoft Internet Explorer ab Version 11.

Die Tags <body></body> und <html></html> sind in Signaturen nicht zugelassen. Falls sie in Signaturen enthalten sind, werden sie entfernt.

Makros für Signaturen

MDaemon unterstützt in den Signaturen Makros, mit deren Hilfe Kontaktdaten des Absenders automatisch in die Signaturen eingefügt werden können. Diese Daten werden den Kontaktdaten des Absenders entnommen, die im Ordner für öffentliche Kontakte seiner Domäne gespeichert sind. Standard- und Domänen-Signaturen können hierdurch mithilfe der Daten des Absenders automatisch individuell gestaltet werden. Zwei Beispiele hierzu: `$CONTACTFULLNAME$` wird umgesetzt in den vollständigen Namen des Absenders, und `$CONTACTEMAILADDRESS$` wird umgesetzt in die E-Mail-Adresse des Absenders. Die Kontaktdaten für die öffentlichen Kontakte können mithilfe von Webmail, des MDaemon Connectors oder über ActiveSync bearbeitet werden. Falls für einen Absender keine Kontaktdaten bestehen, werden Leerstellen eingesetzt. Die verfügbaren Makros sind unten aufgeführt.

Die Benutzer können steuern, welche MDaemon-Signaturen wie in ihre Nachrichten eingefügt werden. Hierzu fügen sie zwei bestimmte Makros in die Nachrichten ein: Das Makro `$SYSTEMSIGNATURE$` wird ersetzt durch die Standard- oder Domänen-Signatur, und das Makro `$ACCOUNTSIGNATURE$` wird ersetzt durch die Signatur des Benutzerkontos.

Namen und IDs	
Vollständiger Name	**$CONTACTFULLNAME$**
Vorname	**$CONTACTFIRSTNAME$**
Zweiter Vorname	**$CONTACTMIDDLENAME$**
Nachname	**$CONTACTLASTNAME$**
Titel	**$CONTACTTITLE$**
Namenszusatz	**$CONTACTSUFFIX$**
Spitzname	**$CONTACTNICKNAME$**
Vorname (Yomi)	**$CONTACTYOMIFIRSTNAME$**
Nachname (Yomi)	**$CONTACTYOMILASTNAME$**
Name des Benutzerkontos	**$CONTACTACCOUNTNAME$**
Kunden-ID	**$CONTACTCUSTOMERID$**
Verwaltungs-ID	**$CONTACTGOVERNMENTID$**
Speichern unter	**$CONTACTFILEAS$**

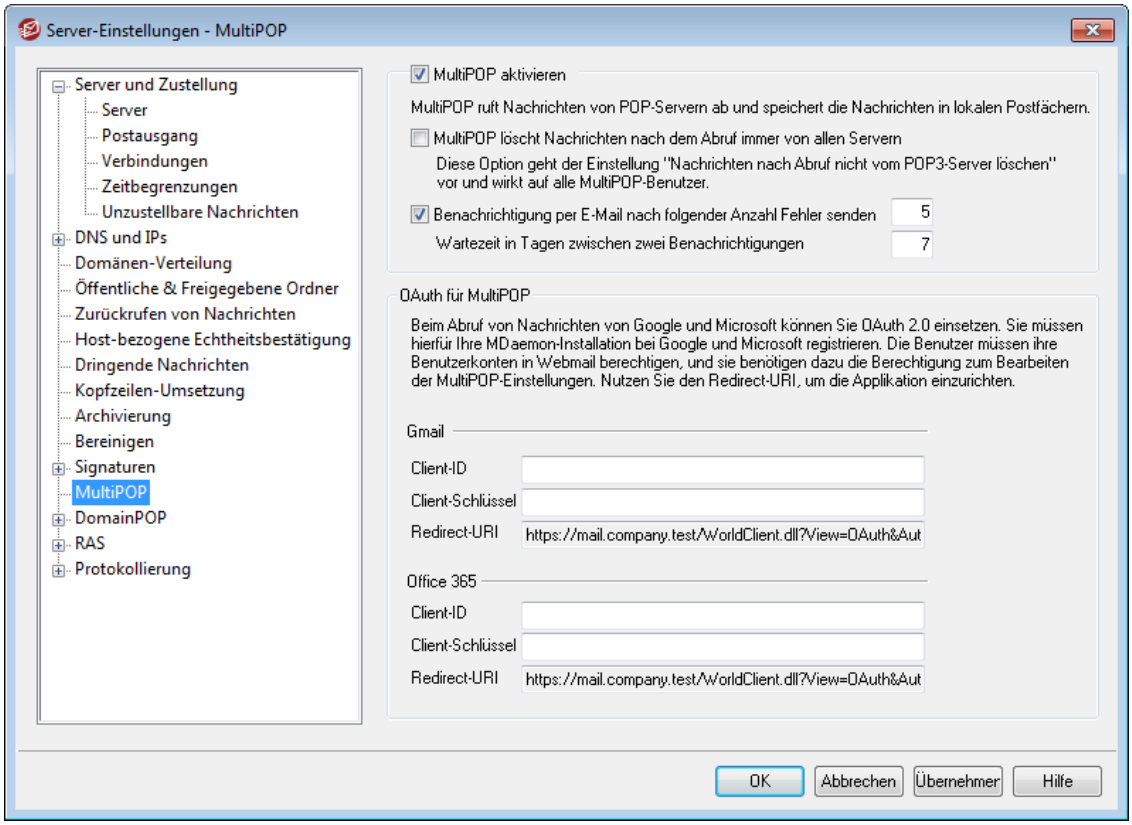
E-Mail-Adressen	
E-Mail-Adresse	**$CONTACTEMAILADDRESS$**
E-Mail-Adresse 2	**$CONTACTEMAILADDRESS2$**
E-Mail-Adresse 3	**$CONTACTEMAILADDRESS3$**
Telefon- und Faxnummern	
Mobiltelefon	**$CONTACTHOMEMOBILE$**
Mobiltelefon 2	**$CONTACTMOBILE2$**
Autotelefon	**$CONTACTCARPHONENUMBER$**
Telefon privat	**$CONTACTHOMEPHONE$**
Telefon privat 2	**$CONTACTHOMEPHONE2$**
Telefax privat	**$CONTACTHOMEFAX$**
Anderes Telefon	**$CONTACTOTHERPHONE$**
Instant Messaging und Web	
IM-Adresse	**$CONTACTIMADDRESS$**
IM-Adresse 2	**$CONTACTIMADDRESS2$**
IM-Adresse 3	**$CONTACTIMADDRESS3$**
MMS-Adresse	**$CONTACTMMSADDRESS$**
Web-Adresse privat	**$CONTACTHOMEWEBADDRESS$**
Adresse	
Adresse privat	**$CONTACTHOMEADDRESS$**
Stadt privat	**$CONTACTHOMECITY$**
Bundesland/Kanton privat	**$CONTACTHOMESTATE$**
PLZ privat	**$CONTACTHOMEZIPCODE$**
Land privat	**$CONTACTHOMECOUNTRY$**
Andere Adresse	**$CONTACTOTHERADDRESS$**
Andere Stadt	**$CONTACTOTHERCITY$**
Anderes Bundesland/ anderer Kanton	**$CONTACTOTHERSTATE$**
Andere PLZ	**$CONTACTOTHERZIPCODE$**
Anderes Land	**$CONTACTOTHERCOUNTRY$**
Geschäftsbezogene Daten	
Firma	**$CONTACTBUSINESSCOMPANY$**

Firma (Yomi)	**$CONTACTYOMICOMPANYNAME$**
Titel/Berufsbezeichnung	**$CONTACTBUSINESSTITLE$**
Büro geschäftlich	**$CONTACTBUSINESSOFFICE$**
Abteilung geschäftlich	**$CONTACTBUSINESSDEPARTMENT$**
Manager geschäftlich	**$CONTACTBUSINESSMANAGER$**
Assistenz geschäftlich	**$CONTACTBUSINESSASSISTANT$**
Telefon Assistenz geschäftlich	**$CONTACTBUSINESSASSISTANTPHONE$**
Telefon zentral geschäftlich	**$CONTACTBUSINESSMAINPHONE$**
Telefon geschäftlich	**$CONTACTBUSINESSPHONE$**
Telefon geschäftlich 2	**$CONTACTBUSINESSPHONE2$**
IP-Telefon geschäftlich	**$CONTACTBUSINESSIPPHONE$**
Fax geschäftlich	**$CONTACTBUSINESSFAX$**
Pager geschäftlich	**$CONTACTBUSINESSPAGER$**
Funkdienst geschäftlich	**$CONTACTBUSINESSRADIO$**
Adresse geschäftlich	**$CONTACTBUSINESSADDRESS$**
Stadt geschäftlich	**$CONTACTBUSINESSCITY$**
Bundesland/Kanton geschäftlich	**$CONTACTBUSINESSSTATE$**
PLZ geschäftlich	**$CONTACTBUSINESSZIPCODE$**
Land geschäftlich	**$CONTACTBUSINESSCOUNTRY$**
Web-Adresse geschäftlich	**$CONTACTBUSINESSWEBADDRESS$**
Weitere Daten	
Ehegatte	**$CONTACTSPOUSE$**
Kinder	**$CONTACTCHILDREN$**
Kategorien	**$CONTACTCATEGORIES$**
Kommentar	**$CONTACTCOMMENT$**

Siehe auch:

Standard-Signaturen 135
Domänen-Manager » Signaturen 202
Domänen-Manager » Client-Signaturen 206
Benutzerkonten-Editor » Signatur 753
Webmail-Einstellungen 345
MC-Client-Einstellungen » Signatur 404

3.1.12 MultiPOP



MultiPOP aktivieren

Mithilfe dieser Option aktivieren Sie den MultiPOP-Server. MultiPOP ruft Nachrichten für Ihre Benutzer von POP-Servern ab und speichert die Nachrichten in den lokalen Postfächern der Benutzer. Das Leistungsmerkmal MultiPOP gestattet die Erstellung einer unbegrenzten Zahl von externen POP3-Postfächern, jeweils bestehend aus Servername, Benutzername und Kennwort, von denen jeweils Nachrichten abgerufen werden sollen. Dies ist für Benutzer mit mehreren E-Mail-Konten auf verschiedenen Servern hilfreich, wenn sie es vorziehen, alle E-Mail gesammelt von nur noch einem Server abzurufen. Bevor die Nachrichten im Postfach des jeweiligen Benutzers abgelegt werden, gelangen sie in die lokale Nachrichten-Warteschlange, sodass sie genau wie alle sonstigen Nachrichten verarbeitet werden können. Autobeantworter und der Inhaltsfilter werden auf diese Nachrichten folglich ebenfalls angewandt. Sie erreichen den Zeitplan für MultiPOP über Einstellungen » Zeitplan » Abruf über MultiPOP 382.

MultiPOP löscht abgerufene Nachrichten immer von allen Servern
Diese Einstellung setzt die Einstellung *Nachrichten nicht vom POP3-Server löschen* (sie ist über den Konfigurationsdialog MultiPOP[739] des Benutzerkonten-Editors zugänglich) systemweit für alle Benutzer außer Kraft. Sie bewirkt, dass alle Nachrichten nach dem Abruf von jedem MultiPOP-Server gelöscht werden.

OAuth für MultiPOP

OAuth 2.0 ist ein Verfahren zur modernen Authentifizierung, das Gmail und Microsoft (Office) 365 bereits erfordern oder in nächster Zeit erfordern werden. Es löst die herkömmlichen Verfahren zur Anmeldung und Authentifizierung (die sog. legacy oder basic authentication) ab. Damit MDaemon mithilfe von OAuth 2.0 über MultiPOP Nachrichten von Gmail oder Microsoft (Office) 365 für Ihre Benutzer abrufen kann, müssen Sie Ihren MDaemon-Server bei Google oder Microsoft registrieren und eine Applikation nach dem Standard OAuth 2.0 erstellen. Sie nutzen dafür die Google-API-Konsole oder das Microsoft Azure Active Directory. Die Vorgehensweise ähnelt der Vorgehensweise, die Ihre Webmail-Benutzer zur Dropbox-Integration[336] anwenden.

Um MultiPOP für den Abruf von Nachrichten von Gmail oder Microsoft (Office) 365 für Ihre Benutzer zu konfigurieren, gehen Sie folgendermaßen vor:

1. Aktivieren Sie die Option **MultiPOP aktivieren** weiter oben.
2. Führen Sie die Anweisungen im Abschnitt **Erstellen und Verbinden Ihrer OAuth-App für MultiPOP**[147] aus, die weiter unten für Gmail und Microsoft (Office) 365 beschrieben sind.
3. Aktivieren Sie die Option **MultiPOP aktivieren** auf der Seite MultiPOP des Benutzerkonten-Editors[739] für jeden Benutzer, dem Sie den Abruf von Nachrichten aus Gmail oder Microsoft (Office) 365 über MultiPOP gestatten wollen.
4. Fügen Sie für jeden dieser Benutzer ein Benutzerkonto für Gmail (`pop.gmail.com:995`) oder Microsoft (Office) 365 (`outlook.office365.com:995`) hinzu, und aktivieren Sie die Option **OAuth verwenden**. Sie können diesen Schritt auch durch Ihre Benutzer selbst in Webmail[317] ausführen lassen. **Beachte:** Bei der Nutzung von Gmail muss jedes Gmail-Benutzerkonto in Ihrer Gmail-OAuth-App in die Gruppe Testbenutzer aufgenommen werden (siehe die Anmerkung zum **Veröffentlichungsstatus** im Abschnitt *Erstellen und Verbinden Ihrer OAuth-App für MultiPOP*[147] weiter unten).
5. Aktivieren Sie auf der Seite Web-Dienste des Benutzerkonten-Editors[720] für jeden betroffenen Benutzer die Option "**...MultiPOP-Einstellungen**".
6. Die Benutzer müssen sich an Webmail anmelden und im Abschnitt Optionen die Seite **Postfächer** aufrufen. Hier müssen die Benutzer ihre Benutzerkonten für Gmail und Microsoft (Office) 365 hinzufügen, falls Sie das noch nicht für die Benutzer erledigt haben. Die Benutzer müssen danach auf **Berechtigung erteilen** klicken und die dann erscheinenden Bedienschritte abarbeiten, um MDaemon die Berechtigung für den Abruf von Nachrichten zu erteilen.

Gmail/Microsoft (Office) 365

Client-ID
Dies ist die eindeutige Client-ID, die Ihrer OAuth-2.0-App für MultiPOP bei der Erstellung in der Google-API-Konsole oder im Microsoft Azure Active Directory zugewiesen wurde. Nachdem Sie Ihre App erstellt haben, kopieren Sie die Client-ID, und fügen Sie sie hier ein.

Client-Schlüssel
Dies ist der eindeutige Client-Schlüssel, der auch als "Client Secret" bezeichnet wird, und der Ihrer OAuth-2.0-App für MultiPOP bei der Erstellung in der Google-API-Konsole oder im Microsoft Azure Active Directory zugewiesen wurde. Nachdem Sie Ihre App erstellt haben, kopieren Sie den Client-Schlüssel, und fügen Sie ihn hier ein. **Beachte**: Wenn Sie einen Client-Schlüssel für eine Microsoft-Azure-App erstellen, müssen Sie diesen Schlüssel unmittelbar während der Erstellung der App kopieren. Der Schlüssel ist nach der Erstellung der App nicht mehr sichtbar. Falls Sie den Schlüssel nicht während der Erstellung kopiert haben, müssen Sie den Schlüssel löschen und einen neuen Schlüssel erstellen.

Redirect-URI
Beim Erstellen Ihrer OAuth-2.0-App für Gmail oder Microsoft (Office) 365 müssen Sie einen Redirect-URI angeben. Dieser Redirect-URI wird je nach Anbieter auch als Weiterleitungs-URI oder Umleitungs-URI bezeichnet. Der Redirect-URI, der im Konfigurationsdialog für MultiPOP angezeigt wird, ist ein Beispiel, das aus dem SMTP-Hostnamen[184] der Standard-Domäne[181] erstellt wird. Er sollte für die Benutzer dieser Domäne bei der Anmeldung an Webmail nutzbar sein. Sie sollten auch für alle anderen MDaemon-Domänen, die Ihre Benutzer für die Anmeldung an Webmail möglicherweise verwenden, solche Redirect-URIs erstellen. Ein Beispiel hierzu: "`https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Office365`" würde für alle Benutzer funktionieren, die sich über die Domäne mail.example.com an Webmail anmelden. Nähere Informationen hierzu finden Sie im Abschnitt **Erstellen und Verbinden Ihrer OAuth-App für MultiPOP** weiter unten.

Beispiele für Redirect-URIs sind:

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

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

Erstellen und Verbinden Ihrer OAuth-App für MultiPOP

Sie finden nachfolgend die einzelnen Bedienschritte für die Erstellung Ihrer OAuth-2.0-App für MultiPOP.

Für Google Gmail

Um MultiPOP die Anmeldung mithilfe von OAuth 2.0 für den Abruf von Nachrichten aus Gmail für Ihre Benutzer zu gestatten, erstellen Sie eine Google-Applikation. Gehen Sie dazu folgendermaßen vor:

1. Rufen Sie in Ihrem Browser die Google-API-Konsole auf.

2. Falls Sie sich in der Projektliste befinden, klicken Sie auf **NEUES PROJEKT**. Falls Sie sich auf der Seite Ressourcen verwalten befinden, klicken Sie auf **(+) PROJEKT ERSTELLEN**.
3. Geben Sie einen **Projektnamen** ein. Falls Sie die Projekt-ID ändern wollen, klicken Sie auf **BEARBEITEN**. Sie können die Projekt-ID auch unverändert lassen. **Beachte:** Die Projekt-ID kann nach der Erstellung des Projekts nicht mehr geändert werden.
4. Klicken Sie im Navigationsbereich links auf **APIs und Dienste | OAuth-Zustimmungsbildschirm**.
5. Wählen Sie den Typ **Extern**, und klicken Sie danach auf **ERSTELLEN**.
6. Geben Sie den **Anwendungsnamen** ein (z.B. MultiPOP OAuth 2.0 für Gmail). Geben Sie eine **Nutzersupport-E-Mail** ein, an die sich die Benutzer wenden können, und geben Sie unter **Kontaktdaten des Entwicklers** eine E-Mail-Adresse ein, an die sich Google bei Änderungen an Ihrem Projekt wenden kann. Weitere Angaben müssen Sie auf dieser Seite für die Erstellung der App nicht machen. Je nach Ihrer Organisation oder Ihren Prüfvorschriften können Sie aber noch das Anwendungslogo und Verknüpfungen zu Ihren Nutzungsbedingungen[363] und der Datenschutzerklärung Ihres Unternehmens hinzufügen. Die Felder für die **Anwendungsdomänen** und die Liste autorisierter Domänen werden automatisch ausgefüllt, wenn Sie in einem späteren Schritt die *Redirect-URIs* hinzufügen. **Beachte:** Diese Informationen werden für den Zustimmungsbildschirm verwendet, den Ihre Benutzer dann angezeigt erhalten, wenn sie MultiPOP für den Abruf der Nachrichten von Gmail berechtigen.
7. Klicken Sie auf **SPEICHERN UND FORTFAHREN**.
8. Klicken Sie auf **BEREICHE HINZUFÜGEN ODER ENTFERNEN**, und geben Sie dann im Abschnitt "Bereiche manuell hinzufügen" **https://mail.google.com/** ein. Klicken Sie danach auf **ZUR TABELLE HINZUFÜGEN**, und klicken Sie danach auf **AKTUALISIEREN**.
9. Klicken Sie auf **SPEICHERN UND FORTFAHREN**.
10. Klicken Sie im Abschnitt Testnutzer auf **ADD USERS** (Benutzer hinzufügen), und geben Sie jedes Gmail-Benutzerkonto ein, von dem Sie Nachrichten abrufen werden. Klicken Sie danach auf **HINZUFÜGEN** (beachten Sie auch die Hinweise zum Veröffentlichungsstatus[149] Ihrer App weiter unten).
11. Klicken Sie auf **SPEICHERN UND FORTFAHREN**.
12. Klicken Sie im Abschnitt Fazit am Ende der Seite auf **ZURÜCK ZUM DASHBOARD**.
13. Klicken Sie im Navigationsbereich links auf **Anmeldedaten**, klicken Sie danach auf **(+) ANMELDEDATEN ERSTELLEN**, und wählen Sie **OAuth-Client-ID** aus.
14. Wählen Sie im Dropdownmenü "Anwendungstyp" den Eintrag **Webanwendung** aus, und klicken Sie danach im Abschnitt "Autorisierte Weiterleitungs-URIs", click **+ URI HINZUFÜGEN**. Geben Sie den Weiterleitungs-URI ein. Der Redirect-URI, der im Konfigurationsdialog für MultiPOP angezeigt wird, ist ein Beispiel, das aus dem SMTP-Hostnamen[184] der Standard-Domäne[181] erstellt wird. Er sollte für die Benutzer dieser Domäne bei der Anmeldung an Webmail nutzbar sein. Sie sollten auch für alle anderen MDaemon-Domänen, die Ihre Benutzer für die Anmeldung an Webmail möglicherweise verwenden, solche Redirect-URIs erstellen. Ein

Beispiel hierzu: "https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Office365" würde für alle Benutzer funktionieren, die sich über die Domäne mail.example.com an Webmail anmelden.

15. Klicken Sie auf **ERSTELLEN**.
16. Kopieren Sie die Daten aus den Feldern **Client-ID** und **Clientschlüssel** in die Felder für die Client-ID und den Client-Schlüssel in Ihrem Konfigurationsdialog MultiPOP.

Veröffentlichungsstatus — Diese Anleitung bezieht sich auf die Erstellung einer Google-App mit dem Veröffentlichungsstatus "**Test**". Dieser Status erfordert das Hinzufügen jedes einzelnen Google-Benutzerkontos, das die App zum Abruf von Nachrichten aus Gmail verwenden wird. Die Höchstgrenze sind hierbei 100 Benutzer. Wenn Ihre Benutzer in Webmail dazu aufgefordert werden, MDaemon die Berechtigung zum Abruf von Nachrichten aus Gmail zu erteilen, erscheint eine Warnmeldung. Sie fordert den Benutzer dazu auf, zu bestätigen, dass Testzugriff auf das Projekt besteht und dass die Risiken verstanden werden, die mit dem Zugriff einer ungeprüften App auf die Daten verbunden sind. Die eingeräumte Berechtigung verfällt nach sieben Tagen; alle Benutzer müssen daher einmal wöchentlich den Zugriff auf Gmail für den Nachrichtenabruf erneut gestatten.

Um diese Einschränkungen und Anforderungen außer Kraft zu setzen, müssen Sie den Status der App auf "**In Produktion**" setzen. Sie müssen dazu unter Umständen einen Prüfprozess durchlaufen. Nähere Informationen über die Prüfung von Apps und den Veröffentlichungsstatus finden Sie in folgenden Artikeln, die Google in englischer Sprache veröffentlicht hat: Erstellen Ihres OAuth-Zustimmungsbildschirms und FAQ zur Prüfung der Authentifizierungs-API.

Für Microsoft (Office) 365

Um MultiPOP die Anmeldung mithilfe von OAuth 2.0 für den Abruf von Nachrichten aus Microsoft (Office) 365 l für Ihre Benutzer zu gestatten, erstellen Sie eine Microsoft-Azure-Applikation. Gehen Sie dazu folgendermaßen vor:

1. Rufen Sie im Azure-Portal die Seite Microsoft Azure Active Directory auf, und klicken Sie im Navigationsbereich links auf **App-Registrierungen** (falls Sie noch nicht über ein Microsoft-Azure-Benutzerkonto verfügen, müssen Sie dieses zuerst erstellen).
2. Klicken Sie auf **+ Neue Registrierung**.
3. Tragen Sie im Feld **Name** den Namen der App ein (z.B. "Mailbox OAuth für Microsoft Office 365").
4. Wählen Sie im Abschnitt "Unterstützte Kontotypen" die Option **Konten in einem beliebigen Organisationsverzeichnis (beliebiger Microsoft Entra ID-Mandant - mandantenfähig)**.

5. Wählen Sie im Abschnitt "Umleitungs-URI" im Dropdownmenü Plattform den Eintrag **Web**. Geben Sie dann Ihren **Redirect-URI** für Microsoft (Office) 365 im Feld Umleitungs-URI ein. Der Redirect-URI, der im Konfigurationsdialog für MultiPOP angezeigt wird, ist ein Beispiel, das aus dem SMTP-Hostnamen[184] der Standard-Domäne[181] erstellt wird. Er sollte für die Benutzer dieser Domäne bei der Anmeldung an Webmail nutzbar sein. Sie sollten auch für alle anderen MDaemon-Domänen, die Ihre Benutzer für die Anmeldung an Webmail möglicherweise verwenden, solche Redirect-URIs erstellen. Ein Beispiel hierzu: "https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Office365" würde für alle Benutzer funktionieren, die sich über die Domäne mail.example.com an Webmail anmelden.
6. Klicken Sie auf **Registrieren**.
7. Speichern Sie die **Anwendungs-ID (Client)**; Sie können diese mithilfe einer Schaltfläche, die neben der ID angezeigt wird, in die Zwischenablage kopieren. Sie können diese ID auch später noch auslesen; klicken Sie dazu im Navigationsbereich links auf **Übersicht**.
8. Falls Sie weitere Redirect-URIs hinzufügen wollen, klicken Sie auf die Verknüpfung **Umleitungs-URIs: 1 vom Typ "Web"** im rechten Bereich. Klicken Sie danach im Abschnitt Umleitungs-URIs auf **URI hinzufügen**, und wiederholen Sie diesen Vorgang, falls nötig. Klicken Sie zum Abschluss auf **Speichern**.
9. Klicken Sie im Navigationsbereich links auf **API-Berechtigungen**.
10. Klicken Sie auf **+ Berechtigung hinzufügen**.
11. Klicken Sie auf **Microsoft Graph**.
12. Klicken Sie auf **Delegierte Berechtigungen**.
13. Blättern Sie nach unten bis zum Abschnitt **POP**, und aktivieren Sie dort den Eintrag **POP.AccessAsUser.All.** Blättern Sie danach weiter nach unten bis zum Abschnitt **User**, und aktivieren Sie dort den Eintrag **User.Read** (User.Read ist bereits per Voreinstellung aktiv).
14. Klicken Sie auf **Berechtigungen hinzufügen**.
15. Klicken Sie im Navigationsbereich links auf **Zertifikate & Geheimnisse**.
16. Klicken Sie auf **+ Neuer geheimer Clientschlüssel**.
17. Geben Sie eine Beschreibung ein (z.B. "Client-Schlüssel für MultiPOP-OAuth-App für Microsoft Office 365").
18. Wählen Sie die Gültigkeitsdauer für den Clientschlüssel aus.
19. Klicken Sie auf **Hinzufügen**.
20. Speichern Sie den erzeugten Clientschlüssel. Sie finden diesen im Feld **Wert**; Sie können ihn mithilfe einer Schaltfläche, die neben dem Clientschlüssel angezeigt wird, in die Zwischenablage kopieren. **Beachte:** Sie können den Clientschlüssel nur jetzt auslesen. Wenn Sie die Seite später erneut aufsuchen, erscheint der Clientschlüssel nicht mehr. Es wird dann eine Schaltfläche **Löschen** angezeigt, mit deren Hilfe Sie den Clientschlüssel löschen können, falls dies erforderlich ist. Nach dem Löschen des Clientschlüssels können Sie einen neuen Clientschlüssel erzeugen.
21. Kopieren Sie die Daten aus den Feldern **Anwendungs-ID (Client)** und **Clientschlüssel** in die Felder für die Client-ID und den Client-Schlüssel in Ihrem Konfigurationsdialog MultiPOP.

Siehe auch:

Benutzerkonten-Editor | MultiPOP 739
Nachrichten-Zeitplanung | Abruf über MultiPOP 382

3.1.13 DomainPOP

Mit Hilfe der Funktion DomainPOP ("Einstellungen » Server-Einstellungen » DomainPOP") kann MDaemon Nachrichten aus einem externen POP-Postfach abrufen und an die eigenen Benutzer weiterverteilen. Dabei werden zunächst alle Nachrichten aus dem angegebenen Postfach beim ISP mit Hilfe des POP3-Protokolls abgerufen. Danach werden die Nachrichten gemäß den konfigurierten Regeln ausgewertet und in den Postfächern der einzelnen Benutzer oder auch in der Extern-Warteschlange abgelegt. Die Verarbeitung erfolgt dabei so, wie wenn die Nachrichten über normale SMTP-Verbindungen empfangen worden wären.

Es ist dabei wichtig zu wissen, dass den Nachrichten aus POP-Postfächern, die mit Hilfe des POP3-Protokolls abgerufen wurden, wichtige Routing-Informationen (manchmal auch "Umschlag" oder "Envelope" genannt) fehlen. Die Routing-Informationen wären nur beim Versand über das für solche Übermittlungen besser geeignete Protokoll SMTP enthalten. Da diese Routing-Informationen nicht zur Verfügung stehen, muss MDaemon die Nachrichten einlesen und durch Auswertung der Kopfzeilen versuchen, den richtigen Adressaten zu bestimmen. Diese Vorgehensweise ist, vorsichtig ausgedrückt, nicht sehr zuverlässig. Kopfzeilen enthalten oft leider nicht ausreichend Informationen, um den Adressaten zu bestimmen. Dieses Fehlen der eigentlich wichtigsten Information einer Nachricht überhaupt – des Empfängers - scheint verwunderlich, aber es ist zu bedenken, dass die Nachricht für eine Auslieferung über das POP-Protokoll an den Empfänger eigentlich gar nicht gedacht war. Bei SMTP wiederum ist der Inhalt einer Nachricht unwichtig, da das Übertragungsprotokoll selbst dem Server schon während der Übermittlung mitteilt, wer der Adressat der Nachricht ist.

MDaemon verfügt über umfassende Auswertungsfunktionen für die Kopfzeilen einer Nachricht, um eine zuverlässige Zustellung zu gewährleisten. Nach dem Abruf einer Nachricht von einem externen Postfach wertet MDaemon sofort alle Kopfzeilen aus und erstellt eine Liste möglicher Empfänger, wobei jede E-Mail-Adresse, die MDaemon in einer ausgewerteten Kopfzeilen findet, mit einbezogen wird.

Sobald dieser Vorgang abgeschlossen ist, teilt MDaemon die Liste in lokale und externe Empfänger auf. Vorher werden noch alle ausgewerteten Adressen auf gültige Aliasnamen 827 überprüft und diese ggf. umgesetzt. Alle lokalen Empfänger (Adressen in einer lokalen Domäne von MDaemon) erhalten je eine Kopie der Nachricht. Wie mit den externen Empfängern zu verfahren ist, wird im entsprechenden Konfigurationsdialog eingestellt. MDaemon kann diese externen Adressen ignorieren, eine Übersicht davon dem Postmaster zuleiten oder sie in die Zustellung einbeziehen. In dem letzten Fall stellt MDaemon eine Kopie der Nachricht dem externen Empfänger tatsächlich zu. Diese letzte Vorgehensweise ist aber nur unter seltenen Umständen angebracht.

Es muss besonders darauf geachtet werden, dass keine doppelten Nachrichten oder Endlosschleifen bei der Zustellung entstehen. Bei Mailinglisten tritt häufig ein besonderes Problem auf, das sich aus dem Fehlen des SMTP-Umschlags ergibt. Üblicherweise enthalten Nachrichten aus Mailinglisten keine Hinweise auf die Empfänger im Nachrichtentext. Stattdessen setzt der Generator der Mailingliste einfach den Namen der Liste in das Adressatenfeld `TO:` ein. Dadurch ergibt sich das Problem, dass MDaemon, wenn das Feld `TO:` den Namen der Liste enthält, nach dem

Abruf der Nachricht dieses Feld auswertet, dabei auf den Namen der Liste stößt und die Nachricht sofort wieder an diese Liste zurück schickt. Dadurch würde aber eine weitere Kopie derselben Nachricht über das POP-Postfach MDaemon wiederum zugeleitet werden, und der Kreislauf würde von vorn beginnen. Um das zu verhindern, muss der Systemverwalter die Funktionen von MDaemon so nutzen, dass Nachrichten aus Mailinglisten entweder gelöscht oder so umbenannt werden, dass sie den richtigen lokalen Empfängern zugehen können. Dazu können auch Routing-Regeln oder Inhaltsfilter benutzt werden.

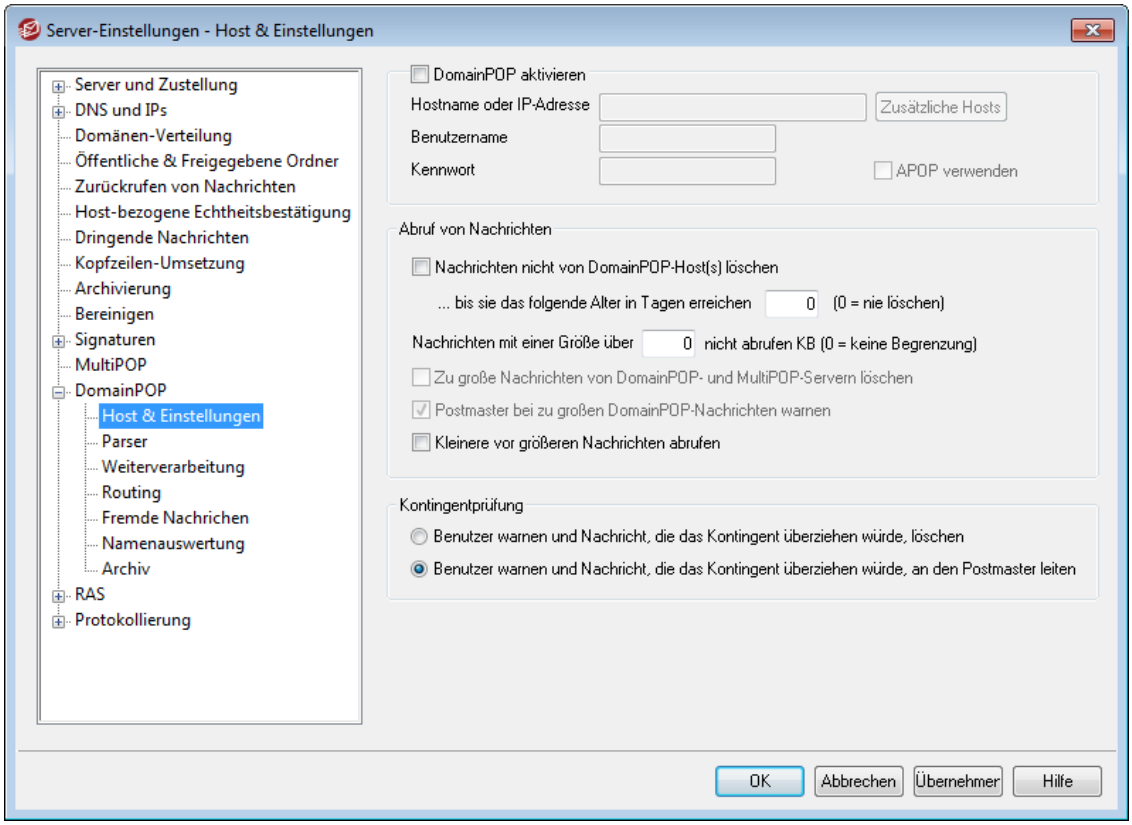
Zusätzliche Probleme entstehen aus der Frage, wie ungewollte doppelte Nachrichten verhindert werden können. Nachrichten, die per SMTP beim POP-Postfach des ISP eingeliefert werden, können leicht ungewollte doppelte Nachrichten erzeugen, sobald sie durch DomainPOP abgerufen wurden. Wird zum Beispiel eine Nachricht an einen Benutzer einer Ihrer lokalen Domänen und ein Durchschlag davon an einen anderen Benutzer derselben lokalen Domäne geschickt, so werden über SMTP zwei Kopien der Nachricht beim ISP eingeliefert, eine für jeden Empfänger. Jede dieser beiden Nachrichten enthält Verweise auf beide Empfänger, einen im Feld `TO:`, den anderen im Feld `CC:`. MDaemon ruft die beiden identischen Nachrichten ab und wertet jeweils beide Adressen aus. Infolgedessen würden beide Empfänger je eine unerwünschte doppelte Nachricht empfangen. Um diese Art doppelter Nachrichten zu verhindern, kann MDaemon anhand einer frei wählbaren Kopfzeile die Nachrichten auf Doppelte untersuchen. Die Kopfzeile `Message-ID` („Nachrichten-ID") ist dafür besonders gut geeignet. In dem obigen Beispiel sind beide Nachrichten identisch und enthalten daher auch denselben Eintrag in der Nachrichten-ID. MDaemon nutzt diesen Eintrag, um die zweite Nachricht bereits während des Abrufens zu identifizieren und zu löschen, noch bevor die Adressauswertung beginnt.

Als letzte Maßnahme gegen doppelte Nachrichten und Endlosschleifen stellt MDaemon fest, wie viele Zwischenstationen (englisch auch als "Hops" bezeichnet) eine Nachricht durchlaufen hat. Jedes Mal, wenn ein SMTP-Mailserver eine Nachricht verarbeitet, "stempelt" er sie mit einer Kopfzeile "Received" ("Empfangen"). MDaemon zählt alle diese Kopfzeilen, wenn eine Nachricht zum ersten Mal ausgewertet wird. Wenn die Summe der Zwischenstationen eine festgelegte Grenze überschreitet, ist die Nachricht wahrscheinlich in einer Endlosschleife gefangen und sollte aus dem Postweg entfernt und ins Defekt-Verzeichnis verschoben werden. Dieser Grenzwert kann im Konfigurationsdialog für die Wiederholungs-Warteschlange[864] gesetzt werden.

Siehe auch:

Inhaltsfilter[648]
Mailinglisten[269]

3.1.13.1 Host & Einstellungen



Eigenschaften des DomainPOP-Hosts

Abruf von Nachrichten über DomainPOP aktivieren
Ist diese Option ausgewählt, ruft MDaemon nach Maßgabe der folgenden Einstellungen Nachrichten von einem DomainPOP-Server ab und verteilt sie an die lokalen Benutzer.

Hostname oder IP-Adresse
Hier wird der Hostname oder die IP-Adresse des abzufragenden DomainPOP-Servers eingetragen.

Zusätzliche Hosts
Ein Klick auf dieses Steuerelement öffnet die Datei `DpopXtra.dat`, in die direkt weitere Hosts eingetragen können; von diesen werden ebenfalls Nachrichten per DomainPOP abgerufen. Die Datei enthält weitere Hinweise und nähere Informationen.

Benutzername
Der Anmeldename für das abzufragende POP-Postfach wird hier eingetragen.

Kennwort
Hier muss das POP- oder APOP-Kennwort für das verwendete Benutzerkonto angegeben werden.

APOP verwenden
Sollen beim Abruf von Nachrichten der Befehl APOP und die Benutzerüberprüfung nach CRAM-MD5 verwendet werden, so muss diese

Option gesetzt sein. Bei der Benutzeranmeldung werden dann die Kennwörter nicht im Klartext gesendet.

Abruf von Nachrichten

Nachrichten nicht von DomainPOP-Host(s) löschen
Ist diese Option aktiv, löscht MDaemon die abgerufenen Nachrichten nicht von dem DomainPOP-Server.

...bis sie das folgende Alter in Tagen erreichen (0 = nie löschen)
Hier wird die Anzahl der Tage festgelegt, für die eine Nachricht auf dem DomainPOP-Host verbleiben kann, bevor sie gelöscht wird. Der Wert 0 bewirkt, dass ältere Nachrichten nicht gelöscht werden.

Manche ISP begrenzen die Dauer, für die die Nachrichten, in dem POP-Postfach verbleiben dürfen.

Nachrichten mit einer Größe über [xx] KB nicht abrufen (0 = keine Begrenzung)
Nachrichten, welche mindestens so groß sind wie hier angegeben, werden vom DomainPOP-Server nicht abgerufen. Der Wert 0 bewirkt, dass alle Nachrichten ohne Ansehen der Größe abgerufen werden.

Zu große Nachrichten von DomainPOP- und MultiPOP-Servern löschen
Wenn diese Option aktiv ist, löscht MDaemon alle Nachrichten, die über der Größenbegrenzung liegen, sofort von DomainPOP- und MultiPOP-Gegenstellen, ohne sie abzurufen.

Postmaster bei zu großen DomainPOP-Nachrichten warnen
Um dem Postmaster eine Warnmitteilung zukommen zu lassen, wenn eine zu große Nachricht beim Abruf per DomainPOP festgestellt wurde, muss diese Option aktiv sein.

Kleinere vor größeren Nachrichten abrufen
Diese Option bewirkt, dass sich die Reihenfolge, in der die Nachrichten abgerufen werden, nach deren Größe richtet – die kleinsten Nachrichten werden vor den größeren Nachrichten abgerufen.

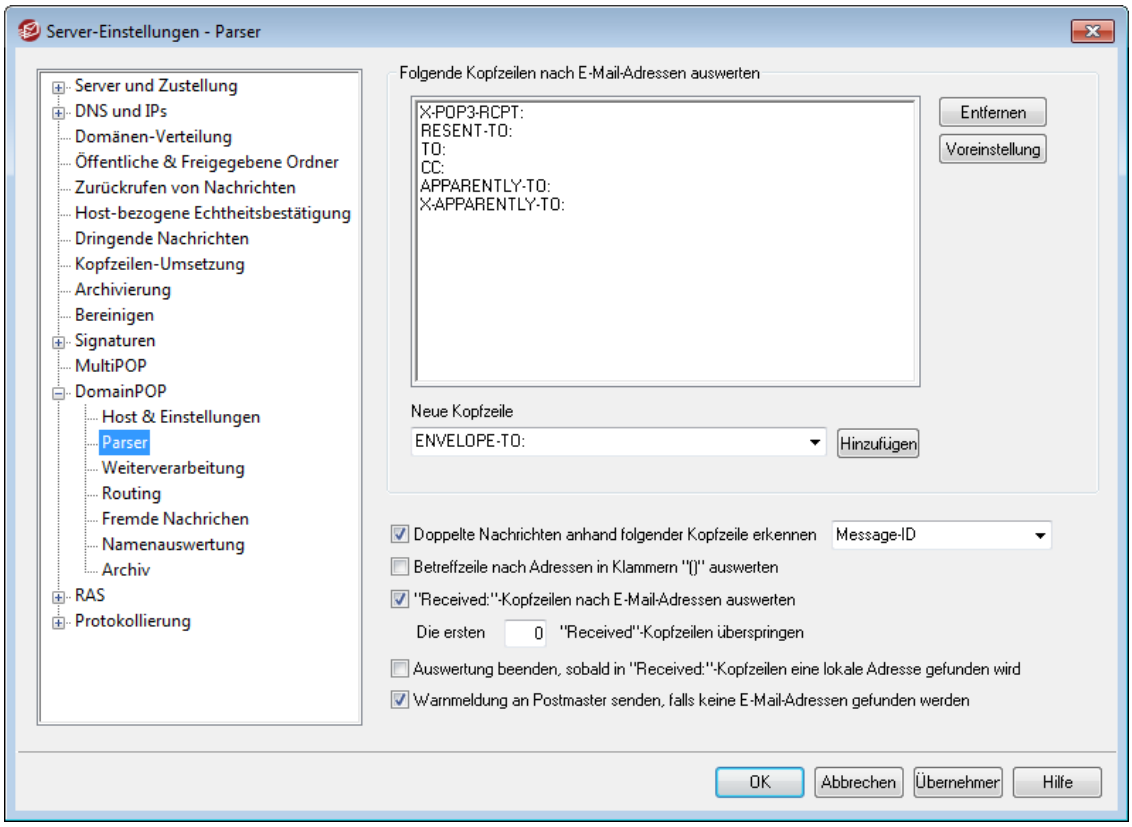
Diese Option bewirkt, dass kleinere Nachrichten schneller abgerufen werden; der Aufwand für die Sortierung und Verarbeitung der Nachrichten im System ist dann aber größer.

Kontingentprüfung

Benutzer warnen und Nachricht, die das Kontingent überziehen würde, löschen
Diese Option veranlasst MDaemon, Nachrichten zu löschen, falls der Adressat sein Speicherplatzkontingent (wie im Konfigurationsdialog Kontingente 731 des Benutzerkonten-Editors festgelegt) ausgeschöpft hat. MDaemon benachrichtigt den betreffenden Benutzer davon, dass seine Kontingent erschöpft ist, und dass deswegen eine Nachricht gelöscht wurde.

Benutzer warnen und Nachricht, die das Kontingent überziehen würde, an den Postmaster leiten
Mit dieser Option löscht MDaemon Nachrichten für Adressaten, die ihre Speicherplatzkontingent ausgeschöpft haben, nicht, sondern leitet sie an den Postmaster weiter. Der Benutzer wird benachrichtigt, dass sein Kontingent erschöpft ist.

3.1.13.2 Parser



Folgende Kopfzeilen nach E-Mail-Adressen auswerten
MDaemon durchsucht die in diesem Feld aufgeführten Kopfzeilen nach E-Mail-Adressen. Es wird jede Kopfzeile in allen Nachrichten nach Adressen ausgewertet.

Entfernen
Dieses Steuerelement löscht die jeweils ausgewählten Einträge aus der Liste.

Voreinstellung
Ein Klick auf dieses Steuerelement löscht den Inhalt der Liste der Kopfzeilen und setzt die per Voreinstellung eingetragenen Kopfzeilen wieder ein. Diese sind für die Adressauswertung üblicherweise ausreichend.

Neue Kopfzeile
Geben Sie hier die Kopfzeile ein, die Sie der Liste der Kopfzeilen hinzufügen wollen.

Hinzufügen
Nachdem Sie die Kopfzeile in das Feld *Neue Kopfzeile* eingetragen haben, klicken Sie auf dieses Steuerelement, um die Kopfzeile der Liste hinzuzufügen.

Doppelte Nachrichten anhand folgender Kopfzeile erkennen
MDaemon erfasst den Inhalt der hier ausgewählten Kopfzeile und prüft diese Kopfzeile in allen Nachrichten desselben Verarbeitungsdurchlaufs darauf, ob ihr Inhalt in mehreren Nachrichten erscheint. Nachrichten, die in der ausgewählten Kopfzeile denselben Inhalt haben, werden nur einmal verarbeitet. Per Voreinstellung wird die Kopfzeile `Message-ID` verwendet.

Betreffzeile nach Adressen in Klammern "()" auswerten
Ist diese Option aktiv, und findet MDaemon eine Adresse in Klammern in der Betreffzeile einer Nachricht, so wird neben anderen ausgewerteten Adressen auch diese Adresse der Liste möglicher Empfänger hinzugefügt.

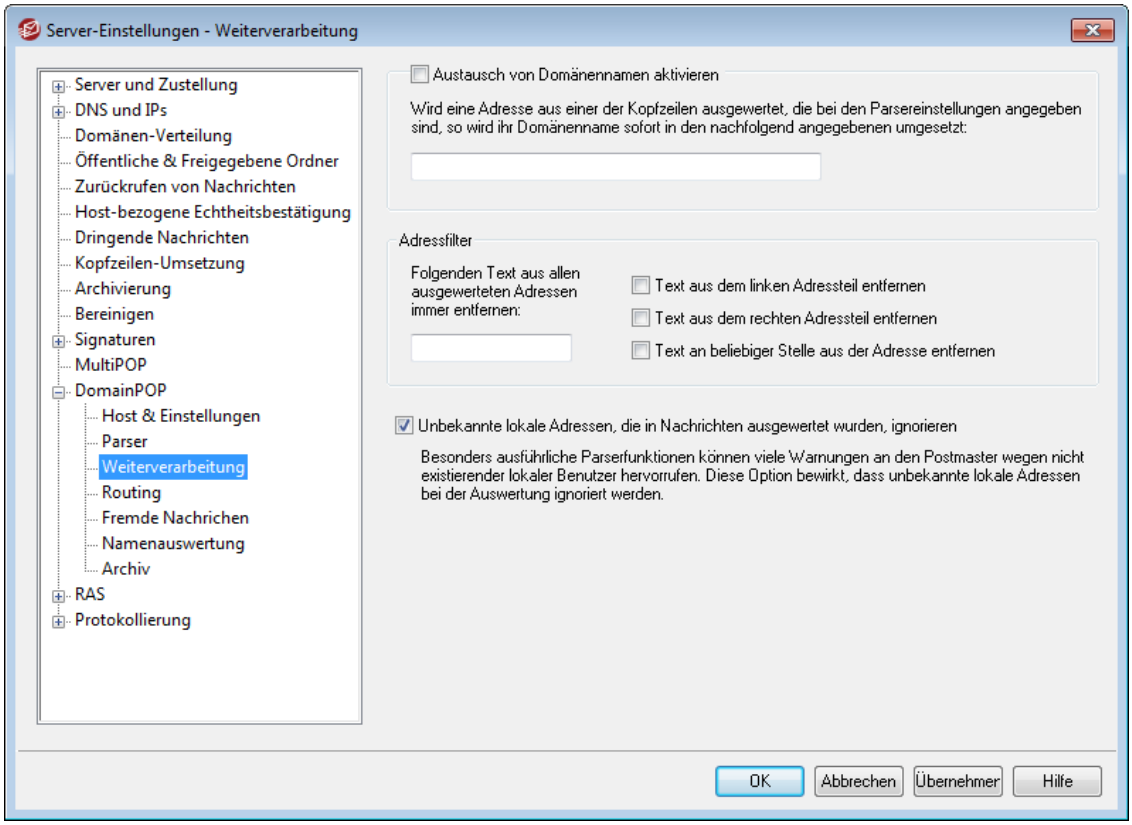
"Received"-Kopfzeilen nach E-Mail-Adressen auswerten
Es ist zulässig, Empfängerinformationen, die eigentlich im SMTP-Umschlag zu finden wären, in den Kopfzeilen "Received" der Nachricht zu speichern. Daher kann die Adresse des Empfängers u.U. durch Auswertung der Received-Kopfzeilen festgestellt werden. Wenn diese Option aktiv ist, versucht MDaemon, durch Auswertung aller "Received"-Kopfzeilen einer Nachricht nach gültigen Adressen den Empfänger festzustellen.

Die ersten xx "Received"-Kopfzeilen überspringen
Manchmal ist es sinnvoll, nicht alle Received-Kopfzeilen zu verarbeiten. Mit dieser Einstellung kann festgelegt werden, wie viele Received-Kopfzeilen MDaemon am Anfang einer Nachricht überspringen soll, bevor mit der Auswertung begonnen wird.

Auswertung beenden, sobald in "Received"-Kopfzeilen eine lokale Adresse gefunden wird
Erkennt MDaemon in den Received-Kopfzeilen eine gültige lokale Adresse, so wird die Auswertung beendet, ohne dass weiter in der Nachricht nach gültigen Adressen gesucht wird.

Warnmeldung an Postmaster senden, falls keine E-Mail-Adressen gefunden werden
Per Voreinstellung sendet MDaemon eine Warnmeldung per E-Mail an den Postmaster, falls der Parser keine E-Mail-Adressen finden konnte. Falls Sie diese Warnmeldungen nicht wünschen, deaktivieren Sie diese Option.

3.1.13.3 Weiterverarbeitung



Austausch von Domänennamen

Austausch von Domänennamen aktivieren
Diese Option kann helfen, die Anzahl der für ein System nötigen Adress-Aliasnamen zu verringern. Nach dem Abruf einer Nachricht werden sofort alle Domänennamen aller Adressen, die in der der abgerufenen Nachricht ausgewertet wurden, durch den hier angegebenen Domänennamen ersetzt.

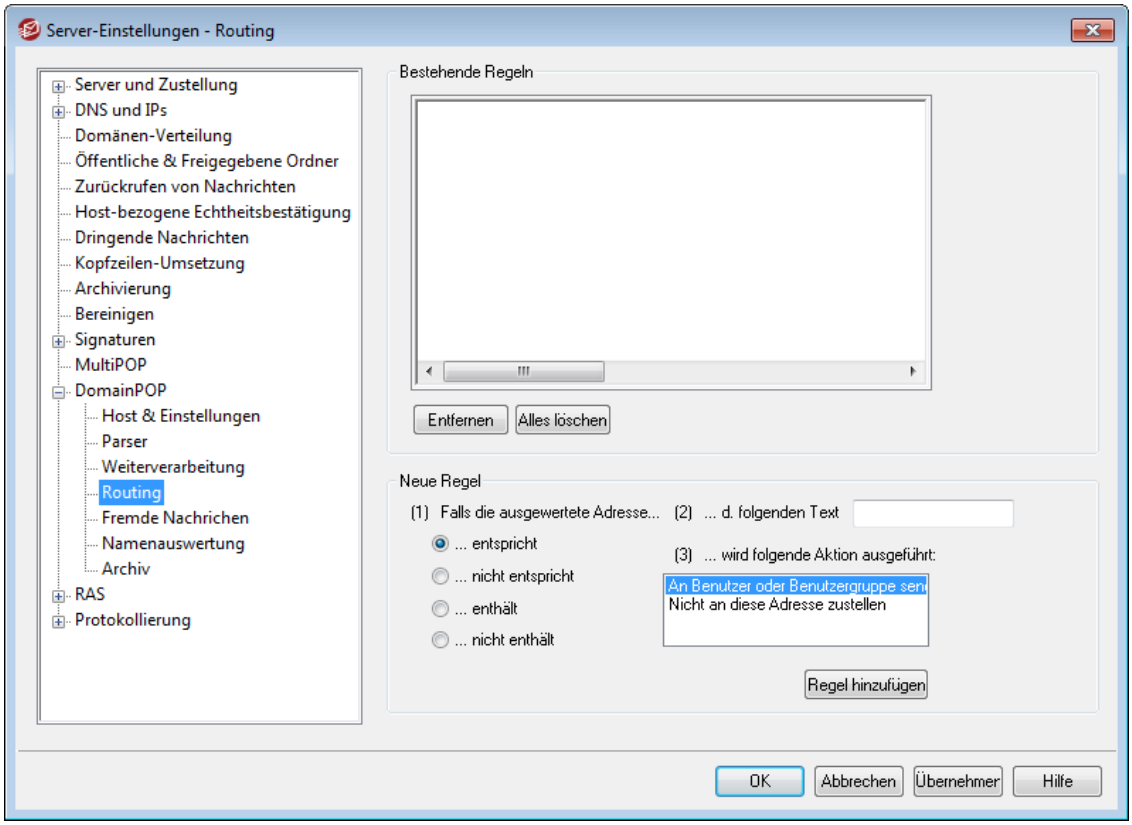
Adressfilter

Folgenden Text aus allen ausgewerteten Adressen immer entfernen
Manche ISP versehen jede Nachricht mit einer Zeile, die Informationen zum Empfänger und zusätzlich Routing-Informationen enthält, die links oder rechts an die Empfängerdaten angefügt werden. Dieser "Stempel" allein wäre für die Auswertung der Empfängeradresse ideal, jedoch würden die zusätzlichen Informationen umfangreiche Aliasnamen notwendig machen, damit eine Auswertung erfolgen kann. Daher kann der überflüssige zusätzliche Text hier angegeben werden; MDaemon löscht ihn dann aus allen ausgewerteten Adressen.

Unbekannte lokale Adressen, die in Nachrichten ausgewertet wurden, ignorieren
Wie oben erläutert, ändert die Funktion "Austausch von Domänennamen" die Domänennamen aller aus einer Nachricht ausgewerteten E-Mail-Adressen in den angegebenen Domänennamen. Dabei können Adressen entstehen, für die auf dem lokalen Server kein Benutzerkonto besteht. Da der Domänennamen gültig, der Postfachname aber nicht gültig wäre, würde MDaemon diese Adressen wie unbekannte lokale Benutzer behandeln. Üblicherweise werden für solche Nachrichten Meldungen über Zustellfehler wegen unbekannter Benutzerkonten

versandt. Klicken Sie hier, um den Versand solcher Fehlermeldungen zu unterbinden.

3.1.13.4 Routing



Bestehende Regeln

In dieser Liste erscheinen die definierten Routing-Regeln, die auf die Nachrichten angewendet werden.

Entfernen
Um eine Regel aus der Liste zu löschen, wählen Sie die Regel aus, und klicken Sie dann auf dieses Steuerelement.

Alles löschen
Durch Anklicken dieses Steuerelements können Sie alle bestehenden Regeln löschen.

Neue Regel

(1) Falls die ausgewertete Adresse...

d. folgenden Text entspricht/nicht entspricht, enthält/nicht enthält
Hier wird die Bedingung definiert, welche bestimmt, ob eine Routing-Regel auf eine Adresse anwendbar ist. MDaemon durchsucht jede Adresse nach dem Eintrag in dem Feld "Text zu Schritt (1)" und verfährt dann je nach der hier getroffenen Einstellung: es wird festgestellt, ob die Adresse übereinstimmt, nicht übereinstimmt oder teilweise übereinstimmt oder nicht übereinstimmt.

...Text zu Schritt (1):
Geben Sie hier den Text an, den MDaemon in der jeweils ausgewerteten Adresse suchen soll.

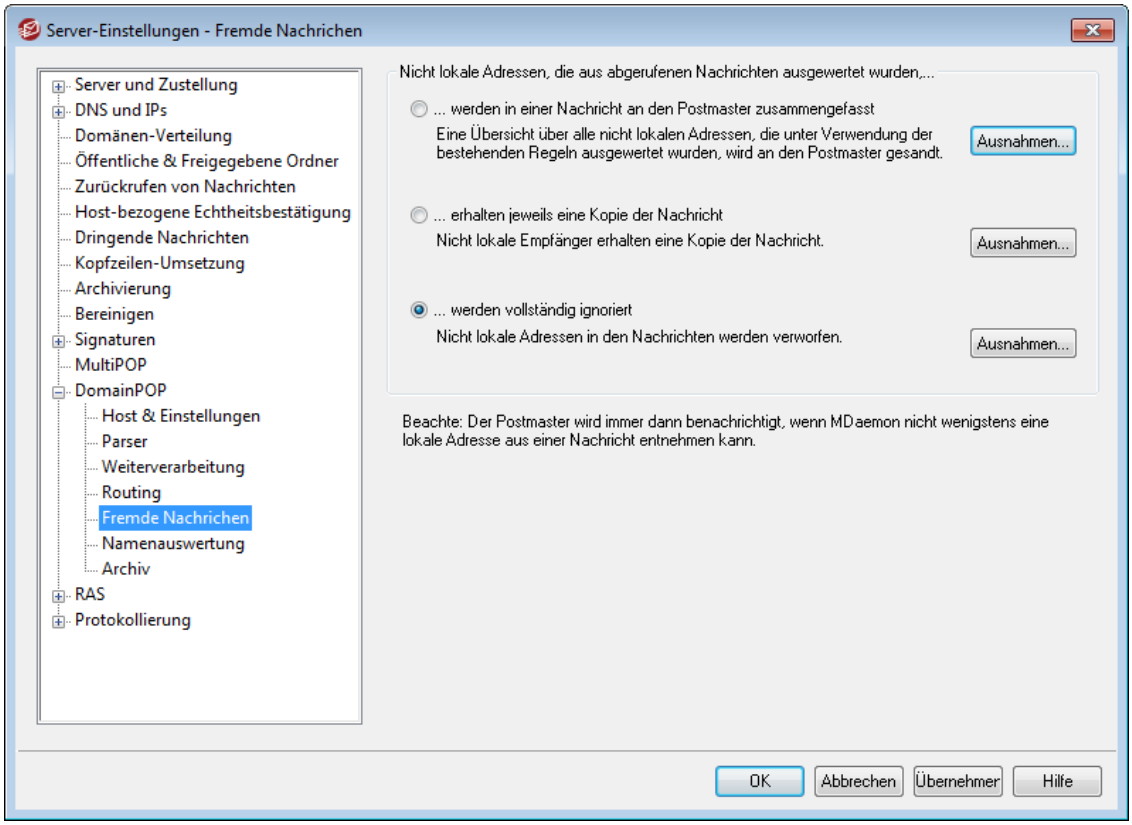
(3) ...wird folgende Aktion ausgeführt:
Diese Auswahl legt fest, wie mit einer Nachricht zu verfahren ist, falls die vorher definierte Bedingung zutrifft. Mögliche Verfahrensweisen sind:

An Benutzer oder Benutzergruppe senden - Die Auswahl dieser Möglichkeit ruft einen Editor auf, in dem eine Liste von E-Mail-Adressen angegeben werden kann, an die je eine Kopie der betreffenden Nachricht zugestellt wird.

Nicht an diese Adresse zustellen - Ist dieser Eintrag gewählt, so wird die Nachricht nicht an die angegebene Adresse zugestellt.

Regel hinzufügen
Nachdem Sie die Daten für die Regel eingegeben haben, klicken Sie auf *Regel hinzufügen*, um die Regel der Liste hinzuzufügen.

3.1.13.5 Fremde Nachrichten



Nicht lokale Adressen, die aus abgerufenen Nachrichten ausgewertet wurden...

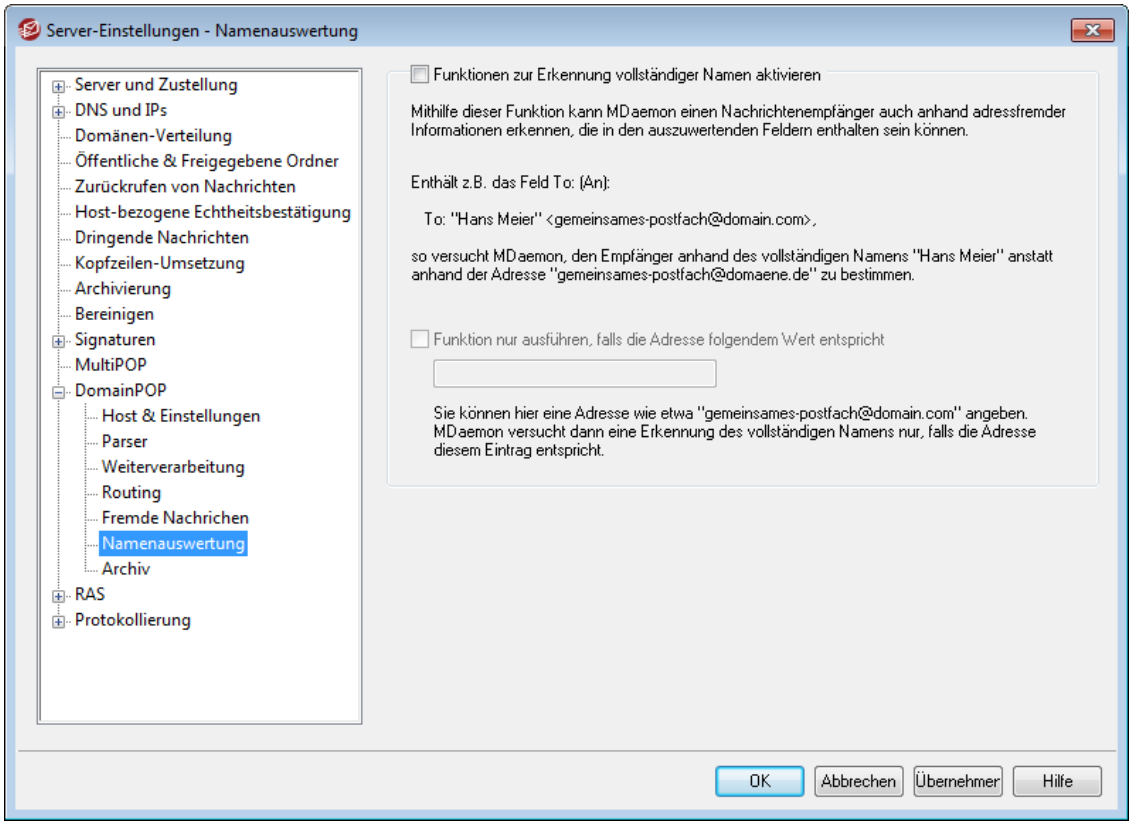
...werden in einer Nachricht an den Postmaster zusammengefasst
Ist diese Option ausgewählt, so sendet MDaemon eine einzelne Kopie der Nachricht zusammen mit einer Liste aller aus der Nachricht mit den vorgegebenen Regeln und Kopfzeilen ausgewerteten nicht-lokalen Adressen an den Postmaster.

...erhalten jeweils eine Kopie der Nachricht
Wenn diese Option aktiv ist, sendet MDaemon eine Kopie der Nachricht an alle nicht-lokalen Empfänger, die aus den Kopfzeilen ausgewertet wurden.

...werden vollständig ignoriert
Mit dieser Einstellung entfernt MDaemon alle nicht-lokalen Adressaten aus der Empfängerliste und verhält sich so, wie wenn die externen Adressen aus der betreffenden Nachricht niemals auswertet worden wären.

Mit Hilfe der verschiedenen Steuerelemente *Ausnahmen...* können Sie Adressen eingeben, die von den jeweiligen Optionen ausgenommen sind.

3.1.13.6 Namenauswertung



Die Namenauswertung funktioniert nur zusammen mit dem Abruf von Nachrichten über DomainPOP. Wenn die Namenauswertung genutzt werden soll, muss daher DomainPOP ebenfalls aktiv sein. DomainPOP ist erreichbar über den Menüeintrag "Einstellungen » Server-Einstellungen » DomainPOP".

Funktionen zur Erkennung vollständiger Namen

Funktionen zur Erkennung vollständiger Namen aktivieren
Mit dieser Funktion kann MDaemon beim Abruf von Nachrichten über DomainPOP nicht nur anhand der E-Mail-Adresse sondern auch anhand des zugehörigen Textes (meist der Vor- und Nachname einer Person) den Empfänger einer Nachricht feststellen.

Die Empfängerkopfzeile `TO:` in einer Nachricht kann beispielsweise so lauten:

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

oder

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

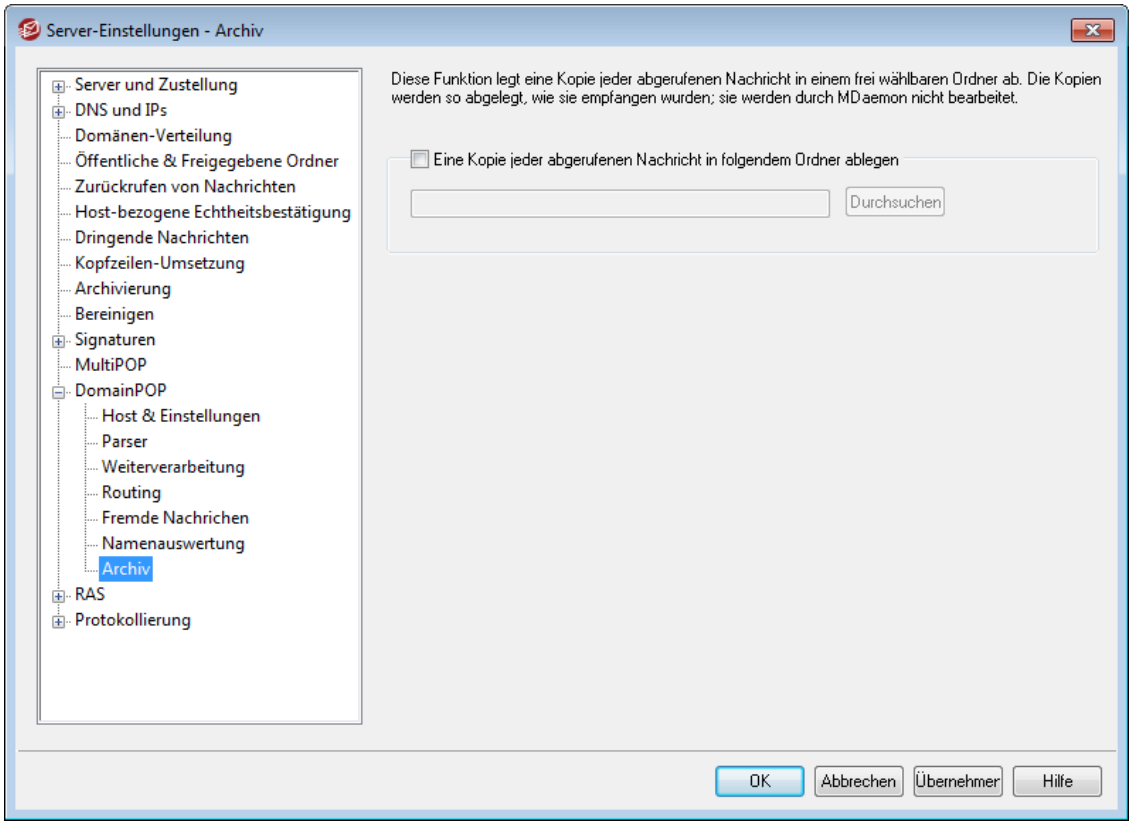
Die Namenauswertung lässt den Teil "`user01@example.com`" außer Betracht. Sie wertet stattdessen den Text "Michael Mason" aus und versucht, diesen Namen in der Benutzerdatenbank von MDaemon zu finden. Falls sich dabei eine Übereinstimmung mit dem vollständigen Namen eines Benutzers ergibt, wird an dessen E-Mail-Adresse zugestellt. Ergibt sich keine Übereinstimmung, so versucht MDaemon die Zustellung anhand der E-Mail-Adresse der Nachricht selbst, im Beispiel "`user01@example.com`".

Der vollständige Name zu einer Adresse darf keine Kommata, Strichpunkte oder Doppelpunkte enthalten.

Funktionen nur ausführen, falls die Adresse folgendem Wert entspricht
Hier kann eine E-Mail-Adresse angegeben werden, die in den ausgewerteten Daten enthalten sein muss, damit die Namenauswertung durchgeführt wird. Damit lässt sich kontrollieren, wann die Namenauswertung zum Einsatz kommt. Sie können beispielsweise als Adresse "`user01@example.com`" angeben, sodass nur bei Nachrichten, deren Adressen diesen Text enthalten, überhaupt die Namenauswertung durchgeführt wird.

Falls z.B. hier "`user01@example.com`" eingetragen ist, bedeutet dies, dass bei "**`TO: 'Michael Mason' <user01@example.com>`**" die Namenauswertung durchgeführt werden kann, bei "**`TO: 'Michael Mason' <user02@example.com>`**" jedoch nicht.

3.1.13.7 Archiv

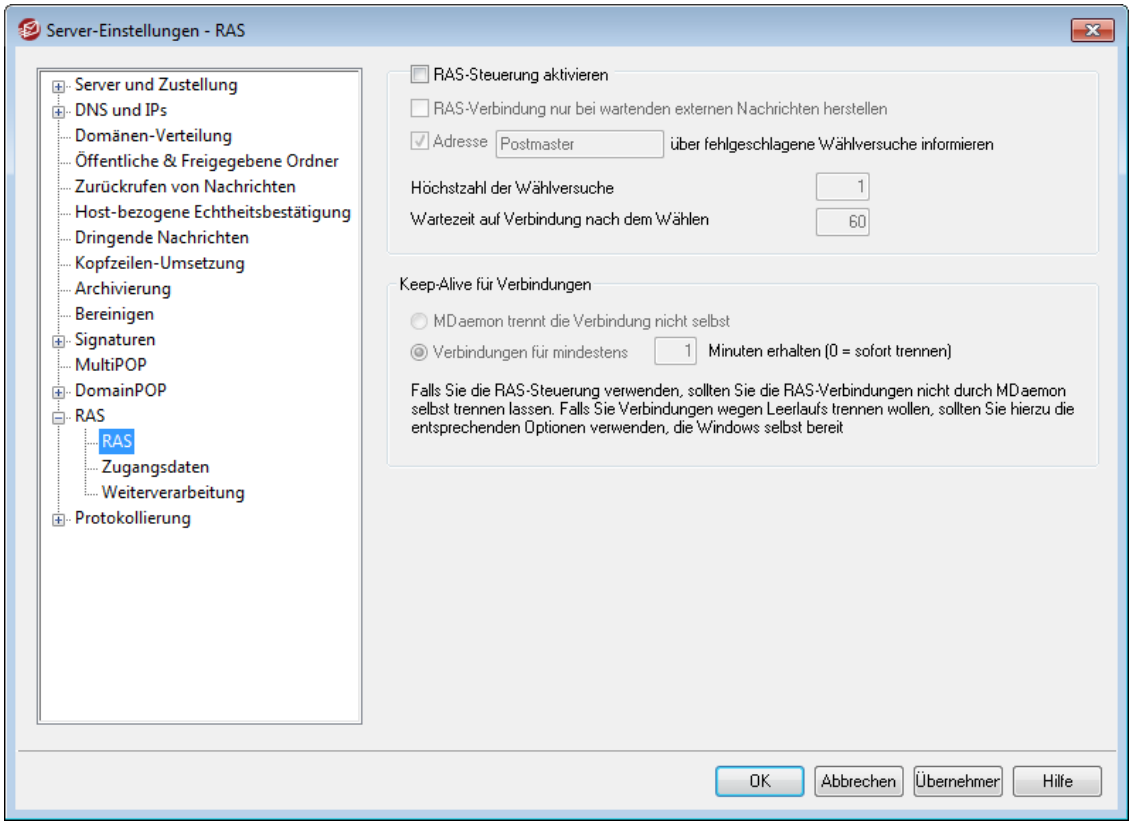


Archiv

Eine Kopie jeder abgerufenen Nachricht in folgendem Ordner ablegen
Diese Option schützt gegen den Verlust abgerufener Nachrichten durch unvorhergesehene Parserfehler oder andere Probleme beim Abrufen großer Nachrichtenmengen. Um eine Kopie jeder abgerufenen Nachricht in dem hier angegebenen Ordner zu speichern, aktivieren Sie diese Option. Die Nachrichten werden so abgelegt, wie sie abgerufen wurden; die Archivkopien werden nicht durch MDaemon bearbeitet.

3.1.14 RAS

3.1.14.1 RAS



Durch Anklicken des Menüeintrags "Einstellungen » Server-Einstellungen » RAS" können Sie die Einstellungen für RAS-Verbindungen einschließlich der Wählverbindungen konfigurieren (solche RAS-Verbindungen werden in manchen Windows-Versionen auch als DFÜ-Verbindungen bezeichnet). Dieser Konfigurationsdialog ist nur verfügbar, falls auf Ihrem System die Remote Access Services installiert sind. MDaemon nutzt diese Einstellungen und die Remote Access Services, falls vor einem Verarbeitungsdurchlauf für externe Nachrichten eine RAS-Verbindung zu Ihrem Internet-Zugangsanbieter hergestellt werden muss.

RAS-Steuerung aktivieren
Ist diese Option aktiv, so verwendet MDaemon die folgenden Einstellungen, um RAS-Verbindungen aufzubauen, bevor externe Nachrichten an externe Hosts gesendet oder von ihnen empfangen werden.

RAS-Verbindung nur bei wartenden externen Nachrichten herstellen
Ist diese Option gesetzt, stellt MDaemon nur dann eine RAS-Verbindung her, wenn externe Nachrichten in der Extern-Warteschlange auf den Versand warten. Dies kann zwar unter Umständen sinnvoll sein, es ist aber zu bedenken, dass MDaemon ohne RAS-Verbindung auch keine Nachrichten **abrufen** kann (es sei denn, diese werden über das lokale Netzwerk übermittelt).

Adresse [Adresse] über fehlgeschlagene Wählversuche informieren
Ist diese Option aktiv, so sendet MDaemon eine Nachricht an die hier angegebene Adresse, wenn ein Verbindungsversuch, gleich aus welchem Grund, fehlschlägt.

Höchstzahl der Wählversuche
MDaemon startet so viele Versuche, die RAS-Verbindung herzustellen, wie hier angegeben, bevor der Vorgang abgebrochen wird.

Wartezeit auf Verbindung nach dem Wählen
Dieser Wert bestimmt, wie lange MDaemon auf den erfolgreichen Verbindungsaufbau der RAS-Verbindung warten soll.

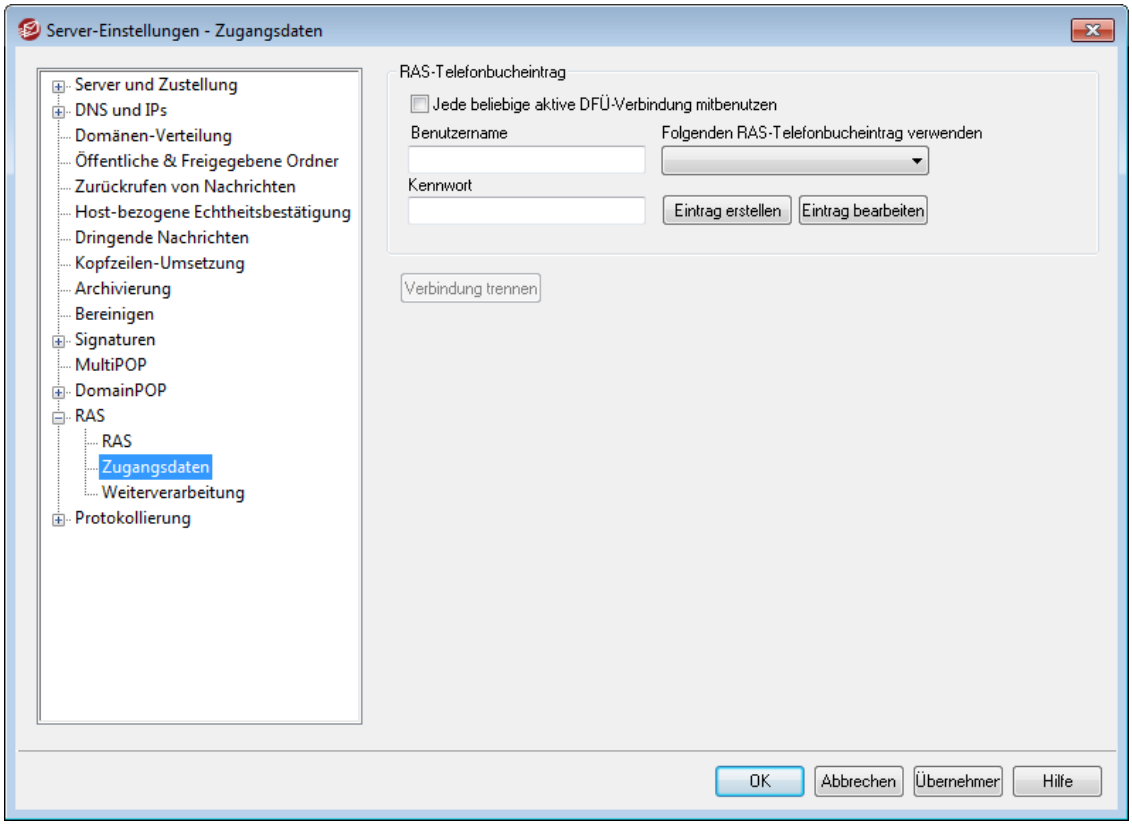
Keep-Alive für Verbindungen

MDaemon trennt die Verbindung nicht selbst
MDaemon trennt eine selbst hergestellte RAS-Verbindung grundsätzlich sofort, wenn der Nachrichtenversand erledigt ist und sich die Verbindung im Leerlauf befindet. Diese Option bewirkt, dass die Verbindung auch nach Abschluss des Nachrichtenversands bestehen bleibt.

MDaemon trennt in keinem Falle Verbindungen, die nicht durch MDaemon selbst hergestellt wurden.

Verbindung für mindestens [xx] Minuten erhalten (0 = sofort trennen)
Diese Option veranlasst MDaemon, die RAS-Verbindung mindestens für die hier angegebene Zeitdauer, jedenfalls aber bis zum Abschluss des Nachrichtenversands zu erhalten.

3.1.14.2 Zugangsdaten



RAS-Telefonbucheintrag

Jede beliebige aktive DFÜ-Verbindung mitbenutzen
Mit dieser Option kann MDaemon jede RAS-Verbindung mitbenutzen, die gerade aktiv ist. Bevor MDaemon zur festgelegten Zeit eine Verbindung herstellt, wird dann immer geprüft, ob schon eine andere DFÜ-Verbindung besteht, die mitbenutzt werden kann. Trifft dies zu, so stellt MDaemon keine eigene Verbindung her.

Benutzername
Dieser Eintrag wird dem ISP während der Anmeldung übermittelt. Er ist der Benutzer- oder Anmeldename, den der ISP erwartet.

Kennwort
Dieser Eintrag muss das zu dem Benutzernamen gehörende Kennwort enthalten. Es wird ebenfalls bei der Anmeldung übermittelt.

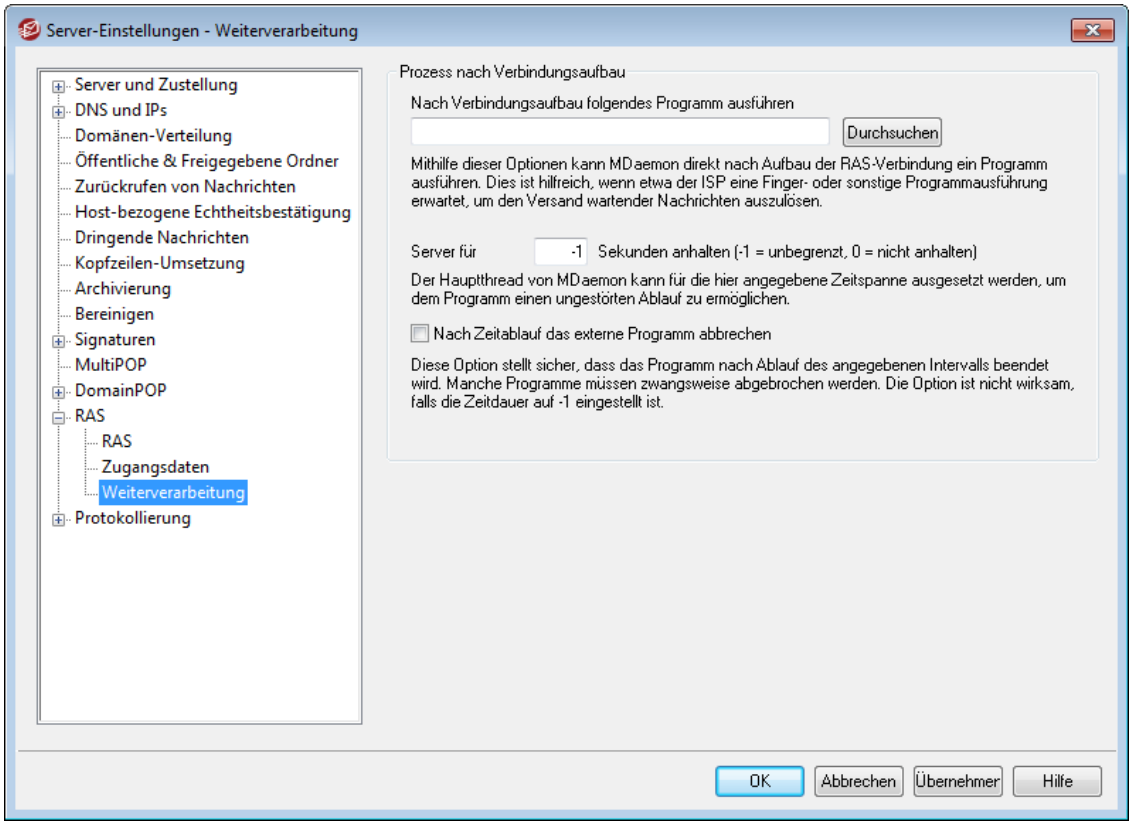
Folgenden RAS-Telefonbucheintrag verwenden
In diesem Auswahlmenü werden die bereits definierten Einträge in den RAS-Profilen von Windows dargestellt. Der zu verwendende Eintrag muss ausgewählt werden.

Neuer Eintrag
Durch Anklicken dieses Steuerelements können Sie einen neuen RAS-Telefonbucheintrag erstellen.

Eintrag bearbeiten
Um den gerade ausgewählten RAS-Telefonbucheintrag zu bearbeiten, klicken Sie auf dieses Steuerelement.

Verbindung trennen
Durch Anklicken dieses Steuerelements wird die RAS-Verbindung sofort getrennt. Es kann nur betätigt werden, falls MDaemon die Verbindung selbst hergestellt hat.

3.1.14.3 Weiterverarbeitung



Prozess nach Verbindungsaufbau

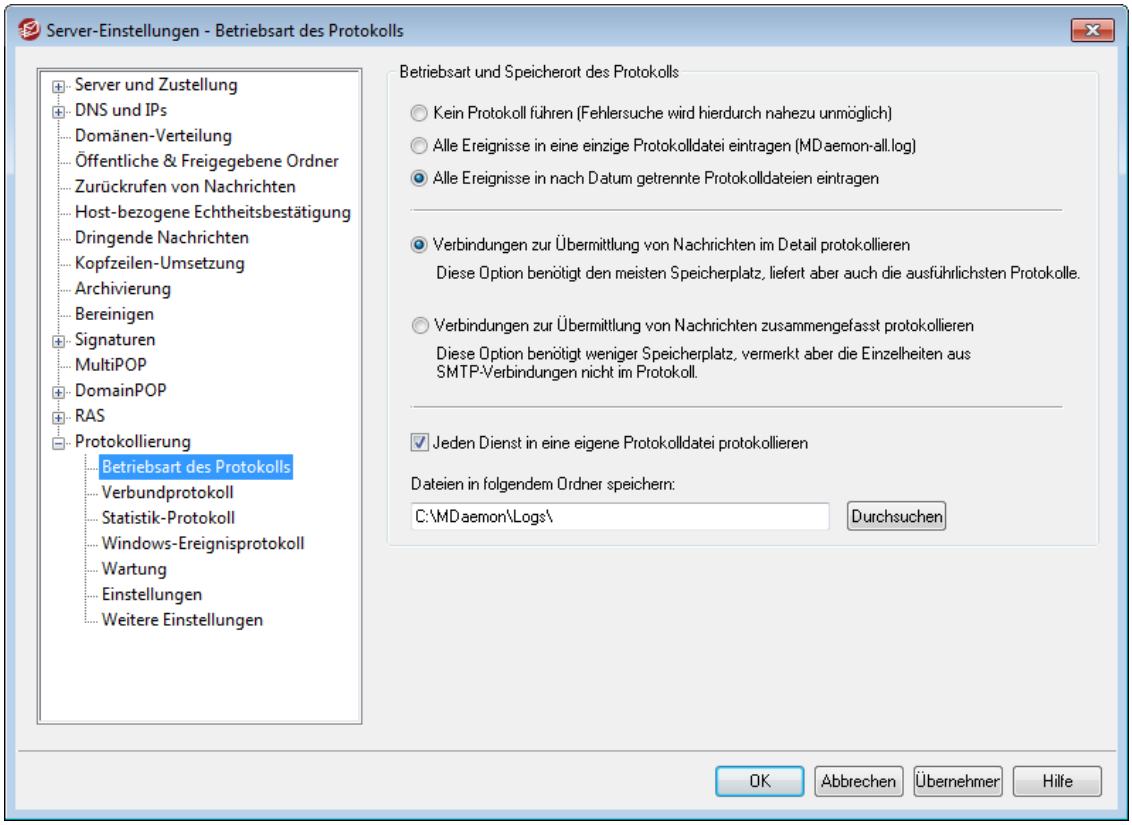
Nach Verbindungsaufbau folgendes Programm ausführen
Falls hier ein Programm angegeben ist, führt MDaemon dieses Programm in einem eigenen Thread aus. Dies ist z.B. dann interessant, wenn das Postfach beim ISP erst durch Finger oder ein anderes Programm entsperrt werden muss.

Server für [xx] Sekunden anhalten (-1 = unbegrenzt, 0 = nicht anhalten)
Falls in dem Feld *Nach Verbindungsaufbau...* ein Programm zur Ausführung angegeben ist, wird der Server für die hier angegebene Zeit angehalten, während er auf den Abschluss des externen Programms wartet. Der Wert -1 bewirkt, dass MDaemon unbegrenzt lange auf die Beendigung des Programms wartet.

Nach Zeitablauf das externe Programm abbrechen
Manche externe Programme können sich nicht selbst beenden oder erwarten zum Abschluss Benutzereingriffe. Dies ist unannehmbar, wenn Software unbeaufsichtigt laufen soll. Wenn diese Option ausgewählt ist, beendet MDaemon den Thread, in dem das externe Programm läuft, sobald die unter *Server für [xx] Sekunden anhalten...* angegebene Wartezeit abgelaufen ist. Die Funktion zum Abbrechen des Programms ist wirkungslos, falls als Wartezeit -1 eingetragen ist.

3.1.15 Protokollierung

3.1.15.1 Betriebsart des Protokolls



Sie erreichen den Konfigurationsdialog für die Einstellungen zur Protokollierung über das Menü "Einstellungen » Server-Einstellungen » Protokollierung". Die Protokollierung ist ein hilfreiches Werkzeug, um Probleme und Fehler zu diagnostizieren, und um zu prüfen, welche Vorgänge der Server unbeaufsichtigt ausgeführt hat.

Das Menü Voreinstellungen enthält mehrere Optionen, mit deren Hilfe festgelegt wird, wie viele Protokollinformationen im rechten Abschnitt der Benutzeroberfläche von MDaemon angezeigt werden. Nähere Informationen hierzu finden Sie unter Voreinstellungen » Benutzeroberfläche 492.

Betriebsart und Speicherort des Protokolls

Kein Protokoll führen
Diese Option schaltet alle Protokollfunktionen ab. Die Protokolldateien werden zwar noch erstellt, aber es werden keine Informationen eingetragen.

Von der Nutzung dieser Option ist abzuraten. Ohne Protokolldateien kann es äußerst schwierig oder sogar unmöglich sein, Probleme im E-Mail-System zu erkennen und zu behandeln.

Alle Ereignisse in eine einzige Protokolldatei eintragen (MDaemon-all.log)
Diese Option bewirkt, dass alle Ereignisse nur in die Datei `MDaemon-all.log` eingetragen werden.

Alle Ereignisse in nach Datum getrennte Protokolldateien eintragen
Hierdurch wird für jeden Tag eine neue Protokolldatei angelegt. Ihr Name richtet sich nach dem Datum des Tages, an dem sie angelegt wird.

Verbindungen zur Übermittlung von Nachrichten im Detail protokollieren
Ist diese Option aktiv, so wird ein genauer Mitschnitt jeder Verbindung zur Übermittlung von Nachrichten in die Protokolldatei eingetragen.

Verbindungen zur Übermittlung von Nachrichten zusammengefasst protokollieren
Hiermit wird nur eine Zusammenfassung einer jeden Verbindung zur Übermittlung von Nachrichten protokolliert.

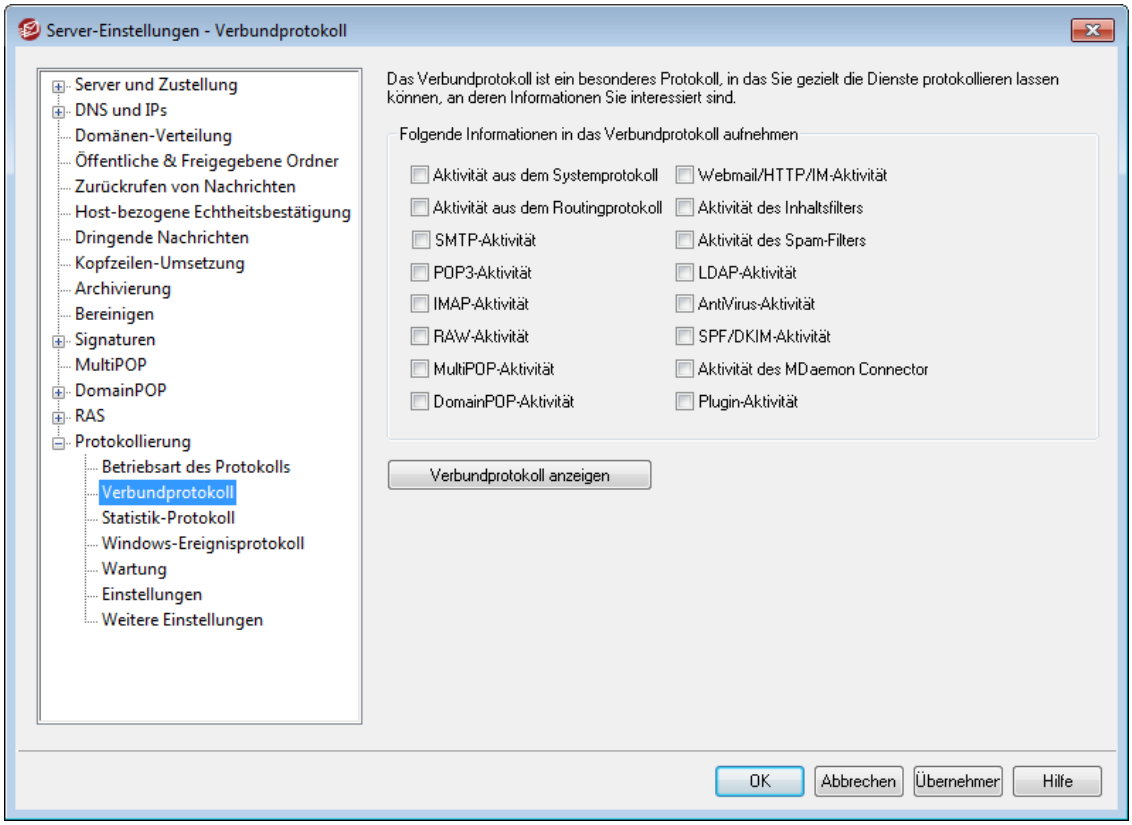
Jeden Dienst in eine eigene Protokolldatei protokollieren
Diese Option bewirkt, dass MDaemon für jeden einzelnen Serverdienst ein getrenntes Protokoll führt, anstatt für alle Dienste ein gemeinsames Protokoll zu unterhalten. Ist diese Option aktiv, so protokolliert MDaemon beispielsweise den SMTP-Verkehr in der Datei `MDaemon-SMTP.log`, die IMAP-Aktivität in der Datei `MDaemon-IMAP.log` usw. Bei Konfigurations-Verbindungen oder MDaemon-Instanzen unter Terminal Services muss diese Option aktiv sein, damit die einzelnen Registerkarten der Benutzeroberfläche die ihnen zugeordneten Protokollinhalte anzeigen können.

Dateien in folgendem Ordner speichern:
Mithilfe dieser Option kann ein besonderer Pfad angegeben werden, in dem die Protokolldateien abgelegt werden sollen.

Die Datei BadAddress.txt

In dem Verzeichnis für die Protokolle speichert MDaemon neben den eigentlichen Protokolldateien auch die Datei `BadAddress.txt`. Schlägt eine Zustellung einer Nachricht für eine bestimmte Adresse mit einem Fehler 5xx fehl, so wird die Adresse, bei der dieser Fehler aufgetreten ist, in die Datei aufgenommen. Anhand der Einträge der Datei lassen sich beispielsweise ungültige E-Mail-Adressen aus Mailinglisten schneller finden als durch eine Suche in den Protokollen über abgehende SMTP-Verbindungen. Diese Datei wird jeden Tag um Mitternacht automatisch gelöscht; es wird so verhindert, dass sie übermäßig groß wird.

3.1.15.2 Verbundprotokoll



Verbundprotokoll

Folgende Informationen in das Verbundprotokoll aufnehmen
Das Verbundprotokoll ist in der Benutzeroberfläche von MDaemon über das Menü Fenster und den Menüeintrag für dasVerbundprotokoll erreichbar. Ein Klick auf diesen Menüeintrag fügt dem Hauptfenster von MDaemon einen Bereich hinzu, in dem die Informationen aus einem oder mehreren Registerkarten des rechten Fensterteils vereinigt werden. Die Optionen in diesem Konfigurationsdialog legen fest, welche Informationen in dem Verbundprotokoll erscheinen sollen. Es stehen die Informationen aus den nachfolgend aufgeführten Registerkarten zur Verfügung:

System—Hierdurch wird die System-Aktivität von MDaemon, wie etwa die Initialisierung der Dienste und das Aktivieren und Deaktivieren der einzelnen Server angezeigt.

Routing—Hierdurch werden Informationen über das Nachrichten-Routing (Von, An, Nachrichten-ID usw.) für jede Nachricht angezeigt, die MDaemon auswertet.

SMTP—Hierdurch werden alle Sende- und Empfangsvorgänge über SMTP angezeigt.

POP3—Hierdurch werden die Übermittlungsvorgänge beim Postabruf durch die Benutzer über POP3 angezeigt.

IMAP—Hierdurch werden IMAP-Mailverbindungen protokolliert.

RAW—Hierdurch wird die Verarbeitung von RAW- und Systemnachrichten protokolliert.

MultiPOP—Hierdurch werden die Vorgänge für den Postabruf über MultiPOP angezeigt.

DomainPOP—Hierdurch wird die DomainPOP-Aktivität angezeigt.

Webmail/HTTP/IM—Hierdurch werden die Aktivitäten von Webmail und der Instant-Messaging-Funktionen angezeigt.

Inhaltsfilter—Hierdurch wird die Aktivität des Inhaltsfilters angezeigt.

Spam-Filter—Hierdurch wird die Aktivität des Spam-Filters angezeigt.

LDAP—Hierdurch wird die LDAP-Aktivität angezeigt.

AntiVirus—Hierdurch wird die AntiVirus-Aktivität angezeigt.

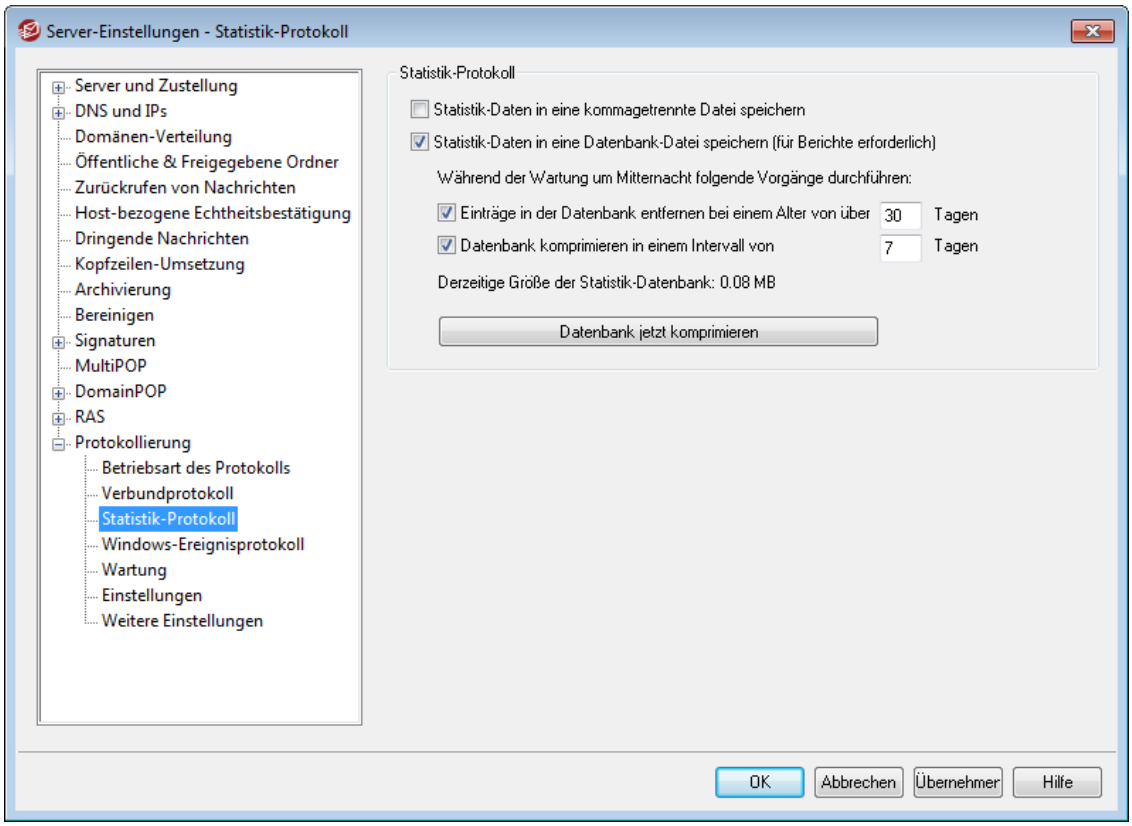
SPF/DKIM—Hierdurch werden die Aktivitäten des Sender-Policy-Frameworks und der DomainKeys angezeigt.

MDaemon Connector—Hierdurch wird die Aktivität des MDaemon Connectors angezeigt.

Plugin-Aktivität—Hierdurch werden die Aktivitäten der MDaemon-Plugins angezeigt.

Verbundprotokoll aktivieren
Ein Klick auf dieses Steuerelement fügt das Verbundprotokoll dem Hauptfenster von MDaemon hinzu. Alternativ kann das Verbundprotokoll auch über das Menü Fenster auf der Benutzeroberfläche von MDaemon aktiviert werden.

3.1.15.3 Statistik-Protokoll



Statistik-Protokoll

Statistik-Daten in eine kommagetrennte Datei speichern
Diese Option bewirkt, dass ein Statistik-Protokoll angelegt und in einer kommagetrennten Datei gespeichert wird. Das Statistikprotokoll enthält Daten über die Anzahl der eingehenden und abgehenden Nachrichten, die das System verarbeitet, sowie Statistiken über Spam, Viren und weitere Informationen. Diese Option ist per Voreinstellung abgeschaltet.

Statistik-Daten in eine Datenbank-Datei speichern (für Berichte erforderlich)
Diese Option bewirkt, dass die Statistikdaten über die Aktivität von MDaemon in eine SQLite-Datenbank gespeichert werden. Diese Datenbank enthält Informationen über die Nutzung der Übertragungsbandbreiten durch MDaemon, die Zahl der eingehenden und abgehenden Nachrichten, Statistiken über Spam und weitere Informationen. Per Voreinstellung wird die Datenbank im Verzeichnis "`MDaemon\StatsDB`" gespeichert. Sie enthält per Voreinstellung die Daten der letzten 30 Tage; diesen Zeitraum können Sie anpassen. Daten, die die Altersgrenze überschritten haben, werden während der Bereinigung um Mitternacht gelöscht. Sie können außerdem festlegen, wie oft MDaemon die Datenbank komprimieren soll, um nicht benötigten Speicherplatz freizugeben.

Mithilfe der Daten aus dieser Datenbank erstellt die MDaemon-Remoteverwaltung verschiedene Berichte für die Globalen Administratoren. Jeder Bericht kann für vordefinierte Zeiträume abgerufen werden, und die Administratoren können außerdem benutzerdefinierte Zeiträume angeben. Die folgenden Berichte stehen den Administratoren zur Verfügung:

- Erweiterte Berichte über die Nutzung der Übertragungsbandbreiten
- Eingehende und abgehende Nachrichten
- Legitime Nachrichten und Junk oder Spam (Prozentsatz der Nachrichten, die Spam sind oder Viren enthalten)
- Eingehende verarbeitete Nachrichten
- Top-Empfänger nach Anzahl der Nachrichten
- Top-Empfänger nach Größe der Nachrichten
- Abgehende verarbeitete Nachrichten
- Top-Spam-Quellen (Domänen)
- Top-Empfänger für Spam
- Abgewiesene Viren nach Zeitraum
- Abgewiesene Viren nach Name

Während der Wartung um Mitternacht folgende Vorgänge durchführen:
Die folgenden Optionen bestimmen die Art der Datenbank-Wartung, die MDaemon während der Bereinigung um Mitternacht durchführt.

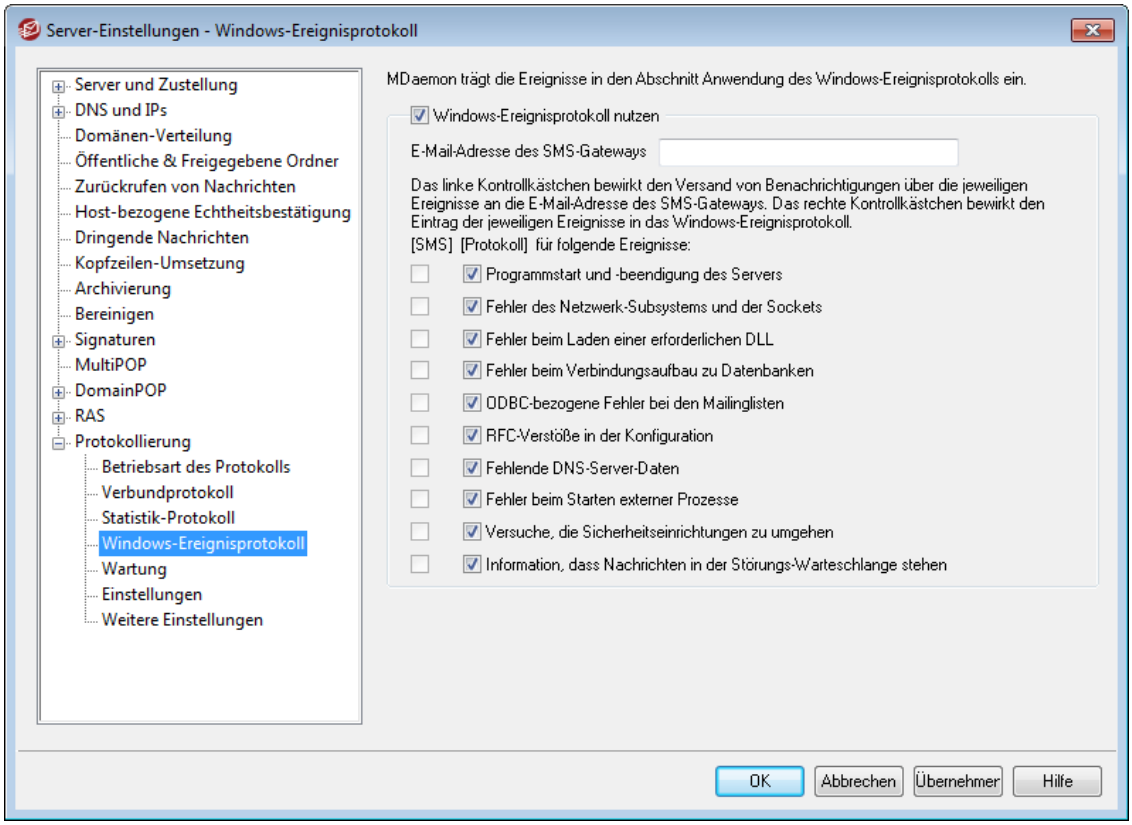
Einträge in der Datenbank entfernen bei einem Alter von über [xx] Tagen
Diese Option bestimmt, wie alt die Einträge in der Statistik-Datenbank werden dürfen, bevor sie aus der Datenbank gelöscht werden. Per Voreinstellung werden Daten gelöscht, die älter als 30 Tage sind.

Datenbank komprimieren in einem Intervall von [xx] Tagen
Diese Option bestimmt das Intervall, in dem die Datenbank komprimiert wird, um nicht benötigten Speicherplatz freizugeben. Die Option ist per Voreinstellung aktiv, und die Datenbank wird per Voreinstellung alle 7 Tage komprimiert.

Derzeitige Größe der Statistik-Datenbank:
Hier wird die derzeitige Größe der Statistik-Datenbank angezeigt.

Datenbank jetzt komprimieren
Um die Datenbank sofort zu komprimieren, klicken Sie auf dieses Steuerelement.

3.1.15.4 Windows-Ereignisprotokoll



Windows-Ereignisprotokoll nutzen
Diese Option bewirkt, dass besonders kritische Systemfehler und Warnmeldungen sowie weitere Ereignisse auch in dem Ereignisprotokoll von Windows vermerkt werden.

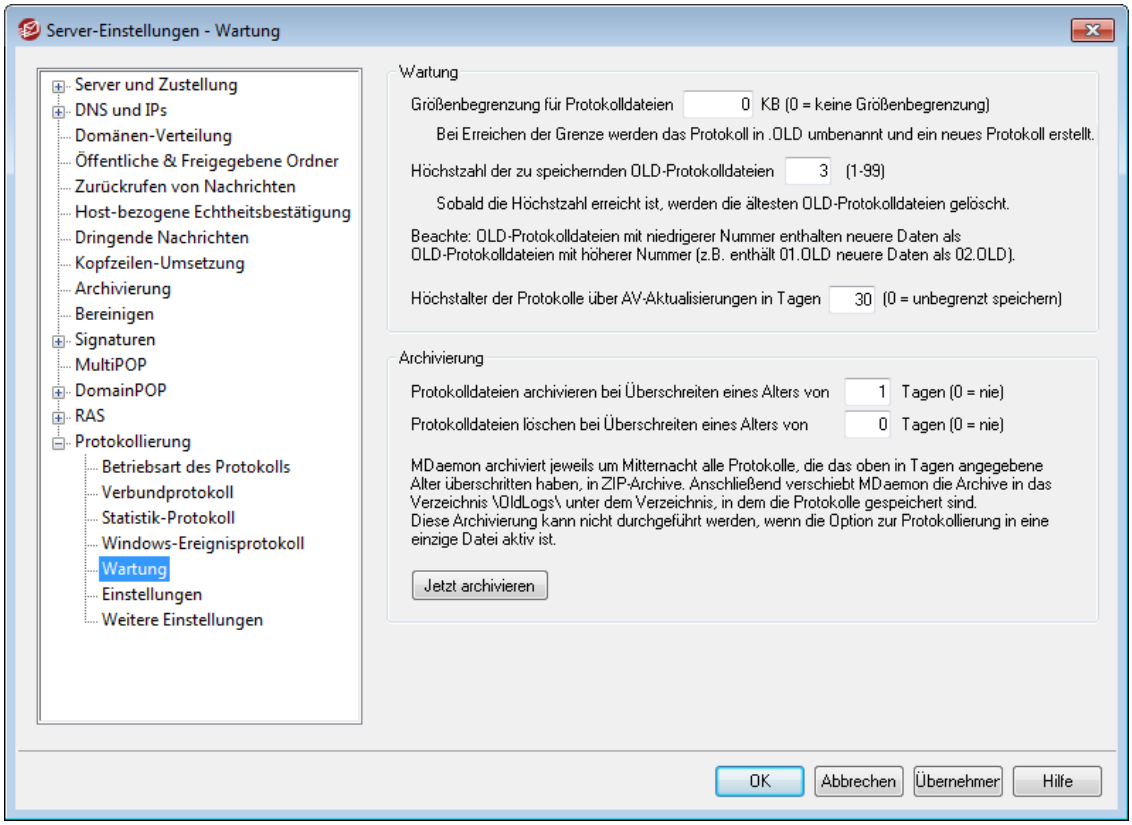
E-Mail-Adresse des SMS-Gateways
Mithilfe dieser Option können Sie Daten über bestimmte, in der nachfolgenden Liste ausgewählte Ereignisse per SMS (Textnachricht) an mobile Endgeräte senden. Tragen Sie hierzu die E-Mail-Adresse für das E-Mail-SMS-Gateway Ihres Dienstleisters oder Netzbetreibers ein. Ein Beispiel hierzu: Für Verizon in den USA lautet die E-Mail-Adresse `[Telefonnummer]@vtext.com` (etwa `8175551212@vtext.com`). Für jedes Ereignis, das Sie per SMS übermitteln wollen,

aktivieren Sie dann das Kontrollkästchen in der Spalte [SMS] der nachfolgenden Liste.

[SMS] | [Protokoll] für folgende Ereignisse:
Mithilfe der Kontrollkästchen in der Spalte SMS bestimmen Sie, welche Ereignisse über SMS weitergemeldet werden sollen. Mithilfe der Kontrollkästchen in der Spalte Protokoll bestimmen Sie, welche Ereignisse in den Abschnitt Anwendungen des Windows-Ereignisprotokolls eingetragen werden sollen. Sie können die Kontrollkästchen in der Spalte SMS nur aktivieren, wenn Sie die E-Mail-Adresse des E-Mail-SMS-Gateways Ihres Netzbetreibers oder Dienstleisters eingetragen haben. Alle Ereignisse, die über SMS weitergemeldet werden, lösen einen Verarbeitungsdurchlauf für die Warteschlange für externe Nachrichten aus. Die Nachrichten an das Gateway werden dabei als dringende Nachrichten behandelt.

Sind SMS-Benachrichtigungen für *Programmstart und -beendigung des Servers* aktiv, so wird nur der Programmstart, nicht aber die Programmbeendigung per SMS weitergemeldet.

3.1.15.5 Wartung



Wartung

Größenbegrenzung für Protokolldateien [xx] KB (0 = keine Größenbegrenzung)
Dieser Wert bestimmt, welche Größe in KB die Protokolldateien jeweils höchstens erreichen dürfen. Ist diese Größe erreicht, so wird die betroffene Protokolldateiumbenannt in "NAMEDERPROTOKOLLDATEI.01.OLD", und eine neue Protokolldatei wird erstellt. Besteht schon eine Datei NAMEDERPROTOKOLLDATEI.01.OLD, so wird

die bestehende Datei entweder gelöscht oder umbenannt in "NAMEDERPROTOKOLLDATEI.02.OLD"; dies hängt von der Einstellung *"Höchstzahl der zu speichernden OLD-Protokolldateien"* ab. Falls Sie die Größe der Protokolldateien nicht begrenzen wollen, tragen Sie "0" ein; dies ist auch die Voreinstellung.

Höchstzahl der zu speichernden OLD-Protokolldateien (1-99)
Ist die Größe der Protokolldateien begrenzt, so bestimmt diese Option, wie viele alte Protokolldateien (.OLD) gespeichert werden, bevor die jeweils älteste Datei gelöscht wird. Die Protokolldateien werden nach dem Schema "NAMEDERPROTOKOLLDATEI.01.OLD", "NAMEDERPROTOKOLLDATEI.02.OLD" usw. benannt, wobei die neueste Datei immer die niedrigste Nummer hat. Ein Beispiel hierzu: SMTP(out).log.01.old enthält neuere Daten als SMTP(out).log.02.old usw. Wird die Höchstzahl erreicht, so wird die älteste Datei gelöscht, sobald wieder eine OLD-Protokolldatei angelegt wird.

Höchstalter der Protokolle über AV-Aktualisierungen in Tagen (0=unbegrenzt archivieren)
Diese Option bestimmt, wie alt die Daten in den Protokollen über die AntiVirus-Aktualisierungen (also avupdate.log) sein dürfen, bevor sie entfernt werden. Daten, die das hier angegebene Höchstalter überschritten haben, werden jeden Tag um Mitternacht und zusätzlich nach jedem Neustart von MDaemon nach einer Aktualisierung aus der Datei gelöscht. Der Wert "0" bewirkt, dass kein Höchstalter festgelegt wird. Die Voreinstellung für das Höchstalter beträgt 30 Tage.

Das Protokoll über AV-Aktualisierungen wird per Voreinstellung angelegt, und seine Größe ist per Voreinstellung auf 5120 KB begrenzt. Falls Sie diese Begrenzung ändern oder die Protokollierung der AV-Aktualisierungen deaktivieren wollen, können Sie hierzu die entsprechenden Optionen im Konfigurationsdialog für die AV-Aktualisierung 678 bearbeiten. Sie erreichen diesen Konfigurationsdialog über **Sicherheit » AntiVirus » AV-Aktualisierung » Aktualisierung konfigurieren » Verschiedenes**.

Archivierung

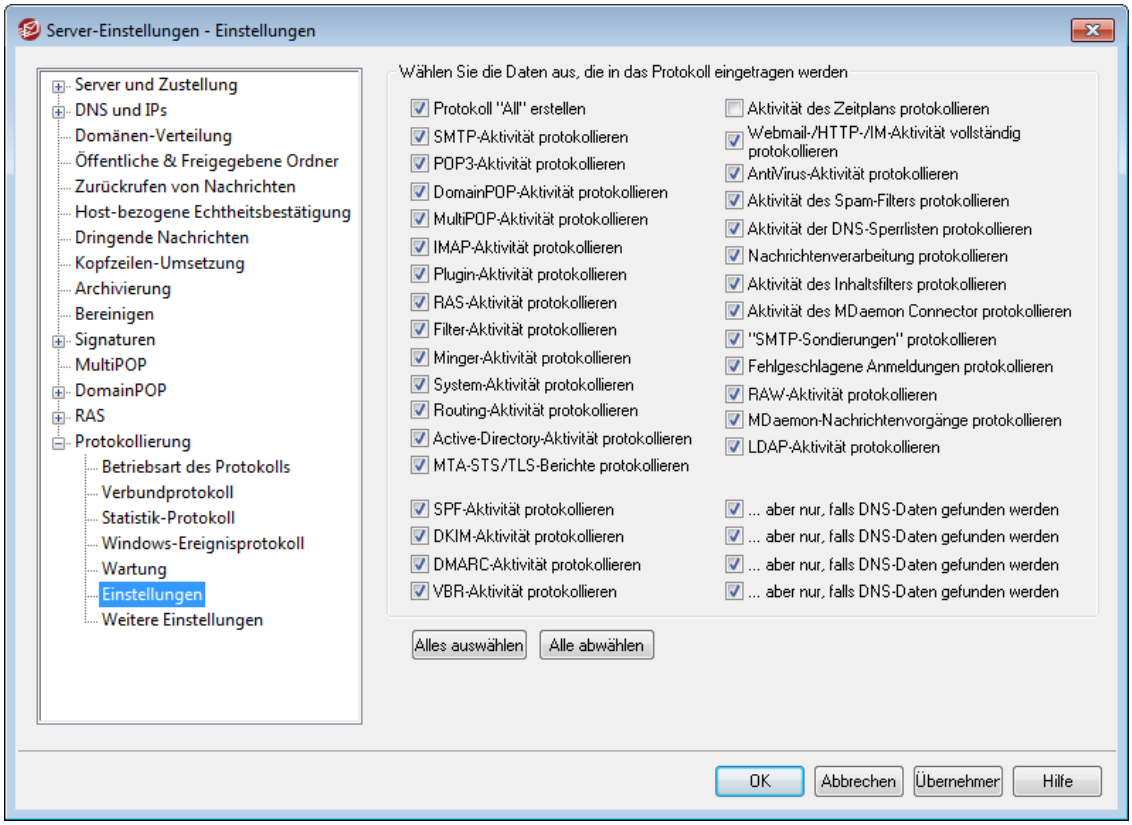
Protokolldateien archivieren bei Überschreiten eines Alters von [xx] Tagen (0=nie)
Diese Option bewirkt, dass MDaemon alle Protokolldateien, deren Alter den angegebenen Schwellwert überschritten hat, automatisch archiviert. Jeden Tag um Mitternacht packt MDaemon die alten *.log- und *.old-Dateien in ein ZIP-Archiv und verschiebt dieses dann in das Unterverzeichnis \Logs\OldLogs\. Die Quelldateien werden danach gelöscht. Dateien, die gerade in Benutzung und damit gesperrt sind, werden nicht archiviert. Ist die Option "*Alle Ereignisse in eine einzige Protokolldatei eintragen (MDaemon-all.log)*" im Abschnitt Betriebsart des Protokolls 167 aktiv, so bleibt diese Funktion wirkungslos.

Protokolldateien löschen bei Überschreiten eines Alters von [XX] Tagen(0=nie)
Diese Option bewirkt, dass MDaemon archivierte Protokolldateien automatisch löscht, sobald ihr Alter das hier in Tagen angegebene Höchstalter überschreitet. Der Wert "0" bewirkt, dass archivierte Protokolldateien nicht automatisch

gelöscht werden. Die Löschung wird jeweils während der Bereinigungsvorgänge um Mitternacht durchgeführt.

Jetzt archivieren
Ein Klick auf dieses Steuerelement startet die Archivierung der alten Protokolldateien sofort. Die automatische Archivierung durch MDaemon um Mitternacht wird nicht mehr abgewartet.

3.1.15.6 Einstellungen



Optionen zum Protokoll

Protokoll "All" erstellen
Diese Option bewirkt, dass ein Sammelprotokoll mit dem Dateinamen "`*-all.log`" angelegt wird, in das alle zu protokollierenden Aktivitäten gesammelt eingetragen werden.

SMTP-Aktivität protokollieren
Mit dieser Option werden alle SMTP-Verbindungen protokolliert, in denen MDaemon Nachrichten sendet und empfängt.

POP3-Aktivität protokollieren
Hiermit werden alle POP-Verbindungen protokolliert, über die die Benutzer Post vom Server abrufen.

DomainPOP-Aktivität protokollieren
Hiermit wird die gesamte DomainPOP-Aktivität protokolliert.

MultiPOP-Aktivität protokollieren
Diese Option bewirkt, dass die gesamte MultiPOP-Aktivität protokolliert wird.

IMAP-Aktivität protokollieren
Hiermit werden auch die IMAP-Verbindungen der Benutzer im Systemprotokoll erfasst.

Plugin-Aktivität protokollieren
Hiermit werden alle Aktivitäten der Plugins protokolliert.

RAS-Aktivität protokollieren
Hiermit protokolliert MDaemon alle Meldungen des DFÜ-Netzwerks oder der RAS. Diese Informationen helfen bei der Fehlersuche bei DFÜ-Verbindungen.

Filter-Aktivität protokollieren
Hiermit wird die Aktivität der Host- und IP-Filter im Systemprotokoll protokolliert.

Minger-Aktivität protokollieren
Hiermit wird die Aktivität des Minger-Servers im Systemprotokoll protokolliert.

System-Aktivität protokolliert
Hiermit werden die System-Aktivitäten protokolliert.

Routing-Aktivität protokollieren
Hiermit werden alle Verarbeitungsvorgänge für Eingangs-, lokale und Extern-Warteschlangen protokolliert.

Active-Directory-Aktivität protokollieren
Hiermit werden die Aktivitäten im Zusammenhang mit dem Active Directory protokollieren.

MTA-STS/TLS-Berichte protokollieren
Hierdurch werden die Aktivitäten im Zusammenhang mit SMTP MTA Strict Transport Security (MTA-STS) protokolliert.

Aktivität des Zeitplans protokollieren
Aktivieren Sie diese Option, um die Aktivität des Zeitplans 378 zu protokollieren.

Webmail-/HTTP-/IM-Aktivität vollständig protokollieren
Diese Option bewirkt, dass die gesamte Aktivität von Webmail, des HTTP-Servers und des MDaemon Instant Messengers protokolliert wird. Ist diese Option abgeschaltet, so werden die Protokolldateien für Webmail und HTTP zwar noch erstellt, sie enthalten aber nur noch die Start- und Beendigungszeiten für Webmail. Andere Informationen für Webmail, HTTP und IM werden in den Dateien dann nicht mehr vermerkt.

AntiVirus-Aktivität protokollieren
Diese Option bewirkt, dass die Aktionen von AntiVirus protokolliert werden.

Aktivität des Spam-Filters protokollieren
Diese Option bewirkt, dass alle Aktionen des Spam-Filters aufgezeichnet werden.

Aktivität der DNS-Sperrlisten protokollieren
Diese Option bewirkt, dass MDaemon auch die gesamte Aktivität der Sperrlistenlisten für DNS protokolliert. Aus diesem Protokoll lassen sich die Gegenstellen, die als gesperrt protokolliert wurden, besonders leicht ersehen.

Nachrichtenverarbeitung protokollieren
MDaemon führt gelegentlich umfangreiche Auswertungen und Parserfunktionen durch, um festzustellen, an welchen Empfänger eine Nachricht zugestellt werden muss. Falls diese Vorgänge ebenfalls protokolliert werden sollen, muss diese Option gesetzt sein.

Aktivität des Inhaltsfilters protokollieren
Diese Option veranlasst MDaemon, alle Aktionen des Inhaltsfilters im Systemprotokoll aufzuzeichnen.

Aktivität des MDaemon Connectors protokollieren
Diese Option bestimmt, ob die Aktivität des MDaemon Connectors protokolliert werden soll.

"SMTP-Sondierungen" protokollieren
Diese Option bewirkt, dass SMTP-Verbindungen auch dann protokolliert werden, wenn die Gegenstelle keine Nachrichten überträgt (also den Befehl DATA nicht sendet).

Fehlgeschlagene Anmeldungen protokollieren
Hiermit werden fehlgeschlagene Versuche zur Echtheitsbestätigung protokolliert.

RAW-Aktivität protokollieren
Hiermit werden die Verarbeitungsvorgänge für RAW-Nachrichten protokolliert.

MDaemon-Nachrichtenvorgänge protokollieren
Hiermit werden die Verarbeitungsvorgänge für Nachrichten in MDaemon protokolliert.

LDAP-Aktivität protokollieren
Hiermit werden alle LDAP-Vorgänge protokolliert.

SPF-Aktivität protokollieren
Diese Einstellung bewirkt, dass die SPF-Abfragen und ihre Ergebnisse protokolliert werden.

> **...aber nur, falls DNS-Daten gefunden werden**
> Falls die SPF-Aktivität protokolliert werden soll, kann die Protokollierung durch diese Einstellung auf jene Fälle beschränkt werden, in denen während der DNS-Abfrage wirklich SPF-Daten gefunden wurden. Die erfolglosen Abfragen, die keinerlei SPF-Daten ergeben, werden dann nicht protokolliert.

DKIM-Aktivität protokollieren
Diese Option bewirkt, dass die Aktivität der DomainKeys-Identified-Mail (DKIM) protokolliert wird.

...aber nur, falls DNS-Daten gefunden werden
Falls die Aktivität der DKIM protokolliert wird, bewirkt diese Option, dass die Aktivität nur protokolliert wird, wenn DNS-Daten gefunden werden.

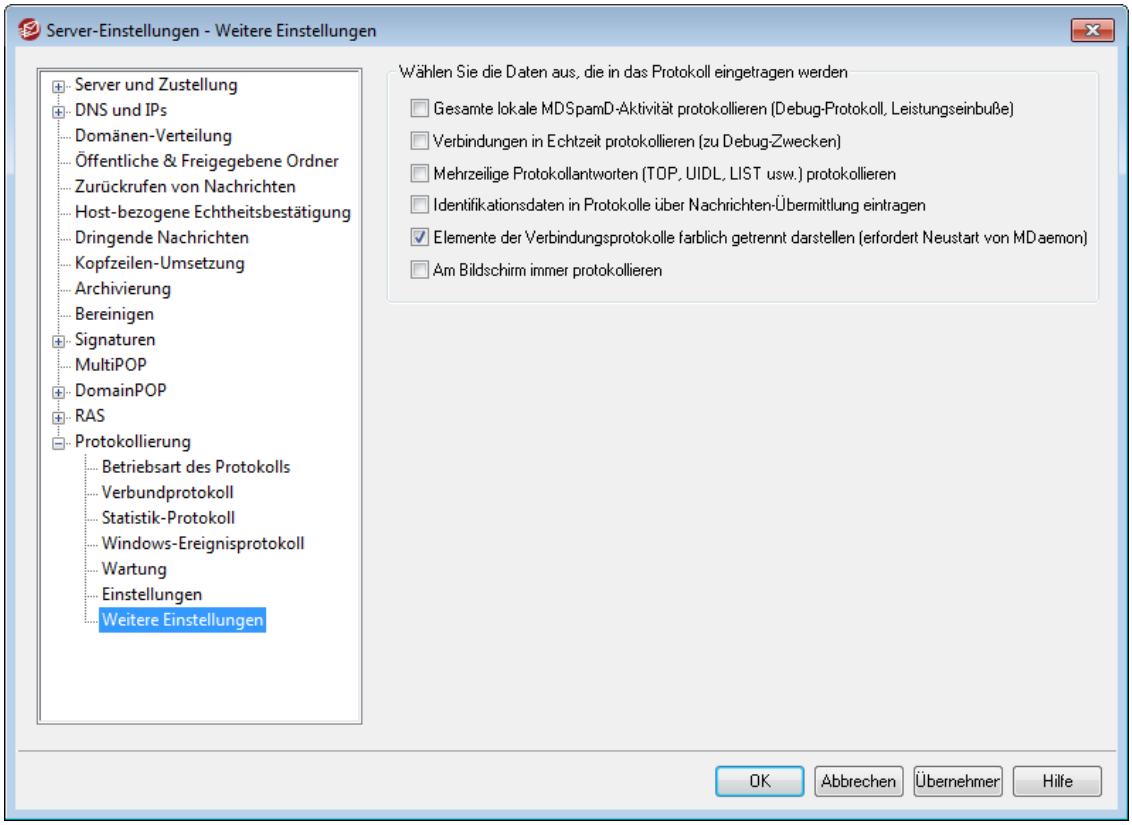
DMARC-Aktivität protokollieren
Diese Option bewirkt, dass die Aktivität der DMARC-Leistungsmerkmale protokolliert wird.

...aber nur, falls DNS-Daten gefunden werden
Falls die Aktivität der DMARC-Leistungsmerkmale protokolliert wird, bewirkt diese Option, dass die Aktivität nur protokolliert wird, wenn DNS-Daten gefunden werden.

VBR-Aktivität protokollieren
Diese Option bewirkt, dass die Aktivität der Zertifizierung von Nachrichten 554 protokolliert wird.

...aber nur, falls DNS-Daten gefunden werden
Falls die Aktivität der Zertifizierung von Nachrichten protokolliert wird, bewirkt diese Option, dass die Aktivität nur protokolliert wird, wenn DNS-Daten gefunden werden.

3.1.15.7 Weitere Einstellungen zur Protokollierung



Wählen Sie die Daten aus, die in das Protokoll eingetragen werden sollen

Gesamte lokale MDSpamD-Aktivität protokollieren (Debug-Protokoll, Leistungseinbuße)
Diese Option bewirkt, dass die gesamte Aktivität des lokalen MDSpamD protokolliert wird (beachte jedoch den Warnhinweis weiter unten).

Verbindungen in Echtzeit protokollieren (Debug-Protokoll, Leistungseinbuße)
Normalerweise wird eine Verbindung erst nach deren Ende protokolliert, um die Systemlast gering zu halten. Mit dieser Option wird jeder Eintrag ins Protokoll sofort in Echtzeit vorgenommen.

Die beiden oben vorstehend erläuterten Optionen können die Leistungsfähigkeit des Mailservers verringern. Ihre Wirkung im Einzelfall hängt von Architektur und Auslastung des Systems ab. Die beiden Optionen sollen in der Regel nur zur Fehlerbehebung (zu Debug-Zwecken) aktiviert werden.

Mehrzeilige Protokollantworten (TOP, UIDL, LIST usw.) protokollieren
Die Antworten auf Protokollbefehle sind manchmal länger als eine Zeile. Um auch die weiteren Zeilen zu protokollieren, muss diese Option aktiv sein.

Diese Option kann möglicherweise den Umfang der protokollierten Informationen drastisch vergrößern. Die Anzahl der Zeilen einer Protokollantwort ist nicht vorhersehbar. Da manche Antworten die Protokolldatei sehr schnell mit unnützer Information überschwemmen (POP TOP gibt beispielsweise den vollständigen Nachrichteninhalt wieder), ist vom Gebrauch dieser Funktion abzuraten, falls die Protokollgröße oder die Ausführlichkeit kritisch sind.

Identifikationsdaten in Protokolle über Nachrichten-Übermittlung eintragen
Diese Option bewirkt, dass ID-Texte des Formats [%d:%d] (Identifikationsnummern) in die Verbindungsprotokolle aufgenommen werden.

Elemente der Verbindungsprotokolle farblich getrennt darstellen (erfordert Neustart von MDaemon)
Diese Option bewirkt, dass die Texte, die auf verschiedenen Registerkarten im Bereich Überwachung und Protokollierung von Ereignissen 76 der Benutzeroberfläche von MDaemon farblich getrennt dargestellt werden. Änderungen an dieser Option werden erst nach einem Neustart von MDaemon wirksam. Weitere Informationen hierzu finden Sie im Abschnitt "Farblich getrennte Darstellung der Elemente aus Verbindungsprotokollen" weiter unten.

Protokoll immer auf Bildschirm ausgeben
Diese Option bewirkt, dass die protokollierten Ereignisse auch dann auf der Benutzeroberfläche von MDaemon ausgegeben werden, wenn MDaemon minimiert oder in den Systray ausgeblendet ist.

So lange diese Option nicht aktiv ist, werden die protokollierten Ereignisse nicht auf der Benutzeroberfläche ausgegeben, wenn MDaemon in den Systray ausgeblendet ist. Daher werden auch die zuletzt protokollierten Ereignisse nicht

angezeigt, wenn das MDaemon-Fenster wieder geöffnet wird. Erst die Ereignisse, die nach dem Öffnen des Fensters protokolliert werden, erscheinen dann auf dem Bildschirm.

Farblich getrennte Darstellung der Elemente aus Verbindungsprotokollen

Die Ereignisse in den Registerkarten Routing, SMTP eing., SMTP abg., IMAP, POP, MultiPOP und DomainPOP auf der Benutzeroberfläche von MDaemon[76] können verschiedenfarbig dargestellt werden, sodass der Betrachter die einzelnen Ereignisse in einer Verbindung besser unterscheiden kann. Das entsprechende Leistungsmerkmal ist per Voreinstellung abgeschaltet. Es kann mithilfe der Option "*Elemente der Verbindungsprotokolle farblich getrennt darstellen*" im Konfigurationsdialog Protokollierung » Weitere Einstellungen[178] sowie im Konfigurationsdialog Voreinstellungen » Benutzeroberfläche[492] aktiviert werden. Die per Voreinstellung verwendeten Farben können durch Bearbeiten des Abschnitts `[Colors]` in der Datei `LogColors.dat` geändert werden. Nachfolgend ist eine Übersicht über die Farben aufgeführt, die per Voreinstellung vergeben sind.

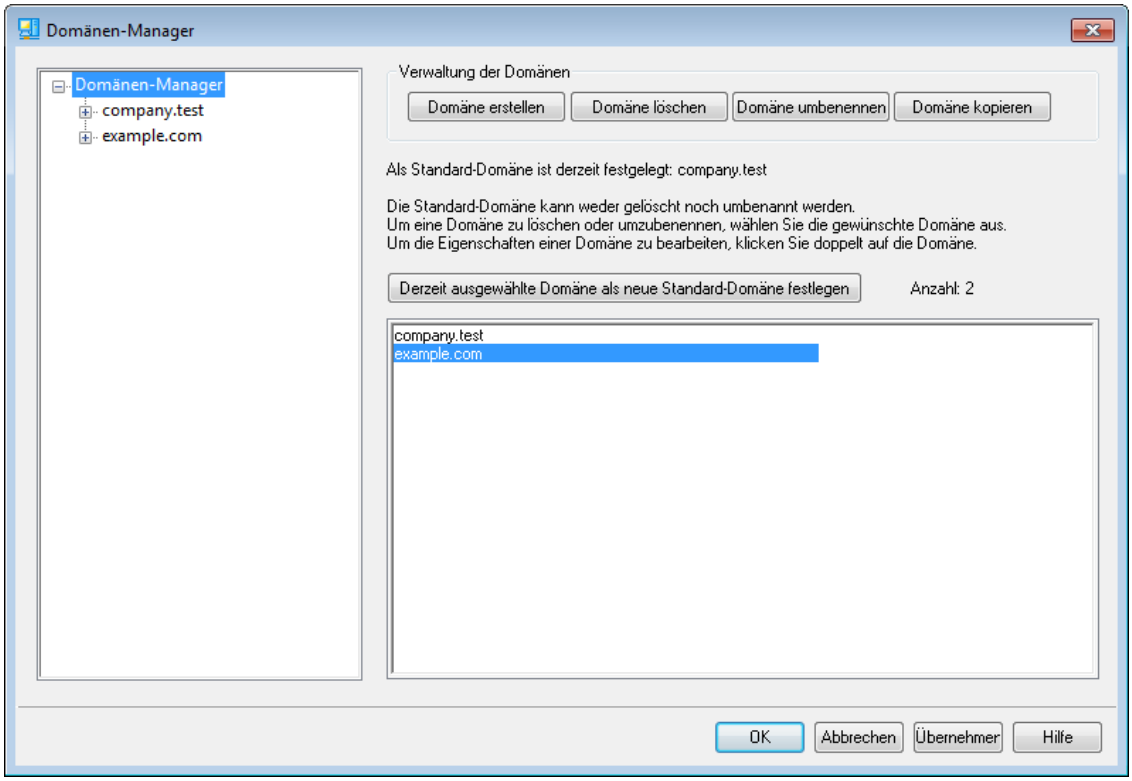
Falls Sie zwar grundsätzlich Farben nutzen, einzelne Elemente aus der oben dargestellten Liste aber nicht andersfarbig darstellen wollen, setzen Sie deren Farbwerte auf 0. Ein Beispiel hierzu ist `SpamFilter=0`; dann wird die Standard-Farbe ("`Default`") genutzt. Diese Möglichkeit besteht nicht bei den Elementen `Background` und `SelectedBackground`. Die Darstellung dieser beiden Elemente kann nur durch Angeben eines anderen vollständigen Farbwertes geändert werden. Die Farbwerte sind in hexadezimaler Schreibweise nach dem Schema 0xbbggrr aufgebaut, wobei bb den Anteil für Blau, gg den Anteil für Grün und rr den Anteil für Rot darstellen. Ein Beispiel hierzu: Der Eintrag "`Error=0x0000ff`" setzt die Farbe für Fehlermeldungen auf Rot. **Beachte:** Die vorstehend dargestellte Reihenfolge der Schreibweise ist gegenüber der üblicherweise verwendeten Schreibweise "`rrggbb`" umgekehrt. Falls Sie Änderungen an den Farben vornehmen, müssen Sie entweder MDaemon neu starten oder die Datei `COLORS.SEM` im Verzeichnis MDaemon's `\APP\` erstellen, damit die Änderungen wirksam werden können.

Voreinstellungen für die Farben für Protokolleinträge

Background=0x000000	Hintergrundfarbe, Schwarz
SelectedBackground=0xff0000	Hintergrundfarbe für markierte Zeilen, Blau
Default=0xffffff	Standard-Textfarbe, Weiß
Processing=0x00ffff	Interne Verarbeitungsvorgänge und Parserdurchläufe, Gelb
DataIn=0x008040	Vom Server der Gegenstelle eingehende Daten, Dunkelgrün
DataOut=0x00ff00	Zum Server der Gegenstelle gesendete Daten, Hellgrün
Error=0x0000ff	Fehlermeldungen, Rot
TCPIP=0xff8000	Vorgänge in Bezug auf TCP/UDP/DNS/PTR, Hellblau
SpamFilter=0x0080ff	Verarbeitung durch Spam-Filter, Orange
AntiVirus=0xdda0dd	Verarbeitung durch AntiVirus, Plum

DKIM=0xff00ff	Vorgänge in Bezug auf DKIM, Fuchsia
VBR=0x40c0ff	Vorgänge in Bezug auf Vouch by Reference, Hellorange
SPF=0x808080	Vorgänge in Bezug auf Sender Policy Framework, Grau
Plugins=0x0080c0	Alle durch Plugins gesendete Nachrichten, Braun
Localq=0x00ffff	Routing in der lokalen Warteschlange, Gelb
Spam=0x0080ff	Routing von Spam-Nachrichten, Orange
Restricted=0x40c0ff	Routing gesperrter Nachrichten, Hellorange
BlackList=0x808080	Routing von Nachrichten auf der Schwarzen Liste, Grau
Gateway=0x00ff00	Routing von Gateway-Nachrichten, Hellgrün
Inboundq=0xff8000	Routing eingehender Nachrichten, Hellblau
PublicFolder=0xdda0dd	Routing von Nachrichten in öffentlichen Ordnern, Plum

3.2 Domänen-Manager



MDaemon enthält umfassende Leistungsmerkmale, die den Betrieb mehrerer Domänen ermöglichen. Diese Leistungsmerkmale werden mithilfe des Domänen-Managers verwaltet. Sie können von hier aus Domänennamen, IP-Adressen, Benutzerkonten, Einstellungen für die Bereinigung von Benutzerkonten und

Nachrichten, Einstellungen für Webmail und weitere domänenspezifische Einstellungen für Ihre Domänen verwalten.

MDaemon unterstützt den Betrieb mit einer IP-Adresse und mehreren IP-Adressen. IP-Adressen können entweder einer Domäne ausschließlich oder mehreren Domänen gemeinsam zugewiesen sein. Einige besonders wichtige Leistungsmerkmale, wie Benutzerkonten, Mailinglisten und Sicherheits-Einstellungen werden nach Domänen getrennt konfiguriert. Beim Erstellen eines Benutzerkontos oder einer Mailingliste muss beispielsweise angegeben werden, zu welcher Domäne das Benutzerkonto oder die Mailingliste gehört. Auch Leistungsmerkmale wie der IP-Filter 563 und die IP-Abschirmung 522 arbeiten in Abhängigkeit von den einzelnen Domänen getrennt.

Einige Leistungsmerkmale, wie die Namenauswertung 160 im System DomainPOP 151, sind ausschließlich an die Standard-Domäne gebunden. Die Standard-Domäne wird auch in verschiedenen Optionen per Voreinstellung angezeigt, etwa beim Erstellen neuer Benutzerkonten oder Mailinglisten. Um die Verarbeitung von Systemnachrichten durch MDaemon zu gewährleisten, verweisen die nachfolgend aufgeführten Standard-Aliasnamen 827 für mehrere reservierte Postfachnamen auf die Standard-Domäne von MDaemon und nicht auf andere etwa vorhandene Domänen:

```
MDaemon@$LOCALDOMAIN$ = MDaemon@<Standard-Domäne>
listserv@$LOCALDOMAIN$ = MDaemon@<Standard-Domäne>
listserver@$LOCALDOMAIN$ = MDaemon@<Standard-Domäne>
list-serv@$LOCALDOMAIN$ = MDaemon@<Standard-Domäne>
```

MDaemon verlangt per Voreinstellung, dass die Benutzer ihre vollständige E-Mail-Adresse (z.B. "benutzer01@example.com")als Benutzernamen bei der Anmeldung angeben. Der Postfachname (im Beispiel "benutzer01") reicht als Benutzername zur Anmeldung nicht aus. Hierbei kann ein Problem auftreten, da manche sehr alte E-Mail-Clients das Zeichen "@" als Teil des Benutzernamens nicht zulassen. Um den Betrieb mit solchen Clients dennoch zu ermöglichen, können Sie als Trennzeichen zwischen Postfachnamen und Domänennamen im Abschnitt System 495 des Konfigurationsdialogs Voreinstellungen ein anderes Zeichen angeben. Das entsprechende Textfeld kann bis zu 10 Zeichen aufnehmen, sodass statt eines einzelnen Zeichens (wie etwa "$") als Trennung auch eine Zeichenkette verwendet werden kann. Tragen Sie dort beispielsweise "**.at.**" ein, so kann ein Benutzername "user02.at.example.com" lauten. Sie können auch auf die Anmeldung mit der vollständigen E-Mail-Adresse verzichten. MDaemon akzeptiert dann auch Benutzernamen, die nur aus dem Postfachnamen bestehen. Dieses Vorgehen ist aber nicht zu empfehlen, da es beim Betrieb von mehr als einer Domäne zu Schwierigkeiten führt.

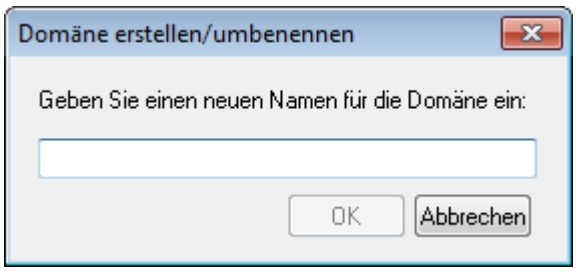
Liste der Domänen

Der Menübaum im linken Teil dieses Konfigurationsdialogs enthält die Liste Ihrer Domänen. Jeder Domäne sind die Verknüpfungen zu den einzelnen Abschnitten der Konfigurationsdialoge aufgeführt, mit deren Hilfe Sie bestimmte Einstellungen nach Domänen getrennt vornehmen können. Die Standard-Domäne erscheint in dem Menübaum stets an erster Stelle, die anderen Domänen sind darunter alphabetisch sortiert aufgeführt. Die Liste der Domänen im rechten Teil dieses Konfigurationsdialogs dient dazu, Domänen zu löschen und umzubenennen und die Standard-Domäne festzulegen. Durch einen Doppelklick auf einen Eintrag in dieser Liste können Sie zu den Einstellungen der angeklickten Domäne wechseln und diese direkt bearbeiten.

Verwaltung der Domänen

Domäne erstellen

Um eine neue Domäne zu erstellen, klicken Sie auf *Domäne erstellen*, tragen Sie den Domänennamen in das Dialogfenster *Domäne erstellen/aktualisieren* ein, und klicken Sie danach auf *OK*.



Der Wert, den Sie hier eintragen, ist üblicherweise ein im Internet registrierter Domänenname, der über einen DNS-Server in die IP-Adresse des Systems aufgelöst werden kann, auf dem MDaemon aufgelöst. Auch ein qualifizierter Aliasname ist möglich. Sie können jedoch auch einen nur intern genutzten oder sonst ungültigen oder nicht registrierten Domänennamen angeben, der im Internet nicht öffentlich verwendet werden kann (etwa "`company.mail`"). In diesem Falle kann es erforderlich sein, die Kopfzeilen-Umsetzung 129 und den Austausch von Domänennamen 157 zu nutzen, um eine ordnungsgemäße Zustellung von Nachrichten zu ermöglichen.

Domäne löschen

Um eine Domäne zu löschen, wählen Sie die Domäne in der Liste aus, klicken Sie auf *Domäne löschen*, und bestätigen Sie die Sicherheitsabfrage mit *Ja*.

Sie können die Standard-Domäne nicht löschen und nicht umbenennen. Falls Sie diese Domäne löschen oder umbenennen wollen, müssen Sie zuvor eine andere Domäne als Standard-Domäne festlegen.

Domäne umbenennen

Um den Namen einer Domäne zu ändern, wählen Sie die Domäne in der Liste aus, klicken Sie auf *Domäne umbenennen*, tragen Sie den neuen Domänennamen in das Dialogfenster *Domäne erstellen/aktualisieren* ein, und klicken Sie danach auf *OK*.

Domäne kopieren

Um eine neue Domäne anzulegen und dabei die Einstellungen aus einer anderen Domäne zu übernehmen, wählen Sie die gewünschte Ursprungsdomäne in der Liste aus, und klicken Sie auf *Domäne kopieren*. Geben Sie dann den Namen für die neue Domäne an. Benutzerkonten, Mailinglisten und ähnliche Einstellungen werden nicht in die neue Domäne kopiert.

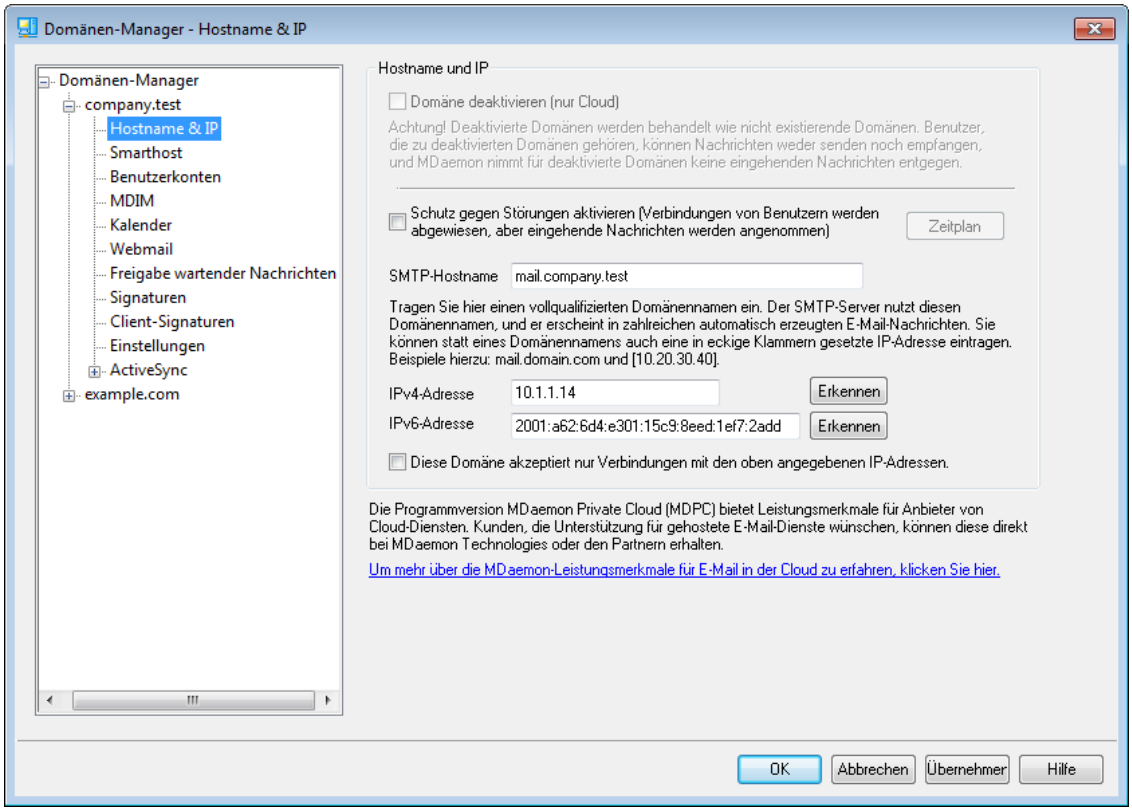
Derzeit ausgewählte Domäne als neue Standard-Domäne festlegen

Um die Standard-Domäne von MDaemon zu ändern, wählen Sie die Domäne in der Liste aus, die Sie als neue Standard-Domäne festlegen wollen, und klicken Sie dann auf dieses Steuerelement.

Siehe auch:

Voreinstellungen » System 495

3.2.1 Hostname & IP



Hostname & IP

Domäne deaktivieren (nur Cloud)
Diese Option deaktiviert die Domäne. MDaemon behandelt deaktivierte Domänen so, wie wenn sie nicht bestehen. Die Benutzer deaktivierter Domänen können Nachrichten weder senden noch empfangen, und MDaemon nimmt keine Nachrichten zur Zustellung an, die an deaktivierte Domänen gerichtet sind. Diese Option steht nur in MDaemon Private Cloud zur Verfügung.

Schutz gegen Störungen aktivieren
Mithilfe dieser Option können Sie für die Domäne den Schutz gegen Störungen aktivieren. Solange der Schutz gegen Störungen aktiv ist, lehnt der Server für die Domäne alle Verbindungen von allen Benutzern für alle Dienste ab. Nachrichten von externen Gegenstellen werden jedoch weiterhin akzeptiert.

Zeitplan
Durch Anklicken dieses Steuerelements können Sie den Zeitplan festlegen, nach dem der Schutz gegen Störungen beginnt und endet. Ein Beispiel hierzu: Ein Zeitplan mit den Daten 01. Mai 2020 bis 30. Juni 2020, montags bis freitags von 17:00 Uhr bis 07:00 Uhr, bewirkt, dass in dem genannten Zeitraum an den genannten Wochentagen zwischen 17:00 und 07:00 Uhr für die Benutzer keine Maildienste zur Verfügung stehen. Wenn Sie das Beginndatum löschen, dann wird der Zeitplan deaktiviert. **Dies führt dazu,**

dass der Schutz gegen Störungen für die Domäne dauerhaft und ohne Zeitbegrenzung aktiv ist.

SMTP-Hostname
In dieses Feld wird der vollqualifizierte Domänenname (nach der englischen Bezeichnung Fully Qualified Domain Name auch abgekürzt FQDN) eingetragen, der bei der Übermittlung von Nachrichten für diese Domäne als Teil der SMTP-Befehle `HELO/EHLO` verwendet wird. Ist die Option *Diese Domäne akzeptiert nur Verbindungen mit der Host-IP-Adresse* weiter unten aktiv, so ist diese Domäne fest an ihre eigene IP-Adresse gebunden. Eingehende Verbindungen für diese IP-Adresse werden dann mit dem richtigen FQDN beantwortet. Dies funktioniert unter Umständen aber auch, wenn diese Option nicht aktiv ist. Bestehen aber zwei oder mehr Domänen, und nutzen diese Domänen dieselbe IP-Adresse, ohne dass eine Domäne fest an die IP-Adresse gebunden ist, dann werden eingehende Verbindungen für diese IP-Adresse mit dem FQDN beantwortet, der in der alphabetisch sortierten Liste zuerst erscheint.

In den meisten Fällen ist der FQDN entweder der *Domänenname* oder der Name einer Subdomäne dieses Domänennamens (wie etwa "`mail.example.com`"). Statt dessen kann auch eine IP-Adresse in dem Format "`[192.0.2.0]`" angegeben werden. Ist kein FQDN angegeben, so nutzt MDaemon den FQDN der Standard-Domäne.

IPv4-/IPv6-Adresse
In diese Felder tragen Sie die IPv4- und IPv6-Adressen ein, die Sie mit dieser Domäne verknüpfen wollen. Fehlen diese Adressen, so versucht MDaemon, verwendbare Adressen automatisch zu erkennen.

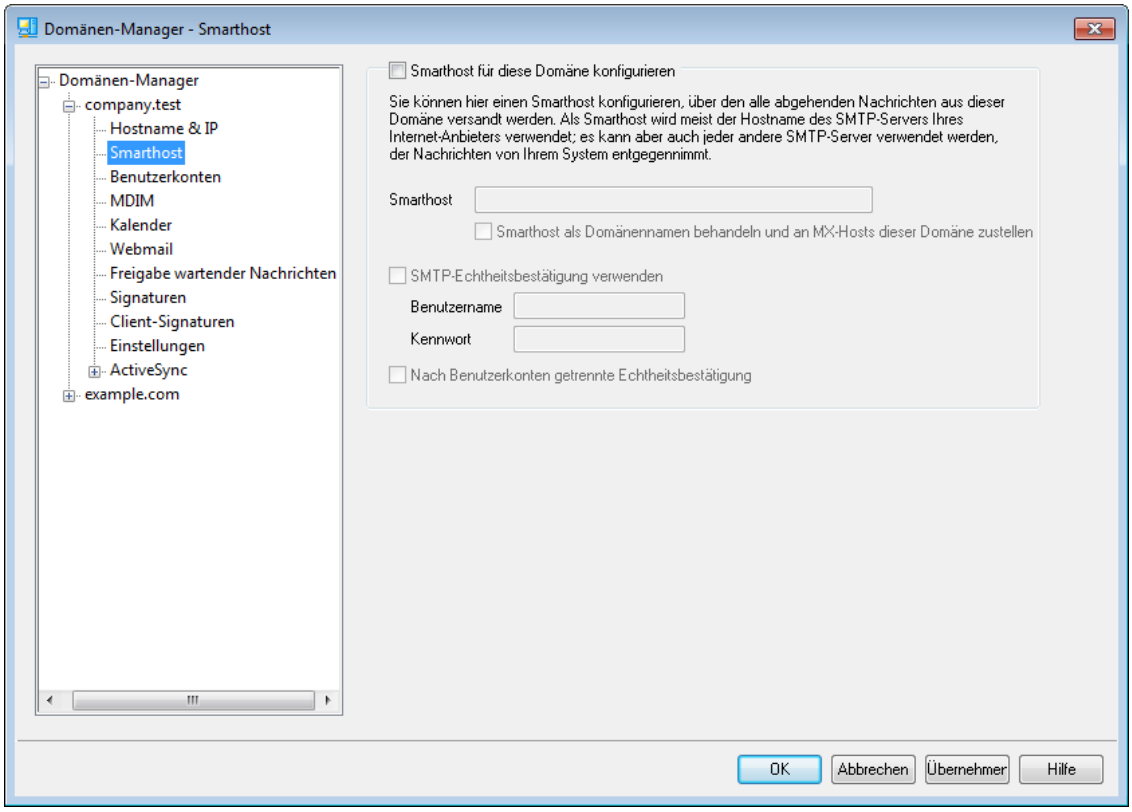
Erkennen
Mithilfe dieser Schaltflächen können Sie die IPv4- und IPv6-Adressen erkennen lassen, die für die beiden Adressfelder in Frage kommen. Sie können nach der Erkennung aus der Liste der erkannten Adressen die gewünschten IP-Adressen auswählen.

Diese Domäne akzeptiert nur Verbindungen mit den oben angegebenen IP-Adressen
Diese Option bewirkt, dass eingehende Verbindungen für die gerade bearbeitete Domäne nur zulässig sind, wenn sie an die oben angegebenen IP-Adressen gerichtet sind. Per Voreinstellung wirkt diese Option nur auf eingehende Verbindungen. Die Bindung der Sockets bei abgehenden Verbindungen wird durch eine Option im Konfigurationsdialog "Server-Einstellungen » Bindungen 114" gesteuert.

Siehe auch:

Domänen-Manager 181
Voreinstellungen » System 495

3.2.2 Smarthost



Smarthost für diese Domäne konfigurieren

Sie können die abgehenden Nachrichten aus der gerade bearbeiteten Domäne über einen bestimmten Smarthost an die Empfänger zustellen lassen. Hierzu aktivieren Sie diese Option, und konfigurieren Sie den Smarthost mithilfe der folgenden Optionen. Die Einstellungen im Konfigurationsdialog Postausgang 97 für die Zustellung abgehender Nachrichten werden für die Domäne nicht mehr berücksichtigt, sobald diese Option aktiv ist. Abgehende Nachrichten aus dieser Domäne werden dann nur noch über den hier konfigurierten Smarthost versandt.

Smarthost
Hier wird der Hostname oder die IP-Adresse des E-Mail-Hosts eingetragen, der als Gateway oder Smarthost genutzt werden soll. Dieser Smarthost ist normalerweise der SMTP-Server bei dem verwendeten ISP.

> Der Name oder die IP-Adresse der Standard-Domäne von MDaemon dürfen hier nicht eingetragen werden. Dieser Eintrag sollte einen ISP oder anderen Mailserver bezeichnen, über den E-Mail versandt werden kann.

Smarthost als Domänennamen behandeln und an MX-Hosts dieser Domäne zustellen
Diese Option bewirkt, dass der angegebene Host nicht als ein bestimmter, auf einen Server verweisender Hostname ausgewertet wird, sondern dass der Hostname als Name einer Domäne behandelt wird. Ist die Option aktiv, dann fragt MDaemon die MX-Server der angegebenen Domäne ab und stellt die Verbindungen mit ihnen her.

SMTP-Echtheitsbestätigung verwenden
Diese Option muss aktiv sein, falls der *Smarthost* eine Echtheitsbestätigung erfordert. Benutzername und Kennwort müssen dann in die folgenden Felder eingetragen werden. Die hier eingetragenen Anmeldedaten werden für alle abgehenden SMTP-Verbindungen zu dem angegebenen Server genutzt. Wird hingegen die Option *Echtheitsbestätigung nach Benutzerkonten getrennt durchführen* weiter unten aktiviert, so führt MDaemon für jede einzelne Nachricht eine eigene Echtheitsbestätigung durch und übermittelt dazu die E-Mail-Adresse und das Kennwort für den Smarthost, die im Feld *Benutzername/Kennwort für Smarthost* für das Benutzerkonto des jeweiligen Absenders eingetragen sind. Dieses Feld ist über den Abschnitt Mail-Dienste[718] des Benutzerkonten-Editors erreichbar.

Benutzername
Geben Sie hier den Benutzernamen oder Anmeldenamen ein.

Kennwort
Geben Sie hier das Kennwort für die Anmeldung beim Smarthost ein.

Nach Benutzerkonten getrennte Echtheitsbestätigung
Diese Option bewirkt, dass beim Versand von Nachrichten über SMTP für jede Nachricht eigene Anmeldedaten für die Echtheitsbestätigung an den oben konfigurierten *Smarthost* gesendet werden. Die hier unter *Benutzername* und *Kennwort* eingetragenen Anmeldedaten werden nicht genutzt. Stattdessen werden für jedes Benutzerkonto die E-Mail-Adresse und das Kennwort für den Smarthost (die beide im Abschnitt Mail-Dienste[718] des Benutzerkonten-Editors eingetragen werden) übermittelt. Sind für ein Benutzerkonto dort kein Benutzername und kein Kennwort für den Smarthost eingetragen, so werden die oben angegebenen Anmeldedaten für das Benutzerkonto verwendet.

Soll für die nach Benutzerkonten getrennte Echtheitsbestätigung nicht das *Kennwort für den Smarthost* sondern das *E-Mail-Kennwort* des Benutzerkontos verwendet werden, so wird dies durch Bearbeiten des folgenden Eintrags in der Datei `MDaemon.ini` erreicht:

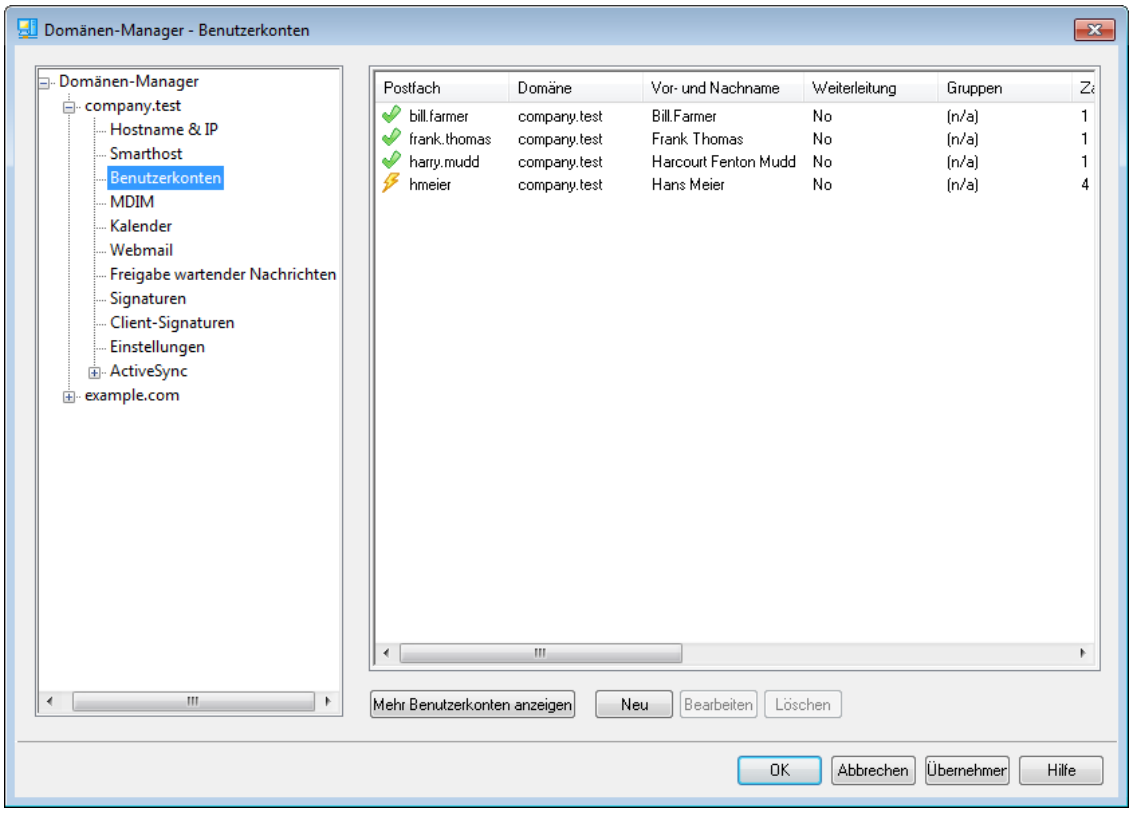
```
[AUTH]
ISPAUTHUsePasswords=Yes (Ja, Voreinstellung ist "No", Nein)
```

Wird die Option `ISPAUTHUsePasswords=Yes` aktiviert, so führt dies dazu, dass mit der Zeit alle Kennwörter der lokalen Benutzerkonten an den Smarthost übermittelt werden. Hieraus kann sich ein Risiko für die Sicherheit des Mailservers ergeben, da die Kennwörter Teil der Zugriffskontrolle sind. Diese Option sollte daher nur genutzt werden, wenn der Smarthost absolut vertrauenswürdig ist. Dürfen die Benutzer ihre *E-Mail-Kennwörter* über Webmail oder auf anderem Wege selbst ändern, so ändern sie damit auch ihre *Kennwörter für den Smarthost*. Die Echtheitsbestätigung beim Smarthost kann dann fehlschlagen, wenn ein *E-Mail-Kennwort* lokal geändert wird, der Smarthost aber von der Änderung keine Kenntnis hat.

Siehe auch:

Domänen-Manager 181
Server-Einstellungen » Postausgang 97
Benutzerkonten-Editor » Mail-Dienste 718

3.2.3 Benutzerkonten



Auf der Seite Benutzerkonten wird eine Liste aller Benutzerkonten in MDaemon angezeigt, die zur gerade bearbeiteten Domäne gehören. In jedem Listeneintrag erscheinen ein Symbol für den Zustand des Benutzerkontos (siehe unten), weiter der Postfachname, der Vor- und Nachname des Benutzers, die Gruppen, denen das Benutzerkonto angehört, die Zahl der Nachrichten und der belegte Speicherplatz (in MB). Die Liste kann wahlweise auf- oder absteigend nach jeder gewünschten Spalte sortiert werden. Ein Klick auf eine Spaltenüberschrift sortiert die Liste nach dieser Spalte aufsteigend, ein erneuter Klick sortiert nach der Spalte absteigend.

Symbole für den Zustand der Benutzerkonten

Benutzerkonto ist ein globaler oder Domänen-Administrator.

Benutzerkonto mit uneingeschränktem Zugriff. Zugriff über POP und IMAP ist zugelassen.

Benutzerkonto mit eingeschränktem Zugriff. Zugriff entweder über POP oder IMAP ist gesperrt.

Eingefrorenes Benutzerkonto. Das Benutzerkonto nimmt Nachrichten entgegen, der Benutzer kann Nachrichten aber weder abrufen noch versenden.

Gesperrtes Benutzerkonto. Jeder Zugriff auf das Benutzerkonto ist gesperrt.

Neu
Dieses Steuerelement öffnet den Benutzerkonten-Editor 714, um ein neues Benutzerkonto anzulegen.

Bearbeiten
Dieses Steuerelement lädt den jeweils ausgewählte Eintrag der Kontenliste in den Benutzerkonten-Editor 714. Die können Benutzerkonten auch durch Doppelklick zum Bearbeiten öffnen.

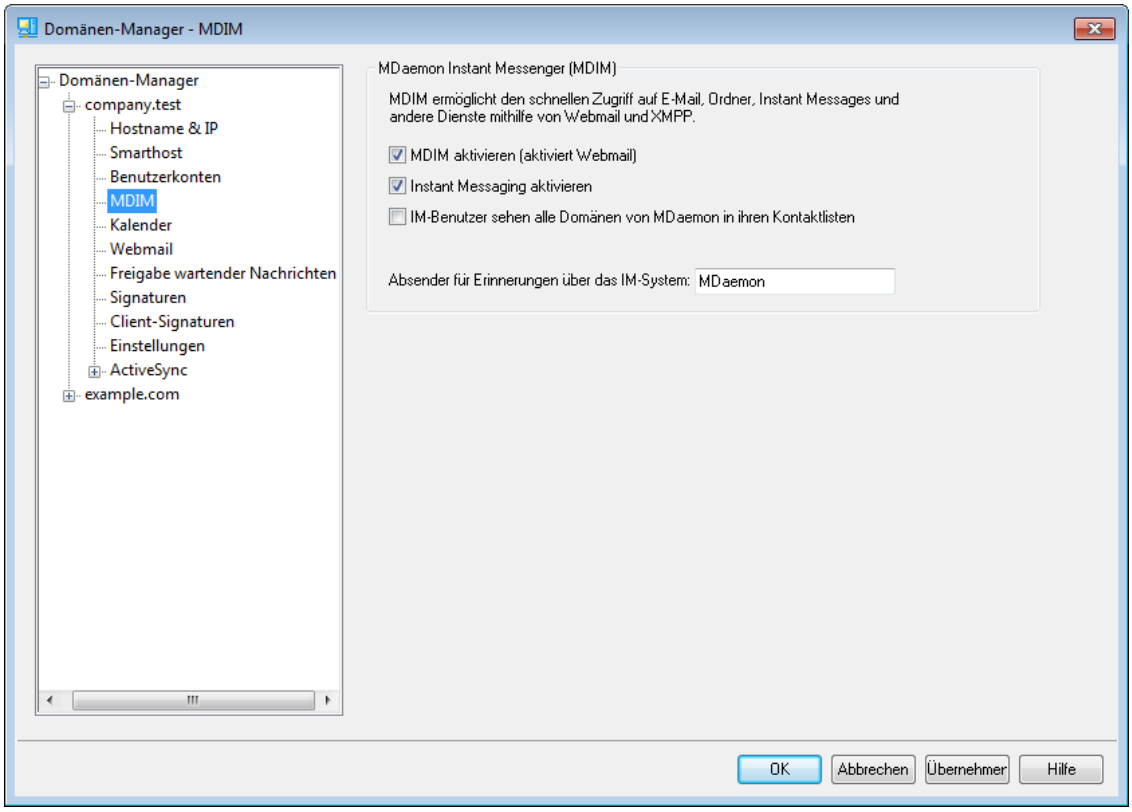
Löschen
Dieses Steuerelement löscht das gewählte Benutzerkonto; vorher wird eine Bestätigungsabfrage eingeblendet.

Mehr Benutzerkonten anzeigen
In der Kontenliste erscheinen nur höchstens 500 Einträge gleichzeitig. Bestehen in der ausgewählten Domäne mehr als 500 Benutzerkonten, so zeigt ein Klick auf diesen Knopf die jeweils nächsten 500 Konten an. Um die Zahl der gleichzeitig angezeigten Konten zu erhöhen, vgl. den oben stehenden Hinweis.

Siehe auch:

Benutzerkonten-Manager 712
Benutzerkonten-Editor 714
Vorlage Neue Benutzerkonten 788

3.2.4 MDIM



Dieser Konfigurationsdialog steuert die Einstellungen für den MDaemon Instant Messenger (MDIM) 318 in der gerade bearbeiteten Domäne. Die Voreinstellungen in diesem Konfigurationsdialog werden durch den Abschnitt Standard-MDaemon Instant Messenger 331 im Konfigurationsdialog Web- & IM-Dienste gesteuert. Die MDIM-Leistungsmerkmale können für einzelne Benutzerkonten mithilfe des Konfigurationsdialogs Web-Dienste 720 und für Gruppen von Benutzerkonten mithilfe des Konfigurationsdialogs Gruppen-Eigenschaften 784 aktiviert und deaktiviert werden.

MDaemon Instant Messenger

MDIM aktivieren (aktiviert Webmail)
Diese Option bewirkt, dass die Webmail-Benutzer der gerade bearbeiteten Domäne per Voreinstellung den MDaemon Instant Messenger aus Webmail herunterladen können. Die Benutzer müssen hierzu die Seite *Optionen » MDaemon Instant Messenger* aufrufen. Um die Installation und die Einrichtung zu erleichtern, wird die Installationsroutine automatisch an das Benutzerkonto des Benutzers angepasst, der sie abruft. Ist diese Option aktiv, so kann MDIM die Leistungsmerkmale Meine Nachrichtenordner nutzen, wodurch die Benutzer direkt aus dem Kontextmenü des MDIM ihre Benutzerkonten auf neue Nachrichten prüfen und WorldClient aufrufen können. MDIM ist per Voreinstellung aktiv.

Instant Messaging aktivieren
Per Voreinstellung können die Benutzer MDIM und XMPP 372-Clients von Drittanbietern nutzen, um Instant Messages mit anderen Benutzern ihrer eigenen Domäne auszutauschen. Um die Nutzung des Instant Messagings durch die Benutzer der Domäne zu verhindern, deaktivieren Sie diese Option.

Alle IM-Nachrichten in Protokolldateien einbeziehen
Diese Option bewirkt, dass der gesamte Instant-Messaging-Verkehr der Domäne in die Datei `InstantMessaging.log` protokolliert wird (diese Datei befindet sich im Verzeichnis `MDaemon/LOGS/`).

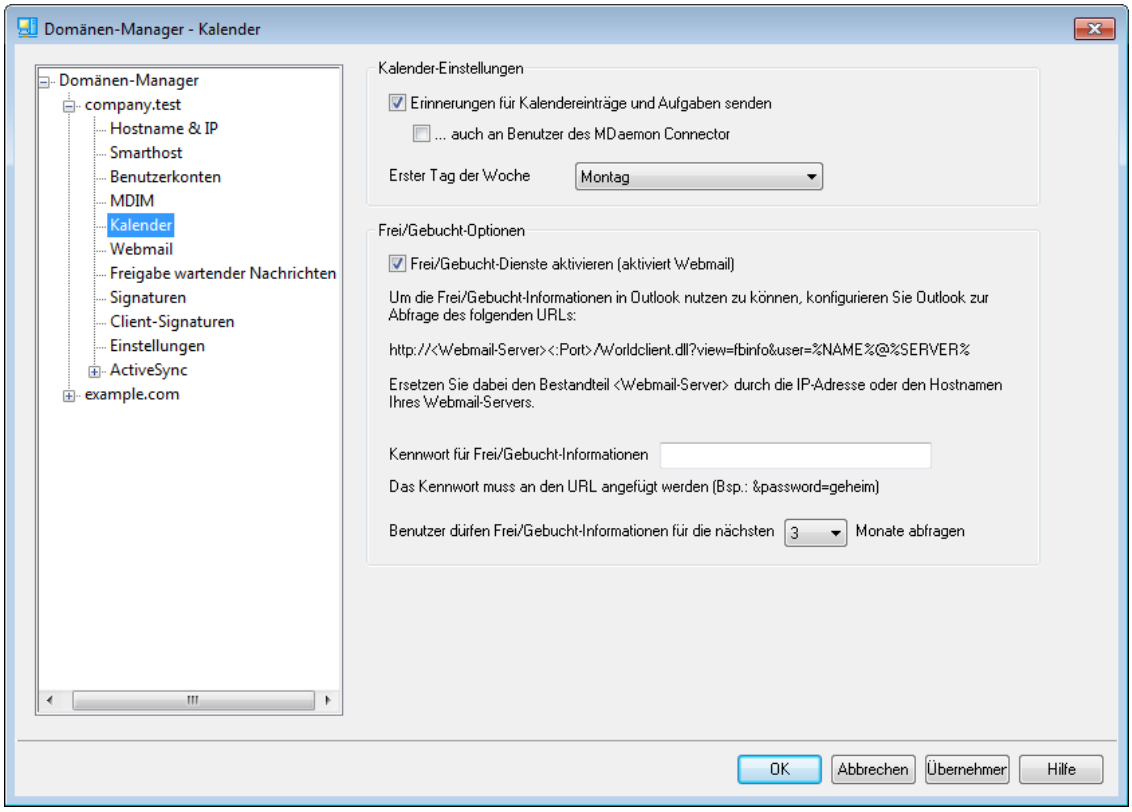
IM-Benutzer sehen alle Domänen von MDaemon in ihren Kontaktlisten
Diese Option bewirkt, dass die Benutzer der gerade bearbeiteten Domäne per Voreinstellung auch solche Kontakte in ihre Kontaktlisten eintragen können, die nicht zu ihrer eigenen MDaemon-Domäne gehören. Sie können dann Kontakte aus allen lokalen MDaemon-Domänen in die Kontaktlisten hinzufügen. Ist diese Option nicht aktiv, so können nur Kontakte in derselben Domäne hinzugefügt werden. Werden auf dem MDaemon-Server beispielsweise die Domänen example.com und example.org betrieben, so bewirkt das Aktivieren dieser Option für die Domäne example.com, dass deren Benutzer Instant-Messaging-Kontakte beider Domänen in ihre Kontaktlisten eintragen können. Ist die Option deaktiviert, so können die Benutzer nur andere Kontakte ihrer eigenen Domäne example.com eintragen. Diese Option ist per Voreinstellung abgeschaltet.

Absender für Erinnerungen über das IM-System [*Text*]
Wird in den Webmail-Kalender eines Benutzers ein Termin eingetragen, so kann dafür eine Terminerinnerung veranlasst werden, die dem Benutzer zu einer bestimmten Zeit zugesandt wird. Ist das IM-System für die Domäne des Benutzers aktiv, so wird ihm die Terminerinnerung über den MDaemon Instant Messenger angezeigt. In diesem Textfeld können Sie den Namen festlegen, der als Absendername für die Erinnerung im Feld "`Von:`" angezeigt wird.

Siehe auch:

Domänen-Manager 181
Webmail » MDaemon Instant Messenger 331
Benutzerkonten-Editor » Web-Dienste 720
Gruppen-Eigenschaften 784

3.2.5 Kalender



Dieser Konfigurationsdialog steuert die Einstellungen für die Kalender-Funktionen von MDaemon in der gerade bearbeiteten Domäne. Die Voreinstellungen in diesem Konfigurationsdialog werden durch den Abschnitt Kalender 333 im Konfigurationsdialog Web- & IM-Dienste gesteuert.

Kalender-Optionen

Erinnerungen für Kalendereinträge und Aufgaben senden
Falls Webmail die Erinnerungsnachrichten für Kalender und Aufgaben über E-Mail und den MDaemon Instant Messenger an die Benutzer senden soll, muss diese Option aktiv sein.

...auch an Benutzer des MDaemon Connectors
Falls die Option "*Erinnerungen für Kalendereinträge und Aufgaben senden*" oben aktiv ist, können durch Aktivieren dieser Option die Erinnerungen auch Benutzern des MDaemon Connectors gesandt werden.

Erster Tag der Woche
Der aus diesem Rollmenü ausgewählte Wochentag erscheint in den Terminkalendern dieser Domäne als erster Tag der Woche.

Frei/Gebucht-Optionen

MDaemon enthält einen Server für Frei/Gebucht-Informationen, mit dessen Hilfe der Organisator einer Besprechung prüfen kann, wann die gewünschten Teilnehmer verfügbar sind. Diese Funktion ist über eine Verknüpfung zur Zeitplanung in der Maske für die Besprechungsplanung in Webmail zugänglich. Die Funktion zeigt die Liste der Besprechungsteilnehmer und eine farbig

gekennzeichnete Übersicht über die Kalender der Teilnehmer. Für jeden Teilnehmer wird in einer eigenen Zeile durch Farbkennzeichnung dargestellt, zu welchen Zeiten er verfügbar ist. Dabei wird nach "belegt", "unter Vorbehalt", "nicht im Büro" und "keine Information" unterschieden. In der Besprechungsplanung kann auch automatisch der nächste verfügbare Termin gesucht werden. Der Server stellt dann den nächstmöglichen Zeitpunkt fest, zu dem alle Teilnehmer verfügbar sind. Anschließend kann eine Besprechungsanfrage an alle Teilnehmer gesendet werden, und die Teilnehmer können zusagen oder ablehnen.

Der Server für die Frei/Gebucht-Informationen, den Webmail bereit stellt, ist auch zu Microsoft Outlook kompatibel. Um den Server zu nutzen, muss in Outlook nur der URL zu dem Frei/Gebucht-Server von Webmail eingetragen werden. Bei Outlook 2002 sind die Einstellungen für die Abfrage von Frei/Gebucht-Informationen beispielsweise über "Extras » Optionen » Kalenderoptionen... » Frei/Gebucht-Optionen..." zugänglich.

In die Maske in Outlook muss folgender URL eingetragen werden:

```
http://<Webmail><:Port>
/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER%
```

Ersetzen Sie dabei "<Webmail>" durch die IP-Adresse oder den Domänennamen Ihres Webmail-Servers und "<:Port>" durch die Portnummer (falls Sie nicht den Standard-Web-Port nutzen). Ein Beispiel:

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%
@%SERVER%
```

Weitere Informationen über die Nutzung von Frei/Gebucht-Informationen bei der Terminplanung enthält die Online-Hilfe von Webmail.

Verwaltung von Frei/Gebucht-Informationen aktivieren
Diese Option schaltet die Funktionen des Frei/Gebucht-Servers für die Benutzer frei.

Kennwort für Frei/Gebucht-Informationen
Soll die Abfrage der Frei/Gebucht-Informationen über Outlook durch ein Kennwort geschützt werden, so muss dieses Kennwort hier eingetragen werden. Die Benutzer müssen dem oben konfigurierten URL in Outlook das Kennwort (im Format "&password=Kennwort") hinzufügen. Ein Beispiel hierzu:

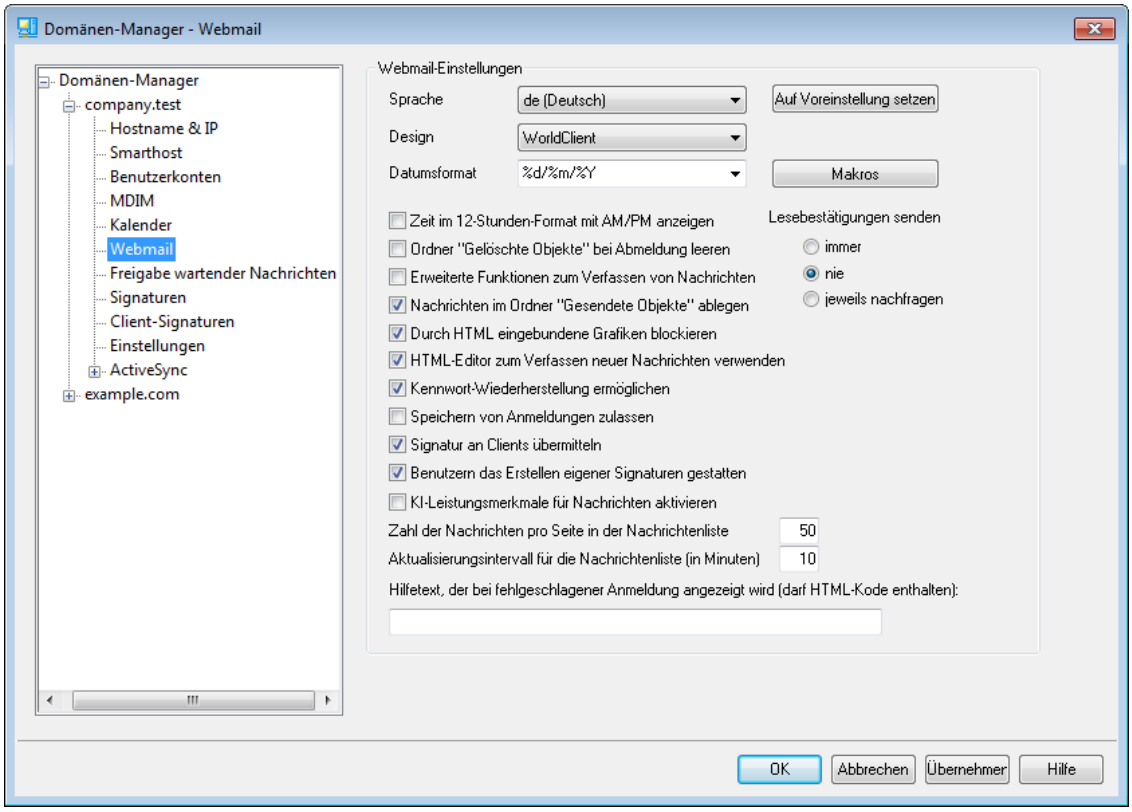
```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME
%@%SERVER%&password=MeinFBServerKennwort
```

Benutzer dürfen Frei/Gebucht-Informationen für die nächsten [xx] Monate abfragen
Diese Option bestimmt, für welchen Zeitraum die Benutzer Frei/Gebucht-Informationen im Voraus abfragen dürfen.

Siehe auch:

Webmail » Kalender 333

3.2.6 Webmail



Dieser Konfigurationsdialog legt die WorldClient-Einstellungen für die gerade bearbeitete Domäne fest. Die Voreinstellungen in diesem Konfigurationsdialog werden durch den Abschnitt WorldClient (Webmail) » Einstellungen[345] im Konfigurationsdialog Web- & IM-Dienste gesteuert. Diese Einstellungen bestimmen in vielen Bereichen, wie die Leistungsmerkmale durch Benutzer genutzt werden können, die sich bei WorldClient anmelden. Die Benutzer selbst können über die Seiten im Menü Optionen in WorldClient viele dieser Einstellungen an ihre Wünsche und Anforderungen anpassen.

WorldClient-Einstellungen

Auf Voreinstellung setzen
Durch Anklicken dieses Steuerelements setzen Sie die Optionen der gerade bearbeiteten Domäne auf die Standard-Einstellungen für Webmail[345] zurück.

Sprache
Durch Auswahl aus diesem Rollmenü wird die Sprache festgelegt, in der die Benutzeroberfläche von Webmail bei der ersten Anmeldung eines Benutzers an der ausgewählten Domäne erscheint. Die Benutzer können dann ihre bevorzugte Sprache über die Einstellungen von Webmail selbst auswählen.

Design
Aus diesem Rollmenü wird das Standard-Design ausgewählt, das Webmail bei der ersten Anmeldung eines Benutzers anzeigt. Die Benutzer können dann das von ihnen bevorzugte Design über die Einstellungen von Webmail auf der Seite Optionen » Benutzeranpassung selbst auswählen.

Datumsformat
Dieses Textfeld definiert das Datumsformat für die Benutzer von Webmail. Über das Steuerelement *Makros* wird eine Liste aller Makros angezeigt, die in diesem Textfeld zulässig sind. Nachfolgend sind alle diese Makros aufgeführt:

%A — Name des Wochentags

%B — Name des Monats

%d — Tag (wird als "01-31" angezeigt)

%m — Monat (wird als "01-12" angezeigt)

%y — Jahreszahl zweistellig

%Y — Jahreszahl vierstellig

In Webmail wird so beispielsweise "`%Y-%m-%d`" in die Datumsanzeige "`2011-12-15`" umgesetzt.

Makros
Ein Klick auf dieses Steuerelement zeigt ein Hilfefenster mit allen Makros an, die für das oben beschriebene Feld *Datumsformat* zulässig sind.

Lesebestätigungen senden
Diese Option bestimmt das Verhalten von Webmail in den Fällen, in denen eingehende Nachrichten eine Anforderung nach einer Lesebestätigung enthalten.

immer
Diese Option bewirkt, dass MDaemon dem Absender eine Bestätigung darüber sendet, dass die Nachricht gelesen wurde. Der Webmail-Benutzer, der die Nachricht erhalten hat, erhält dabei keine Information darüber, dass eine Lesebestätigung verlangt oder versandt wurde.

nie
Diese Option bewirkt, dass Webmail die Anforderungen nach Lesebestätigungen ignoriert.

jeweils nachfragen
Diese Option bewirkt, dass der Webmail-Benutzer jeweils gefragt wird, ob er eine Lesebestätigung versenden will. Die Abfrage erscheint, wenn der Benutzer eine Nachricht öffnet, die eine Anforderung nach einer Lesebestätigung enthält.

Zeit im 12-Stunden-Format mit AM/PM anzeigen
Diese Option bewirkt, dass die Uhrzeit in Webmail im 12-Stunden-Format mit den Zusätzen AM und PM angezeigt wird. So lange diese Option nicht aktiv ist, zeigt Webmail die Zeit im 24-Stunden-Format an. Die Benutzer können diese Einstellung über die Option "*Uhrzeit im 12-Stunden-Format mit AM/PM anzeigen*" auf der Seite Optionen » Kalender in Webmail selbst ändern.

Ordner "Gelöschte Objekte" bei Abmeldung leeren
Diese Option bewirkt, dass der Ordner *Gelöschte Objekte* eines Benutzers bei dessen Abmeldung aus Webmail geleert wird. Die Benutzer können diese Einstellung über die Einstellungen von Webmail selbst ändern.

Erweiterte Funktionen zum Verfassen von Nachrichten
Mit dieser Einstellung stehen den Benutzern beim Verfassen neuer Nachrichten erweiterte Möglichkeiten zur Verfügung. So lange diese Funktion nicht aktiv ist, wird lediglich das normale Fenster zum Verfassen neuer Nachrichten geöffnet. Die Benutzer können diese Einstellung über die Seite Optionen » E-Mail verfassen in Webmail selbst ändern.

Nachrichten im Ordner "Gesendete Objekte" ablegen
Diese Option bewirkt, dass eine Kopie jeder gesendeten Nachricht in dem Ordner *Gesendete Objekte* des jeweiligen Benutzerkontos abgelegt wird. Die Benutzer können diese Einstellung über die Seite Optionen » E-Mail verfassen in Webmail selbst ändern.

Durch HTML eingebundene Grafiken blockieren
Diese Option verhindert, dass Grafikdateien, die in E-Mail-Nachrichten im HTML-Format eingebunden sind und auf externen Servern liegen, in Webmail automatisch angezeigt werden. Will der Benutzer diese Grafiken sehen, so muss er eine Informationsleiste anklicken, die im Browserfenster oberhalb der Nachricht erscheint. Diese Funktion dient der Verhinderung von Spam-Nachrichten, da viele Spam-Nachrichten Grafiken mit besonderen URLs enthalten, die die E-Mail-Adresse des Benutzers, der die Nachricht betrachtet, identifizieren. Wird eine solche Grafik von dem externen Server abgerufen, so erhält der Spammer hierdurch die Bestätigung, dass die zugehörige E-Mail-Adresse gültig ist und gelesen wird. Die Option ist per Voreinstellung aktiv.

Nachrichten in neuem Browserfenster verfassen
Diese Option bewirkt, dass zum Verfassen von Nachrichten ein neues Browserfenster geöffnet wird, und dass die Editorfunktionen nicht im Hauptfenster dargestellt werden. Falls Sie nicht wünschen, dass ein gesondertes Fenster geöffnet wird, deaktivieren Sie diese Option. Die Benutzer können diese Einstellung über die Einstellungen zum Verfassen neuer Nachrichten in Webmail selbst ändern.

HTML-Editor zum Verfassen neuer Nachrichten verwenden
Diese Option erlaubt es den Benutzern, Nachrichten im Rich-Text-Format (HTML) zu verfassen. Die Benutzer können diese Einstellung über die Seite Optionen » E-Mail verfassen in Webmail selbst ändern.

Kennwort-Wiederherstellung ermöglichen
Diese Option ermöglicht solchen Benutzer der Domäne die Kennwort-Wiederherstellung, die über die Berechtigung zum Bearbeiten ihres Kennworts 720 verfügen. Diese Benutzer können in Webmail eine alternative E-Mail-Adresse hinterlegen und sich an diese E-Mail-Adresse eine Verknüpfung zum Zurücksetzen ihres Kennworts senden lassen, falls sie Ihr Kennwort einmal vergessen sollten. Um dieses Leistungsmerkmal einzurichten, müssen die berechtigen Benutzer im Konfigurationsdialog Optionen » Sicherheit in Webmail die alternative E-Mail-Adresse und ihr Kennwort angeben. Benutzern, die sich danach mit einem falschen Kennwort an Webmail anzumelden versuchen, wird die Verknüpfung "Haben Sie Ihr Kennwort vergessen?" angezeigt. Nach Anklicken dieser Verknüpfung werden sie aufgefordert, die alternative E-Mail-Adresse für die Kennwort-Wiederherstellung einzugeben, die sie zuvor in Webmail eingetragen haben. Geben sie die Adresse richtig ein, so sendet Webmail an die Adresse eine Nachricht mit einer Verknüpfung zu der Seite, auf der die Benutzer ein neues Kennwort festlegen können. Dieses Leistungsmerkmal ist per Voreinstellung abgeschaltet.

Sie können dieses Leistungsmerkmal nach Benutzern getrennt aktivieren. Hierzu bearbeiten Sie den folgenden Eintrag in der Datei `user.ini` für die betroffenen Benutzer (z.B. `\Users\example.com\frank\WC\user.ini`):

```
[User]
EnablePasswordRecovery=Yes (Ja, oder "=No", Nein, um dieses
Leistungsmerkmal für den gerade bearbeiteten Benutzer zu
deaktivieren.)
```

Speichern von Anmeldungen bei Zwei-Faktor-Authentifizierung zulassen (auch für Remoteverwaltung)
Wird bei einer Anmeldung an Webmail oder an der Remoteverwaltung die Zwei-Faktor-Authentifizierung genutzt, so erscheint per Voreinstellung eine Option zum Speichern der Anmeldung auf der Abfrageseite für die Zwei-Faktor-Authentifizierung. Aktiviert der Benutzer diese Option, so wird für eine gewisse Zeit (siehe hierzu "*Speichern von Anmeldungen zulassen*" weiter unten) der zweite Faktor bei der Anmeldung nicht mehr abgefragt. Falls Sie diese Speicherung der Anmeldung nicht zulassen und stattdessen die Abfrage des zweiten Faktors bei jeder Anmeldung erzwingen wollen, deaktivieren Sie diese Option. **Beachte:** Diese Option steht nur in der Webschnittstelle der MDaemon-Remoteverwaltung (MDRA) 350 zur Verfügung.

Speichern von Anmeldungen zulassen
Diese Option bewirkt, dass auf der Anmeldeseite von MDaemon Webmail die Option *Anmeldung speichern* erscheint, wenn der Benutzer der Domäne eine Verbindung mit Webmail über den https 327-Port hergestellt hat. Aktiviert der Benutzer vor der Anmeldung diese Option, so wird die folgende Anmeldung auf dem gerade verwendeten Endgerät gespeichert. Stellt der Benutzer später wieder eine Webmail-Verbindung her, so wird der Benutzer automatisch angemeldet. Die Anmeldung bleibt gespeichert, bis der Benutzer sich ausdrücklich aus Webmail abmeldet, oder bis der Token zur Speicherung der Anmeldung verfällt.

Per Voreinstellung wird die Anmeldung für höchstens 30 Tage gespeichert; nach diesem Zeitraum muss sich der Benutzer wieder mit Benutzernamen und Kennwort anmelden. Sie können diesen Zeitraum durch Ändern des Werts für die Option *Token für gespeicherte Anmeldungen laufen nach folgender Anzahl Tagen ab* auf der Weboberfläche der MDaemon-Remoteverwaltung (MDRA) 350 verlängern. Sie können den Zeitraum auch durch Bearbeiten des Eintrags `RememberUserExpiration=30` in der Datei `Domains.ini` im Verzeichnis `\MDaemon\WorldClient\` ändern. Der längste zulässige Zeitraum beträgt 365 Tage. **Beachte:** Die Zwei-Faktor-Authentifizierung 720 (2FA) nutzt eigene Token mit gesondert festgelegter Gültigkeitsdauer. Sie können die Gültigkeitsdauer dieser Token durch Bearbeiten des Eintrags `TwoFactorAuthRememberUserExpiration=30`, im Abschnitt `[Default:Settings]` der Datei `Domains.ini` im Verzeichnis `\MDaemon\WorldClient\` ändern. Ist der Token für die Zwei-Faktor-Authentifizierung wegen Ablaufs der Gültigkeitsdauer verfallen, so wird die Anmeldung durch die Zwei-Faktor-Authentifizierung auch dann erforderlich, wenn der Token für die Speicherung der Anmeldung noch gültig ist.

Die Option *Speichern von Anmeldungen zulassen* ist per Voreinstellung abgeschaltet. Sie wirkt nur auf die gerade bearbeitete Domäne. Die systemweite Option finden Sie im Abschnitt Einstellungen 345 des Konfigurationsdialogs Webmail.

Mithilfe der Option *Speichern von Anmeldungen zulassen* können die Benutzer die Anmeldungen auch auf mehreren Geräten speichern. Die Benutzer sollten veranlasst werden, diese Option nicht in öffentlichen Netzen einzusetzen. Sie können die Token zur Speicherung der Anmeldungen auch für alle Benutzer insgesamt zurücksetzen, sodass sich die Benutzer erneut anmelden müssen. Dies kann beispielsweise angezeigt sein, falls für ein Benutzerkonto der Verdacht auf einen Einbruch oder sicherheitsrelevanten Vorfall besteht. In der MDaemon-Remoteverwaltung steht hierfür das Steuerelement *Speichern von Anmeldungen zurücksetzen* zur Verfügung. Nach Anklicken dieses Steuerelements müssen sich alle Benutzer erneut anmelden.

Signatur an Clients übermitteln
Um die Client-Signaturen 206 an die Webmail-Benutzer der gerade bearbeiteten Domäne zu übermitteln, aktivieren Sie diese Option. Hierdurch wird in Webmail eine Signatur mit der Bezeichnung "System" erstellt, die über das Menü **Optionen » E-Mail verfassen** erreichbar ist. Die Benutzer können diese Signatur automatisch in das Editorfenster übernehmen lassen, wenn sie neue Nachrichten verfassen. Ist diese Option aktiv, und wurde aber im Abschnitt Client-Signaturen des Domänen-Managers keine Client-Signatur konfiguriert, so wird die Option Standard-Client-Signaturen 140 verwendet. Ist auch keine Standard-Client-Signatur konfiguriert, so erscheint die Signatur der Bezeichnung System in Webmail nicht.

Benutzern das Erstellen eigener Signaturen gestatten
Diese Option gestattet den Benutzer der Domäne die Erstellung eigener benutzerdefinierter Signaturen in Webmail. Die Benutzer können dann auswählen, welche Signatur sie beim Verfassen von Nachrichten automatisch in das Editorfenster übernehmen wollen. Ist diese Option deaktiviert und den Benutzern das Erstellen eigener Signaturen damit nicht gestattet, und ist zugleich die Option *Signatur an Clients übermitteln* weiter oben aktiv, so können die Benutzer in Webmail nur die Client-Signatur 140 (in Webmail ist das die Signatur mit der Bezeichnung System) automatisch in das Editorfenster übernehmen. Die Signatur-Optionen in Webmail sind erreichbar über **Optionen » E-Mail verfassen**.

Zahl der Nachrichten pro Seite in der Nachrichtenliste
Diese Option steuert, wie viele Nachrichten auf jeder Seite der Nachrichtenliste für die einzelnen Nachrichten-Ordner erscheinen. Enthält ein Ordner mehr Nachrichten, als hier angegeben sind, so erscheinen über und unter der Nachrichtenliste Steuerelemente, mit denen der Benutzer die nun mehrseitige Nachrichtenliste durchblättern kann. Die Benutzer können diese Einstellung in Webmail selbst ändern.

Aktualisierungsintervall für die Nachrichtenliste (in Minuten)
Hier wird der Zeitabstand in Minuten festgelegt, nach dem Webmail die Nachrichtenliste automatisch aktualisiert. Die Benutzer können diese Einstellung auf der Seite Optionen » Benutzeranpassung in Webmail selbst ändern.

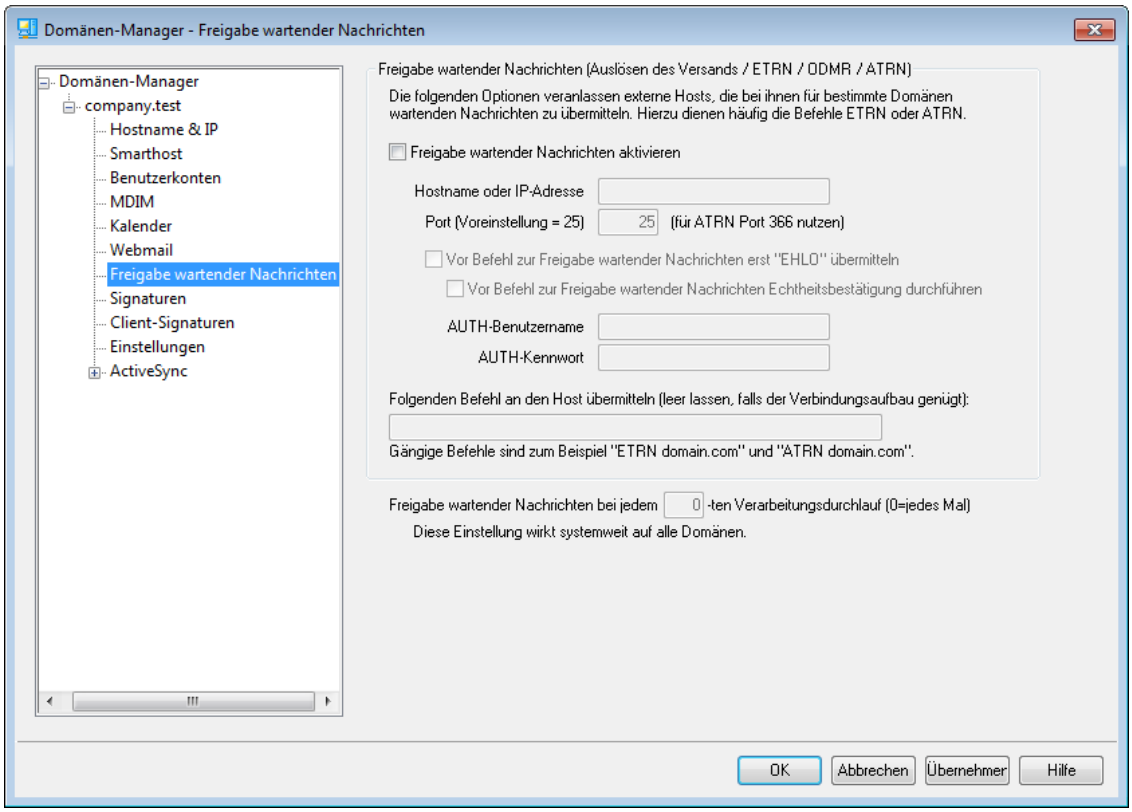
Hilfetext, der bei fehlgeschlagener Anmeldung angezeigt wird (darf HTML-Kode enthalten)
In diesem Textfeld können Sie einen Text (entweder als reinen Text oder im HTML-Format) angeben, den Webmail im Anmeldedialog anzeigt, falls bei der Anmeldung eines Benutzers ein Fehler auftritt. Der Text erscheint unter dem folgenden Text: "*Ihre Anmeldedaten sind ungültig. Bitte versuchen Sie es erneut. Falls Sie Unterstützung benötigen, wenden Sie sich bitte an den Administrator Ihres E-Mail-Systems.*". Sie können in diesem Text Ihren Benutzern beispielsweise eine Verknüpfung zu einer anderen Seite anbieten oder Kontaktdaten für eine Stelle anzeigen, an die sich die Benutzer im Fall von Fehlern bei der Anmeldung an Webmail wenden können.

Sind mehrere Domänen auf dem Server vorhanden, so arbeitet dieses Leistungsmerkmal nur dann richtig, wenn für jede Domäne ein gültiger SMTP-Hostname 184 konfiguriert ist. Fehlt dieser Hostnamen, so wird der Text der Standard-Domäne 181 angezeigt. Sind beispielsweise mehrere Domänen auf dem Server vorhanden, werden alle Webmail-Benutzer zur Anmeldung aber auf denselben Hostnamen geleitet, so wird unter Umständen ein domänenspezifischer Hilfetext bei fehlgeschlagener Anmeldung nicht angezeigt.

Siehe auch:

Webmail » Einstellungen 345

3.2.7 Freigabe wartender Nachrichten



Freigabe wartender Nachrichten (ETRN/ODMR/ATRN)

Gegenstelle zur Freigabe und Übermittlung wartender Nachrichten auffordern
Wenn MDaemon Post für externe Empfänger bearbeitet, kann MDaemon eine Verbindung zu einem beliebigen Rechner auf einem beliebigen Port herstellen und eine frei wählbare Zeichenkette übertragen. Hilfreich ist dies besonders dann, wenn eine Gegenstelle erst einen Befehl abwartet, bevor sie mit dem Versand der für das lokale System bereit liegenden Nachrichten beginnt. Solche Befehle sind z.B. `ATRN`, `ETRN`, und `QSND`. Diese Funktion kann auch genutzt werden, falls der benutzte ISP nur durch eine kurze `FINGER`- oder `TELNET`-Verbindung feststellen kann, dass das lokale System eine Verbindung hergestellt hat.

Hostname oder IP-Adresse
An diesen Host soll die Aufforderung zur Freigabe wartender Nachrichten übermittelt werden.

Port
Hier wird der zu benutzende Port angegeben. Die Voreinstellung 25 (der SMTP-Port) ist für `ETRN` und `QSND` geeignet. Für `ATRN` wird üblicherweise der Port 366, für `FINGER` der Port 79 verwendet.

"EHLO" vor Übermittlung des Befehls senden
Diese Option sollte nur aktiviert werden, wenn für die Aufforderung zur Freigabe wartender Nachrichten eine Verbindung zu einem SMTP-Server hergestellt wird. Die Option veranlasst den Aufbau einer SMTP-Verbindung mit der angegebenen Gegenstelle, wobei unmittelbar nach dem SMTP-Befehl "`EHLO`" die oben angegebene Zeichenkette gesendet wird.

Echtheitsbestätigung über SMTP AUTH durchführen (für ATRN erforderlich)
Manche ISP verlangen, dass ihre Kunden eine Echtheitsbestätigung über ESMTP AUTH durchführen, bevor sie zur Freigabe wartender Nachrichten auffordern dürfen. Dies soll verhindern, dass nicht hierzu berechtigte Benutzer den Versand von Nachrichten anderer Benutzer auslösen. Falls der benutzte ISP eine solche Echtheitsbestätigung verlangt, aktivieren Sie diese Option, und tragen Sie die nötigen Anmeldedaten in die folgenden Felder ein.

Wird der Befehl ATRN für die Freigabe wartender Nachrichten genutzt, so ist eine Echtheitsbestätigung zwingend erforderlich.

Benutzername
Geben Sie hier den Benutzernamen ein, der als Teil des AUTH-Befehls logon an die Gegenstelle übermittelt wird.

Kennwort
Geben Sie hier das AUTH-Kennwort ein.

Folgenden Befehl an die Gegenstelle senden (leer lassen, falls der Verbindungsaufbau allein genügt)
In diesem Feld muss die Zeichenkette angegeben werden, welche als Aufforderung zur Freigabe wartender Nachrichten an die Gegenstelle übermittelt werden soll. So müssen z.B. für den Befehl `ETRN` dieser Befehl und dann der Name der Domäne, für welche die Nachrichten bereit liegen, angegeben werden. Bei

abweichenden Verfahren müssen andere Texte gesendet werden. Auskünfte dazu, ob bei dem verwendeten ISP zur Freigabe wartender Nachrichten aufgefordert werden muss und wie hier vorzugehen ist, erteilt der ISP. Falls der ISP die Funktion On-Demand Mail Relay (ODMR, Postrelais bei Bedarf) 201 unterstützt, empfiehlt es sich, diese Funktionen, soweit möglich, zu nutzen. Für diese Funktionen muss in dieser Option der Befehl ATRN eingetragen werden.

Aufforderung zur Freigabe bei jedem [xx]-ten Verarbeitungsdurchlauf senden (0=jedes Mal)
Per Voreinstellung fordert MDaemon bei jedem Verarbeitungsdurchlauf für externe Nachrichten zur Freigabe wartender Nachrichten auf. Falls das unerwünscht ist, kann hier das Intervall eingetragen werden, in dem die Aufforderung erfolgen soll. Der Wert 3 bewirkt etwa, dass nur bei jedem dritten Verarbeitungsdurchlauf für externe Nachrichten zur Freigabe wartender Nachrichten aufgefordert wird.

Diese Einstellung wirkt systemweit auf alle Domänen.

3.2.7.1 On-Demand Mail Relay (ODMR, Nachrichtenrelais bei Bedarf)

Die zurzeit empfohlene Methode zum Auslösen des Versands, die soweit möglich genutzt werden sollte, ist ODMR (kurz für On-Demand Mail Relay, Nachrichtenrelais bei Bedarf). Sie ist den anderen Methoden, wie etwa ETRN, vor allem deshalb überlegen, weil sie eine Echtheitsbestätigung zwingend vorschreibt. Sie nutzt außerdem den neuen ESMTP-Befehl `ATRN`. Dieser Befehl setzt nicht voraus, dass der Client eine feste IP-Adresse hat, weil er den Datenfluss zwischen Server und Client sofort umkehrt und die jeweils wartenden Nachrichten über die bestehende Verbindung übermittelt, ohne dass dafür eine zusätzliche Verbindung hergestellt werden muss (wie es etwa noch bei ETRN nötig ist).

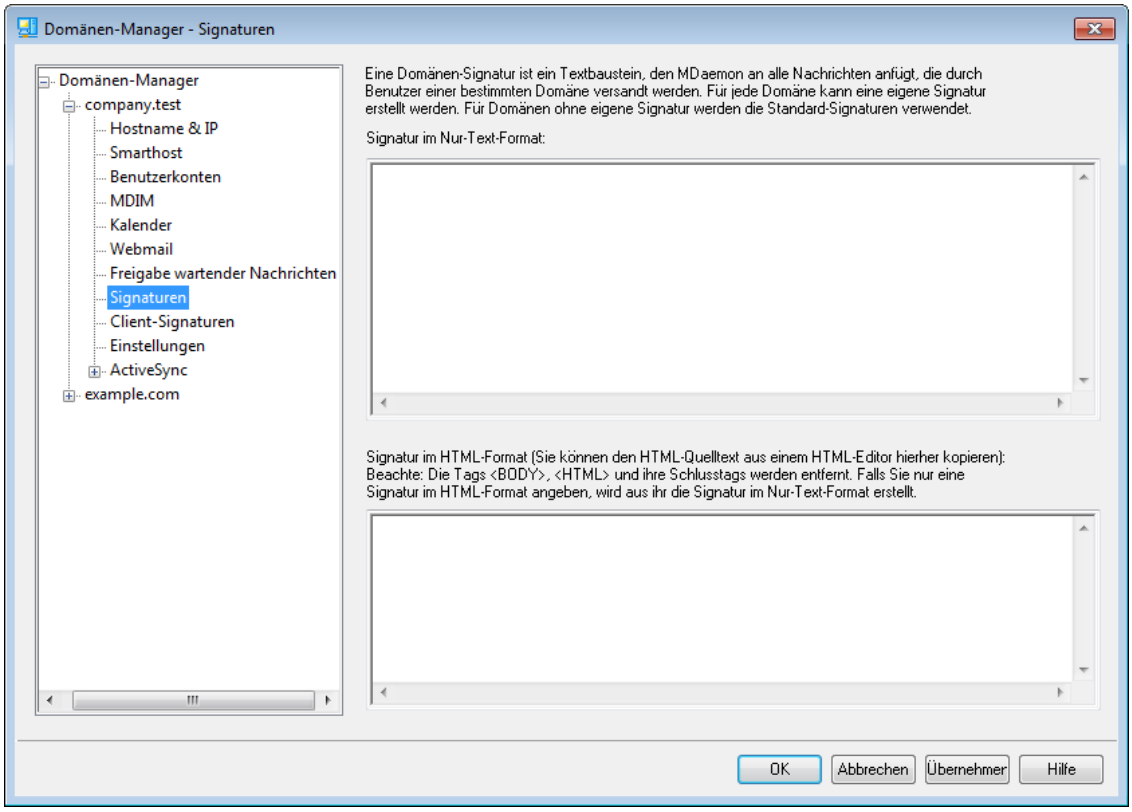
MDaemon unterstützt ODMR als Client vollständig und nutzt hierzu den Befehl `ATRN` und die Einstellungen zur Freigabe wartender Nachrichten 199. Als Server unterstützt MDaemon ODMR für die Domänen-Gateways; die entsprechenden Einstellungen sind im Abschnitt Freigabe wartender Nachrichten 264 im Gateway-Editor zu finden.

Da nicht alle Mailserver ODMR unterstützen, sollten Sie mit Ihrem ISP Rücksprache halten, bevor Sie versuchen, die entsprechenden Funktionen einzusetzen.

Siehe auch:

Gateway-Editor » Freigabe wartender Nachrichten 264

3.2.8 Signaturen



Mithilfe dieses Konfigurationsdialogs können Sie eine Signatur definieren, die allen abgehenden Nachrichten Ihrer MDaemon-Benutzer aus der gerade bearbeiteten Domäne hinzugefügt wird. Falls Sie hier für die gerade bearbeitete Domäne keine eigenen Signaturen angeben, verwendet MDaemon die Standard-Signaturen 135. Signaturen werden werden am Ende des Nachrichtentextes eingefügt. Eine Ausnahme hiervon bilden Nachrichten in Mailinglisten, für die ein Schlusstext 296 definiert ist; bei solchen Nachrichten wird der Schlusstext nach der Signatur eingefügt. Im Abschnitt Signatur 753 des Benutzerkonten-Editors können Sie zusätzlich eigene getrennte Signaturen für jedes Benutzerkonto festlegen. Signaturen der Benutzerkonten werden unmittelbar vor den Standard- oder Domänen-Signaturen eingefügt.

Signatur im Nur-Text-Format

In dieses Textfeld können Sie eine Signatur im Nur-Text-Format eintragen. Falls Sie für die Verwendung im Teil "text/html" von Multipart-Nachrichten eine hierzu passende HTML-Signatur festlegen wollen, tragen Sie deren HTML-Quellkode in das Textfeld *Signatur im HTML-Format* weiter unten ein. MDaemon nutzt dann für jeden Teil der Multipart-Nachricht die passende Signatur. Ist keine HTML-Signatur festgelegt, so wird die Signatur im Nur-Text-Format in beide Teile der Nachricht eingefügt. Ist keine Signatur im Nur-Text-Format festgelegt, so wird die Signatur aus der Signatur im HTML-Format erstellt.

Signatur im HTML-Format (Sie können den HTML-Quelltext aus einem HTML-Editor hierher kopieren)

In dieses Textfeld können Sie eine Signatur im HTML-Format eintragen. Diese Signatur wird in den Teil "text/html" von Multipart-Nachrichten eingefügt. Falls Sie sowohl in dieses Textfeld wie auch in das Textfeld *Signatur im Nur-Text-Format* weiter oben je eine Signatur eintragen, nutzt MDaemon für jeden Teil der Multipart-

Nachricht die passende Signatur. Ist keine Signatur im Nur-Text-Format festgelegt, so wird sie aus der Signatur im HTML-Format erstellt.

Sie können eine Signatur im HTML-Format erstellen, indem Sie den HTML-Kode unmittelbar in dieses Textfeld eintragen, oder indem Sie den HTML-Kode in einem HTML-Editor erstellen und dann über die Zwischenablage in dieses Textfeld kopieren. Sie können in eine Signatur im HTML-Format auch Grafikdateien unmittelbar (inline) einbetten; hierzu steht das Makro `$ATTACH_INLINE:Pfad_zur_Grafikdatei$` zur Verfügung.

Ein Anwendungsbeispiel stellt der nachfolgend dargestellte HTML-Kode dar:

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \grafiken\mr_t_and_arnold.jpg$">
```

Sie können Grafiken auch mithilfe der MDaemon-Remoteverwaltung 350 in die Signaturen einfügen. Hierzu stehen Ihnen folgende Vorgehensweisen zur Verfügung:

- Klicken Sie in der Remoteverwaltung im Abschnitt Signaturen auf das Steuerelement "Grafik" in der Symbolleiste des HTML-Editors, und geben Sie dann den URL der gewünschten Grafikdatei an, oder laden Sie eine Grafikdatei hoch.
- Klicken Sie in der Remoteverwaltung im Abschnitt Signaturen auf das Steuerelement "Grafik hinzufügen" in der Symbolleiste des HTML-Editors.
- Falls Sie Chrome, FireFox, Safari oder den MS Internet Explorer ab Version 10 nutzen, ziehen Sie eine Grafikdatei in den HTML-Editor im Abschnitt Signaturen, und legen Sie sie dort ab.
- Falls Sie Chrome, FireFox oder den MS Internet Explorer ab Version 11 nutzen, können Sie die Grafik aus der Zwischenablage direkt in den HTML-Editor im Abschnitt Signaturen kopieren.

Die Tags <body></body> und <html></html> sind in Signaturen nicht zugelassen. Falls sie in Signaturen enthalten sind, werden sie entfernt.

Makros für Signaturen

MDaemon unterstützt in den Signaturen Makros, mit deren Hilfe Kontaktdaten des Absenders automatisch in die Signaturen eingefügt werden können. Diese Daten werden den Kontaktdaten des Absenders entnommen, die im Ordner für öffentliche Kontakte seiner Domäne gespeichert sind. Standard- und Domänen-Signaturen können hierdurch mithilfe der Daten des Absenders automatisch individuell gestaltet werden. Zwei Beispiele hierzu: `$CONTACTFULLNAME$` wird umgesetzt in den vollständigen Namen des Absenders, und `$CONTACTEMAILADDRESS$` wird umgesetzt in die E-Mail-Adresse des Absenders. Die Kontaktdaten für die öffentlichen Kontakte können mithilfe von Webmail, des MDaemon Connectors oder über ActiveSync bearbeitet werden. Falls für einen Absender keine Kontaktdaten bestehen, werden Leerstellen eingesetzt. Die verfügbaren Makros sind unten aufgeführt.

Die Benutzer können steuern, welche MDaemon-Signaturen wie in ihre Nachrichten eingefügt werden. Hierzu fügen sie zwei bestimmte Makros in die Nachrichten ein: Das Makro `$SYSTEMSIGNATURE$` wird ersetzt durch die Standard- oder Domänen-Signatur, und das Makro `$ACCOUNTSIGNATURE$` wird ersetzt durch die Signatur des Benutzerkontos.

Namen und IDs	
Vollständiger Name	**$CONTACTFULLNAME$**
Vorname	**$CONTACTFIRSTNAME$**
Zweiter Vorname	**$CONTACTMIDDLENAME$**
Nachname	**$CONTACTLASTNAME$**
Titel	**$CONTACTTITLE$**
Namenszusatz	**$CONTACTSUFFIX$**
Spitzname	**$CONTACTNICKNAME$**
Vorname (Yomi)	**$CONTACTYOMIFIRSTNAME$**
Nachname (Yomi)	**$CONTACTYOMILASTNAME$**
Name des Benutzerkontos	**$CONTACTACCOUNTNAME$**
Kunden-ID	**$CONTACTCUSTOMERID$**
Verwaltungs-ID	**$CONTACTGOVERNMENTID$**
Speichern unter	**$CONTACTFILEAS$**
E-Mail-Adressen	
E-Mail-Adresse	**$CONTACTEMAILADDRESS$**
E-Mail-Adresse 2	**$CONTACTEMAILADDRESS2$**
E-Mail-Adresse 3	**$CONTACTEMAILADDRESS3$**
Telefon- und Faxnummern	
Mobiltelefon	**$CONTACTHOMEMOBILE$**
Mobiltelefon 2	**$CONTACTMOBILE2$**
Autotelefon	**$CONTACTCARPHONENUMBER$**
Telefon privat	**$CONTACTHOMEPHONE$**
Telefon privat 2	**$CONTACTHOMEPHONE2$**
Telefax privat	**$CONTACTHOMEFAX$**
Anderes Telefon	**$CONTACTOTHERPHONE$**
Instant Messaging und Web	
IM-Adresse	**$CONTACTIMADDRESS$**
IM-Adresse 2	**$CONTACTIMADDRESS2$**
IM-Adresse 3	**$CONTACTIMADDRESS3$**
MMS-Adresse	**$CONTACTMMSADDRESS$**
Web-Adresse privat	**$CONTACTHOMEWEBADDRESS$**

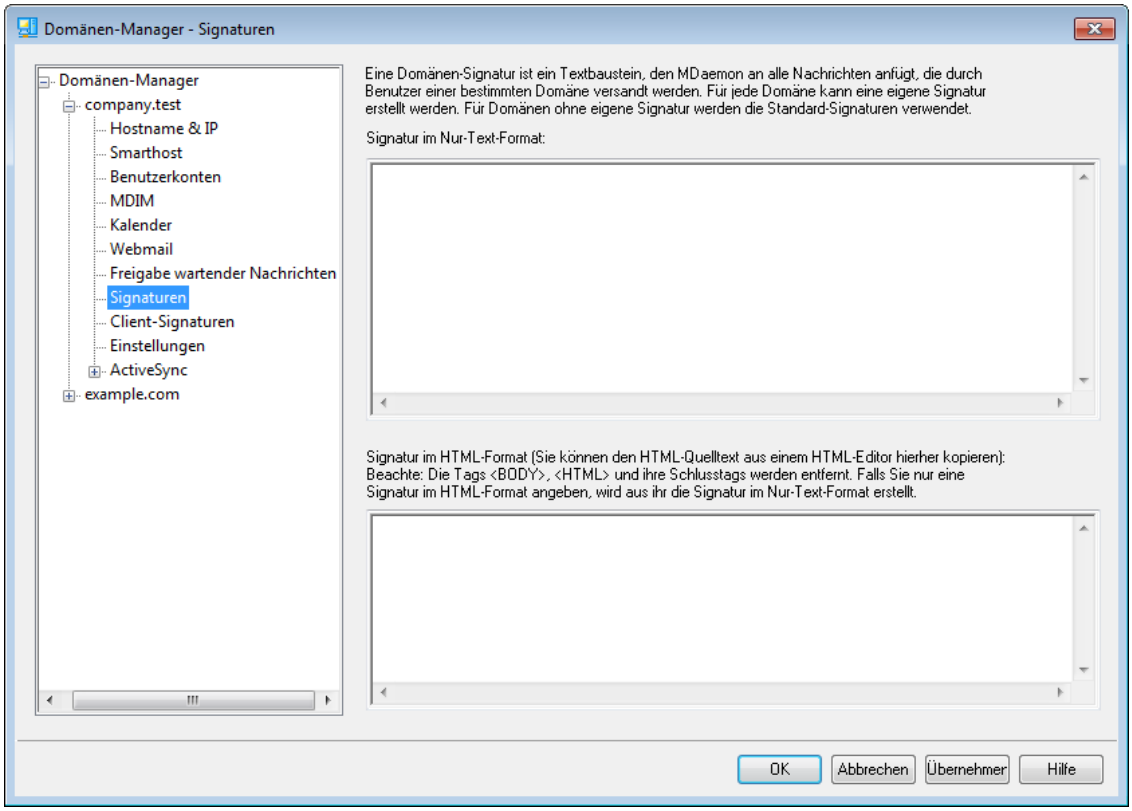
Adresse	
Adresse privat	$CONTACTHOMEADDRESS$
Stadt privat	$CONTACTHOMECITY$
Bundesland/Kanton privat	$CONTACTHOMESTATE$
PLZ privat	$CONTACTHOMEZIPCODE$
Land privat	$CONTACTHOMECOUNTRY$
Andere Adresse	$CONTACTOTHERADDRESS$
Andere Stadt	$CONTACTOTHERCITY$
Anderes Bundesland/ anderer Kanton	$CONTACTOTHERSTATE$
Andere PLZ	$CONTACTOTHERZIPCODE$
Anderes Land	$CONTACTOTHERCOUNTRY$
Geschäftsbezogene Daten	
Firma	$CONTACTBUSINESSCOMPANY$
Firma (Yomi)	$CONTACTYOMICOMPANYNAME$
Titel/Berufsbezeichnung	$CONTACTBUSINESSTITLE$
Büro geschäftlich	$CONTACTBUSINESSOFFICE$
Abteilung geschäftlich	$CONTACTBUSINESSDEPARTMENT$
Manager geschäftlich	$CONTACTBUSINESSMANAGER$
Assistenz geschäftlich	$CONTACTBUSINESSASSISTANT$
Telefon Assistenz geschäftlich	$CONTACTBUSINESSASSISTANTPHONE$
Telefon zentral geschäftlich	$CONTACTBUSINESSMAINPHONE$
Telefon geschäftlich	$CONTACTBUSINESSPHONE$
Telefon geschäftlich 2	$CONTACTBUSINESSPHONE2$
IP-Telefon geschäftlich	$CONTACTBUSINESSIPPHONE$
Fax geschäftlich	$CONTACTBUSINESSFAX$
Pager geschäftlich	$CONTACTBUSINESSPAGER$
Funkdienst geschäftlich	$CONTACTBUSINESSRADIO$
Adresse geschäftlich	$CONTACTBUSINESSADDRESS$
Stadt geschäftlich	$CONTACTBUSINESSCITY$

Bundesland/Kanton geschäftlich	**$CONTACTBUSINESSSTATE$**
PLZ geschäftlich	**$CONTACTBUSINESSZIPCODE$**
Land geschäftlich	**$CONTACTBUSINESSCOUNTRY$**
Web-Adresse geschäftlich	**$CONTACTBUSINESSWEBADDRESS$**
Weitere Daten	
Ehegatte	**$CONTACTSPOUSE$**
Kinder	**$CONTACTCHILDREN$**
Kategorien	**$CONTACTCATEGORIES$**
Kommentar	**$CONTACTCOMMENT$**

Siehe auch:

Standard-Signaturen 135
Benutzerkonten-Editor » Signatur 753

3.2.9 Client-Signaturen



Mithilfe dieses Konfigurationsdialogs können Sie eine Standard-Signatur für Clients definieren, die Sie dann an MDaemon Webmail 345 und an den MDaemon Connector 404 übermitteln können. Die Signatur kann durch Ihre Benutzer beim Verfassen von E-Mail-Nachrichten eingesetzt werden. Sie können die nachfolgend aufgeführten Makros 208 nutzen, um die Signatur benutzerindividuell zu gestalten. Die

Signatur kann Elemente enthalten, die sich für jeden Benutzer unterscheiden, insbesondere Vor- und Nachname, E-Mail-Adresse, Telefonnummer und weiteres. Mithilfe des Konfigurationsdialogs Standard-Client-Signaturen[140] können Sie Signaturen erstellen, die verwendet werden, falls keine eigene Signatur für die Domäne konfiguriert ist. Besteht für eine Domäne eine solche eigene Signatur, so wird sie für diese Domäne statt der Standard-Signatur verwendet. Signaturen werden werden am Ende des Nachrichtentextes eingefügt. Mithilfe der Option *Signatur an Clients übermitteln*[345] können Sie die Client-Signatur an Webmail übermitteln. Mithilfe der Option *Client-Signatur an Microsoft Outlook übermitteln*[404] können Sie die Client-Signatur an den MDaemon Connector übermitteln. In den Webmail-Optionen zum Verfassen von Nachrichten trägt die so übermittelte Client-Signatur die Bezeichnung "System". Für den MDaemon Connector können Sie eine Bezeichnung für die Signatur festlegen, die in Microsoft Outlook erscheint.

Signatur im Nur-Text-Format

In dieses Textfeld können Sie eine Signatur im Nur-Text-Format eintragen. Falls Sie für die Verwendung im Teil "text/html" von Multipart-Nachrichten eine hierzu passende HTML-Signatur festlegen wollen, tragen Sie deren HTML-Quellkode in das Textfeld *Signatur im HTML-Format* weiter unten ein. MDaemon nutzt dann für jeden Teil der Multipart-Nachricht die passende Signatur. Ist keine HTML-Signatur festgelegt, so wird die Signatur im Nur-Text-Format in beide Teile der Nachricht eingefügt.

Signatur im HTML-Format (Sie können den HTML-Quelltext aus einem HTML-Editor hierher kopieren)

In dieses Textfeld können Sie eine Signatur im HTML-Format eintragen. Diese Signatur wird in den Teil "text/html" von Multipart-Nachrichten eingefügt. Falls Sie sowohl in dieses Textfeld wie auch in das Textfeld *Signatur im Nur-Text-Format* weiter oben je eine Signatur eintragen, nutzt MDaemon für jeden Teil der Multipart-Nachricht die passende Signatur. Ist keine HTML-Signatur festgelegt, so wird die Signatur im Nur-Text-Format in beide Teile der Nachricht eingefügt. Ist keine Signatur im Nur-Text-Format festgelegt, so wird die Signatur aus der Signatur im HTML-Format erstellt.

Sie können eine Signatur im HTML-Format erstellen, indem Sie den HTML-Kode unmittelbar in dieses Textfeld eintragen, oder indem Sie den HTML-Kode in einem HTML-Editor erstellen und dann über die Zwischenablage in dieses Textfeld kopieren. Sie können in eine Signatur im HTML-Format auch Grafikdateien unmittelbar (inline) einbetten; hierzu steht das Makro `$ATTACH_INLINE:Pfad_zur_Grafikdatei$` zur Verfügung.

Ein Anwendungsbeispiel stellt der nachfolgend dargestellte HTML-Kode dar:

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \grafiken\mr_t_and_arnold.jpg$">
```

Sie können Grafiken auch mithilfe der MDaemon-Remoteverwaltung[350] in die Signaturen einfügen. Hierzu stehen Ihnen folgende Vorgehensweisen zur Verfügung:

- Klicken Sie in der Remoteverwaltung im Abschnitt Standard-Signaturen auf das Steuerelement "Grafik" in der Symbolleiste des HTML-Editors, und wählen Sie dann die Registerkarte Upload aus.
- Klicken Sie in der Remoteverwaltung im Abschnitt Standard-Signaturen auf das Steuerelement "Grafik hinzufügen" in der Symbolleiste des HTML-Editors.

- Falls Sie Chrome, FireFox, Safari oder den MS Internet Explorer ab Version 10 nutzen, ziehen Sie eine Grafikdatei in den HTML-Editor im Abschnitt Standard-Signaturen, und legen Sie sie dort ab.
- Falls Sie Chrome, FireFox oder den MS Internet Explorer ab Version 11 nutzen, können Sie die Grafik aus der Zwischenablage direkt in den HTML-Editor im Abschnitt Standard-Signaturen kopieren.

Vorgehensweise zum Einfügen von Grafiken

Sie können Grafiken in Signaturen einfügen. Hierzu stehen die folgenden Vorgehensweisen zur Verfügung:

- Klicken Sie in der Symbolleiste des HTML-Editors auf das Symbol "Grafik", und geben Sie den URL der gewünschten Grafikdatei ein. Sie können auch mithilfe des Steuerelements "Hochladen" eine Grafikdatei hochladen.
- Klicken Sie in der Symbolleiste des HTML-Editors auf das Symbol "Grafik hinzufügen", um eine Grafikdatei hochzuladen.
- Ziehen Sie eine Grafikdatei in das Eingabefeld für den Signaturtext, und legen Sie sie dort ab. Diese Vorgehensweise funktioniert bei Nutzung von Google Chrome, Mozilla FireFox, Apple Safari und dem Microsoft Internet Explorer ab Version 10.
- Kopieren Sie eine Grafikdatei aus der Zwischenablage in das Eingabefeld für den Signaturtext. Diese Vorgehensweise funktioniert bei Nutzung von Google Chrome, Mozilla FireFox und dem Microsoft Internet Explorer ab Version 11.

Die Tags <body></body> und <html></html> sind in Signaturen nicht zugelassen. Falls sie in Signaturen enthalten sind, werden sie entfernt.

Makros für Signaturen

MDaemon unterstützt in den Signaturen Makros, mit deren Hilfe Kontaktdaten des Absenders automatisch in die Signaturen eingefügt werden können. Diese Daten werden den Kontaktdaten des Absenders entnommen, die im Ordner für öffentliche Kontakte seiner Domäne gespeichert sind. Standard- und Domänen-Signaturen können hierdurch mithilfe der Daten des Absenders automatisch individuell gestaltet werden. Zwei Beispiele hierzu: `$CONTACTFULLNAME$` wird umgesetzt in den vollständigen Namen des Absenders, und `$CONTACTEMAILADDRESS$` wird umgesetzt in die E-Mail-Adresse des Absenders. Die Kontaktdaten für die öffentlichen Kontakte können mithilfe von Webmail, des MDaemon Connectors oder über ActiveSync bearbeitet werden. Falls für einen Absender keine Kontaktdaten bestehen, werden Leerstellen eingesetzt. Die verfügbaren Makros sind unten aufgeführt.

Die Benutzer können steuern, welche MDaemon-Signaturen wie in ihre Nachrichten eingefügt werden. Hierzu fügen sie zwei bestimmte Makros in die Nachrichten ein: Das Makro `$SYSTEMSIGNATURE$` wird ersetzt durch die Standard- oder Domänen-Signatur, und das Makro `$ACCOUNTSIGNATURE$` wird ersetzt durch die Signatur des Benutzerkontos.

Namen und IDs

Vollständiger Name	**$CONTACTFULLNAME$**
Vorname	**$CONTACTFIRSTNAME$**
Zweiter Vorname	**$CONTACTMIDDLENAME$**
Nachname	**$CONTACTLASTNAME$**
Titel	**$CONTACTTITLE$**
Namenszusatz	**$CONTACTSUFFIX$**
Spitzname	**$CONTACTNICKNAME$**
Vorname (Yomi)	**$CONTACTYOMIFIRSTNAME$**
Nachname (Yomi)	**$CONTACTYOMILASTNAME$**
Name des Benutzerkontos	**$CONTACTACCOUNTNAME$**
Kunden-ID	**$CONTACTCUSTOMERID$**
Verwaltungs-ID	**$CONTACTGOVERNMENTID$**
Speichern unter	**$CONTACTFILEAS$**
E-Mail-Adressen	
E-Mail-Adresse	**$CONTACTEMAILADDRESS$**
E-Mail-Adresse 2	**$CONTACTEMAILADDRESS2$**
E-Mail-Adresse 3	**$CONTACTEMAILADDRESS3$**
Telefon- und Faxnummern	
Mobiltelefon	**$CONTACTHOMEMOBILE$**
Mobiltelefon 2	**$CONTACTMOBILE2$**
Autotelefon	**$CONTACTCARPHONENUMBER$**
Telefon privat	**$CONTACTHOMEPHONE$**
Telefon privat 2	**$CONTACTHOMEPHONE2$**
Telefax privat	**$CONTACTHOMEFAX$**
Anderes Telefon	**$CONTACTOTHERPHONE$**
Instant Messaging und Web	
IM-Adresse	**$CONTACTIMADDRESS$**
IM-Adresse 2	**$CONTACTIMADDRESS2$**
IM-Adresse 3	**$CONTACTIMADDRESS3$**
MMS-Adresse	**$CONTACTMMSADDRESS$**
Web-Adresse privat	**$CONTACTHOMEWEBADDRESS$**
Adresse	

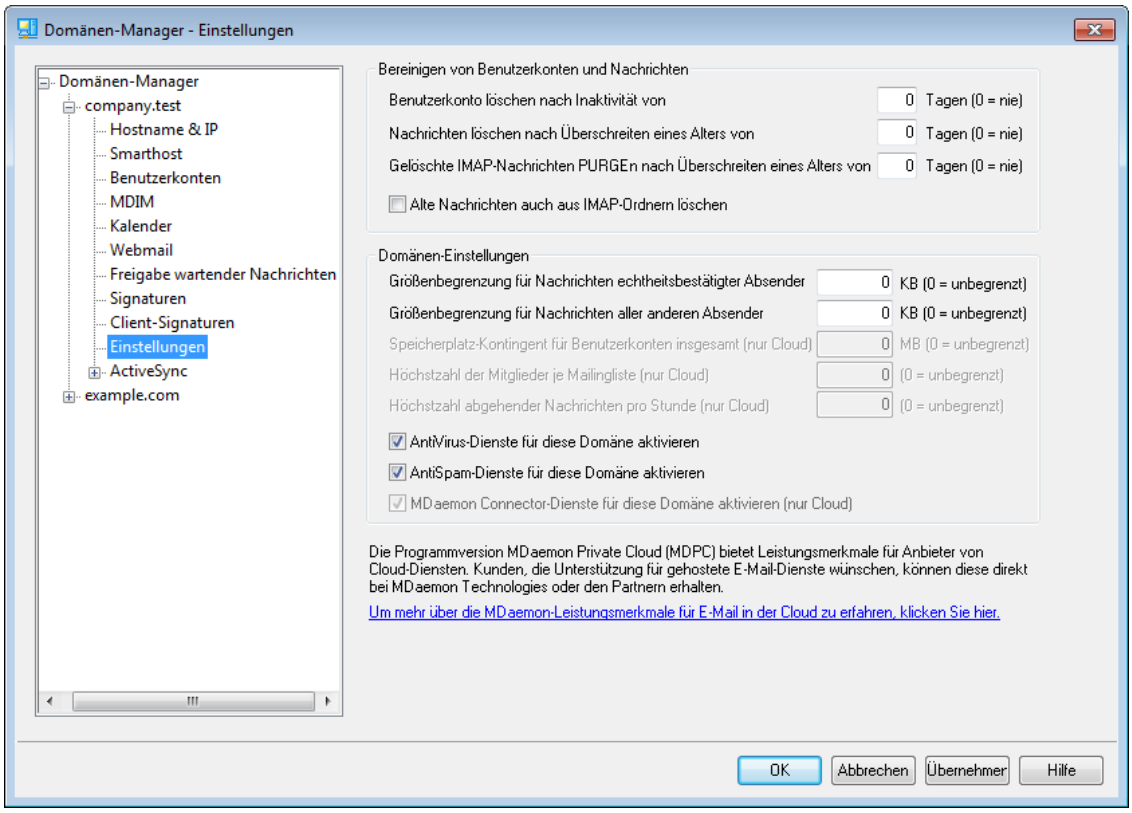
Adresse privat	**$CONTACTHOMEADDRESS$**
Stadt privat	**$CONTACTHOMECITY$**
Bundesland/Kanton privat	**$CONTACTHOMESTATE$**
PLZ privat	**$CONTACTHOMEZIPCODE$**
Land privat	**$CONTACTHOMECOUNTRY$**
Andere Adresse	**$CONTACTOTHERADDRESS$**
Andere Stadt	**$CONTACTOTHERCITY$**
Anderes Bundesland/ anderer Kanton	**$CONTACTOTHERSTATE$**
Andere PLZ	**$CONTACTOTHERZIPCODE$**
Anderes Land	**$CONTACTOTHERCOUNTRY$**
Geschäftsbezogene Daten	
Firma	**$CONTACTBUSINESSCOMPANY$**
Firma (Yomi)	**$CONTACTYOMICOMPANYNAME$**
Titel/Berufsbezeichnung	**$CONTACTBUSINESSTITLE$**
Büro geschäftlich	**$CONTACTBUSINESSOFFICE$**
Abteilung geschäftlich	**$CONTACTBUSINESSDEPARTMENT$**
Manager geschäftlich	**$CONTACTBUSINESSMANAGER$**
Assistenz geschäftlich	**$CONTACTBUSINESSASSISTANT$**
Telefon Assistenz geschäftlich	**$CONTACTBUSINESSASSISTANTPHONE$**
Telefon zentral geschäftlich	**$CONTACTBUSINESSMAINPHONE$**
Telefon geschäftlich	**$CONTACTBUSINESSPHONE$**
Telefon geschäftlich 2	**$CONTACTBUSINESSPHONE2$**
IP-Telefon geschäftlich	**$CONTACTBUSINESSIPPHONE$**
Fax geschäftlich	**$CONTACTBUSINESSFAX$**
Pager geschäftlich	**$CONTACTBUSINESSPAGER$**
Funkdienst geschäftlich	**$CONTACTBUSINESSRADIO$**
Adresse geschäftlich	**$CONTACTBUSINESSADDRESS$**
Stadt geschäftlich	**$CONTACTBUSINESSCITY$**
Bundesland/Kanton geschäftlich	**$CONTACTBUSINESSSTATE$**

PLZ geschäftlich	**$CONTACTBUSINESSZIPCODE$**
Land geschäftlich	**$CONTACTBUSINESSCOUNTRY$**
Web-Adresse geschäftlich	**$CONTACTBUSINESSWEBADDRESS$**
Weitere Daten	
Ehegatte	**$CONTACTSPOUSE$**
Kinder	**$CONTACTCHILDREN$**
Kategorien	**$CONTACTCATEGORIES$**
Kommentar	**$CONTACTCOMMENT$**

Siehe auch:

Standard-Client-Signaturen 140
Standard-Signaturen 135
Domänen-Manager » Signaturen 202
Benutzerkonten-Editor » Signatur 753
Domänen-Manager » Webmail-Einstellungen 194
MC-Client-Einstellungen » Signatur 404

3.2.10 Einstellungen



Bereinigen von Benutzerkonten und Nachrichten

Die folgenden Optionen dienen dazu, festzulegen, ob und wann MDaemon inaktive Benutzerkonten oder alte Nachrichten löscht. Jeden Tag um Mitternacht löscht MDaemon alle Nachrichten und Benutzerkonten, welche die hier gesetzten Alters- und Zeitgrenzen überschritten haben. Ähnliche Einstellungen stehen im Abschnitt Kontingente 731 des Benutzerkonten-Editors zur Verfügung; diese Einstellungen gehen für die einzelnen Benutzerkonten den hier getroffenen Einstellungen vor.

Die Datei `AccountPrune.txt` im Verzeichnis "…`MDaemon\App\`" enthält weitere Informationen und Befehlszeilenparameter.

Benutzerkonto löschen nach Inaktivität von [xx] Tagen (0 = nie)
Diese Option bestimmt, wie lange ein Benutzerkonto in dieser Domäne inaktiv sein darf, bevor es gelöscht wird. Der Wert 0 bewirkt, dass Benutzerkonten nicht wegen Inaktivität gelöscht werden.

Nachrichten löschen nach Überschreiten eines Alters von [xx] Tagen (0 = nie)
Diese Option bestimmt, wie viele Tage lang eine Nachricht im Postfach eines Benutzers liegen darf, bevor sie gelöscht wird. Der Wert 0 bewirkt, dass die Nachrichten nicht wegen ihres Alters gelöscht werden. **Beachte:** Diese Option wirkt auf die Nachrichten in IMAP-Ordnern nur dann, wenn Sie auch die Option "*Alte Nachrichten auch aus IMAP-Ordnern löschen*" weiter unten aktivieren.

Gelöschte IMAP-Nachrichten PURGEn nach Überschreiten eines Alters von [xx] Tagen (0 = nie)
Diese Option bestimmt, wie lange IMAP-Nachrichten noch in den Benutzerverzeichnissen verbleiben dürfen, nachdem sie zur Löschung vorgemerkt wurden. Nachrichten, bei denen die hier angegebene Grenze überschritten ist, werden aus den Postfächern gelöscht. Der Wert 0 bedeutet, dass zur Löschung vorgemerkte Nachrichten nicht wegen ihres Alters gelöscht werden.

Alte Nachrichten auch aus IMAP-Ordnern löschen
Diese Option bewirkt, dass die Option "*Nachrichten löschen nach Überschreiten eines Alters von [xx] Tagen*" weiter oben auch auf Nachrichten in IMAP-Ordnern wirkt. Ist diese Option abgeschaltet, dann werden normale Nachrichten in IMAP-Ordnern nicht wegen Überschreitens eines Höchstalters gelöscht.

Domänen-Optionen

Größenbegrenzung für Nachrichten echtheitsbestätigter Absender [xx] KB (0=unbegrenzt)
Mithilfe dieser Option können Sie die Größe solcher Nachrichten begrenzen, die echtheitsbestätigte Absender an Empfänger in dieser Domäne senden dürfen. Der Wert wird in KB angegeben. Er beträgt per Voreinstellung 0, wodurch keine Größenbegrenzung wirksam wird. Falls Sie eine Begrenzung für nicht echtheitsbestätigte Absender setzen möchten, können Sie die folgende Option *"...aller anderen Absender"* hierfür nutzen.

Größenbegrenzung für Nachrichten aller anderen Absender [xx] KB (0=unbegrenzt)
Mithilfe dieser Option können Sie die Größe solcher Nachrichten begrenzen, die nicht echtheitsbestätigte Absender an Empfänger in dieser Domäne senden dürfen. Der Wert wird in KB angegeben. Er beträgt per Voreinstellung 0, wodurch

keine Größenbegrenzung wirksam wird. Falls Sie eine Begrenzung für echtheitsbestätigte Absender setzen möchten, können Sie die Option *"...aller anderen Absender"* weiter oben hierfür nutzen.

Speicherplatz-Kontingent für Benutzerkonten insgesamt (nur Cloud) [x] MB (0=unbegrenzt)
Mithilfe dieser Option können Sie den Speicherplatz begrenzen, den die Domäne belegen darf. Diese Option steht nur in MDaemon Private Cloud zur Verfügung.

Höchstzahl der Mitglieder je Mailingliste (nur Cloud) [x] (0=unbegrenzt)
Mithilfe dieser Option können Sie die Höchstzahl zulässiger Mitglieder je Mailingliste für diese Domäne begrenzen. Diese Option steht nur in MDaemon Private Cloud zur Verfügung. Es steht auch eine entsprechende, systemweit wirksame Option im Abschnitt Einstellungen 272 des Mailinglisten-Managers zur Verfügung.

Höchstzahl abgehender Nachrichten pro Stunde (nur Cloud) [x] (0=unbegrenzt)
Diese Option begrenzt die Höchstzahl abgehender Nachrichten, die eine Domäne pro Stunde versenden darf. Sobald diese Höchstzahl erreicht ist, verbleiben weitere abgehende Nachrichten in der Warteschlange. Sie werden erst wieder zugestellt, wenn die Höchstzahl zurückgesetzt ist. Die Höchstzahl wird zu Beginn jeder Stunde und bei jedem Neustart des Servers zurückgesetzt. Diese Option steht nur in MDaemon Private Cloud zur Verfügung.

AntiVirus-Dienste für diese Domäne aktivieren
Aktivieren Sie diese Option, um die AntiVirus 648-Einstellungen für diese Domäne zu übernehmen.

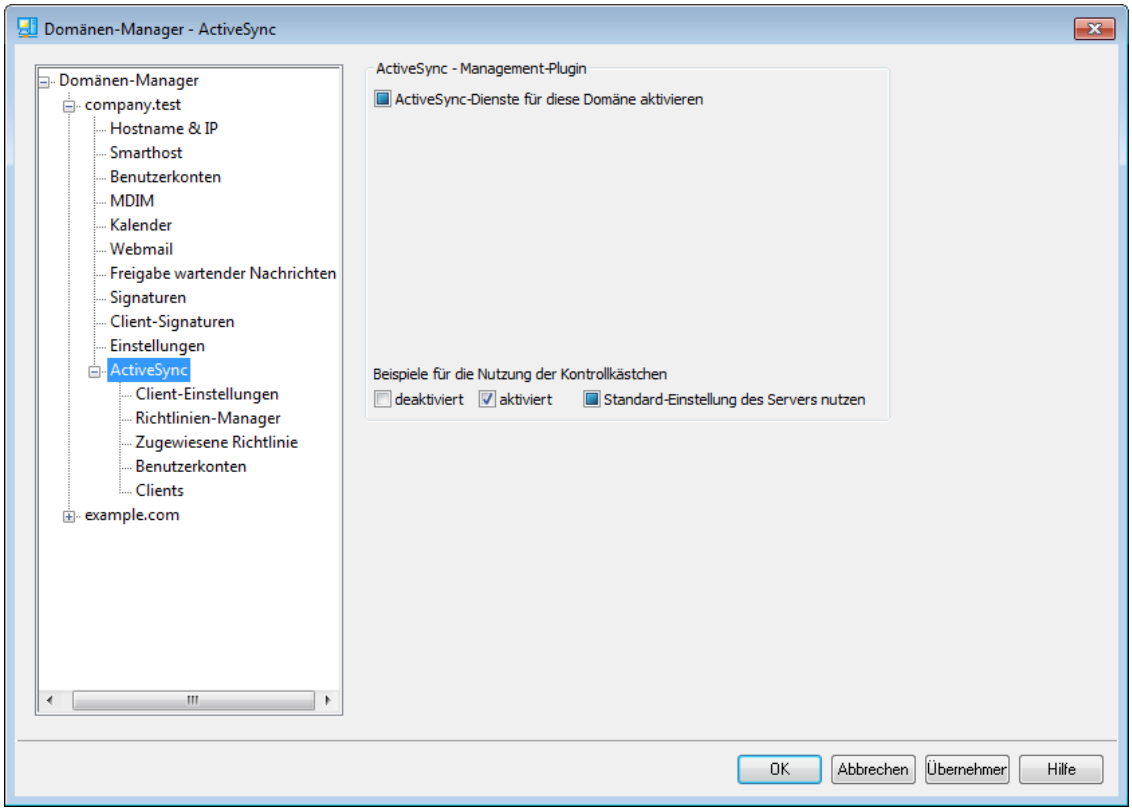
AntiSpam-Dienste für diese Domäne aktivieren
Diese Option bewirkt, dass die Einstellungen des Spam-Filters von MDaemon auch auf die gerade bearbeitete Domäne angewendet werden.

MDaemon-Connector-Dienste für diese Domäne aktivieren (nur Cloud)
Diese Option aktiviert die Dienste des MDaemon Connectors 385 für diese Domäne.

Siehe auch:

Benutzerkonten-Editor » Kontingente 731

3.2.11 ActiveSync



In diesem Abschnitt des Domänen-Managers verwalten Sie die Einstellungen für ActiveSync 416 für die gerade bearbeitete Domäne. Sie können die ActiveSync-Einstellungen und -Voreinstellungen für alle Domänen Abschnitt Domänen 437 des ActiveSync-Managers bearbeiten.

ActiveSync für MDaemon - Management-Plugin

ActiveSync-Dienste für diese Domäne aktivieren
Diese Option bestimmt, ob die Benutzer der gerade bearbeiteten Domäne per Voreinstellung auf Ihre E-Mail- und PIM-Daten mithilfe von ActiveSync-Clients zugreifen können. Per Voreinstellung erbt diese Option den Wert aus der Standard-Einstellung für ActiveSync 437. Sie können diese geerbte Einstellung ändern, indem Sie das Kontrollkästchen hier aktivieren und deaktivieren. Sie können die hier getroffene Einstellung auch für einzelne Benutzerkonten 454 und Clients 464 ändern, auf die Sie die hier getroffene Einstellung nicht anwenden wollen. **Beachte:** Falls Sie ActiveSync für die gerade bearbeitete Domäne deaktivieren, erscheint eine Sicherheitsabfrage, ob Sie allen Benutzern dieser Domäne die Berechtigung zur Nutzung von ActiveSync entziehen wollen. Um allen Benutzern, die die Berechtigung zur Nutzung von ActiveSync bereits haben, diese Berechtigung zu belassen, klicken Sie auf **Nein**. Um allen Benutzern, die die Berechtigung zur Nutzung von ActiveSync bereits haben, diese Berechtigung zu entziehen, klicken Sie auf **Ja**.

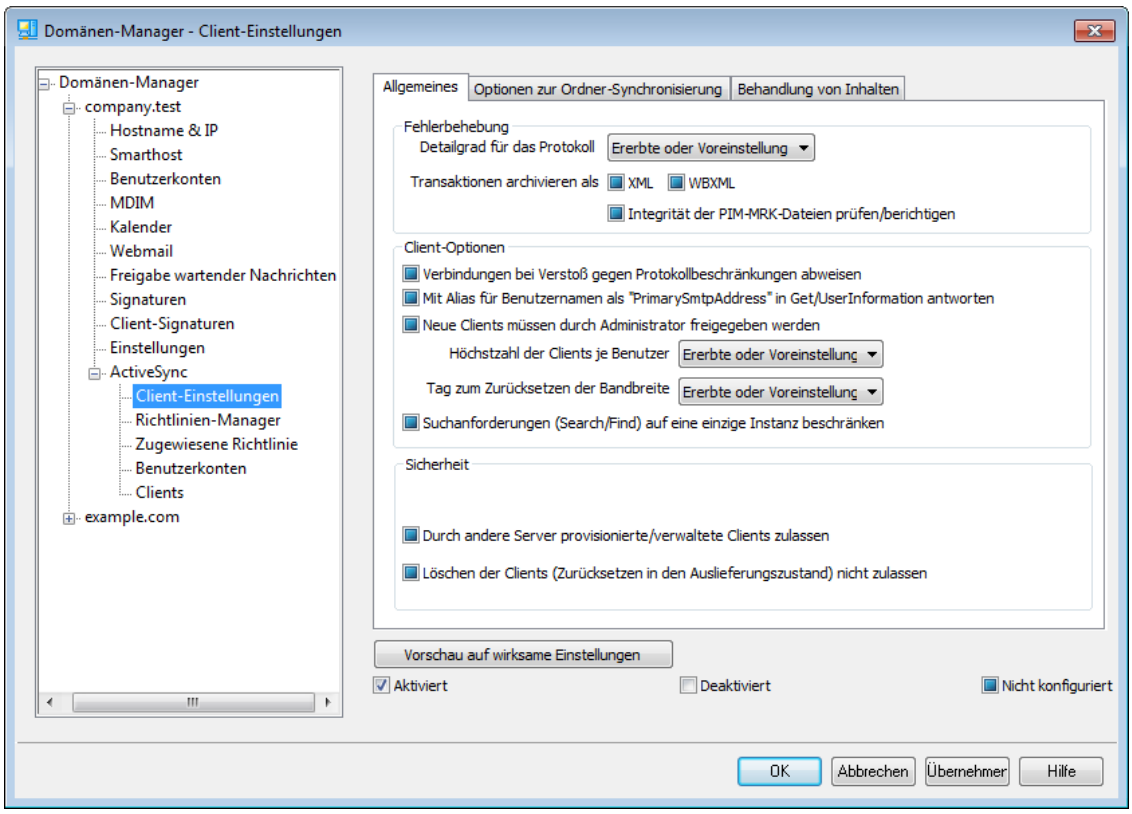
Diese Einstellung bestimmt nur, ob die Benutzerkonten der Domäne per Voreinstellung ActiveSync nutzen dürfen, wenn der ActiveSync-Server ausgeführt wird. Die globale Option **ActiveSync-Dienst für MDaemon aktivieren** 416 muss jedenfalls aktiv sein, damit den Benutzerkonten oder

Domänen der Zugriff über ActiveSync grundsätzlich ermöglicht werden kann.

Siehe auch:

ActiveSync » Domänen 437
ActiveSync » Benutzerkonten 454
ActiveSync » Clients 464

3.2.11.1 Client-Einstellungen



In diesem Konfigurationsdialog legen Sie die Voreinstellungen für Benutzerkonten und Clients fest, die Mitglieder der gerade bearbeiteten Domäne sind. Per Voreinstellung werden hier die geerbten oder die Voreinstellungen genutzt. Der übergeordnete Knoten, von dem die Einstellungen geerbt werden, ist dabei der Konfigurationsdialog für die globalen Client-Einstellungen 422. Entsprechend verhalten sich auch die Benutzerkonten 456 der gerade bearbeiteten Domäne. Sie erben ihre Einstellungen von dem vorliegenden Konfigurationsdialog, der für sie der übergeordnete Knoten ist. Änderungen in diesem Konfigurationsdialog werden auch in die Konfigurationsdialoge der Benutzerkonten übernommen. Unter der Ebene der Benutzerkonten folgt die Ebene der einzelnen Clients 241. Auch für sie stehen eigene Konfigurationsdialoge zur Verfügung, die ihre Einstellungen von den Einstellungen der Benutzerkonten erben. Diese mehrstufige Konfigurationsstruktur ermöglicht das Ändern von Einstellungen für alle Benutzerkonten und Clients einer Domäne über den vorliegenden Konfigurationsdialog und die abweichende Festlegung einzelner Einstellungen auch für einzelne Benutzerkonten und Clients, je nach Bedarf.

Allgemeines

Fehlerbehebung

Detailgrad für das Protokoll
ActiveSync für MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Einstellung erben Per Voreinstellung wird die Einstellung für den Detailgrad aus der Hierarchie der Client-Einstellungen vom jeweils übergeordneten Knoten ererbt. Clients übernehmen dabei die Einstellung aus dem jeweiligen Client-Typ, Client-Typen übernehmen die Einstellung von den Benutzerkonten, Benutzerkonten übernehmen die Einstellung von den Gruppen, und so weiter. Die globale Einstellung für alle Clients wird durch die Einstellung für den Detailgrad im Konfigurationsdialog Diagnose 432 bestimmt.

Transaktionen archivieren als [XML | WBXML]
Mithilfe der Optionen *XML...* und *WBXML...* können Sie die zugehörigen Daten speichern; diese Daten können die Fehlersuche erleichtern. Die systemweit wirksamen Optionen sind per Voreinstellung abgeschaltet.

Integrität der PIM-MRK-Dateien prüfen/berichtigen
Diese Option führt für die PIM-Daten der betroffenen Clients Prüf- und Korrekturvorgänge durch. Sie sollen bekannte Probleme erkennen, die eine ordnungsgemäße Synchronisierung verhindern können. Zu diesen Problemen zählen insbesondere doppelte iCal-UIDs und leere Datenfelder, die eigentlich verpflichtend Daten enthalten müssen. Die systemweit wirksame Option ist per Voreinstellung abgeschaltet.

Client-Optionen

Verbindungen bei Verstoß gegen Protokollbeschränkungen abweisen
Diese Option bewirkt, dass Verbindungen von Clients abgewiesen werden, falls sie versuchen eine nicht für die Clients *Zugelassene Protokollversion* zu verwenden. Per Voreinstellung ist diese Option abgeschaltet; dies bedeutet, dass die Protokollbeschränkung keine Verbindungen solcher Clients verhindern, die andere als die zugelassenen Protokollversionen verwenden. Solange die Option abgeschaltet ist, weist MDaemon die Clients zwar an, nur die zugelassenen Protokollversionen zu verwenden, lässt aber bei Nutzung anderer Protokollversionen die Verbindung trotzdem zu. Nähere Informationen finden Sie unter Protokollbeschränkungen 434.

Mit Alias für Benutzernamen als "PrimarySmtpAddress" in Get/UserInformation antworten
Diese Option gestattet es dem Dienst, als Antwort auf eine Anforderung Settings/Get/UserInformation eine etwa vorhandene Alias-Adresse oder eine sekundäre Adresse des betroffenen Benutzerkontos als primäre Adresse zu übermitteln. Hierdurch wird ein Problem umgangen, das mit einer iOS-Aktualisierung nach Version 9.x verursacht wird, und das verhinderte, dass Clients unter einer etwa vorhandenen Alias-Adresse Nachrichten versenden konnten. Die Nutzung dieser Option bewirkt eine nicht standardkonforme Antwort auf die Anforderung Settings/GetUserInformation.

Neue Clients müssen durch Administrator freigegeben werden
Diese Option bewirkt, dass neue Clients sich erst dann mit Benutzerkonten synchronisieren können, wenn sie zunächst durch einen Administrator freigegeben wurden. In der Liste der Clients 464 sind alle Clients aufgeführt, die noch die Freigabe erwarten, und die Administratoren können sie über diese Liste freigeben. Diese Option ist per Voreinstellung abgeschaltet.

Höchstzahl der Clients je Benutzer
Mithilfe dieser Option können Sie die Anzahl der ActiveSync-Clients und -Endgeräte begrenzen, die mit jedem MDaemon-Benutzerkonto verknüpft sein können. Der hier angegebene Wert ist die Höchstzahl zulässiger Clients. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt. Diese Option steht nur in den Client-Einstellungen auf globaler, Domänen- und Benutzerebene zur Verfügung, nicht jedoch in den Client-Einstellungen für die einzelnen Clients.

Tag zum Zurücksetzen der Bandbreite
Mithilfe dieser Option können Sie Tag bestimmen, an dem in jedem Monat die Bandbreiten-Nutzungsstatistik für die ActiveSync-Endgeräte zurückgesetzt wird. Dieser Vorgang wird während der normalen Bereinigungsvorgänge um Mitternacht aufgeführt und, wie auch andere Bereinigungsvorgänge, in das Protokoll System eingetragen. Der globale Wert lautet per Voreinstellung 0 (nicht zurücksetzen), sodass per Voreinstellung die Nutzungsstatistik nicht zurückgesetzt wird. Für untergeordnete Knoten können Sie abweichende Einstellungen treffen, etwa, um die Einstellung an den Tag anzugleichen, an dem für das betroffene Endgeräte ein neuer Abrechnungszeitraum des Netzbetreibers beginnt.

Sicherheit

Vom Länder-Filter ausnehmen
Wenn Sie diese Option in den Einstellungen eines ActiveSync-Clients aktivieren,

kann das Endgerät den Länder-Filter[574] umgehen. Hierdurch kann ein berechtigter Benutzer auf sein Benutzerkonto über ActiveSync beispielsweise auch dann zugreifen, wenn er sich in einem Land befindet, für das Versuche zur Echtheitsbestätigung ansonsten durch den Länder-Filter unterbunden werden. Ein Endgerät kann nur dann vom Länder-Filter ausgenommen sein, wenn es innerhalb des durch die Option Inaktive Clients entfernen nach [x] Tagen[418] im Abschnitt Anpassung bestimmten Zeitraums eine echtheitsbestätigte Verbindung über ActiveSync erfolgreich hergestellt hat.

Adresse der Gegenstelle in Dynamische Freigabeliste aufnehmen
Wenn Sie ein Endgerät vom Länder-Filter ausnehmen, können Sie durch Aktivieren dieser Option die IP-Adresse, von der aus das Endgerät die Verbindung herstellt, in die Freigabeliste eintragen lassen. Hierdurch können beispielsweise andere Clients, die von der selben IP-Adresse aus eine Verbindung herstellen, ebenfalls zugelassen werden.

Durch andere Server provisionierte/verwaltete Clients zulassen
Per Voreinstellung dürfen Clients auch dann Verbindungen zu MDaemon aufbauen, wenn sie auf die Übermittlung der Provisionierungs- und Richtliniendaten durch den ActiveSync-Server hin melden, dass sie auch durch einen oder mehrere andere ActiveSync-Server verwaltet werden. Bei einer solchen Mehrfachverwaltung kann es nicht sichergestellt werden, dass alle auf Ihrem System bestehenden Richtlinien durch den Client auch umgesetzt werden; dies gilt insbesondere dann, wenn sie Richtlinien des anderen ActiveSync-Servers widersprechen. In vielen Fällen setzen die Clients die am stärksten einschränkende Richtlinie um, falls mehrere einander widersprechende Richtlinien vorhanden sind. Um Verbindungen von Clients zu unterbinden, die durch andere ActiveSync-Server verwaltet werden, deaktivieren Sie diese Option.

Löschen der Clients (Zurücksetzen in den Auslieferungszustand) nicht zulassen
Wenn diese Option aktiv ist, dann können ActiveSync-Clients nicht in den **Auslieferungszustand zurückgesetzt** und damit vollständig gelöscht werden. Wenn Sie Clients ferngesteuert in den Auslieferungszustand zurücksetzen wollen, müssen Sie diese Option deaktivieren. Diese Option ist per Voreinstellung deaktiviert. Nähere Informationen finden Sie auf der Seite Clients im Abschnitt **Vollständiges Löschen eines ActiveSync-Clients**[464].

Optionen zur Ordner-Synchronisierung

Optionen zur Ordner-Synchronisierung

Folgende Ordner ausnehmen

Freigegebene Absender/Gesperrte Absender
Per Voreinstellung werden die Kontaktordner mit Freigabelisten und Sperrlisten der Benutzer nicht mit den Geräten synchronisiert. Diese Ordner dienen üblicherweise nur in MDaemon zum Erkennen und Filtern von Spam. Ihre Inhalte brauchen daher nicht auf den Geräten als Kontakte angezeigt zu werden.

Benutzerdefinierte Nachrichten-Ordner
Per Voreinstellung können alle Standard- und benutzerdefinierten Nachrichten-Ordner mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-Nachrichtenordner synchronisiert werden

können. Die Standard-Nachrichtenordner sind insbesondere Posteingang, Gesendete Objekte, Gelöschte Objekte und Entwürfe. Ordner, die die Benutzer selbst anlegen, werden dann nicht mehr synchronisiert. Diese Option ist per Voreinstellung abgeschaltet.

Benutzerdefinierte PIM-Ordner
Per Voreinstellung können alle PIM-Ordner (insbesondere Kontakte, Kalender, Notizen und Aufgaben) mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-PIM-Ordner synchronisiert werden können. Ist diese Option aktiv, so wird beispielsweise für jeden Benutzer nur der Standard-Kalender synchronisiert, auch wenn er über mehrere Kalender-Ordner verfügt. Diese Option ist per Voreinstellung abgeschaltet.

Folgende Ordner einschließen

Hierarchie der öffentlichen Ordner
Diese Option bewirkt, dass die öffentlichen Ordner 309, auf die die Benutzer Zugriff haben, in den Ordnerlisten der Benutzer auf ihren ActiveSync-Geräten erscheinen. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der öffentlichen Ordner 309, auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Traversieren öffentlicher Ordner zulassen (legt Ordnernamen offen)
Benutzerkonten, die auf Unterordner in öffentlichen Ordnern zugreifen oder diese synchronisieren wollen, müssen per Voreinstellung sowohl für den betroffenen Unterordner als auch für alle ihm übergeordneten öffentlichen Ordner 309 über die Berechtigung Ordner anzeigen 311 verfügen. Fehlt einem Benutzerkonto diese Berechtigung für einen übergeordneten öffentlichen Ordner, so kann er auch den gewünschten Unterordner nicht synchronisieren und nicht auf ihn zugreifen, und zwar auch dann nicht, wenn das Benutzerkonto für diesen Unterordner selbst die erforderliche Berechtigung hat. Mithilfe dieser Option können Sie den Clients Zugriff auf und Synchronisierung von Unterordnern ermöglichen, ohne dass die Clients Berechtigungen für die übergeordneten öffentlichen Ordner haben. **Beachte:** Ist diese Option aktiv, so erlangt der Client zwangsläufig Kenntnis von den Namen der übergeordneten Ordner, auch wenn er für ihre Inhalte keine Zugriffsrechte hat. Hieraus kann sich ein Sicherheitsrisiko ergeben. Die Option ist per Voreinstellung abgeschaltet.

Höchstzahl zulässiger öffentlicher Ordner
Diese Option begrenzt die Zahl der öffentlichen Ordner, die auf den betroffenen Geräten dargestellt werden können. Ist eine solche Höchstzahl angegeben, dann übermittelt der Server so lange Einträge in der Ordnerliste, bis die Höchstzahl erreicht ist. Danach übermittelt der Server keine Ordner mehr an die Geräte. Die Reihenfolge, in der die Ordner dabei verarbeitet werden, kann weder festgelegt noch vorher bestimmt werden. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt.

Freigegebene Ordner
Diese Option nimmt auch die gemeinsam genutzten Ordner 122, auf die die Benutzer Zugriff haben, in die Ordnerlisten auf ihren ActiveSync-Geräten auf. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der freigegebenen Ordner[742], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Behandlung von Inhalten

Optionen zur Behandlung von Inhalten

Aufgaben/Erinnerungen für durch Clients gekennzeichnete Nachrichtenelemente erstellen
Diese Option ermöglicht es MDaemon, die Benutzer an gekennzeichnete Elemente zu erinnern. Hierzu wird für jede gekennzeichnete E-Mail-Nachricht eine Aufgabe erstellt, wenn der Client dies anfordert. Die globale Option für dieses Leistungsmerkmal ist per Voreinstellung aktiv.

Aktualisierung nach jeder Änderung der Besprechung senden
Manche Clients versenden aktualisierte Besprechungseinladungen nicht richtig, nachdem eine Besprechung geändert wurde. Diese Option bewirkt, dass der ActiveSync-Dienst immer dann aktualisierte Besprechungseinladungen sendet, wenn der Besprechungsorganisator eine Besprechung aktualisiert hat. Diese Option sollte nur für Clients[464] und Client-Typen[481] aktiviert werden, die die aktualisierten Besprechungseinladungen nicht richtig versenden, da sonst aktualisierte Besprechungseinladungen doppelt versandt werden. Aus diesem Grund ist diese Einstellung nur auf den Seiten Clients und Client-Typen verfügbar.

Lesebestätigung für alle versandten Nachrichten anfordern
Diese Option bewirkt, dass der Server für alle durch einen Client versandten E-Mail-Nachrichten Lesebestätigungen anfordert. Diese Option ist per Voreinstellung abgeschaltet.

Vom Absender angeforderte Lesebestätigung senden, sobald Nachricht als gelesen gekennzeichnet ist
Diese Option bewirkt, dass der Server Anforderungen von Lesebestätigungen beachtet und die Lesebestätigungen dann versendet, wenn eine Nachricht durch den Client als gelesen gekennzeichnet wird. Diese Option ist per Voreinstellung abgeschaltet.

Unter dem in der Antwortadresse (ReplyTo) angegebenen Alias senden
Manche Clients gestatten den Absendern nicht den Versand von E-Mail-Nachrichten unter einem Alias. Dieses Leistungsmerkmal wurde im der Version 16.x des Protokolls Exchange ActiveSync (EAS)[434] erstmals unterstützt, aber manche Clients unterstützen die Version 16.x nicht. So nutzt beispielsweise Microsoft Outlook für Windows nur EAS 14.0 und gestattet zwar den Benutzern die Angabe einer anderen Adresse, unter der eine Nachricht versandt werden soll, aber die dann erstellte Nachricht gibt die Auswahl des Benutzers nicht richtig wieder. Diese Option gestattet die Nutzung des Feldes für die Antwortadresse (ReplyTo) zum Versand von Nachrichten dann, wenn als Antwortadresse ein gültiger Alias[827] des Benutzers eingetragen ist. Die globale Option ist per Voreinstellung aktiv.

Öffentliche Kontakte virtuell mit den Standard-Kontakten zusammenführen
Diese Option bewirkt, dass die öffentlichen Kontakte und die Standard-Kontakte der Benutzer auf ihren Geräten als zusammengeführt dargestellt werden. Die

Datenbestände der Kontakte bleiben hierbei getrennt; es werden also keine Kontakte zwischen den Kontaktordnern der Benutzer kopiert. Diese Option kann insbesondere für solche Clients hilfreich sein, die das Durchsuchen der Globalen Adressliste (GAL) nicht unterstützen. Diese Option ist per Voreinstellung abgeschaltet.

Absender sperren, wenn Nachricht in Ordner Junk-Email verschoben wird
Ist diese Option aktiv, so wird die Absender-Adresse (Felder Sender und From) einer E-Mail-Adresse in den Kontaktordner für gesperrte Absender eingetragen, sobald ein Client die zugehörige E-Mail-Nachricht in den Ordner für Spam-Nachrichten verschiebt.

Antworten auf Besprechungsanfragen nach Zusage, Ablehnung usw. zwingend senden
Ist diese Option aktiv, so versendet der ActiveSync-Dienst eine Antwort an den Besprechungsorganisator immer dann, wenn ein Client auf eine Besprechungseinladung zusagt, sie ablehnt oder eine sonstige Aktion für die Einladung ausführt. Diese Option ist für solche Clients nützlich, die solche Antworten nicht selbst richtig senden.

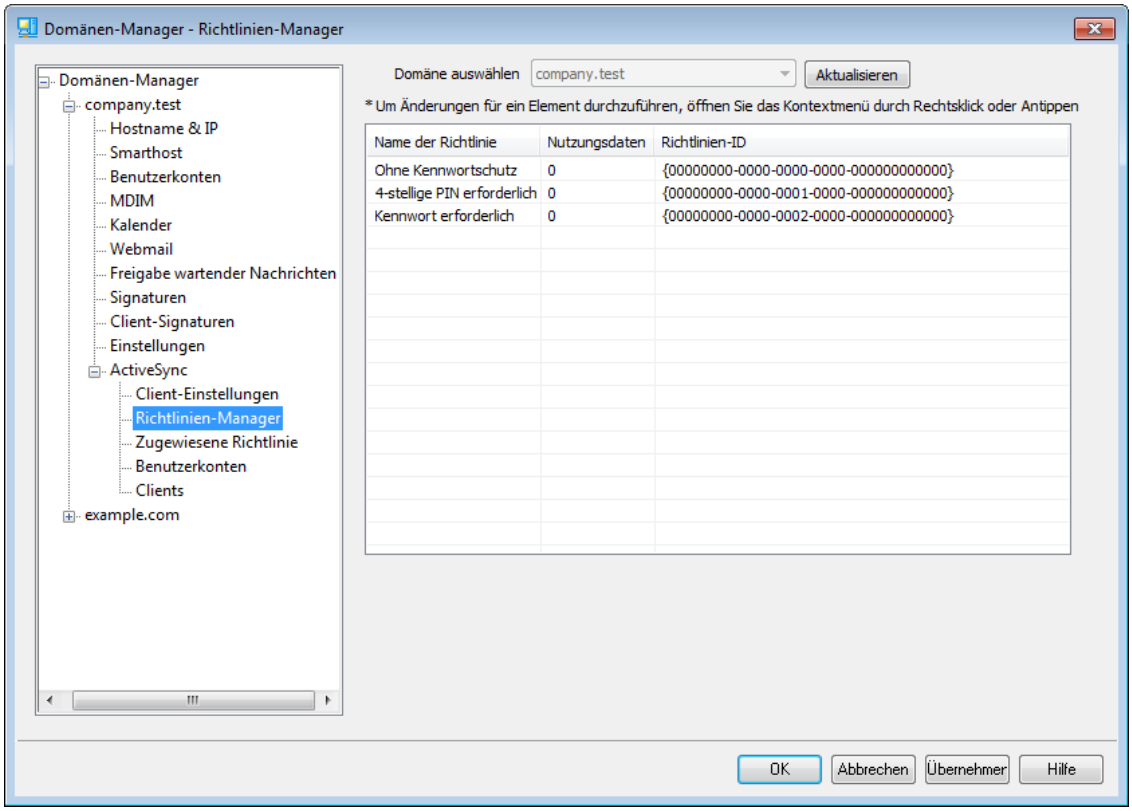
Vorschau auf tatsächlich wirksame Einstellungen

Dieses Steuerelement ist auf allen untergeordneten Konfigurationsdialogen für die Client-Einstellungen (Domänen 437, Benutzerkonten 454 und Clients 464) verfügbar. Per Voreinstellung werden die Optionen auf diesen Konfigurationsdialogen nicht von den übergeordneten Konfigurationsdialogen geerbt. Sie können sich daher mithilfe dieses Steuerelements die Einstellungen anzeigen lassen, die auf den jeweils gerade dargestellten Konfigurationsdialog wirken.

Siehe auch:

ActiveSync » Client-Einstellungen 422
ActiveSync » Benutzerkonten 454
ActiveSync » Clients 464

3.2.11.2 Richtlinien-Manager



Mithilfe dieses Konfigurationsdialogs können Sie die ActiveSync-Geräterichtlinien verwalten. Die Richtlinien können ActiveSync-Geräten zugewiesen werden und steuern auf ihnen verschiedene Optionen. Es stehen Ihnen vordefinierte Richtlinien zur Verfügung, und Sie können selbst Richtlinien erstellen, bearbeiten und löschen. Es stehen Standard-Richtlinien zur Verfügung, und Sie können darüber hinaus eigene Richtlinien erstellen, bearbeiten und löschen. Sie können Benutzerkonten[454] und bestimmten Clients[464] on den entsprechenden Konfigurationsdialogen für zugewiesene Richtlinien sowohl die Standard-Richtlinien als auch abweichende eigene Richtlinien zuweisen.

Bitte beachten Sie, dass nicht alle ActiveSync-Endgeräte alle Richtlinien erkennen. Auch können in der Art der Umsetzung Unterschiede auftreten. Manche Geräte ignorieren bestimmte Elemente und Einstellungen der Richtlinien insgesamt; andere erfordern einen Neustart des Geräts, damit Änderungen wirksam werden. Eine Richtlinie kann jedenfalls frühestens dann wirksam werden, wenn das betroffene Gerät selbst eine Verbindung zum ActiveSync-Server herstellt. Eine "Push-Übermittlung" der Richtlinien an die Geräte, ohne dass diese eine Verbindung zum Server herstellen, ist nicht möglich.

ActiveSync-Richtlinien

Um Änderungen vorzunehmen, öffnen Sie durch Rechtsklick in diesem Bereich das Kontextmenü. Es stehen dann folgende Menüeinträge zur Verfügung:

Richtlinie erstellen
Durch Anklicken dieser Schaltfläche öffnen Sie den Editor für ActiveSync-Richtlinien 446, mit dessen Hilfe Sie die Richtlinien erstellen und bearbeiten können.

Richtlinie löschen
Um eine Richtlinie zu löschen, wählen Sie die gewünschte benutzerdefinierte Richtlinie aus der Übersicht aus, und klicken Sie dann auf *Richtlinie löschen*. Es erscheint eine Sicherheitsabfrage. Um Ihre Entscheidung zum Löschen der Richtlinie zu bestätigen, klicken Sie auf **Ja**. Die vordefinierten Richtlinien können nicht gelöscht werden.

Richtlinie bearbeiten
Um eine Richtlinie zu bearbeiten, wählen Sie die gewünschte benutzerdefinierte Richtlinie aus der Übersicht aus, und klicken Sie dann auf *Richtlinie bearbeiten*. Nehmen Sie die gewünschten Änderungen im Editor für ActiveSync-Richtlinien vor, und klicken Sie dann auf **OK**. Die vordefinierten Richtlinien können nicht bearbeitet werden.

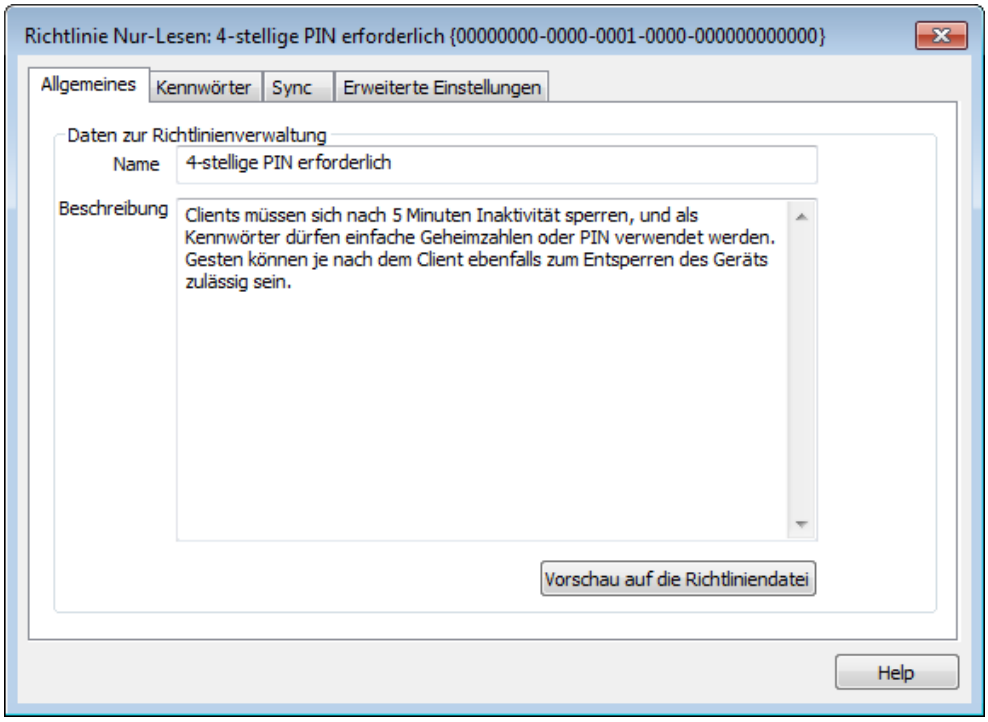
Richtlinien-Nutzungsdaten anzeigen
Durch Anklicken dieser Schaltfläche erhalten Sie eine Übersicht aller Domänen, Benutzerkonten und Clients, denen eine Richtlinie zugewiesen ist. Um diese Übersicht zu erhalten, wählen Sie die gewünschte Richtlinie aus, und klicken Sie dann auf diese Schaltfläche.

Editor für ActiveSync-Richtlinien

Der Editor für ActiveSync-Richtlinien ist in vier Registerkarten unterteilt: Allgemeines, Kennwörter, Sync und Erweiterte Einstellungen. Die Registerkarte Erweiterte Einstellungen ist nur dann sichtbar, wenn Sie die Option *Bearbeiten erweiterter Richtlinienoptionen zulassen* 416 aktivieren. Sie finden diese Option im Konfigurationsdialog ActiveSync-System.

Allgemeines

Auf dieser Registerkarte legen Sie einen Namen und eine Beschreibung für die Richtlinie fest. Sie können auch eine Vorschau auf die Richtliniendatei mit dem aus der Richtlinie erstellten XML-Kode erhalten.



Daten zur Richtlinienverwaltung

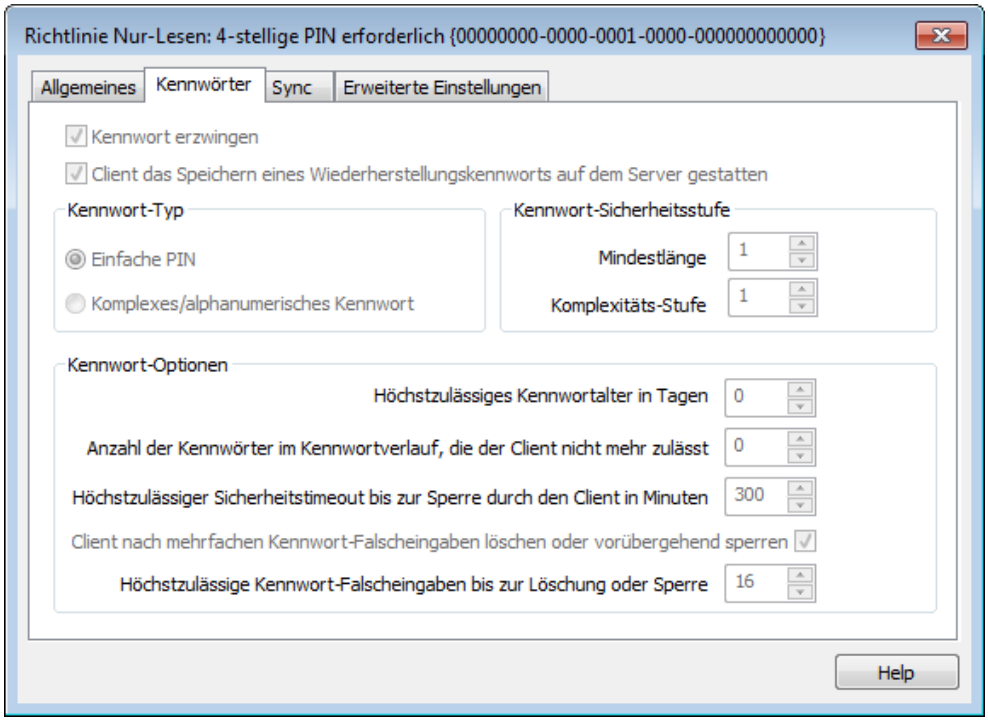
Name
Geben Sie hier den Namen für die benutzerdefinierte Richtlinie ein.

Beschreibung
Geben Sie hier eine Beschreibung für die benutzerdefinierte Richtlinie ein. Diese Beschreibung erscheint unterhalb der Liste der Richtlinien, wenn Sie diese Richtlinie.

Vorschau auf die Richtliniendatei
Um eine Vorschau auf die Richtliniendatei mit dem XML-Kode für die gerade bearbeitete Richtlinie zu erhalten, klicken Sie auf dieses Steuerelement.

Kennwörter

Auf dieser Registerkarte legen Sie die Optionen und Anforderungen an die Kennwörter fest.



Kennwort erzwingen
Diese Option bewirkt, dass auf dem Gerät ein Kennwort gesetzt werden muss. Sie ist per Voreinstellung abgeschaltet.

Gerät das Speichern eines Wiederherstellungskennworts auf dem Server gestatten
Diese Option ermöglicht es den Clients, die ActiveSync-Option zum Wiederherstellen von Kennwörtern zu nutzen. Diese Option speichert auf dem Server ein vorübergehend nutzbares Wiederherstellungskennwort; mit seiner Hilfe kann das Gerät entsperrt werden, falls das Kennwort vergessen wurde. Der Systemverwalter kann dieses Wiederherstellungskennwort im Abschnitt Details 464 für das jeweilige Gerät finden. Die meisten Geräte unterstützen diese Funktion nicht.

Kennwort-Typ

Einfache PIN
Die Wirkung dieser Option hängt wesentlich von der Implementation auf dem jeweiligen Gerät ab. Im Allgemeinen bewirkt diese Option, dass für das Kennwort nur die *Mindestlänge* eingehalten werden muss, ansonsten aber keine Anforderungen an die Komplexität gestellt werden. Diese Option lässt daher auch einfache Kennwörter zu, wie etwa "111", "aaa", "1234", "ABCD" und ähnliches.

Komplexes/alphanumerisches Kennwort
Diese Option erzwingt komplexere und sicherere Gerätekennwörter als die Option *Einfache PIN*. Die Option *Komplexitäts-Stufe* bestimmt im Zusammenhang mit dieser Option die genauen Anforderungen an die Komplexität des Kennworts. Diese Option ist per Voreinstellung aktiv, falls die Richtlinie die Nutzung eines Kennworts erzwingt.

Kennwort-Sicherheitsstufe

Mindestlänge
Diese Option bewirkt, dass das Gerätekennwort mindestens die hier festgelegte Länge haben muss. Die Mindestlänge kann 1 bis 16 Zeichen betragen. Der Wert beträgt per Voreinstellung 1.

Komplexitäts-Stufe
Diese Option bestimmt die Anforderungen an *komplexe/alphanumerische Kennwörter.* Der Wert der Komplexitäts-Stufe legt fest, wie viele verschiedene Zeichenarten das Kennwort enthalten muss. Zeichenarten sind dabei Großbuchstaben, Kleinbuchstaben, Ziffern und nicht-alphanumerische Zeichen (etwa Satzzeichen und Sonderzeichen). Sie können 1 bis 4 verschiedene Zeichentypen verlangen. Wird hier beispielsweise der Wert 2 eingetragen, so muss das Kennwort mindestens zwei verschiedene Zeichenarten aus der Auswahl Großbuchstaben, Kleinbuchstaben, Ziffern und nicht-alphanumerische Zeichen enthalten. Der Wert beträgt per Voreinstellung 1.

Kennwort-Optionen

Höchstzulässiges Kennwortalter in Tagen
Diese Option bewirkt, dass das Gerätekennwort geändert werden muss, sobald es das hier in Tagen angegebene Alter überschritten hat. Sie ist per Voreinstellung abgeschaltet (Wert "0").

Anzahl der Kennwörter im Kennwortverlauf, die das Gerät nicht mehr zulässt
Diese Option bewirkt, dass auf dem Geräte eine Kennwortchronik geführt wird, die verhindert, dass die Benutzer einmal verwendete Gerätekennwörter zu bald wieder verwenden. Der Wert der Option legt fest, wie viele Kennwörter in der Kennwortchronik gespeichert werden. Wird hier etwa der wert "2" eingetragen, und ändert der Benutzer das Gerätekennwort, so darf er als neues Kennwort die letzten beiden Kennwörter, die er verwendet hat, nicht erneut verwenden. Die Option ist per Voreinstellung abgeschaltet (Wert "0").

Höchstzulässiger Sicherheitstimeout bis zur Sperre durch das Gerät in Minuten
Diese Option bestimmt, wie lange ein Gerät ohne Benutzereingaben in Bereitschaft bleiben darf, bevor es sich selbst sperrt. Nach dieser Sperre muss der Benutzer das Gerätekennwort eingeben, wenn er das Gerät wieder nutzen will. Diese Option ist per Voreinstellung abgeschaltet (Wert "0").

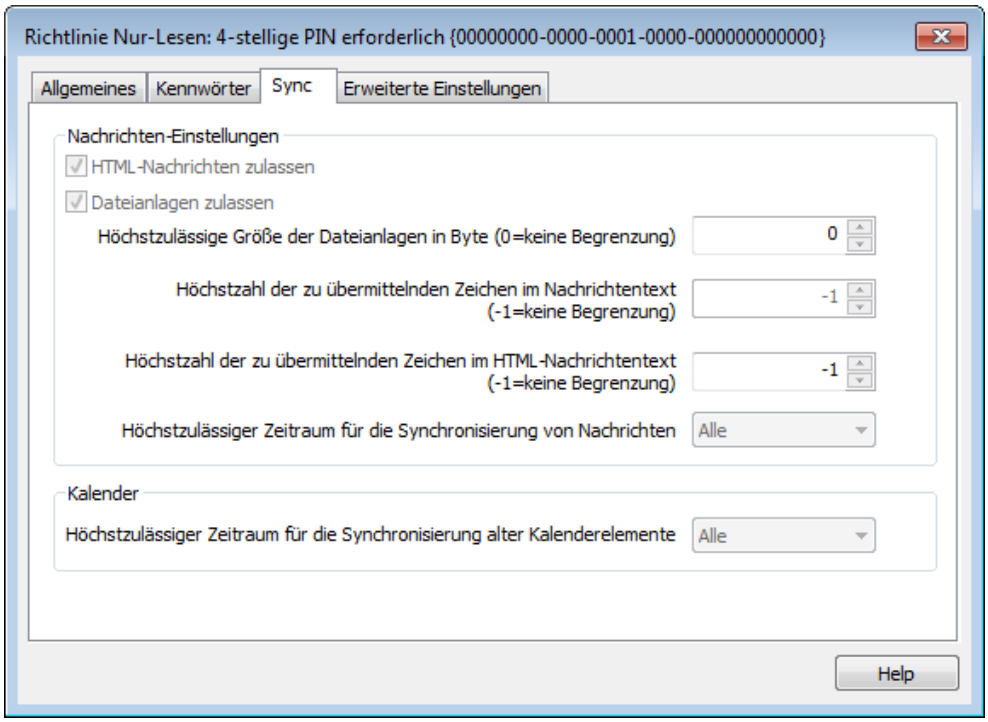
Gerät nach mehrfachen Kennwort-Falscheingaben löschen oder vorübergehend sperren
Diese Option bewirkt, dass sich das Gerät für eine bestimmte Zeit gegen weitere Eingabeversuche sperrt oder sämtliche Daten automatisch löscht, falls der Benutzer das Kennwort mehrfach hintereinander falsch eingibt und dabei die hier festgelegte Höchstzahl an Versuchen überschreitet. Diese Option ist per Voreinstellung abgeschaltet.

Höchstzulässige Kennwort-Falscheingaben bis zur Löschung oder Sperre
Diese Option legt fest, wie viele Versuche für den Benutzer zulässig sind, das Gerätekennwort richtig einzugeben, bevor sich das Gerät sperrt oder löscht. Welche Aktion das Gerät danach durchführt, hängt von dem Gerät

selbst ab. Die Option ist per Voreinstellung abgeschaltet. Diese Option wirkt nur, wenn die Option *Gerät nach mehrfachen Kennwort-Falscheingaben löschen oder vorübergehend sperren* weiter oben aktiv ist.

Sync

Auf dieser Registerkarte konfigurieren Sie verschiedene Optionen für HTML-Nachrichten, die Nutzung von Dateianlagen, die Begrenzung des Datenvolumens für die Übertragung und die Zeiträume, für die E-Mail- und Kalenderdaten synchronisiert werden dürfen.



Nachrichten-Einstellungen

HTML-Nachrichten zulassen
Per Voreinstellung können E-Mail-Nachrichten im HTML-Format an ActiveSync-Clients übermittelt und mit ihnen synchronisiert werden. Falls Sie die Übermittlung und Synchronisierung auf Nur-Text-Nachrichten beschränken wollen, deaktivieren Sie diese Option.

Dateianlagen zulassen
Diese Option gestattet den Geräten das Herunterladen von Dateianlagen. Die Option ist per Voreinstellung aktiv.

Höchstzulässige Größe der Dateianlagen in Byte (0=keine Begrenzung)
Diese Option bestimmt, wie groß Dateianlagen höchstens sein dürfen, damit sie noch automatisch auf das Gerät übermittelt werden. Per Voreinstellung besteht keine Größenbegrenzung (Wert "0").

Höchstzahl der zu übermittelnden Zeichen im Nachrichtentext (-1=keine Begrenzung)
Dieser Wert legt die Höchstzahl der Zeichen im Nachrichtentext von Nur-

Text-Nachrichten fest, die an den Client übermittelt werden. Enthält der Nachrichtentext mehr Zeichen, so wird der Nachrichtentext nach Erreichen des hier festgelegten Grenzwerts abgeschnitten. Per Voreinstellung ist keine Begrenzung aktiv (Wert -1). Falls Sie diesen Wert auf 0 setzen, werden nur die Kopfzeilen der Nachrichten übermittelt.

Höchstzahl der zu übermittelnden Zeichen im HTML-Nachrichtentext (-1=keine Begrenzung)
Dieser Wert legt die Höchstzahl der Zeichen im Nachrichtentext von HTML-Nachrichten fest, die an den Client übermittelt werden. Enthält der Nachrichtentext mehr Zeichen, so wird der Nachrichtentext nach Erreichen des hier festgelegten Grenzwerts abgeschnitten. Per Voreinstellung ist keine Begrenzung aktiv (Wert -1). Falls Sie diesen Wert auf 0 setzen, werden nur die Kopfzeilen der Nachrichten übermittelt.

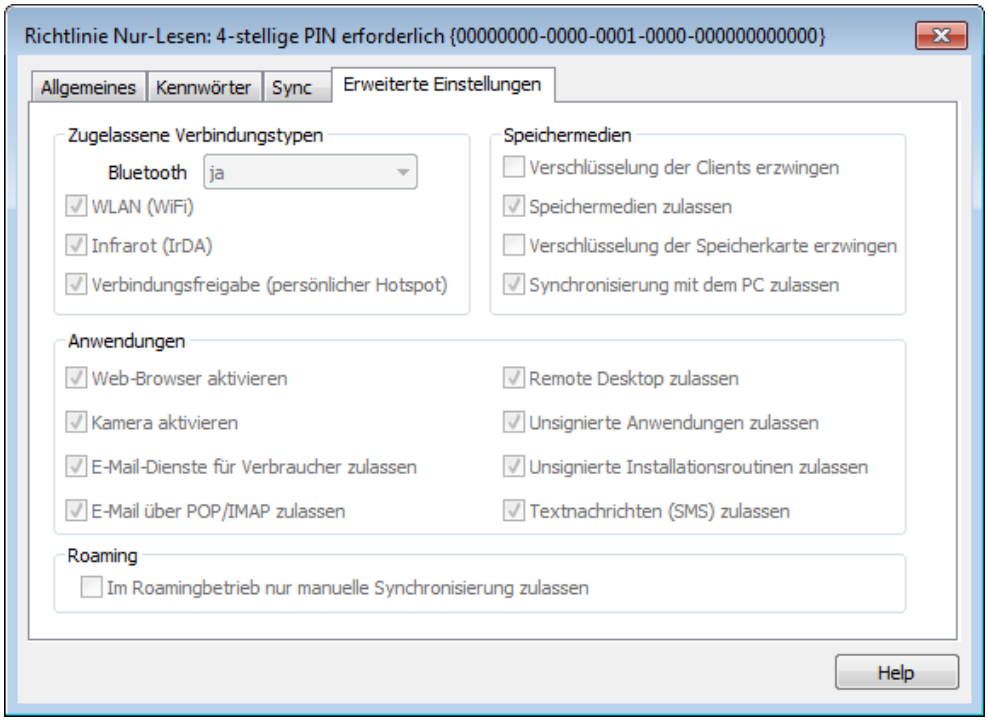
Höchstzulässiger Zeitraum für die Synchronisierung von Nachrichten
Dieses Intervall bestimmt den Zeitraum, jeweils gerechnet von dem aktuellen Tag, für den E-Mail-Nachrichten mit dem Gerät synchronisiert werden können. Per Voreinstellung ist der Wert "Alle" aktiv, sodass alle E-Mail-Nachrichten unabhängig von ihrem Alter mit dem Gerät synchronisiert werden können.

Kalender

Höchstzulässiger Zeitraum für die Synchronisierung alter Kalenderelemente
Dieses Intervall bestimmt den Zeitraum, jeweils gerechnet von dem aktuellen Tag, für den Kalendereinträge mit dem Gerät synchronisiert werden können. Per Voreinstellung ist der Wert "Alle" aktiv, sodass alle Kalendereinträge unabhängig von ihrem Alter mit dem Gerät synchronisiert werden können.

Erweiterte Einstellungen

Auf dieser Registerkarte legen Sie die zugelassenen Verbindungstypen und Anwendungen sowie Einstellungen zu Speichermedien, Verschlüsselung und Roaming fest.



Diese Registerkarte ist nur dann sichtbar, wenn Sie die Option *Bearbeiten erweiterter Richtlinienoptionen zulassen* 416 aktivieren. Sie finden diese Option im Konfigurationsdialog ActiveSync für MDaemon.

Zugelassene Verbindungstypen

Bluetooth

Diese Option bestimmt, ob das Gerät Bluetooth-Verbindungen zulässt. Um Bluetooth-Verbindungen zuzulassen, wählen Sie **ja**, um Bluetooth-Verbindungen zu unterbinden, wählen Sie **nein**, und um Bluetooth-Verbindungen zuzulassen, aber auf Verbindungen mit Freisprechanlagen zu beschränken, wählen Sie **Freisprechen**. Die Voreinstellung für diese Option ist **ja**.

WLAN (WiFi)

Diese Option bestimmt, ob das Gerät WLAN-Verbindungen (WiFi) zulässt. Die Option ist per Voreinstellung aktiv.

Infrarot (IrDA)

Diese Option bestimmt, ob das Gerät Infrarot-Verbindungen (IrDA) zulässt. Die Option ist per Voreinstellung aktiv.

Verbindungsfreigabe (persönlicher Hotspot)

Diese Option bestimmt, ob das Gerät als persönlicher Hotspot arbeiten und die Internet-Verbindungsfreigabe anbieten darf. Die Option ist per Voreinstellung aktiv.

Speichermedien

Geräteverschlüsselung erzwingen

Diese Option bewirkt, dass die Verschlüsselung der Inhalte auf dem Gerät erforderlich ist. Sie wird jedoch nicht durch alle Geräte umgesetzt. Sie ist

per Voreinstellung abgeschaltet.

Speichermedien zulassen
Diese Option bewirkt, dass das Gerät die Nutzung von Speicherkarten zulässt. Die Option ist per Voreinstellung aktiv.

Verschlüsselung der Speicherkarte erzwingen
Diese Option bewirkt, dass das Gerät die Speicherkarten zwingend verschlüsselt. Die Option ist per Voreinstellung abgeschaltet.

Synchronisierung mit dem PC zulassen
Diese Option lässt die Synchronisierung mit PCs über ActiveSync zu. Die Option ist per Voreinstellung aktiv.

Anwendungen

Web-Browser aktivieren
Diese Option bewirkt, dass der Browser auf dem Gerät genutzt werden darf. Sie wird auf einigen Geräten nicht unterstützt, und sie wirkt unter Umständen nicht auf Browser von Drittanbietern. Diese Option ist per Voreinstellung aktiv.

Kamera aktivieren
Diese Option bewirkt, dass die Kamera auf dem Gerät genutzt werden darf. Sie ist per Voreinstellung aktiv.

E-Mail-Dienste für Verbraucher zulassen
Diese Option bewirkt, dass der Benutzer auf dem Gerät persönliche E-Mail-Konten einrichten kann. Ist diese Option deaktiviert, dann hängt es von dem jeweils eingesetzte ActiveSync-Client ab, welche Arten von E-Mail-Benutzerkonten und E-Mail-Diensten noch nutzbar sind. Die Option ist per Voreinstellung aktiv.

E-Mail über POP/IMAP zulassen
Diese Option gestattet die Nutzung der Protokolle POP und IMAP für E-Mail-Benutzerkonten. Die Option ist per Voreinstellung aktiv.

Remote Desktop zulassen
Diese Option gestattet dem Client die Nutzung des Remote Desktops. Die Option ist per Voreinstellung aktiv.

Unsignierte Anwendungen zulassen
Diese Option gestattet die Nutzung unsignierte Anwendungen auf dem Gerät. Die Option ist per Voreinstellung aktiv.

Unsignierte Installationsroutinen zulassen
Diese Option gestattet das Ausführen unsignierter Installationsroutinen auf dem Gerät. Die Option ist per Voreinstellung aktiv.

Textnachrichten (SMS) zulassen
Diese Option gestattet den Versand und Empfang von Textnachrichten auf dem Gerät. Die Option ist per Voreinstellung aktiv.

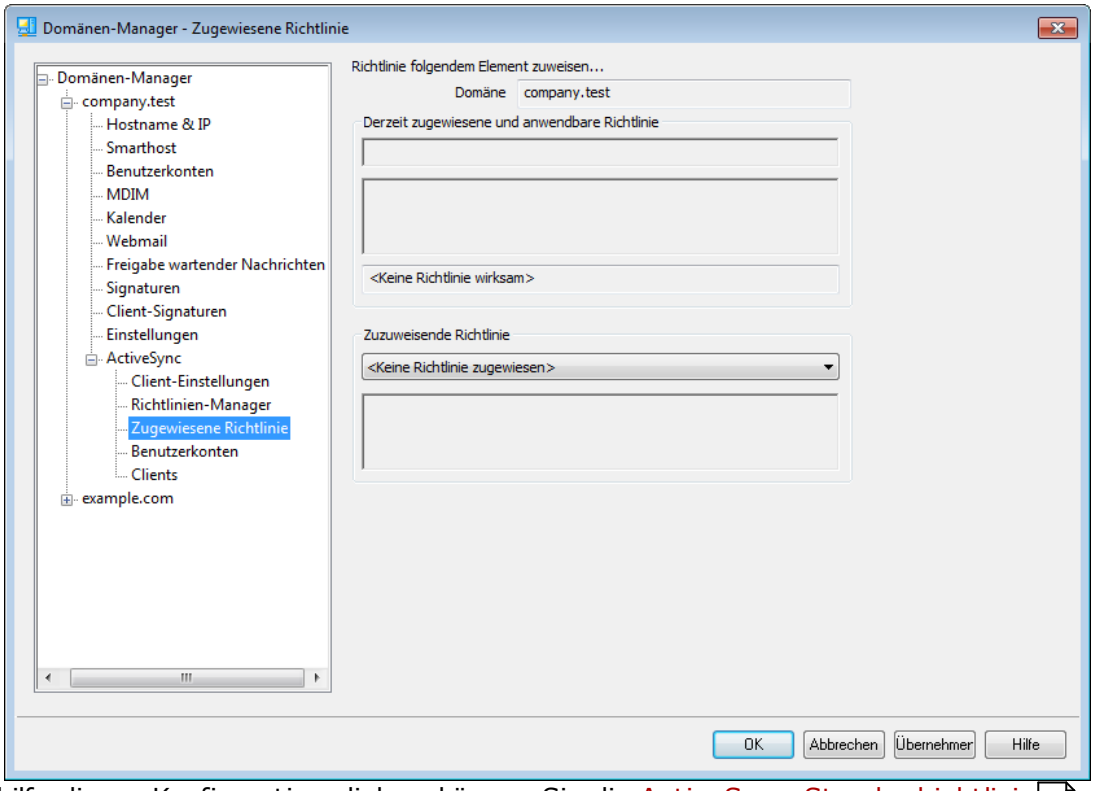
Roaming

Im Roamingbetrieb nur manuelle Synchronisierung zulassen
Diese Option bewirkt, dass die Synchronisierung mit einem Gerät nur manuell vorgenommen werden kann, und eine automatische Synchronisierung unterbleibt, sobald sich das Gerät im Daten-Roamingbetrieb befindet. Die automatische Synchronisierung kann während des Daten-Roamings erhöhte Entgelte verursachen. Welche Entgelte tatsächlich anfallen, hängt von dem Netzbetreiber und der Vertragsart ab. Diese Option ist per Voreinstellung abgeschaltet.

Siehe auch:

Domänen-Manager » Zugewiesene Richtlinie 231
ActiveSync » Benutzerkonten 454
ActiveSync » Clients 464

3.2.11.3 Zugewiesene Richtlinie



Mithilfe dieses Konfigurationsdialogs können Sie die ActiveSync-Standardrichtlinie 222 bestimmen, die der gerade bearbeiteten Domäne zugewiesen wird. Stellt ein ActiveSync-Client eine Verbindung mit einem Benutzerkonto der gerade bearbeiteten Domäne her, und ist für das Benutzerkonto keine eigene, abweichende Richtlinie konfiguriert, dann wird dem Client die Standard-Richtlinie zugewiesen.

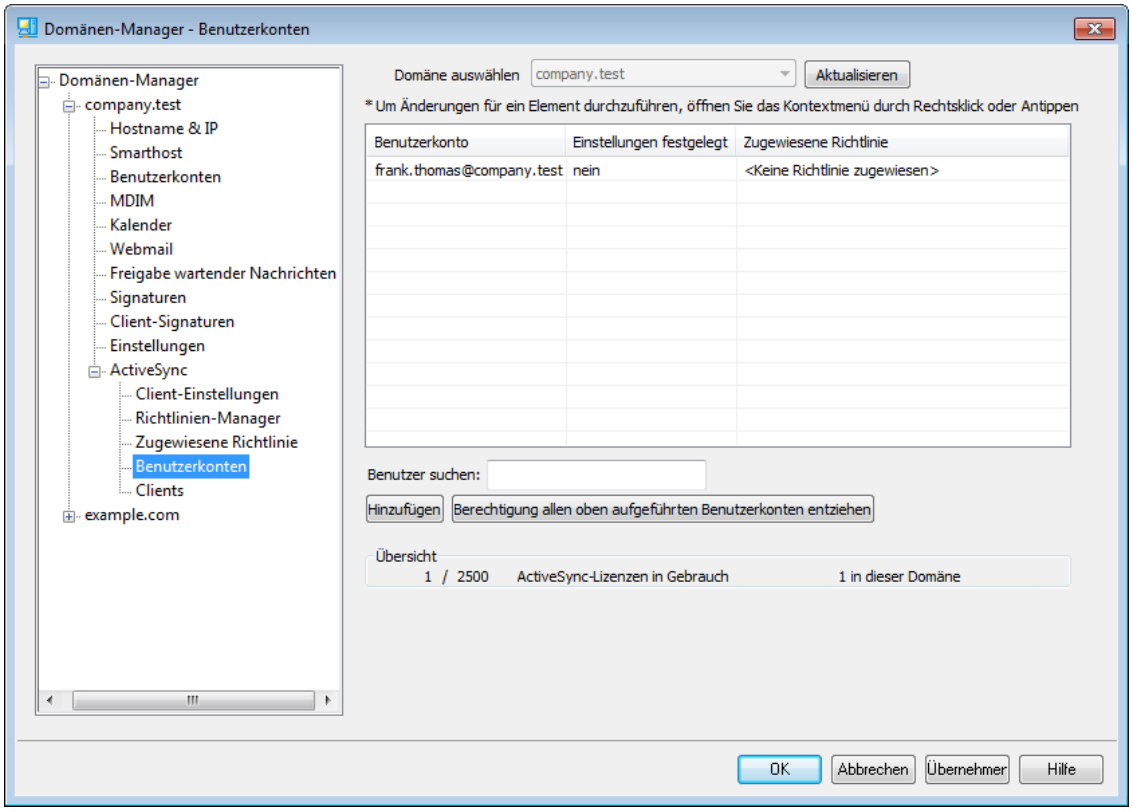
Zuweisen einer ActiveSync-Standardrichtlinie

Um der gerade bearbeiteten Domäne eine ActiveSync-Standardrichtlinie zuzuweisen, wählen Sie aus dem Dropdown-Menü im Abschnitt **Zuzuweisende Richtlinie** die gewünschte Richtlinie aus, und klicken Sie danach auf **OK**.

Siehe auch:

Domänen-Manager » Richtlinien-Manager 222
ActiveSync » Benutzerkonten 454
ActiveSync » Clients 464

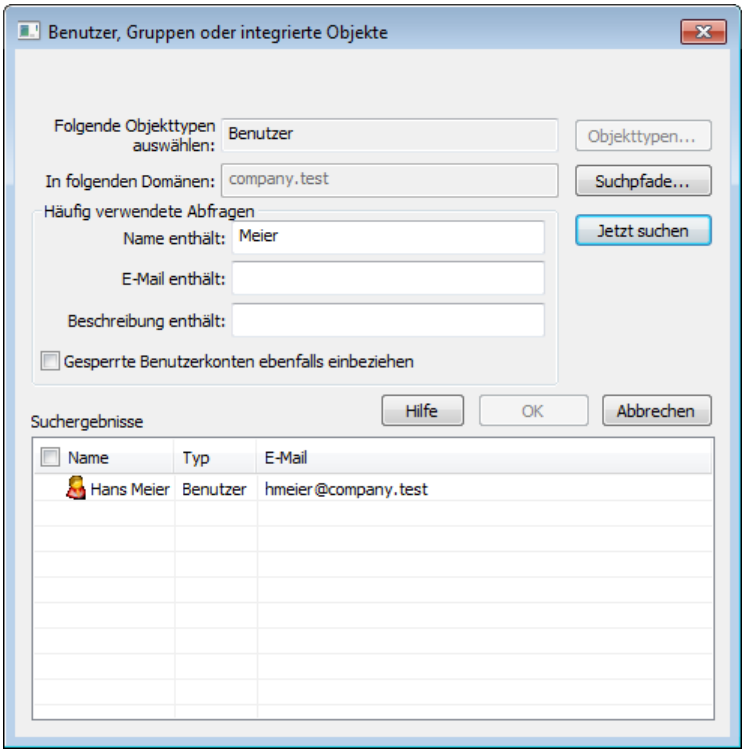
3.2.11.4 Benutzerkonten



Mithilfe dieses Konfigurationsdialogs können Sie bestimmen, welche Benutzerkonten ActiveSync nutzen dürfen. Sie können Benutzerkonten von Hand hinzufügen und entfernen, alle Benutzerkonten gleichzeitig für die Nutzung von ActiveSync freischalten, die Berechtigung widerrufen, oder MDaemon so konfigurieren, dass die Benutzerkonten bei der ersten Nutzung von ActiveSync automatisch die Berechtigung für die Nutzung erhalten.

Benutzerkonten manuell die Berechtigung erteilen

Um einem Benutzerkonto die Berechtigung für die Nutzung von ActiveSync manuell zu erteilen, klicken Sie auf **Hinzufügen**. Hierdurch wird der Dialog zur Auswahl von Benutzerkonten aufgerufen; in diesem Dialog können Sie die gewünschten Benutzerkonten suchen und auswählen.



In folgenden Suchpfaden auswählen
Um die Domänen auszuwählen, die Sie durchsuchen wollen, klicken Sie auf **Suchpfade...**. Sie können alle lokalen oder bestimmte lokale MDaemon-Domänen auswählen.

Häufig verwendete Abfragen
Mithilfe der Optionen in diesem Abschnitt können Sie die Suche eingrenzen. Sie können den Benutzernamen, E-Mail-Adresse und die Beschreibungen[714] der Benutzerkonten durchsuchen und hierbei vollständige oder Teile der Texte suchen. Um alle Benutzer zu erfassen, die im angegebenen Suchpfad enthalten sind, lassen Sie diese Felder leer.

Gesperrte Benutzerkonten ebenfalls einbeziehen
Diese Option bewirkt, dass die Suche auch gesperrte Benutzerkonten[714] erfasst.

Jetzt suchen
Nachdem Sie die Suchkriterien festgelegt haben, beginnen Sie die Suche durch Anklicken dieses Steuerelements.

Suchergebnisse
Nachdem die Suche ausgeführt wurde, erscheinen die Suchergebnisse in diesem Abschnitt. Wählen Sie alle gewünschten Benutzerkonten aus, und klicken Sie dann auf **OK**, um sie in die Liste der berechtigten Benutzerkonten aufzunehmen.

Berechtigung für Benutzerkonten widerrufen

Um einem Benutzerkonto die Berechtigung zur Nutzung von ActiveSync zu entziehen, wählen Sie das Benutzerkonto aus der Liste aus, und klicken Sie danach auf **Berechtigung dem ausgewählten Benutzerkonto entziehen**. Um allen

Benutzerkonten die Berechtigung zur Nutzung von ActiveSync zu entziehen, klicken Sie auf **Berechtigung allen oben aufgeführten Benutzerkonten entziehen.**

Falls auf Ihrem Server die Option *Benutzerkonten beim ersten Zugriff über ActiveSync Berechtigung zur Nutzung erteilen* aktiv ist, können Sie durch das Widerrufen der Freischaltung für ein Benutzerkonto zwar das Benutzerkonto aus der Liste entfernen; das Benutzerkonto wird jedoch wieder für die Nutzung von ActiveSync freigeschaltet werden, sobald sich ein ActiveSync-Gerät bei dem Benutzerkonto anmeldet.

Benutzerkonten beim ersten Zugriff über ActiveSync Berechtigung zur Nutzung erteilen

Diese Option bewirkt, dass alle Benutzerkonten automatisch für die Nutzung von ActiveSync freigeschaltet werden, sobald sie zum ersten Mal eine Verbindung mit MDaemon über ActiveSync herstellen.

Zuweisen einer ActiveSync-Richtlinie

Um einem Benutzerkonto eine Richtlinie 445 zuzuweisen, gehen Sie folgendermaßen vor:

1. Wählen Sie das betreffende Benutzerkonto aus der Dropdown-Liste aus.
2. Klicken Sie auf **Richtlinie zuweisen**. Hierdurch wird der Konfigurationsdialog *Richtlinie anwenden* aufgerufen.
3. Wählen Sie aus der Dropdown-Liste im Bereich *Zuzuweisende Richtlinie* die gewünschte Richtlinie aus.
4. Klicken Sie auf **OK**.

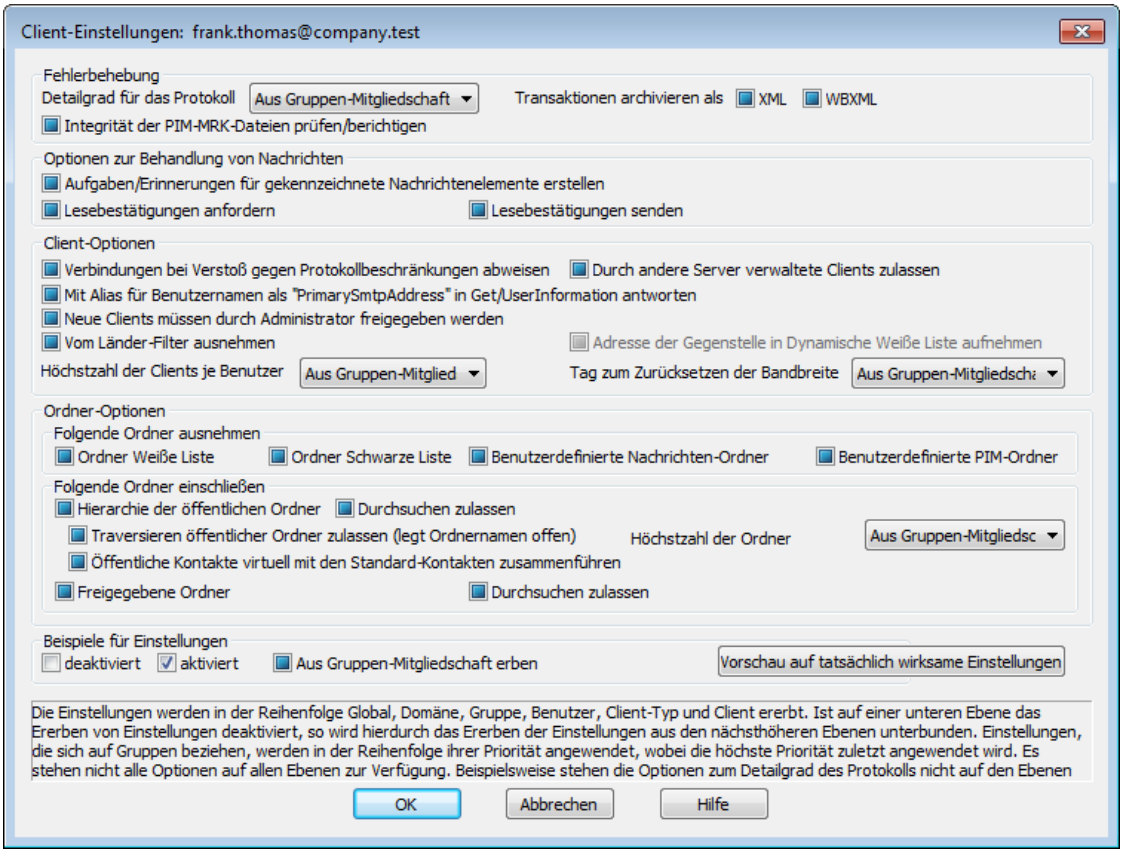
Die ausgewählte Richtlinie wird allen Geräten zugewiesen, die eine Verbindung mit diesem Benutzerkonto herstellen.

Durchsuchen der Liste berechtigter Benutzerkonten

Falls auf Ihrem System zahlreichen Benutzerkonten die Berechtigung zur Nutzung von ActiveSync erteilt ist, können Sie mithilfe des Textfeldes **Benutzer suchen** die Liste nach bestimmten Kriterien filtern. Geben Sie hierzu die ersten Buchstaben der gewünschten E-Mail-Adresse ein.

Einstellungen

Um die Client-Einstellungen für das Benutzerkonto zu verwalten, klicken Sie auf **Einstellungen**. Die hier getroffenen Einstellungen werden auf alle ActiveSync-Clients angewendet, die eine Verbindung mit diesem Benutzerkonto herstellen.



Per Voreinstellung werden alle Einstellungen in diesem Konfigurationsdialog vom übergeordneten Knoten geerbt, oder es werden die Voreinstellungen genutzt. Der übergeordnete Knoten für diesen Konfigurationsdialog sind die Client-Einstellungen der Domäne 215. Alle Änderungen in den Client-Einstellungen der Domäne wirken sich auch auf den vorliegenden Konfigurationsdialog aus. Nehmen Sie an dem hier vorliegenden Konfigurationsdialog Änderungen vor, so übergehen diese Änderungen für das gerade bearbeitete Benutzerkonto die Client-Einstellungen der Domäne.

Allgemeines

Fehlerbehebung

Detailgrad für das Protokoll

ActiveSync für MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Einstellung erben Per Voreinstellung wird die Einstellung für den Detailgrad aus der Hierarchie der Client-Einstellungen vom jeweils übergeordneten Knoten ererbt. Clients übernehmen dabei die Einstellung aus dem jeweiligen Client-Typ, Client-Typen übernehmen die Einstellung von den Benutzerkonten, Benutzerkonten übernehmen die Einstellung von den Gruppen, und so weiter. Die globale Einstellung für alle Clients wird durch die Einstellung für den Detailgrad im Konfigurationsdialog Diagnose 432 bestimmt.

Transaktionen archivieren als [XML | WBXML]
Mithilfe der Optionen *XML...* und *WBXML...* können Sie die zugehörigen Daten speichern; diese Daten können die Fehlersuche erleichtern. Die systemweit wirksamen Optionen sind per Voreinstellung abgeschaltet.

Integrität der PIM-MRK-Dateien prüfen/berichtigen
Diese Option führt für die PIM-Daten der betroffenen Clients Prüf- und Korrekturvorgänge durch. Sie sollen bekannte Probleme erkennen, die eine ordnungsgemäße Synchronisierung verhindern können. Zu diesen Problemen zählen insbesondere doppelte iCal-UIDs und leere Datenfelder, die eigentlich verpflichtend Daten enthalten müssen. Die systemweit wirksame Option ist per Voreinstellung abgeschaltet.

Client-Optionen

Verbindungen bei Verstoß gegen Protokollbeschränkungen abweisen
Diese Option bewirkt, dass Verbindungen von Clients abgewiesen werden, falls sie versuchen eine nicht für die Clients *Zugelassene Protokollversion* zu verwenden. Per Voreinstellung ist diese Option abgeschaltet; dies bedeutet, dass die Protokollbeschränkung keine Verbindungen solcher Clients verhindern, die andere als die zugelassenen Protokollversionen verwenden. Solange die Option abgeschaltet ist, weist MDaemon die Clients zwar an, nur die zugelassenen Protokollversionen zu verwenden, lässt aber bei Nutzung anderer Protokollversionen die Verbindung trotzdem zu. Nähere Informationen finden Sie unter Protokollbeschränkungen 434.

Mit Alias für Benutzernamen als "PrimarySmtpAddress" in Get/UserInformation antworten
Diese Option gestattet es dem Dienst, als Antwort auf eine Anforderung Settings/Get/UserInformation eine etwa vorhandene Alias-Adresse oder eine sekundäre Adresse des betroffenen Benutzerkontos als primäre Adresse zu übermitteln. Hierdurch wird ein Problem umgangen, das mit einer iOS-Aktualisierung nach Version 9.x verursacht wird, und das verhinderte, dass Clients unter einer etwa vorhandenen Alias-Adresse Nachrichten versenden konnten. Die Nutzung dieser Option bewirkt eine nicht standardkonforme Antwort auf die Anforderung Settings/GetUserInformation.

Neue Clients müssen durch Administrator freigegeben werden
Diese Option bewirkt, dass neue Clients sich erst dann mit Benutzerkonten synchronisieren können, wenn sie zunächst durch einen Administrator freigegeben wurden. In der Liste der Clients[464] sind alle Clients aufgeführt, die noch die Freigabe erwarten, und die Administratoren können sie über diese Liste freigeben. Diese Option ist per Voreinstellung abgeschaltet.

Höchstzahl der Clients je Benutzer
Mithilfe dieser Option können Sie die Anzahl der ActiveSync-Clients und -Endgeräte begrenzen, die mit jedem MDaemon-Benutzerkonto verknüpft sein können. Der hier angegebene Wert ist die Höchstzahl zulässiger Clients. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt. Diese Option steht nur in den Client-Einstellungen auf globaler, Domänen- und Benutzerebene zur Verfügung, nicht jedoch in den Client-Einstellungen für die einzelnen Clients.

Tag zum Zurücksetzen der Bandbreite
Mithilfe dieser Option können Sie Tag bestimmen, an dem in jedem Monat die Bandbreiten-Nutzungsstatistik für die ActiveSync-Endgeräte zurückgesetzt wird. Dieser Vorgang wird während der normalen Bereinigungsvorgänge um Mitternacht aufgeführt und, wie auch andere Bereinigungsvorgänge, in das Protokoll System eingetragen. Der globale Wert lautet per Voreinstellung 0 (nicht zurücksetzen), sodass per Voreinstellung die Nutzungsstatistik nicht zurückgesetzt wird. Für untergeordnete Knoten können Sie abweichende Einstellungen treffen, etwa, um die Einstellung an den Tag anzugleichen, an dem für das betroffene Endgeräte ein neuer Abrechnungszeitraum des Netzbetreibers beginnt.

Sicherheit

Vom Länder-Filter ausnehmen
Wenn Sie diese Option in den Einstellungen eines ActiveSync-Clients aktivieren, kann das Endgerät den Länder-Filter[574] umgehen. Hierdurch kann ein berechtigter Benutzer auf sein Benutzerkonto über ActiveSync beispielsweise auch dann zugreifen, wenn er sich in einem Land befindet, für das Versuche zur Echtheitsbestätigung ansonsten durch den Länder-Filter unterbunden werden. Ein Endgerät kann nur dann vom Länder-Filter ausgenommen sein, wenn es innerhalb des durch die Option Inaktive Clients entfernen nach [x] Tagen[418] im Abschnitt Anpassung bestimmten Zeitraums eine echtheitsbestätigte Verbindung über ActiveSync erfolgreich hergestellt hat.

> **Adresse der Gegenstelle in Dynamische Freigabeliste aufnehmen**
> Wenn Sie ein Endgerät vom Länder-Filter ausnehmen, können Sie durch Aktivieren dieser Option die IP-Adresse, von der aus das Endgerät die Verbindung herstellt, in die Freigabeliste eintragen lassen. Hierdurch können beispielsweise andere Clients, die von der selben IP-Adresse aus eine Verbindung herstellen, ebenfalls zugelassen werden.

Durch andere Server provisionierte/verwaltete Clients zulassen
Per Voreinstellung dürfen Clients auch dann Verbindungen zu MDaemon aufbauen, wenn sie auf die Übermittlung der Provisionierungs- und Richtliniendaten durch den ActiveSync-Server hin melden, dass sie auch durch einen oder mehrere andere ActiveSync-Server verwaltet werden. Bei einer solchen Mehrfachverwaltung kann es nicht sichergestellt werden, dass alle auf Ihrem System bestehenden Richtlinien durch den Client auch umgesetzt werden; dies gilt insbesondere dann, wenn sie Richtlinien des anderen ActiveSync-

Servers widersprechen. In vielen Fällen setzen die Clients die am stärksten einschränkende Richtlinie um, falls mehrere einander widersprechende Richtlinien vorhanden sind. Um Verbindungen von Clients zu unterbinden, die durch andere ActiveSync-Server verwaltet werden, deaktivieren Sie diese Option.

Löschen der Clients (Zurücksetzen in den Auslieferungszustand) nicht zulassen
Wenn diese Option aktiv ist, dann können ActiveSync-Clients nicht in den **Auslieferungszustand zurückgesetzt** und damit vollständig gelöscht werden. Wenn Sie Clients ferngesteuert in den Auslieferungszustand zurücksetzen wollen, müssen Sie diese Option deaktivieren. Diese Option ist per Voreinstellung deaktiviert. Nähere Informationen finden Sie auf der Seite Clients im Abschnitt **Vollständiges Löschen eines ActiveSync-Clients** 464.

Optionen zur Ordner-Synchronisierung

Optionen zur Ordner-Synchronisierung

Folgende Ordner ausnehmen

Freigegebene Absender/Gesperrte Absender
Per Voreinstellung werden die Kontaktordner mit Freigabelisten und Sperrlisten der Benutzer nicht mit den Geräten synchronisiert. Diese Ordner dienen üblicherweise nur in MDaemon zum Erkennen und Filtern von Spam. Ihre Inhalte brauchen daher nicht auf den Geräten als Kontakte angezeigt zu werden.

Benutzerdefinierte Nachrichten-Ordner
Per Voreinstellung können alle Standard- und benutzerdefinierten Nachrichten-Ordner mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-Nachrichtenordner synchronisiert werden können. Die Standard-Nachrichtenordner sind insbesondere Posteingang, Gesendete Objekte, Gelöschte Objekte und Entwürfe. Ordner, die die Benutzer selbst anlegen, werden dann nicht mehr synchronisiert. Diese Option ist per Voreinstellung abgeschaltet.

Benutzerdefinierte PIM-Ordner
Per Voreinstellung können alle PIM-Ordner (insbesondere Kontakte, Kalender, Notizen und Aufgaben) mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-PIM-Ordner synchronisiert werden können. Ist diese Option aktiv, so wird beispielsweise für jeden Benutzer nur der Standard-Kalender synchronisiert, auch wenn er über mehrere Kalender-Ordner verfügt. Diese Option ist per Voreinstellung abgeschaltet.

Folgende Ordner einschließen

Hierarchie der öffentlichen Ordner
Diese Option bewirkt, dass die öffentlichen Ordner 309, auf die die Benutzer Zugriff haben, in den Ordnerlisten der Benutzer auf ihren ActiveSync-Geräten erscheinen. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der öffentlichen Ordner 309, auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Traversieren öffentlicher Ordner zulassen (legt Ordnernamen offen)
Benutzerkonten, die auf Unterordner in öffentlichen Ordnern zugreifen oder diese synchronisieren wollen, müssen per Voreinstellung sowohl für den betroffenen Unterordner als auch für alle ihm übergeordneten öffentlichen Ordner[309] über die Berechtigung Ordner anzeigen[311] verfügen. Fehlt einem Benutzerkonto diese Berechtigung für einen übergeordneten öffentlichen Ordner, so kann er auch den gewünschten Unterordner nicht synchronisieren und nicht auf ihn zugreifen, und zwar auch dann nicht, wenn das Benutzerkonto für diesen Unterordner selbst die erforderliche Berechtigung hat. Mithilfe dieser Option können Sie den Clients Zugriff auf und Synchronisierung von Unterordnern ermöglichen, ohne dass die Clients Berechtigungen für die übergeordneten öffentlichen Ordner haben. **Beachte:** Ist diese Option aktiv, so erlangt der Client zwangsläufig Kenntnis von den Namen der übergeordneten Ordner, auch wenn er für ihre Inhalte keine Zugriffsrechte hat. Hieraus kann sich ein Sicherheitsrisiko ergeben. Die Option ist per Voreinstellung abgeschaltet.

Höchstzahl zulässiger öffentlicher Ordner
Diese Option begrenzt die Zahl der öffentlichen Ordner, die auf den betroffenen Geräten dargestellt werden können. Ist eine solche Höchstzahl angegeben, dann übermittelt der Server so lange Einträge in der Ordnerliste, bis die Höchstzahl erreicht ist. Danach übermittelt der Server keine Ordner mehr an die Geräte. Die Reihenfolge, in der die Ordner dabei verarbeitet werden, kann weder festgelegt noch vorher bestimmt werden. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt.

Freigegebene Ordner
Diese Option nimmt auch die gemeinsam genutzten Ordner[122], auf die die Benutzer Zugriff haben, in die Ordnerlisten auf ihren ActiveSync-Geräten auf. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der freigegebenen Ordner[742], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Behandlung von Inhalten

Optionen zur Behandlung von Inhalten

Aufgaben/Erinnerungen für durch Clients gekennzeichnete Nachrichtenelemente erstellen
Diese Option ermöglicht es MDaemon, die Benutzer an gekennzeichnete Elemente zu erinnern. Hierzu wird für jede gekennzeichnete E-Mail-Nachricht eine Aufgabe erstellt, wenn der Client dies anfordert. Die globale Option für dieses Leistungsmerkmal ist per Voreinstellung aktiv.

Aktualisierung nach jeder Änderung der Besprechung senden
Manche Clients versenden aktualisierte Besprechungseinladungen nicht richtig, nachdem eine Besprechung geändert wurde. Diese Option bewirkt, dass der ActiveSync-Dienst immer dann aktualisierte Besprechungseinladungen sendet, wenn der Besprechungsorganisator eine Besprechung aktualisiert hat. Diese Option sollte nur für Clients[464] und Client-Typen[481] aktiviert werden, die die aktualisierten Besprechungseinladungen nicht richtig versenden, da sonst

aktualisierte Besprechungseinladungen doppelt versandt werden. Aus diesem Grund ist diese Einstellung nur auf den Seiten Clients und Client-Typen verfügbar.

Lesebestätigung für alle versandten Nachrichten anfordern
Diese Option bewirkt, dass der Server für alle durch einen Client versandten E-Mail-Nachrichten Lesebestätigungen anfordert. Diese Option ist per Voreinstellung abgeschaltet.

Vom Absender angeforderte Lesebestätigung senden, sobald Nachricht als gelesen gekennzeichnet ist
Diese Option bewirkt, dass der Server Anforderungen von Lesebestätigungen beachtet und die Lesebestätigungen dann versendet, wenn eine Nachricht durch den Client als gelesen gekennzeichnet wird. Diese Option ist per Voreinstellung abgeschaltet.

Unter dem in der Antwortadresse (ReplyTo) angegebenen Alias senden
Manche Clients gestatten den Absendern nicht den Versand von E-Mail-Nachrichten unter einem Alias. Dieses Leistungsmerkmal wurde im der Version 16.x des Protokolls Exchange ActiveSync (EAS) 434 erstmals unterstützt, aber manche Clients unterstützen die Version 16.x nicht. So nutzt beispielsweise Microsoft Outlook für Windows nur EAS 14.0 und gestattet zwar den Benutzern die Angabe einer anderen Adresse, unter der eine Nachricht versandt werden soll, aber die dann erstellte Nachricht gibt die Auswahl des Benutzers nicht richtig wieder. Diese Option gestattet die Nutzung des Feldes für die Antwortadresse (ReplyTo) zum Versand von Nachrichten dann, wenn als Antwortadresse ein gültiger Alias 827 des Benutzers eingetragen ist. Die globale Option ist per Voreinstellung aktiv.

Öffentliche Kontakte virtuell mit den Standard-Kontakten zusammenführen
Diese Option bewirkt, dass die öffentlichen Kontakte und die Standard-Kontakte der Benutzer auf ihren Geräten als zusammengeführt dargestellt werden. Die Datenbestände der Kontakte bleiben hierbei getrennt; es werden also keine Kontakte zwischen den Kontaktordnern der Benutzer kopiert. Diese Option kann insbesondere für solche Clients hilfreich sein, die das Durchsuchen der Globalen Adressliste (GAL) nicht unterstützen. Diese Option ist per Voreinstellung abgeschaltet.

Absender sperren, wenn Nachricht in Ordner Junk-Email verschoben wird
Ist diese Option aktiv, so wird die Absender-Adresse (Felder Sender und From) einer E-Mail-Adresse in den Kontaktordner für gesperrte Absender eingetragen, sobald ein Client die zugehörige E-Mail-Nachricht in den Ordner für Spam-Nachrichten verschiebt.

Antworten auf Besprechungsanfragen nach Zusage, Ablehnung usw. zwingend senden
Ist diese Option aktiv, so versendet der ActiveSync-Dienst eine Antwort an den Besprechungsorganisator immer dann, wenn ein Client auf eine Besprechungseinladung zusagt, sie ablehnt oder eine sonstige Aktion für die Einladung ausführt. Diese Option ist für solche Clients nützlich, die solche Antworten nicht selbst richtig senden.

Vorschau auf tatsächlich wirksame Einstellungen

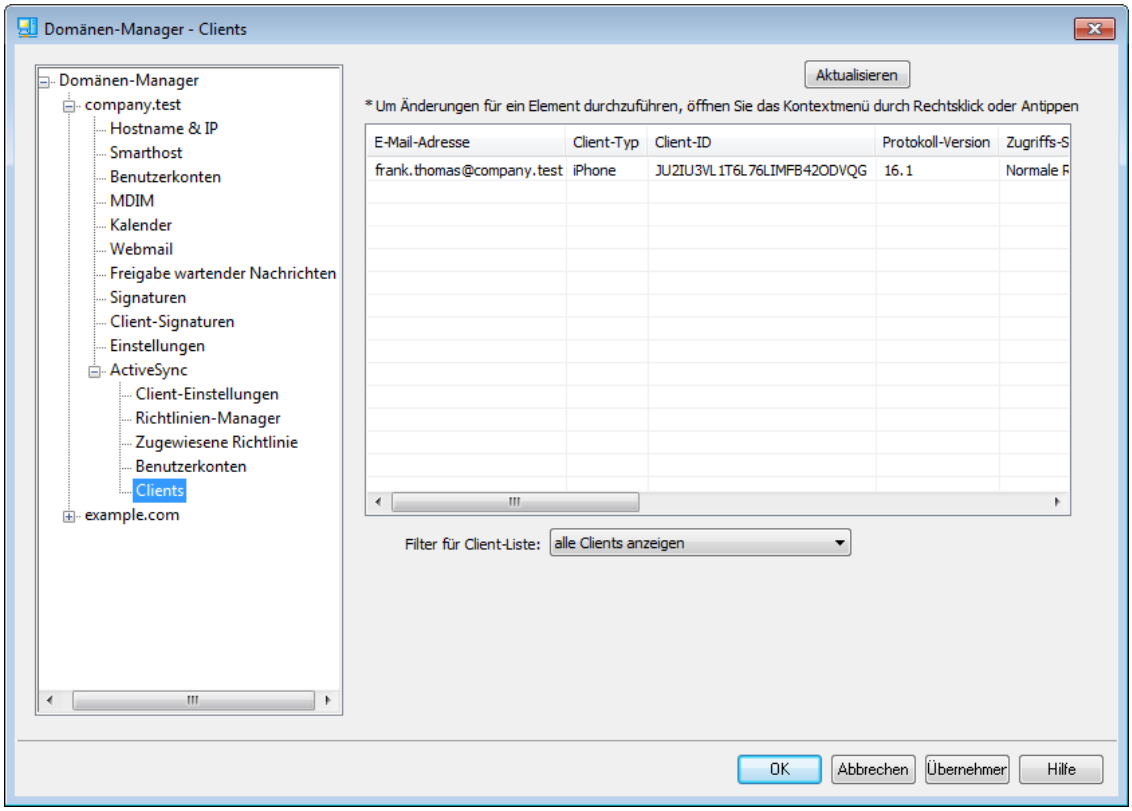
Dieses Steuerelement ist auf allen untergeordneten Konfigurationsdialogen für die

Client-Einstellungen (Domänen 437, Benutzerkonten 454 und Clients 464) verfügbar. Per Voreinstellung werden die Optionen auf diesen Konfigurationsdialogen nicht von den übergeordneten Konfigurationsdialogen geerbt. Sie können sich daher mithilfe dieses Steuerelements die Einstellungen anzeigen lassen, die auf den jeweils gerade dargestellten Konfigurationsdialog wirken.

Siehe auch:

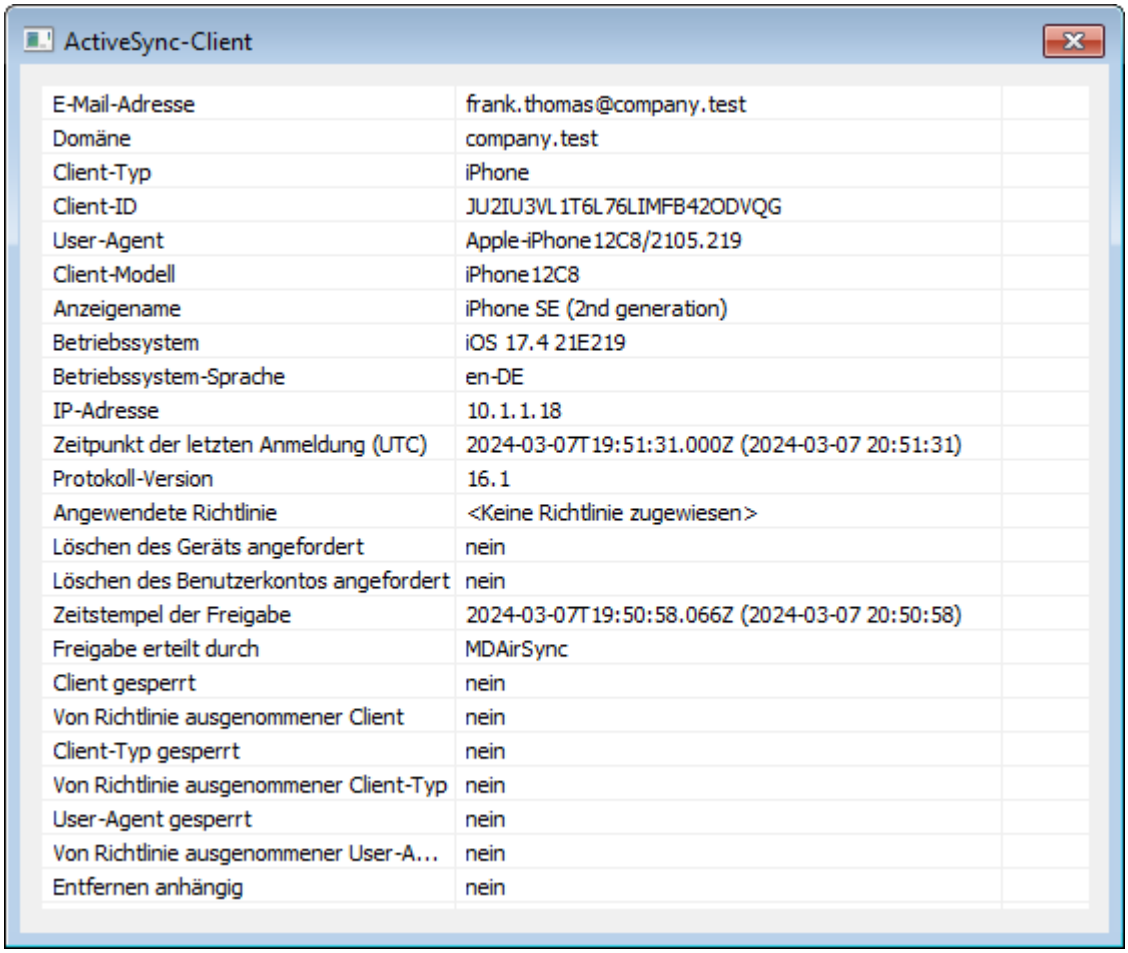
ActiveSync » Client-Einstellungen 422
ActiveSync » Domänen 437
ActiveSync » Clients 464

3.2.11.5 Clients



In diesem Konfigurationsdialog finden Sie einen Eintrag für jedes ActiveSync-Endgerät, das mit der gerade bearbeiteten Domäne verbunden ist.

Details zu ActiveSync-Clients



Um Detailinformationen über Endgeräte einzusehen, wählen Sie den Eintrag für das Endgerät aus, und klicken Sie dann auf **Details**, oder klicken Sie doppelt auf den Eintrag des Endgeräts. In dem Konfigurationsdialog Details können Sie Informationen über das Gerät einsehen, dem Gerät Richtlinien zuweisen, seine Client-Einstellungen bearbeiten und das Gerät in den Sperrlisten und Freigabelisten[429] erfassen.

Geräte-Einstellungen

Um die Einstellungen für ein Gerät zu bearbeiten, wählen Sie das Gerät aus, und klicken Sie auf **Einstellungen**. Per Voreinstellung werden diese Einstellungen aus den Client-Einstellungen des zugehörigen Benutzerkontos[454] geerbt. Nähere Informationen finden Sie weiter unten unter Verwalten der Client-Einstellungen eines Geräts.

Zuweisen einer ActiveSync-Richtlinie

Um einem Gerät eine Richtlinie[445] zuzuweisen, gehen Sie folgendermaßen vor:

1. Führen Sie auf dem Eintrag des gewünschten Geräts in der Übersicht einen Rechtsklick aus.
2. Klicken Sie auf **Richtlinie anwenden**. Hierdurch wird der Konfigurationsdialog Richtlinie zuweisen aufgerufen.
1. Wählen Sie aus dem Auswahlmenü der **zuzuweisenden Richtlinien** die gewünschte Richtlinie aus.

3. Klicken Sie auf **OK**.

Statistik

Um Statistikdaten für ein Gerät einzusehen, führen Sie einen Rechtsklick auf dem Eintrag des gewünschten Geräts aus, und klicken Sie danach auf **Statistiken anzeigen**. Es öffnet sich die Übersicht Client-Statistik, auf der verschiedene Daten zur Nutzungsstatistik des Geräts einsehbar sind.

Statistik zurücksetzen

Um die Statistikdaten für ein Gerät zurückzusetzen, führen Sie auf dem Eintrag des gewünschten Geräts einen Rechtsklick aus, und klicken Sie danach auf **Statistiken zurücksetzen.** Bestätigen Sie die anschließenden Sicherheitsabfrage durch Anklicken von **OK**.

Entfernen eines ActiveSync-Clients

Um einen ActiveSync-Clients zu entfernen, führen Sie einen Rechtsklick auf dem Eintrag des gewünschten Clients aus, und klicken Sie danach auf **Löschen**. Beantworten Sie die anschließende Sicherheitsabfrage mit **Ja**. Hierdurch werden der Client aus der Liste entfernt und alle Informationen zur Synchronisierung aus MDaemon gelöscht. Führt der entfernte Client später noch einmal eine Synchronisierung über ActiveSync auf dem Server durch, dann behandelt MDaemon den Client so, wie wenn er auf dem Server noch nie verwendet worden wäre. Alle Gerätedaten müssen dann mit MDaemon neu synchronisiert werden.

Vollständiges Löschen eines ActiveSync-Clients

Ist dem ausgewählten ActiveSync-Client eine Richtlinie 445 zugewiesen, und hat der Client die Richtlinie übernommen und entsprechend geantwortet, dann kann dieser Client ferngesteuert vollständig gelöscht werden. Um den Client vollständig zu löschen, führen Sie auf dem Client einen Rechtsklick aus (bei Nutzung der MDaemon-Remoteverwaltung wählen Sie den Client aus), und klicken Sie danach auf **Gerät löschen**. Sobald der Client das nächste Mal eine Verbindung zu MDaemon herstellt, übermittelt MDaemon den Löschbefehl an den Client und fordert ihn auf, sich in den Auslieferungszustand zurückzusetzen. Je nach Client kann dies zur Löschung aller Inhalte, auch etwa installierter Apps, führen. Solange der ActiveSync-Eintrag für den Client besteht, übermittelt MDaemon den Löschbefehl auch bei jedem späteren Verbindungsaufbau erneut. Falls Sie den Client löschen wollen, tragen Sie ihn zunächst in die Sperrliste 429 ein, damit er künftig keine Verbindungen mehr zu MDaemon herstellen kann. Wird ein gelöschtes Endgerät beispielsweise wiedergefunden, und soll er wieder Verbindungen zum Server herstellen können, dann wählen Sie das Gerät aus, und klicken Sie auf **Löschvorgänge abbrechen**. Entfernen Sie das Gerät außerdem aus der Sperrliste.

Daten aus dem Benutzerkonto eines ActiveSync-Clients löschen

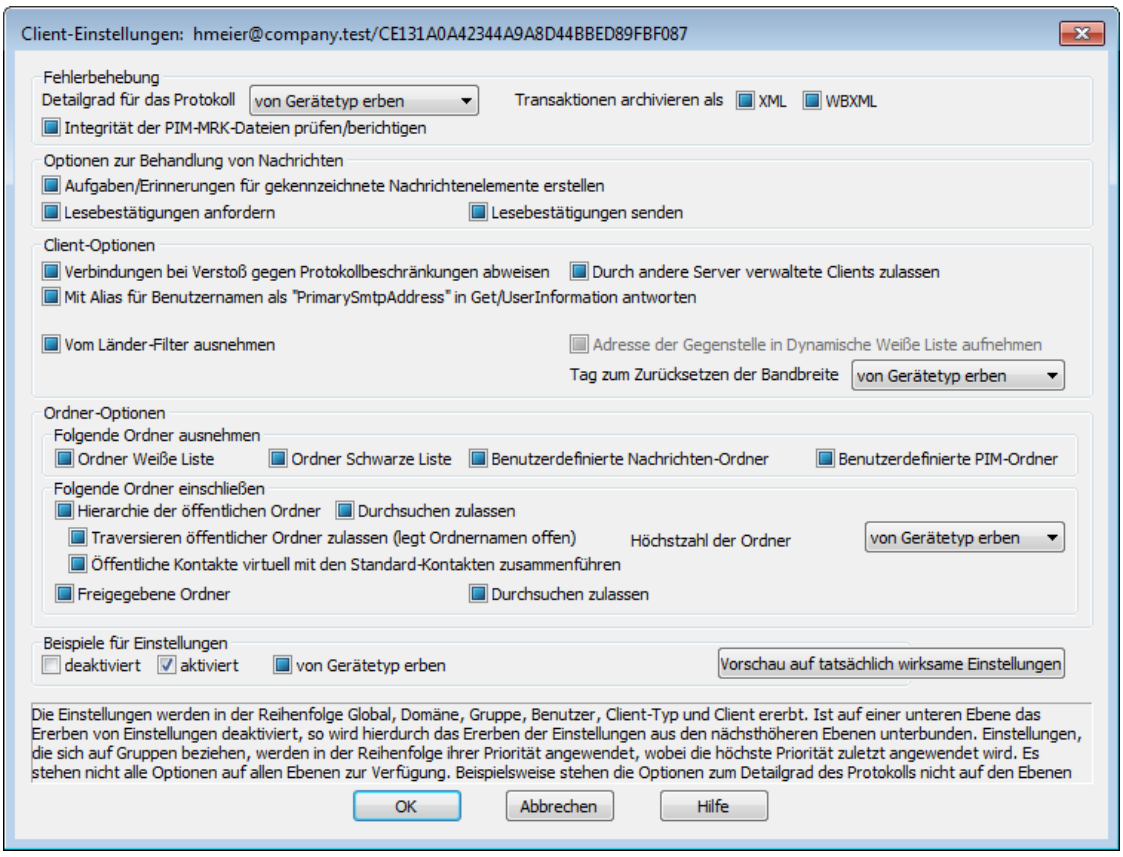
Um die Nachrichten und PIM-Daten von einem Client oder Endgerät zu löschen, führen Sie auf dem Eintrag des gewünschten Geräts einen Rechtsklick aus, und klicken Sie danach auf **Nachrichten des Benutzerkontos und PIM-Elemente vom Client löschen**. Dieser Löschvorgang ist dem vollständigen Löschen eines ActiveSync-Clients ähnlich, das weiter oben beschrieben ist. Es werden aber nicht alle Daten des Clients gelöscht, sondern es werden nur die Daten des Benutzerkontos entfernt, wie etwa E-Mail-Nachrichten, Kalendereinträge, Kontakte und ähnliche Daten. Alle anderen Daten, wie Apps, Fotos und Musik, bleiben unverändert.

Client freigeben

Ist im Konfigurationsdialog ActiveSync - Client-Einstellungen 422 die Option "*Neue Clients müssen durch Administrator freigegeben werden*" aktiv, so können Sie mit diesem Steuerelement Clients freigeben, Wählen Sie dazu den gewünschten Client aus, und klicken Sie danach auf **Client zur Synchronisierung berechtigen**. Nach der Freigabe kann sich der Client mit dem Server synchronisieren.

Verwalten der Client-Einstellungen eines Geräts

Die Client-Einstellungen für einzelne Geräte gestatten Ihnen die Verwaltung der Client-Einstellungen für bestimmte einzelne Endgeräte.



Per Voreinstellung werden alle Optionen in diesem Konfigurationsdialog vom übergeordneten Knoten geerbt, oder es werden die Standardeinstellungen verwendet. Im Falle der Client-Einstellungen ist der übergeordnete Knoten das Benutzerkonto, dem das Gerät zugeordnet ist. Seine Client-Einstellungen werden im Konfigurationsdialog Client-Einstellungen 454 des Benutzerkontos konfiguriert, dem das Gerät zugeordnet ist. Änderungen, die Sie in diesem Konfigurationsdialog vornehmen, übergehen die auf Client-Ebene festgelegten Einstellungen für dieses Gerät.

Allgemeines

Fehlerbehebung

Detailgrad für das Protokoll

ActiveSync für MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten

Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Einstellung erben Per Voreinstellung wird die Einstellung für den Detailgrad aus der Hierarchie der Client-Einstellungen vom jeweils übergeordneten Knoten ererbt. Clients übernehmen dabei die Einstellung aus dem jeweiligen Client-Typ, Client-Typen übernehmen die Einstellung von den Benutzerkonten, Benutzerkonten übernehmen die Einstellung von den Gruppen, und so weiter. Die globale Einstellung für alle Clients wird durch die Einstellung für den Detailgrad im Konfigurationsdialog Diagnose 432 bestimmt.

Transaktionen archivieren als [XML | WBXML]
Mithilfe der Optionen *XML...* und *WBXML...* können Sie die zugehörigen Daten speichern; diese Daten können die Fehlersuche erleichtern. Die systemweit wirksamen Optionen sind per Voreinstellung abgeschaltet.

Integrität der PIM-MRK-Dateien prüfen/berichtigen
Diese Option führt für die PIM-Daten der betroffenen Clients Prüf- und Korrekturvorgänge durch. Sie sollen bekannte Probleme erkennen, die eine ordnungsgemäße Synchronisierung verhindern können. Zu diesen Problemen zählen insbesondere doppelte iCal-UIDs und leere Datenfelder, die eigentlich verpflichtend Daten enthalten müssen. Die systemweit wirksame Option ist per Voreinstellung abgeschaltet.

Client-Optionen

Verbindungen bei Verstoß gegen Protokollbeschränkungen abweisen
Diese Option bewirkt, dass Verbindungen von Clients abgewiesen werden, falls sie versuchen eine nicht für die Clients *Zugelassene Protokollversion* zu verwenden. Per Voreinstellung ist diese Option abgeschaltet; dies bedeutet, dass die Protokollbeschränkung keine Verbindungen solcher Clients verhindern, die andere als die zugelassenen Protokollversionen verwenden. Solange die Option abgeschaltet ist, weist MDaemon die Clients zwar an, nur die zugelassenen Protokollversionen zu verwenden, lässt aber bei Nutzung anderer Protokollversionen die Verbindung trotzdem zu. Nähere Informationen finden Sie

unter Protokollbeschränkungen 434.

Mit Alias für Benutzernamen als "PrimarySmtpAddress" in Get/UserInformation antworten
Diese Option gestattet es dem Dienst, als Antwort auf eine Anforderung Settings/Get/UserInformation eine etwa vorhandene Alias-Adresse oder eine sekundäre Adresse des betroffenen Benutzerkontos als primäre Adresse zu übermitteln. Hierdurch wird ein Problem umgangen, das mit einer iOS-Aktualisierung nach Version 9.x verursacht wird, und das verhinderte, dass Clients unter einer etwa vorhandenen Alias-Adresse Nachrichten versenden konnten. Die Nutzung dieser Option bewirkt eine nicht standardkonforme Antwort auf die Anforderung Settings/GetUserInformation.

Neue Clients müssen durch Administrator freigegeben werden
Diese Option bewirkt, dass neue Clients sich erst dann mit Benutzerkonten synchronisieren können, wenn sie zunächst durch einen Administrator freigegeben wurden. In der Liste der Clients 464 sind alle Clients aufgeführt, die noch die Freigabe erwarten, und die Administratoren können sie über diese Liste freigeben. Diese Option ist per Voreinstellung abgeschaltet.

Höchstzahl der Clients je Benutzer
Mithilfe dieser Option können Sie die Anzahl der ActiveSync-Clients und -Endgeräte begrenzen, die mit jedem MDaemon-Benutzerkonto verknüpft sein können. Der hier angegebene Wert ist die Höchstzahl zulässiger Clients. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt. Diese Option steht nur in den Client-Einstellungen auf globaler, Domänen- und Benutzerebene zur Verfügung, nicht jedoch in den Client-Einstellungen für die einzelnen Clients.

Tag zum Zurücksetzen der Bandbreite
Mithilfe dieser Option können Sie Tag bestimmen, an dem in jedem Monat die Bandbreiten-Nutzungsstatistik für die ActiveSync-Endgeräte zurückgesetzt wird. Dieser Vorgang wird während der normalen Bereinigungsvorgänge um Mitternacht aufgeführt und, wie auch andere Bereinigungsvorgänge, in das Protokoll System eingetragen. Der globale Wert lautet per Voreinstellung 0 (nicht zurücksetzen), sodass per Voreinstellung die Nutzungsstatistik nicht zurückgesetzt wird. Für untergeordnete Knoten können Sie abweichende Einstellungen treffen, etwa, um die Einstellung an den Tag anzugleichen, an dem für das betroffene Endgeräte ein neuer Abrechnungszeitraum des Netzbetreibers beginnt.

Sicherheit

Vom Länder-Filter ausnehmen
Wenn Sie diese Option in den Einstellungen eines ActiveSync-Clients aktivieren, kann das Endgerät den Länder-Filter 574 umgehen. Hierdurch kann ein berechtigter Benutzer auf sein Benutzerkonto über ActiveSync beispielsweise auch dann zugreifen, wenn er sich in einem Land befindet, für das Versuche zur Echtheitsbestätigung ansonsten durch den Länder-Filter unterbunden werden. Ein Endgerät kann nur dann vom Länder-Filter ausgenommen sein, wenn es innerhalb des durch die Option Inaktive Clients entfernen nach [x] Tagen 418 im Abschnitt Anpassung bestimmten Zeitraums eine echtheitsbestätigte Verbindung über ActiveSync erfolgreich hergestellt hat.

Adresse der Gegenstelle in Dynamische Freigabeliste aufnehmen
Wenn Sie ein Endgerät vom Länder-Filter ausnehmen, können Sie durch

Aktivieren dieser Option die IP-Adresse, von der aus das Endgerät die Verbindung herstellt, in die Freigabeliste eintragen lassen. Hierdurch können beispielsweise andere Clients, die von der selben IP-Adresse aus eine Verbindung herstellen, ebenfalls zugelassen werden.

Durch andere Server provisionierte/verwaltete Clients zulassen
Per Voreinstellung dürfen Clients auch dann Verbindungen zu MDaemon aufbauen, wenn sie auf die Übermittlung der Provisionierungs- und Richtliniendaten durch den ActiveSync-Server hin melden, dass sie auch durch einen oder mehrere andere ActiveSync-Server verwaltet werden. Bei einer solchen Mehrfachverwaltung kann es nicht sichergestellt werden, dass alle auf Ihrem System bestehenden Richtlinien durch den Client auch umgesetzt werden; dies gilt insbesondere dann, wenn sie Richtlinien des anderen ActiveSync-Servers widersprechen. In vielen Fällen setzen die Clients die am stärksten einschränkende Richtlinie um, falls mehrere einander widersprechende Richtlinien vorhanden sind. Um Verbindungen von Clients zu unterbinden, die durch andere ActiveSync-Server verwaltet werden, deaktivieren Sie diese Option.

Löschen der Clients (Zurücksetzen in den Auslieferungszustand) nicht zulassen
Wenn diese Option aktiv ist, dann können ActiveSync-Clients nicht in den **Auslieferungszustand zurückgesetzt** und damit vollständig gelöscht werden. Wenn Sie Clients ferngesteuert in den Auslieferungszustand zurücksetzen wollen, müssen Sie diese Option deaktivieren. Diese Option ist per Voreinstellung deaktiviert. Nähere Informationen finden Sie auf der Seite Clients im Abschnitt **Vollständiges Löschen eines ActiveSync-Clients** 464.

Optionen zur Ordner-Synchronisierung

Optionen zur Ordner-Synchronisierung

Folgende Ordner ausnehmen

Freigegebene Absender/Gesperrte Absender
Per Voreinstellung werden die Kontaktordner mit Freigabelisten und Sperrlisten der Benutzer nicht mit den Geräten synchronisiert. Diese Ordner dienen üblicherweise nur in MDaemon zum Erkennen und Filtern von Spam. Ihre Inhalte brauchen daher nicht auf den Geräten als Kontakte angezeigt zu werden.

Benutzerdefinierte Nachrichten-Ordner
Per Voreinstellung können alle Standard- und benutzerdefinierten Nachrichten-Ordner mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-Nachrichtenordner synchronisiert werden können. Die Standard-Nachrichtenordner sind insbesondere Posteingang, Gesendete Objekte, Gelöschte Objekte und Entwürfe. Ordner, die die Benutzer selbst anlegen, werden dann nicht mehr synchronisiert. Diese Option ist per Voreinstellung abgeschaltet.

Benutzerdefinierte PIM-Ordner
Per Voreinstellung können alle PIM-Ordner (insbesondere Kontakte, Kalender, Notizen und Aufgaben) mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-PIM-Ordner synchronisiert werden können. Ist diese Option aktiv, so wird beispielsweise für jeden Benutzer nur der Standard-Kalender synchronisiert, auch wenn er über mehrere Kalender-

Ordner verfügt. Diese Option ist per Voreinstellung abgeschaltet.

Folgende Ordner einschließen

Hierarchie der öffentlichen Ordner
Diese Option bewirkt, dass die öffentlichen Ordner[309], auf die die Benutzer Zugriff haben, in den Ordnerlisten der Benutzer auf ihren ActiveSync-Geräten erscheinen. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der öffentlichen Ordner[309], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Traversieren öffentlicher Ordner zulassen (legt Ordnernamen offen)
Benutzerkonten, die auf Unterordner in öffentlichen Ordnern zugreifen oder diese synchronisieren wollen, müssen per Voreinstellung sowohl für den betroffenen Unterordner als auch für alle ihm übergeordneten öffentlichen Ordner[309] über die Berechtigung Ordner anzeigen[311] verfügen. Fehlt einem Benutzerkonto diese Berechtigung für einen übergeordneten öffentlichen Ordner, so kann er auch den gewünschten Unterordner nicht synchronisieren und nicht auf ihn zugreifen, und zwar auch dann nicht, wenn das Benutzerkonto für diesen Unterordner selbst die erforderliche Berechtigung hat. Mithilfe dieser Option können Sie den Clients Zugriff auf und Synchronisierung von Unterordnern ermöglichen, ohne dass die Clients Berechtigungen für die übergeordneten öffentlichen Ordner haben. **Beachte:** Ist diese Option aktiv, so erlangt der Client zwangsläufig Kenntnis von den Namen der übergeordneten Ordner, auch wenn er für ihre Inhalte keine Zugriffsrechte hat. Hieraus kann sich ein Sicherheitsrisiko ergeben. Die Option ist per Voreinstellung abgeschaltet.

Höchstzahl zulässiger öffentlicher Ordner
Diese Option begrenzt die Zahl der öffentlichen Ordner, die auf den betroffenen Geräten dargestellt werden können. Ist eine solche Höchstzahl angegeben, dann übermittelt der Server so lange Einträge in der Ordnerliste, bis die Höchstzahl erreicht ist. Danach übermittelt der Server keine Ordner mehr an die Geräte. Die Reihenfolge, in der die Ordner dabei verarbeitet werden, kann weder festgelegt noch vorher bestimmt werden. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt.

Freigegebene Ordner
Diese Option nimmt auch die gemeinsam genutzten Ordner[122], auf die die Benutzer Zugriff haben, in die Ordnerlisten auf ihren ActiveSync-Geräten auf. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der freigegebenen Ordner[742], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Behandlung von Inhalten

Optionen zur Behandlung von Inhalten

Aufgaben/Erinnerungen für durch Clients gekennzeichnete Nachrichtenelemente erstellen
Diese Option ermöglicht es MDaemon, die Benutzer an gekennzeichnete Elemente zu erinnern. Hierzu wird für jede gekennzeichnete E-Mail-Nachricht eine Aufgabe erstellt, wenn der Client dies anfordert. Die globale Option für dieses Leistungsmerkmal ist per Voreinstellung aktiv.

Aktualisierung nach jeder Änderung der Besprechung senden
Manche Clients versenden aktualisierte Besprechungseinladungen nicht richtig, nachdem eine Besprechung geändert wurde. Diese Option bewirkt, dass der ActiveSync-Dienst immer dann aktualisierte Besprechungseinladungen sendet, wenn der Besprechungsorganisator eine Besprechung aktualisiert hat. Diese Option sollte nur für Clients 464 und Client-Typen 481 aktiviert werden, die die aktualisierten Besprechungseinladungen nicht richtig versenden, da sonst aktualisierte Besprechungseinladungen doppelt versandt werden. Aus diesem Grund ist diese Einstellung nur auf den Seiten Clients und Client-Typen verfügbar.

Lesebestätigung für alle versandten Nachrichten anfordern
Diese Option bewirkt, dass der Server für alle durch einen Client versandten E-Mail-Nachrichten Lesebestätigungen anfordert. Diese Option ist per Voreinstellung abgeschaltet.

Vom Absender angeforderte Lesebestätigung senden, sobald Nachricht als gelesen gekennzeichnet ist
Diese Option bewirkt, dass der Server Anforderungen von Lesebestätigungen beachtet und die Lesebestätigungen dann versendet, wenn eine Nachricht durch den Client als gelesen gekennzeichnet wird. Diese Option ist per Voreinstellung abgeschaltet.

Unter dem in der Antwortadresse (ReplyTo) angegebenen Alias senden
Manche Clients gestatten den Absendern nicht den Versand von E-Mail-Nachrichten unter einem Alias. Dieses Leistungsmerkmal wurde im der Version 16.x des Protokolls Exchange ActiveSync (EAS) 434 erstmals unterstützt, aber manche Clients unterstützen die Version 16.x nicht. So nutzt beispielsweise Microsoft Outlook für Windows nur EAS 14.0 und gestattet zwar den Benutzern die Angabe einer anderen Adresse, unter der eine Nachricht versandt werden soll, aber die dann erstellte Nachricht gibt die Auswahl des Benutzers nicht richtig wieder. Diese Option gestattet die Nutzung des Feldes für die Antwortadresse (ReplyTo) zum Versand von Nachrichten dann, wenn als Antwortadresse ein gültiger Alias 827 des Benutzers eingetragen ist. Die globale Option ist per Voreinstellung aktiv.

Öffentliche Kontakte virtuell mit den Standard-Kontakten zusammenführen
Diese Option bewirkt, dass die öffentlichen Kontakte und die Standard-Kontakte der Benutzer auf ihren Geräten als zusammengeführt dargestellt werden. Die Datenbestände der Kontakte bleiben hierbei getrennt; es werden also keine Kontakte zwischen den Kontaktordnern der Benutzer kopiert. Diese Option kann insbesondere für solche Clients hilfreich sein, die das Durchsuchen der Globalen Adressliste (GAL) nicht unterstützen. Diese Option ist per Voreinstellung abgeschaltet.

Absender sperren, wenn Nachricht in Ordner Junk-Email verschoben wird
Ist diese Option aktiv, so wird die Absender-Adresse (Felder Sender und From) einer E-Mail-Adresse in den Kontaktordner für gesperrte Absender eingetragen, sobald ein Client die zugehörige E-Mail-Nachricht in den Ordner für Spam-Nachrichten verschiebt.

Antworten auf Besprechungsanfragen nach Zusage, Ablehnung usw. zwingend senden
Ist diese Option aktiv, so versendet der ActiveSync-Dienst eine Antwort an den Besprechungsorganisator immer dann, wenn ein Client auf eine Besprechungseinladung zusagt, sie ablehnt oder eine sonstige Aktion für die Einladung ausführt. Diese Option ist für solche Clients nützlich, die solche Antworten nicht selbst richtig senden.

Vorschau auf tatsächlich wirksame Einstellungen

Dieses Steuerelement ist auf allen untergeordneten Konfigurationsdialogen für die Client-Einstellungen (Domänen 437, Benutzerkonten 454 und Clients 464) verfügbar. Per Voreinstellung werden die Optionen auf diesen Konfigurationsdialogen nicht von den übergeordneten Konfigurationsdialogen geerbt. Sie können sich daher mithilfe dieses Steuerelements die Einstellungen anzeigen lassen, die auf den jeweils gerade dargestellten Konfigurationsdialog wirken.

Siehe auch:

ActiveSync » Benutzerkonten 454
ActiveSync » Sicherheit 429

3.3 Gateway-Manager

Der Gateway-Manager ist erreichbar über die Menüeinträge `Einstellungen » Gateway-Manager...`. Diese Funktion stellt nützliche Verwaltungsoptionen für den Betrieb mehrerer Domänen sowie den Betrieb als Backup-Server zur Verfügung.

Folgendes Beispiel soll den Anwendungsbereich verdeutlichen:

Angenommen, Sie wollen als Backup-Server oder Ausfallsicherung für eine dritte Stelle arbeiten und dabei deren eingehende Nachrichten empfangen und in einem Ordner auf Ihrem Server ablegen. Sie wollen die Domäne der dritten Stelle aber nicht selbst betreiben und auch die einzelnen Benutzerkonten nicht betreuen. Im Beispiel lautet der Domänenname der dritten Stelle "`example.com`".

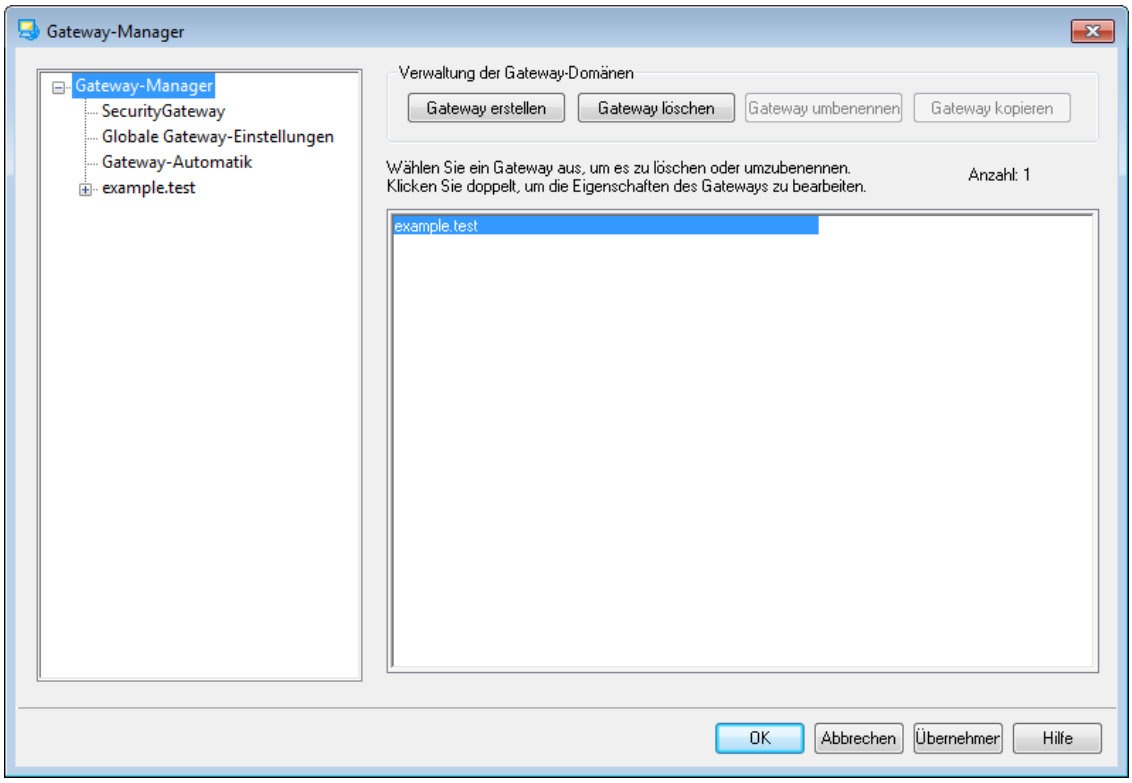
Sie klicken nun im Gateway-Manager auf *Gateway erstellen* und tragen den Namen "`example.com`" als *Domänennamen* ein. Danach wählen Sie den Speicherort, in dem die eingehenden Nachrichten für die Domäne abgelegt werden. Alle Nachrichten, die MDaemon für diese Domäne erhält, werden getrennt von den übrigen Nachrichten dort abgelegt, und zwar unabhängig den Empfängern, an die die Nachrichten gerichtet sind.

Als nächstes bestimmen Sie, auf welche Weise die Nachrichten an den eigentlichen E-Mail-Server der Domäne, der die Benutzerkonten unterhält, übermittelt werden sollen. Hierfür stehen zwei Möglichkeiten zur Verfügung: *Gespeicherte Nachrichten bei jedem Verarbeitungsdurchlauf für externe Nachrichten zustellen* im Konfigurationsdialog Domäne 257 und die Optionen zur Freigabe wartender Nachrichten 264. Sie können außerdem ein MDaemon-

Benutzerkonto anlegen und sein Nachrichtenverzeichnis[717] auf denselben Verzeichnispfad[257] verweisen lassen, den auch das Gateway benutzt.

Schließlich müssen Sie wahrscheinlich die DNS-Einträge der Domäne `example.com` so anpassen, dass Ihr MDaemon-Server als MX-Host für diese Domäne erscheint.

Es stehen für Gateways viele weitere Funktionen und Optionen zur Verfügung, aber das oben dargestellte Beispiel ist die Grundform eines Gateways. Es stehen jedoch auch Möglichkeiten zur Verfügung, atypische Anwendungsfälle abzudecken, etwa, wenn eine Domäne betrieben werden soll, obwohl sie im Internet offiziell gar nicht besteht, etwa "`company.mail`". Der Empfang von Nachrichten für ein eigentlich ungültigen Domänennamen ist möglich, falls der Domänenname innerhalb einer Adresse der Standard-Domäne[181] "verborgen" wird. Es können Adressen erstellt werden, die die Standard-Domäne durchlaufen und dann an den Gateway weitergeleitet werden. Ist der Name Ihrer Standard-Domäne beispielsweise `example.com`, und betreiben Sie einen Gateway für `company.mail`, so können Benutzer Nachrichten an "`bob@company.mail`" zustellen lassen, indem sie die Adresse "`bob{company.mail}@example.com`" als Empfängeradresse nutzen. Da "`example.com`" die registrierte Domäne ist, die durch MDaemon versorgt wird, wird diese Nachricht zunächst an MDaemon zugestellt. MDaemon setzt die Adresse dann in das Format "`bob@company.mail`" und stellt die Nachricht an den entsprechenden Gateway zu. Die einfachste Methode ist es natürlich, einen gültigen Domänennamen für das Gateway zu registrieren und seine DNS- und MX-Einträge auf `example.com` verweisen zu lassen.



Liste der Gateways

Im Navigationsbereich auf der linken Seite dieses Konfigurationsdialogs finden Sie die Liste Ihrer Gateways. Jeder Eintrag eines Gateways enthält Verknüpfungen mit den Abschnitten des Konfigurationsdialogs, in denen verschiedene Einstellungen für den Gateway getroffen werden. Hierüber ist auch der Zugriff auf die Globalen Gateway-Einstellungen[254] und die Gateway-

Automatik[255] möglich. Die Liste der Gateways auf der rechten Seite dieses Konfigurationsdialogs nutzen Sie zum Löschen und Umbenennen von Gateways. In dieser Liste können Sie die Gateways außerdem durch Doppelklick zum Bearbeiten in den Gateway-Editor laden.

Verwaltung der Gateway-Domänen

Gateway erstellen

Um einen neuen Gateway zu erstellen, klicken Sie auf **Gateway erstellen**, geben Sie im Dialogfenster *Gateway-Domäne erstellen/umbenennen* den Namen des Gateways ein (z.B. example.mail), und klicken Sie danach auf **OK**.

Der Name, den Sie hier eingeben, entspricht üblicherweise einem Domänennamen, der durch DNS-Server in die IP-Adresse des lokalen Systems aufgelöst wird, auf dem der Server ausgeführt wird. Er kann auch einem qualifizierten Aliasnamen entsprechen. Alternativ können Sie für den Gateway einen nur internen oder sonst nicht allgemein gültigen, nicht öffentlichen Domänennamen wählen (etwa "`company.mail`"). In einem solchen Fall müssen Sie allerdings die oben beschriebenen Verfahren zur Zuordnung des Domänennamens nutzen oder mithilfe des Inhaltsfilters die Nachrichten so bearbeiten, dass sie ihre Empfänger auch erreichen.

Gateway löschen

Um einen Gateway zu löschen, wählen Sie den Gateway in der Liste aus, klicken Sie danach auf **Gateway löschen**, und bestätigen Sie die Sicherheitsabfrage.

Gateway umbenennen

Um den Namen eines Gateways zu ändern, wählen Sie den Gateway aus der Liste aus, klicken Sie danach auf **Gateway umbenennen**, geben Sie im Dialogfenster *Gateway-Domäne erstellen/umbenennen* den neuen Namen des Gateways an, und klicken Sie schließlich auf **OK**.

Gateway kopieren

Um ein neues Gateway anzulegen und dabei die Einstellungen aus einem anderen Gateway zu übernehmen, wählen Sie das gewünschte Ursprungsgateway in der Liste aus, und klicken Sie auf *Gateway kopieren*. Geben Sie dann den Namen für das neue Gateway an.

Gateway-Editor

Der Gateway-Editor enthält die folgenden Konfigurationsdialoge:

Domäne[257]
In diesem Abschnitt können Sie den Gateway aktivieren und deaktivieren, das Verzeichnis zum Speichern von Nachrichten für den Gateway festlegen, und Einstellungen zur Zustellung von Nachrichten und zur Behandlung von Dateianlagen treffen.

Prüfung[259]
Ist der Server, der die externe Domäne versorgt, so eingerichtet, dass er die Daten über Postfächer, Aliasnamen und Mailinglisten an einen LDAP- oder Active-Directory-Server übermittelt, oder unterhält er einen Minger-Server für die Adressprüfung durch externe Gegenstellen, so können mithilfe der Einstellungen in diesem Abschnitt eingehende Nachrichten daraufhin geprüft werden, ob ihre Empfängeradressen gültig sind. Es lässt sich so vermeiden, dass alle Nachrichten

an den Domänen-Gateway als gültig betrachtet und angenommen werden müssen.

Weiterleitung 263
In diesem Abschnitt können eine Gegenstelle oder eine Adresse definiert werden, an die Nachrichten für die Domäne sofort nach Eingang weitergeleitet werden. Es wird dort auch festgelegt, ob Kopien der weitergeleiteten Nachrichten aufbewahrt werden sollen und auf welchem Port die Nachrichten weitergeleitet werden sollen.

Freigabe wartender Nachrichten 264
Die Einstellungen in diesem Abschnitt steuern, wie MDaemon auf ETRN- und ATRN-Befehle reagiert, die für diese Domäne eingehen und den Versand der gespeicherten Nachrichten auslösen sollen. Auch mehrere weitere Einstellungen zur Freigabe wartender Nachrichten werden hier konfiguriert.

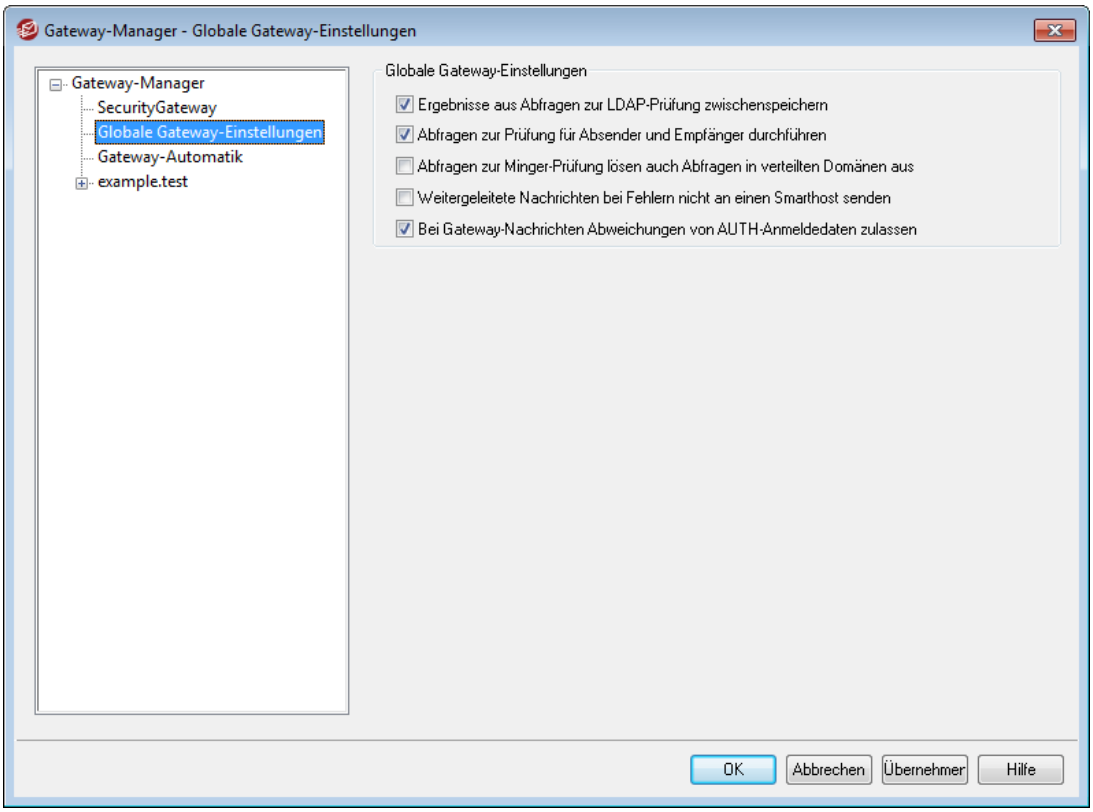
Kontingente 267
In diesem Abschnitt wird festgelegt, wie viel Speicherplatz die Domäne belegen darf und wie viele Nachrichten für sie höchstens vorgehalten werden dürfen.

Einstellungen 268
Dieser Abschnitt enthält einige weitere Einstellungen für den ausgewählten Domänen-Gateway. Insbesondere lassen sich AntiVirus- und AntiSpam-Prüfungen für den Gateway aktivieren und deaktivieren, Anforderungen für die Echtheitsbestätigung bei der Freigabe wartender Nachrichten definieren, ein Kennwort für die Echtheitsbestätigung einrichten und der Zugriff auf bestimmte IP-Adressen beschränken.

Siehe auch:

Globale Gateway-Einstellungen 254
Gateway-Automatik 255
Domänen-Manager 181

3.3.1 Globale Gateway-Einstellungen



Globale Gateway-Einstellungen

Die folgenden Einstellungen sind systemweit gültig; sie beziehen sich nicht nur auf den gerade bearbeiteten Gateway.

Ergebnisse aus Abfragen zur LDAP-Prüfung zwischenspeichern
Diese Option bewirkt, dass die Ergebnisse der Adressprüfung[259] durch LDAP im Cache zwischengespeichert werden und für einen begrenzten Zeitraum für neue Abfragen zur Verfügung stehen.

Abfragen zur Prüfung für Absender und Empfänger durchführen
Diese Option bewirkt, dass MDaemon sowohl Empfänger wie auch Absender der Nachrichten für diesen Gateway prüft, wenn die Optionen zur Prüfung[259] aktiv sind. Diese Option ist per Voreinstellung aktiv. Wird sie deaktiviert, so prüft MDaemon nur die Empfänger.

Abfragen zur Minger-Prüfung lösen auch Abfragen in verteilten Domänen aus
Diese Option wirkt sich bei der Nutzung von Minger[855] zur Adressprüfung durch Domänen-Gateways aus. Ist die Option aktiv, so löst jede Abfrage eines Minger-Servers, der im Konfigurationsdialog Prüfung[259] eingerichtet ist, gleichzeitig auch eine Abfrage der anderen Hosts aus, die verteilte Domänen[117] versorgen. Diese Option wirkt auf alle Gateways, die Minger zur Adressprüfung nutzen.

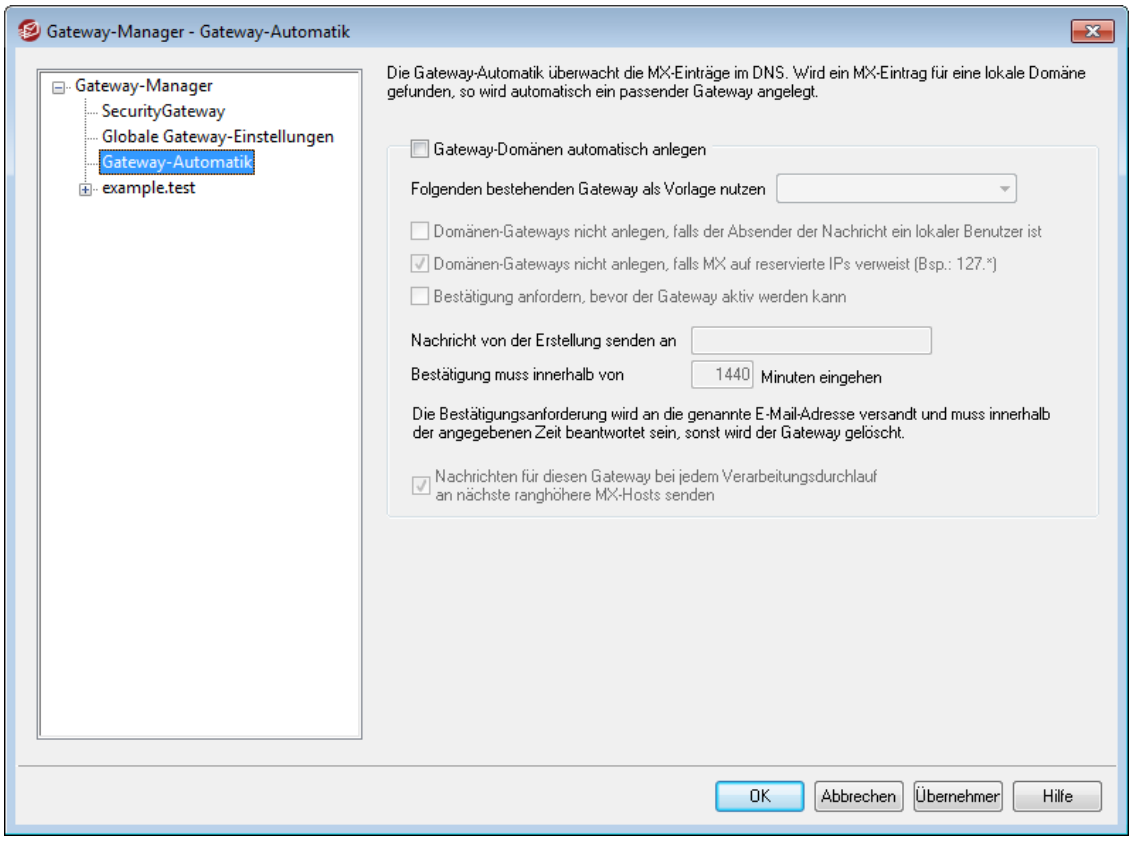
Weitergeleitete Nachrichten bei Fehlern nicht an einen Smarthost senden
Diese Option verhindert, dass weitergeleitete Nachrichten nach Fehlern in der Zustellung über einen Smarthost gesendet werden. Diese Option ist per Voreinstellung abgeschaltet.

Bei Gateway-Nachrichten Abweichungen von AUTH-Anmeldedaten zulassen
Diese Option bewirkt, dass Gateway.Nachrichten von den Anforderungen der folgenden beiden Optionen aus dem Konfigurationsdialog SMTP-Echtheitsbestätigung[524] ausgenommen sind: *Anmeldedaten müssen mit der Adresse aus dem Antwortpfad übereinstimmen* und *Anmeldedaten müssen mit der Adresse aus der Absenderkopfzeile "From:" übereinstimmen*. Um diese beiden Anforderungen auch auf Gateway-Nachrichten anzuwenden, deaktivieren Sie diese Option. Es kann dann allerdings zu Problemen bei Speicherung und Weiterleitung von Gateway-Nachrichten kommen.

Siehe auch:

Gateway-Manager[250]
Gateway-Editor » Prüfung[259]
Minger[855]
Verteilte Domänen[117]

3.3.2 Gateway-Automatik



Automatisches Anlegen von Gateways

Die Einstellungen in diesem Menü ermöglichen es MDaemon, automatisch einen neuen Domänen-Gateway für eine bislang unbekannte Domäne anzulegen, wenn eine Gegenstelle versucht, Post für diese Domäne an MDaemon zuzustellen und eine DNS-Abfrage ergibt, dass die IP-Adresse von MDaemon ein gültiger MX der bislang unbekannten Domäne ist.

Ein Beispiel hierzu:

Die IP-Adresse der Hauptdomäne von MDaemon ist `192.0.2.0`, und eine Nachricht für eine unbekannte Domäne mit dem Namen `example.com` wird per SMTP angeliefert. Ist die Gateway-Automatik aktiv, führt MDaemon eine Abfrage der MX- und A-Einträge für `example.com` durch, um festzustellen, ob `192.0.2.0` ein bekannter Mailserver (MX) für diese Domäne ist. Ergibt die Abfrage, dass die IP-Adresse von MDaemon ein gültiger MX-Eintrag für `example.com` ist, so legt MDaemon automatisch einen neuen Domänen-Gateway für diese Domäne an und nimmt entsprechende Nachrichten entgegen. Nachrichten an `example.com` werden dann in einem besonderen Verzeichnis abgelegt und, falls gewünscht, bei jedem Verarbeitungsdurchlauf für externe Post an den nächsten ranghöheren MX-Host übermittelt Mit dieser Funktion wird es möglich, den eigenen Server als Ausfallsicherung für eine andere Domäne einzusetzen, indem die IP-Adresse des eigenen Systems als alternativer MX-Eintrag für die andere Domäne in die DNS-Datenbank eingetragen wird.

Um diese Funktion zu sichern, kann MDaemon so konfiguriert werden, dass er eine Bestätigungsanforderung an eine wahlfrei festgelegte E-Mail-Adresse sendet. Während MDaemon danach auf die Bestätigung wartet, wird Post für die fragliche Domäne zwar entgegen genommen, jedoch nicht zugestellt. Die Bestätigung muss innerhalb einer vorher bestimmten Frist eingegangen sein; andernfalls werden der automatisch angelegte Gateway wieder entfernt, und alle gespeicherten Nachrichten gelöscht. Geht die Bestätigung fristgerecht ein, so werden die zwischengespeicherten Nachrichten normal zugestellt.

Böswillige Personen oder "Spammer" könnten diese Funktion missbrauchen, indem sie ihren DNS-Server so konfigurieren, dass er die IP-Adresse der angegriffenen MDaemon-Installation als einen seiner eigenen MX-Einträge ausweist. Die Gateway-Automatik muss daher mit Vorsicht eingesetzt werden. Um möglichen Missbrauch auszuschließen, empfiehlt es sich sehr, die Funktion *Bestätigung anfordern, bevor der Gateway aktiv werden kann* zu verwenden, wo immer es möglich ist.

Gateway-Domänen automatisch anlegen
Mit dieser Option richtet MDaemon neue Domänen-Gateways auf Grundlage der DNS-Abfrage automatisch ein.

Folgenden bestehenden Gateway als Vorlage nutzen
Aus diesem Rollmenü wird ein Domänen-Gateway ausgewählt, dessen Einstellungen MDaemon als Vorlage für alle zukünftig automatisch zu erstellenden Gateways nutzen wird.

Domänen-Gateways nicht anlegen, falls der Absender der Nachricht ein lokaler Benutzer ist
Diese Option verhindert, dass Nachrichten, die von lokalen Benutzern versandt werden, das automatische Anlegen eines Gateways auslösen.

Domänen-Gateways nicht anlegen, falls MX auf reservierte IPs verweist (Bsp.: 127.*)
Diese Option unterbindet das automatische Anlegen eines Gateways, falls der MX-Eintrag auf eine reservierte IP-Adresse verweist, wie etwa 127.*, 192.* und ähnliche.

Bestätigung anfordern, bevor der Gateway aktiv werden kann
Diese Option bewirkt, dass MDaemon eine Bestätigungsnachricht an eine vorher festgelegte E-Mail-Adresse sendet, um festzustellen, ob ein automatisch angelegter Gateway zulässig ist. MDaemon nimmt zwar Post für die fragliche Domäne zwar an, stellt sie aber bis zum Eintreffen der Bestätigung nicht zu.

Nachricht von der Erstellung senden an
Hier wird die Adresse eingetragen, an welche die Bestätigungsnachrichten versandt werden sollen.

Bestätigung muss innerhalb von [xx] Minuten eingehen
Diese Einstellung begrenzt die Zeit, für die MDaemon auf die Antwort auf eine versandt Bestätigungsnachricht wartet, auf die hier in Minuten angegebene Dauer. Wird diese Begrenzung überschritten, so wird der fragliche Gateway wieder gelöscht.

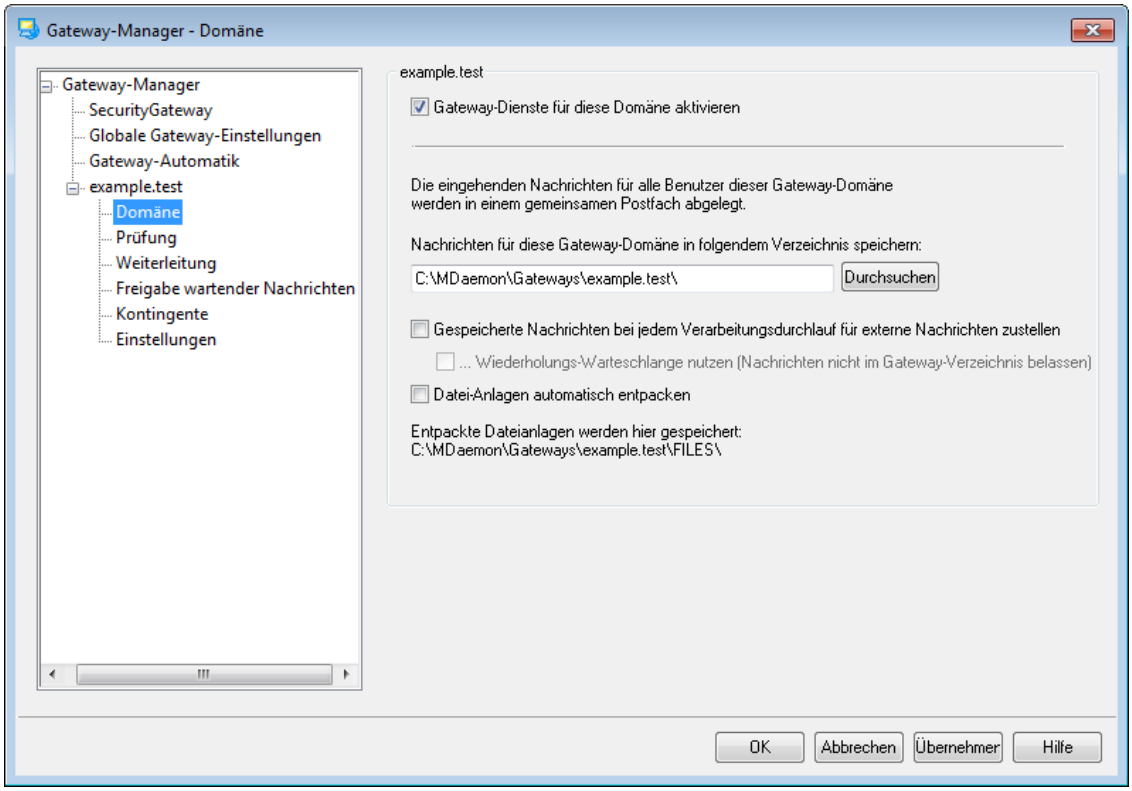
Nachrichten für diesen Gateway bei jedem Verarbeitungsdurchlauf an nächste ranghöhere MX-Hosts senden
Diese Option bewirkt, dass MDaemon die Nachrichten dieses Gateways bei jedem Verarbeitungsdurchlauf der Warteschlange für externe Nachrichten an den nächsten ranghöheren MX-Host übermittelt.

Siehe auch:

Gateway-Manager 250

3.3.3 Gateway-Editor

3.3.3.1 Domäne



Gateway-Domäne

Diesen Gateway aktivieren
Durch Aktivieren dieser Option aktivieren Sie auch den Domänen-Gateway.

Domänenname
Hier wird der Name der neuen Domäne eingetragen, für welche MDaemon als Gateway oder Empfänger für Nachrichten arbeiten soll.

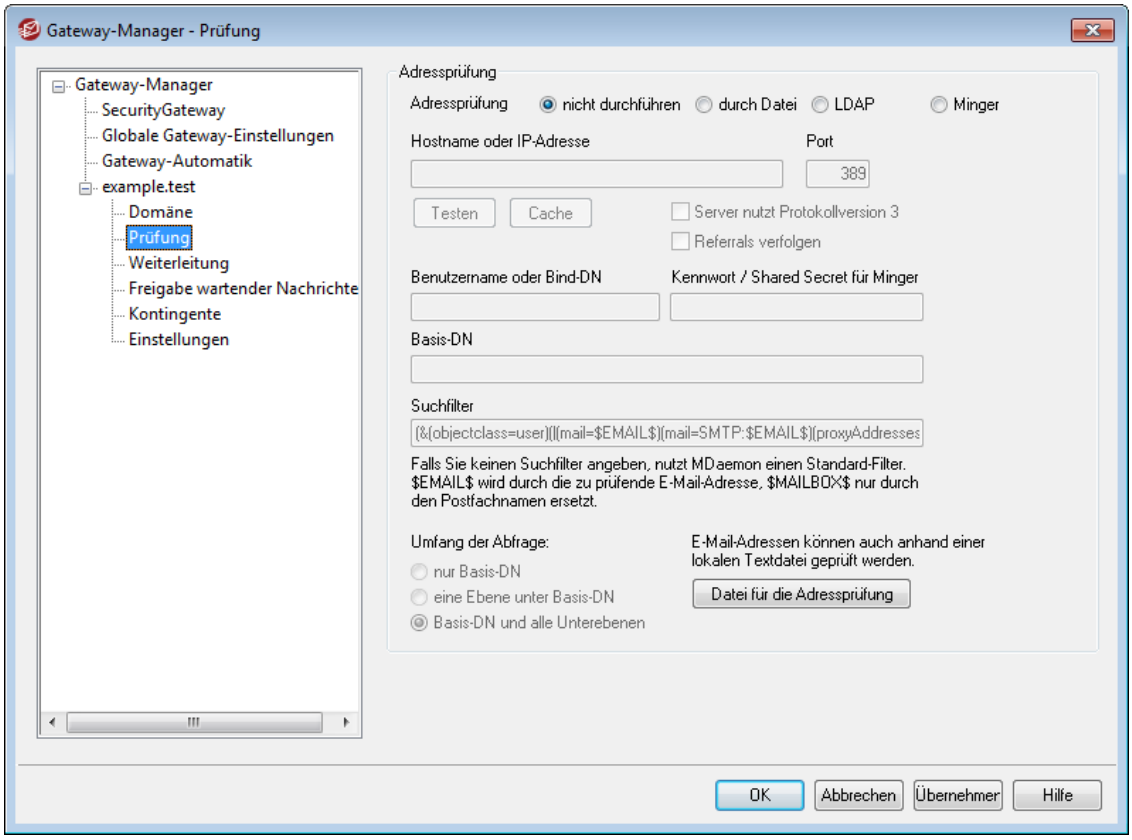
Nachrichten für diese Domäne hier speichern:
In diesem Verzeichnis wird die gesamte für diese Domäne eingehende Post gespeichert. Alle Nachrichten werden in demselben Verzeichnis gespeichert, unabhängig von den einzelnen Empfängern, an die die Nachrichten gerichtet sind.

Gespeicherte Nachrichten bei jedem Verarbeitungsdurchlauf für externe Nachrichten zustellen
MDaemon speichert üblicherweise Nachrichten, die an Domänen-Gateways gerichtet sind, bis der Gateway eine Verbindung herstellt und die Nachrichten abruft. Es kann jedoch gewünscht sein, dass MDaemon versucht, die Nachrichten direkt über SMTP zuzustellen, und nicht abwartet, bis sie abgeholt werden. Ist diese Option aktiv, so versucht MDaemon bei jedem Verarbeitungsdurchlauf für externe Post, die Nachrichten zuzustellen. Das Postfach des Gateways arbeitet dabei vorübergehend als externe Warteschlange. Nachrichten, die nicht zugestellt werden können, verbleiben im Postfach des Gateways, bis sie durch die Empfängerdomäne abgerufen oder über SMTP erfolgreich zugestellt wurden. Sie werden nicht in der Warteschlange für externe Post oder in der Wiederholungs-Warteschlange abgelegt. Falls Sie den DNS für die Gateway-Domäne jedoch nicht richtig eingerichtet haben, oder falls MDaemon alle abgehenden Nachrichten über einen Smarthost versendet, kann die Nutzung dieser Option dazu führen, dass die Nachrichten in einer Endlosschleife gefangen und schließlich als unzustellbar behandelt werden.

Wiederholungs-Warteschlange nutzen (Nachrichten nicht im Gateway-Verzeichnis belassen)
Mit dieser Option können Sie die Wiederholungs-Warteschlange 864 für die Zustellung der Nachrichten nutzen. Diese Option ist per Voreinstellung abgeschaltet; dies bedeutet, dass die Nachrichten im Ordner des Gateways abgelegt bleiben, auch wenn sie nicht zugestellt werden können.

Datei-Anlagen automatisch entpacken
Manche Mail-Server verlangen, dass Datei-Anlagen erst entpackt werden, bevor die Nachrichten in den Postweg gelangen dürfen. Um dieser Anforderung zu entsprechen, kann MDaemon eingehende Datei-Anlagen im MIME-Format automatisch auspacken und in dem Unterverzeichnis `\Files\` unterhalb des Nachrichten-Ordners der Domäne ablegen.

3.3.3.2 Prüfung



Ein weit verbreiteter Nachteil von Domänen-Gateways und Servern, die als Ausfallsicherung oder "Backup-Server" arbeiten, ist, dass sie üblicherweise nicht feststellen können, ob eine eingehende Nachricht an ein bestehendes Benutzerkonto gerichtet und damit zulässig ist oder nicht. Ein Beispiel hierzu: Trifft bei dem Backup-Server der Domäne `example.com` eine Nachricht für `user01@example.com` ein, so kann der Backup-Server nicht feststellen, ob auf dem Hauptserver der Domäne `example.com` tatsächlich ein Benutzerkonto, ein Aliasname oder eine Mailingliste für den Namen "user01" besteht. Der Backup-Server hat also nur die Möglichkeit, alle eingehenden Nachrichten anzunehmen. Da Spam-Versender Nachrichten oft an viele ungültige E-Mail-Adressen senden, kann die gezeigte Vorgehensweise zu einem sehr hohen Spam-Aufkommen auf dem Backup-Server führen.

MDaemon enthält Funktionen, mit deren Hilfe eine Prüfung solcher Adressen möglich ist. Ist der Server, der die außen liegende Domäne versorgt, so eingerichtet, dass er die Daten über Postfächer, Aliasnamen und Mailinglisten an einen LDAP- oder Active-Directory-Server übermittelt, oder unterhält er einen Minger-Server zur Prüfung von Adressen durch Dritte, so kann mithilfe der Einstellungen in diesem Konfigurationsdialog konfiguriert werden, wo sich der LDAP- oder Minger-Server befindet. Trifft nun im oben genannten Beispiel eine Nachricht für `example.com` ein, so kann der Server die Empfängeradresse anhand des außen liegenden Servers prüfen und feststellen, ob sie gültig ist.

Adressprüfung

Adressprüfung

nicht durchführen
Diese Option bewirkt, dass eine Adressprüfung für diesen Domänen-Gateway nicht durchgeführt wird. MDaemon geht bei allen für die Domäne eingehenden Nachrichten davon aus, dass sie an gültige Empfänger gerichtet sind. MDaemon kann dabei nicht feststellen, ob die Adressen in der Domäne wirklich gültig sind.

durch Datei
Diese Option bewirkt, dass die Datei `GatewayUsers.dat` als ausschließliche Datenquelle für die Prüfung genutzt wird, ob die Empfängeradressen eingehender Nachrichten in der Domäne gültig sind. Diese Liste bezieht sich auf alle Domänen-Gateways, enthält Empfänger aus allen diesen Gateways, und wird bei Auswahl eines anderen Prüfverfahrens als ergänzende Datenquelle für gültige E-Mail-Adressen herangezogen. Nur bei Auswahl des Prüfverfahrens durch Datei wird sie als alleinige und abschließende Datenquelle genutzt. Die Datei kann durch Anklicken des Steuerelements *Datei für die Adressprüfung* weiter unten aufgerufen und bearbeitet werden.

durch LDAP
Diese Option aktiviert die externe Kontenüberprüfung durch einen LDAP-Server oder ein Active Directory. Trifft eine Nachricht für die externe Domäne ein, so fragt MDaemon deren LDAP-Server oder Active Directory ab, um festzustellen, ob die Nachricht an einen gültigen Empfänger gerichtet ist. Ergibt die Prüfung, dass die Adresse nicht gültig ist, wird die Nachricht abgewiesen. Ist der LDAP- oder Active-Directory-Server nicht erreichbar, oder schlägt die Verbindung fehl, so nimmt MDaemon an, dass die Nachricht gültig ist.

durch Minger
Diese Option bewirkt, dass MDaemon den Minger-Server der Domäne abfragt, um die Empfängeradressen für die Domäne auf Gültigkeit zu prüfen. Kann MDaemon keine Verbindung mit dem Minger-Server herstellen, so nimmt MDaemon an, die Adresse sei gültig. Im Konfigurationsdialog Optionen[268] steht auch eine systemweit gültige Option zur Verfügung, die MDaemon veranlasst, auch die anderen Hosts für verteilte Domänen[117] abzufragen.

Hostname oder IP-Adresse
Hier müssen der Hostname oder die IP-Adresse des LDAP-, Active-Directory- oder Minger-Servers der externen Domäne eingegeben werden. MDaemon fragt diesen Server ab, um festzustellen, ob die Empfängeradressen der eingehenden Nachrichten in der externen Domäne, für die MDaemon als Gateway oder Backup-Server arbeitet, gültig sind.

Port
Hier wird der Port eingetragen, den der LDAP-, Active-Directory- oder Minger-Server der externen Domäne nutzt. MDaemon verwendet ihn zur Kontenüberprüfung über LDAP, Active Directory oder Minger.

Testen
Ein Klick auf dieses Steuerelement prüft, ob die Einstellungen zur externen Kontenüberprüfung gültig sind. MDaemon versucht dazu, eine Verbindung mit dem

angegebenen LDAP/AD-Server herzustellen und die angegebenen Daten abzufragen.

Cache
Ein Klick auf dieses Steuerelement öffnet den Cache für LDAP und Minger. Der Cache kann mithilfe einer Option im Konfigurationsdialog Optionen 268 aktiviert und deaktiviert werden.

Server nutzt Protokollversion 3
Diese Option bewirkt, dass für die Prüfung das LDAP-Protokoll der Version 3 genutzt wird.

Referrals verfolgen
Bisweilen ist auf einem LDAP-Server das eigentlich angeforderte Objekt nicht gespeichert; der Server kann aber über einen Verweis auf den Speicherort des Objekts verfügen und den Client dorthin verweisen. Diese Option bewirkt, dass während der Prüfung solche Verweise ausgewertet und verfolgt werden. Sie ist per Voreinstellung deaktiviert.

Benutzername oder Bind-DN
Hier wird der Benutzername oder eindeutige Name eingetragen, der auf dem LDAP-/AD-Server über Administratorrechte verfügt. MDaemon verwendet ihn, um die Empfängeradressen bei Nachrichten für die externe Domäne, für die MDaemon als Gateway oder Backup-Server arbeitet, auf Gültigkeit zu prüfen. Dieser DN wird bei den Bind-Vorgängen auch zur Echtheitsbestätigung genutzt.

Kennwort / Shared Secret für Minger
Dieses Kennwort wird zusammen mit dem Eintrag *Bind-DN* für die Anmeldung beim LDAP- oder Active-Directory-Server genutzt. Beim Zugriff auf einen Minger-Server wird es als Shared Secret genutzt.

Basis-DN
Hier wird der eindeutige Name oder Distinguished Name (DN) oder der Ausgangspunkt im Verzeichnisbaum (englisch "Directory Information Tree", kurz DIT) eingetragen, von dem aus MDaemon den LDAP-Server bei Adressüberprüfungen abfragt.

Suchfilter
Hier wird der LDAP- und Active-Directory-Suchfilter eingetragen, der bei der Abfrage im Rahmen der Adressprüfung eingesetzt wird. MDaemon richtet einen Standard-Suchfilter automatisch ein, der in den meisten Fällen funktionieren sollte.

Umfang der Abfrage:

Hier wird der Umfang der LDAP- und Active-Directory-Abfrage definiert.

nur Basis-DN
Diese Option begrenzt die Abfrage auf den oben angegebenen Basis-DN. Die Suche wird über diesen Punkt im DIT hinaus nicht ausgedehnt.

eine Ebene unter Basis-DN
Diese Option erstreckt die LDAP- und Active-Directory-Abfrage auf die Ebene unterhalb des angegebenen Basis-DN.

Basis-DN und alle Unterebenen
Diese Option erstreckt die LDAP-Abfrage auf den angegebenen Basis-DN und alle darunter liegenden Ebenen im DIT.

Datei für die Adressprüfung
Ein Klick auf dieses Steuerelement öffnet die Liste der für die Gateways gültigen E-Mail-Adressen, die in der Datei `GatewayUsers.dat` erfasst sind. Die Datei enthält eine Liste der Adressen, die MDaemon als gültige Empfänger für eingehende Nachrichten betrachtet, die an Gateway-Domänen gerichtet sind. Unabhängig von dem gewählten Prüfverfahren nutzt MDaemon diese Datei immer als zusätzliche Datenquelle für gültige Adressen. Nur bei Nutzung des Prüfverfahrens durch Datei nutzt MDaemon diese Datei als alleinige und abschließende Datenquelle für die Prüfung.

Nutzung mehrerer Konfigurationsdatensätze für LDAP-Abfragen zur Kontenprüfung

Sie können mehrere LDAP-Konfigurationen für die Prüfung der Benutzerkonten von Gateway-Domänen nutzen. Um weitere LDAP-Konfigurationsdatensätze anzulegen, müssen Sie die erste LDAP-Konfiguration normal durchführen und dann die Datei `GATEWAYS.DAT` einem Texteditor von Hand bearbeiten.

Die zusätzlichen Parametersätze müssen nach folgendem Muster angelegt und in die Datei eingetragen werden:

```
LDAPHost1=<Hostname>
LDAPPort1=<Port>
LDAPBaseEntry1=<Basis-DN>
LDAPRootDN1=<Root-DN>
LDAPObjectClass1=USER
LDAPRootPass1=<Kennwort>
LDAPMailAttribute1=mail
```

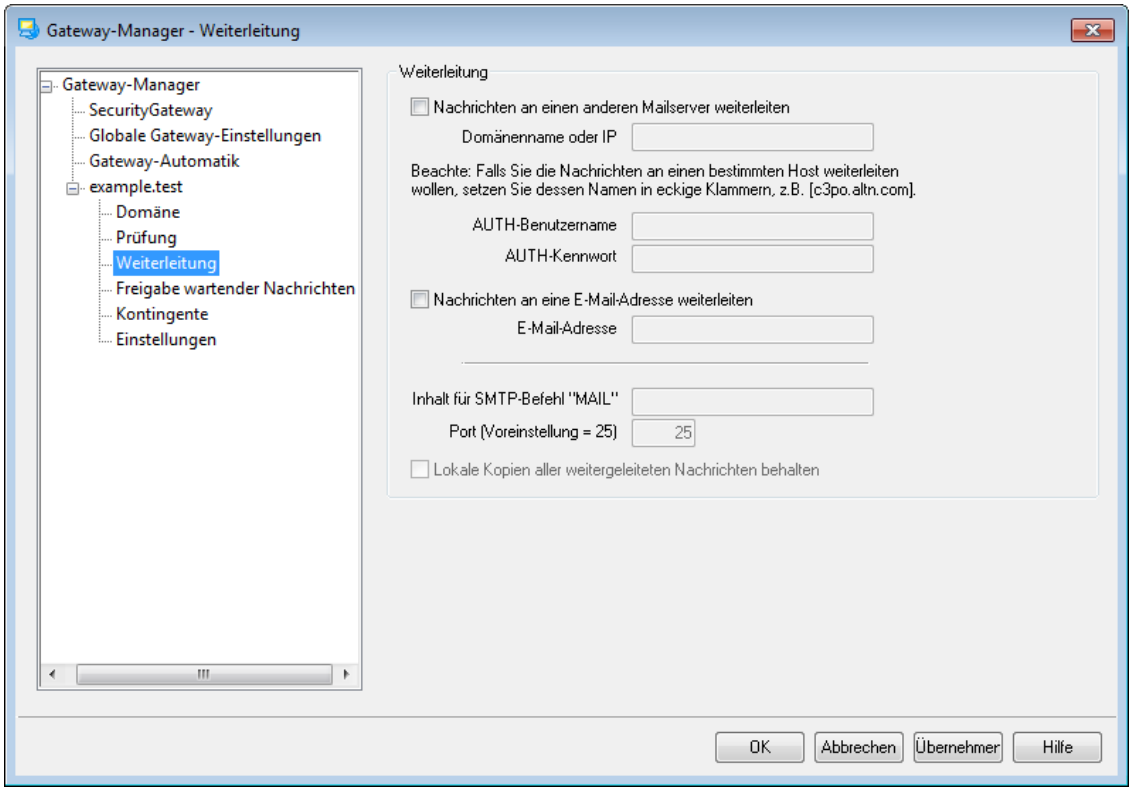
Für jeden neuen Datensatz muss der Zähler im Namen des jeweiligen Parameters um den Wert 1 erhöht werden. In dem Beispiel oben endet jeder Parameter auf 1. Beim nächsten Parametersatz muss jeder Parameter auf 2 enden, danach auf 3, und so weiter.

MDaemon führt mehrere LDAP-Abfragen nacheinander aus, bis ein Treffer gefunden wird. Tritt ein Fehler auf, oder werden keine Treffer gefunden, so werden keine weiteren Prüfungen durchgeführt.

Siehe auch:

Optionen zu LDAP/Adressbuch 824
Minger 855

3.3.3.3 Weiterleitung



Weiterleitung

Nachrichten an folgende Domäne weiterleiten
Manchmal ist es vorteilhaft, einfach alle Nachrichten für eine Domäne weiterzuleiten, sobald sie eintreffen. Soll MDaemon so verfahren, muss hier die IP-Adresse oder der Hostname des SMTP-Servers angegeben werden, an den die Post gesandt werden soll. Sollen die Nachrichten an einen bestimmten Host weitergeleitet werden, so muss dessen Name in eckige Klammern gesetzt werden (z.B. `[host1.example.net]`). Mithilfe der Optionen AUTH-Benutzername und AUTH-Kennwort können Sie die Anmeldedaten für den Server hinterlegen, an den Sie die Nachrichten weiterleiten wollen.

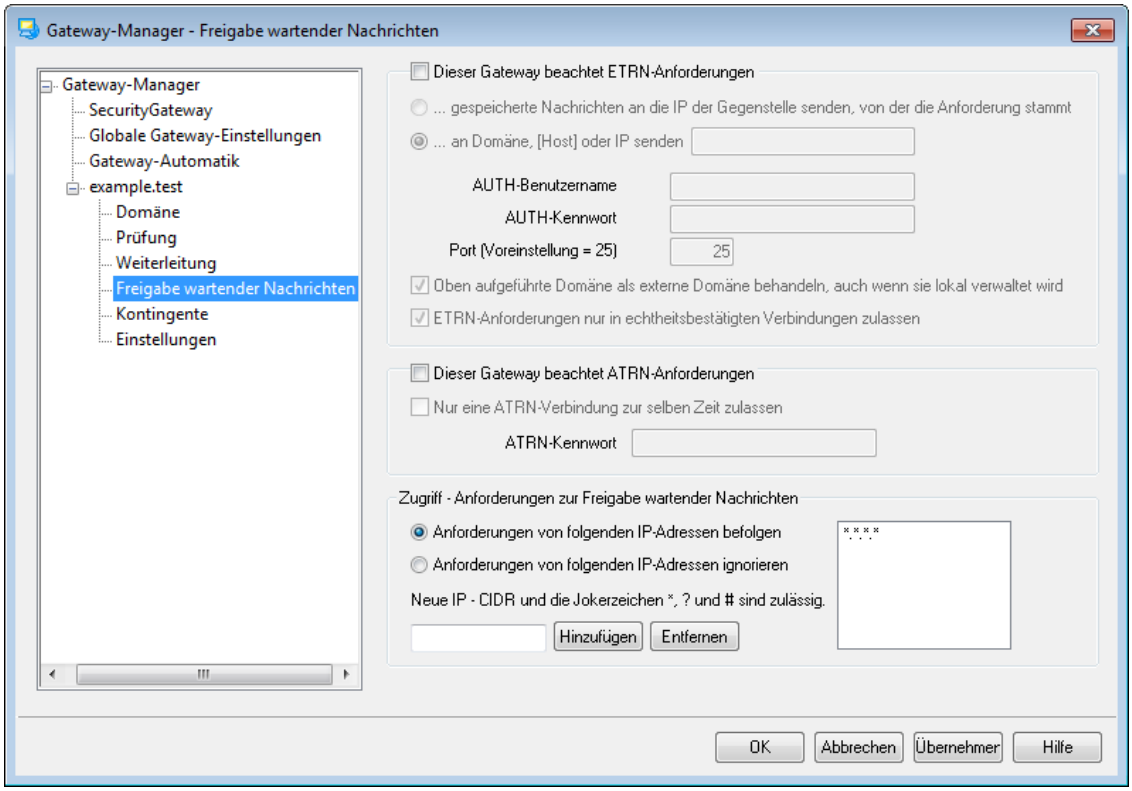
Nachrichten an eine E-Mail-Adresse weiterleiten
Sollen alle eingehenden Nachrichten für diese Client-Domäne direkt an eine bestimmte E-Mail-Adresse weitergeleitet werden, so ist diese hier anzugeben.

Inhalt für SMTP-Befehl "MAIL"
MDaemon verwendet diese Adresse für den SMTP-Befehl "Mail From" ("Nachricht von").

Port (Voreinstellung = 25)
MDaemon verwendet diese TCP-Portnummer zur Weiterleitung.

Lokale Kopien aller weitergeleiteten Nachrichten behalten
Mit dieser Option speichert MDaemon eine lokale Archiv-Kopie aller weitergeleiteten Nachrichten.

3.3.3.4 Freigabe wartender Nachrichten



ETRN

Dieser Gateway beachtet ETRN-Anforderungen
Wenn diese Option aktiv ist, beantwortet MDaemon ETRN-Befehle, die von geeigneten Gegenstellen für die Domäne übermittelt werden, für welche MDaemon als E-Mail-Gateway arbeitet. Der Befehl ETRN ist ein erweiterter SMTP-Befehl; er zeigt einem Server, der Post für eine bestimmte Domäne bereithält, an, dass der Versand dieser Post jetzt beginnen soll. Empfängt MDaemon einen solchen ETRN-Befehl für eine Domäne, sendet er sofort die gesamte Post, die für die betreffende Domäne bereit gehalten wird, über neue unabhängige SMTP-Verbindungen. Dabei ist wichtig, zu beachten, dass in der SMTP-Verbindung, in welcher der Befehl ETRN gesendet wurde, keine Post ausgetauscht wird. MDaemon stellt zum Nachrichtenversand neue unabhängige SMTP-Verbindungen her, damit die SMTP-Umschläge erhalten bleiben. Wichtig ist weiter, dass der Rechner, an den MDaemon die wartende Post sendet, vielleicht nicht sofort mit dem Nachrichtenempfang beginnen kann. ETRN stellt nur sicher, dass der Nachrichtenversand beginnen kann und dass die Nachrichten in die Warteschlange aufgenommen werden. Der Versand als solcher unterliegt denselben Beschränkungen, die der Systemverwalter für andere Nachrichten-Verarbeitungsdurchläufe festgelegt hat, und muss möglicherweise bis zum nächsten planmäßigen Verarbeitungsdurchlauf aufgeschoben werden. Wegen dieser Einschränkungen empfiehlt es sich, statt der Methode ETRN die Funktion On-Demand Mail Relay (ODMR) 201 und den dazu gehörenden Befehl ATRN zu verwenden. Diese Funktion wird allerdings nicht von allen Clients und Servern unterstützt und steht folglich nur dann zur Verfügung, wenn die Client-Domäne einen Server benutzt, der die Funktion anbietet. MDaemon unterstützt ODMR sowohl auf der Server- wie auch auf der Client-Seite ohne Einschränkungen.

MDaemon verlangt per Voreinstellung, dass eine Gegenstelle vor Übermittlung des Befehls ETRN erst über ESMTP-AUTH eine Echtheitsbestätigung durchführt. Die Gegenstelle muss dabei den *Domänennamen* 257 und das *ATRN-Kennwort* des Gateways als Anmeldedaten übermitteln. Falls Sie auf diese Echtheitsbestätigung verzichten wollen, können Sie im Abschnitt Optionen 268 die Option *Freigabe wartender Nachrichten über ETRN erfordert Echtheitsbestätigung* abschalten.

...gespeicherte Nachrichten an die IP der Gegenstelle senden, von der die Anforderung stammt
Diese Option bewirkt, dass MDaemon alle gespeicherten Nachrichten an die IP-Adresse sendet, von der der ETRN-Befehl ausging. Die Gegenstelle muss dabei als SMTP-Server arbeiten, damit sie die Nachrichten empfangen kann.

...an Domäne, [Host] oder IP senden
Hier wird der Hostname, der Domänenname oder die IP-Adresse angegeben, an welchen die gespeicherte Post nach einem erfolgreichen ETRN-Befehl gesendet werden soll. Die empfangende Gegenstelle muss über einen SMTP-Server verfügen, sonst kann sie die Nachrichten nicht empfangen. Beachte: Wird in diesem Feld ein Domänenname angegeben, so können A- und MX-Einträge genutzt werden, je nach dem, welche Ergebnisse die DNS-Abfrage während der Zustellung erbringt. Falls die Nachrichten an einen bestimmten Host gesandt werden sollen, muss der Hostname in eckige Klammern gesetzt (z.B. `[host1.example.net]`) oder die IP-Adresse dieses Hosts angegeben werden. Mithilfe der Optionen AUTH-Benutzername und AUTH-Kennwort können Sie die Zugangsdaten für den Server festlegen.

Oben aufgeführte Domäne wie eine externe behandeln, auch wenn sie lokal verwaltet wird
Falls die angegebene Domäne eine lokale Domäne ist, die Post an sie aber so ausgegeben werden soll, wie es bei externen Domänen geschieht, muss diese Option aktiv sein.

Post über folgenden TCP-Port versenden
Bei der Übermittlung der für diese Domäne gespeicherten Post wird diese Portnummer verwendet.

ETRN-Anforderungen nur in echtheitsbestätigten Verbindungen zulassen
Ist der Gateway im Dialog Freigabe wartender Nachrichten so konfiguriert, dass ESMTP-Befehle ETRN angenommen werden, so ist per Voreinstellung auch diese Option aktiv und bewirkt, dass eine Gegenstelle vor der Aufforderung zur Freigabe wartender Nachrichten über den ESMTP-Befehl AUTH eine Echtheitsbestätigung durchführen muss. Ist diese Option aktiv, so muss auch ein entsprechendes Kennwort in das Feld "*ATRN-Kennwort*" im Abschnitt Freigabe wartender Nachrichten 264 eingetragen werden.

Soll die Echtheitsbestätigung bei ETRN nicht verlangt werden, muss diese Option abgeschaltet sein.

ATRN

Dieser Gateway beachtet ATRN-Anforderungen
Soll MDaemon ATRN-Befehle für die oben angegebene Domäne ausführen, ist diese Option zu aktivieren. ATRN ist ein ESMTP-Befehl, der beim On-Demand Mail Relay (ODMR) 201 zum Einsatz kommt. Diese Methode ist die derzeit beste zum Hosten von E-Mail-Diensten; sie ist anderen Methoden, wie z.B. ETRN, weit überlegen, weil sie eine Anmeldung verlangt, bevor der Versand der wartenden Post ausgelöst werden kann, und weil sie ohne feste IP-Adresse arbeitet. Die feste IP-Adresse ist überflüssig, weil der Datenfluss zwischen MDaemon und der Gegenstelle automatisch umgekehrt wird; die Nachrichten können sofort ausgegeben werden, ohne dass erst eine neue Verbindung hergestellt werden müsste. (Anders verhält es sich bei ETRN: Dort wird, nachdem der Befehl ETRN abgesetzt wurde, eine neue Verbindung aufgebaut.) Client-Domänen ohne feste IP-Adresse können somit ihre Post abrufen, ohne POP3 oder DomainPOP zu verwenden. Dies erleichtert die Zustellung die Benutzer, da die ursprünglichen SMTP-Umschläge erhalten bleiben.

ATRN erfordert eine Verbindung mit Echtheitsbestätigung über AUTH. Die Anmeldedaten für die Echtheitsbestätigung können im Abschnitt Optionen 268 eingetragen werden.

Nur eine ATRN-Anforderung zur selben Zeit zulassen
Diese Option bewirkt, dass höchstens eine ATRN-Verbindung zur selben Zeit aufgebaut werden kann.

ATRN-Kennwort
Wird der Versand über ATRN ausgelöst, oder ist die Option *Freigabe wartender Nachrichten über ETRN erfordert Echtheitsbestätigung* weiter oben aktiv, so muss hier das ATRN-Kennwort für den Gateway angegeben werden.

Die Domäne, für die MDaemon als E-Mail-Gateway arbeitet, muss zur Echtheitsbestätigung ihren Domänennamen als Benutzernamen angeben. Lautet der Name des Domänen-Gateways beispielsweise "example.com", und wird ATRN für die Aufforderung zur Freigabe wartender Nachrichten verwendet, so müssen als Benutzername "example.com" und als Kennwort das hier angegebene ATRN-Kennwort verwendet werden.

Zugriff - Anforderungen zur Freigabe wartender Nachrichten

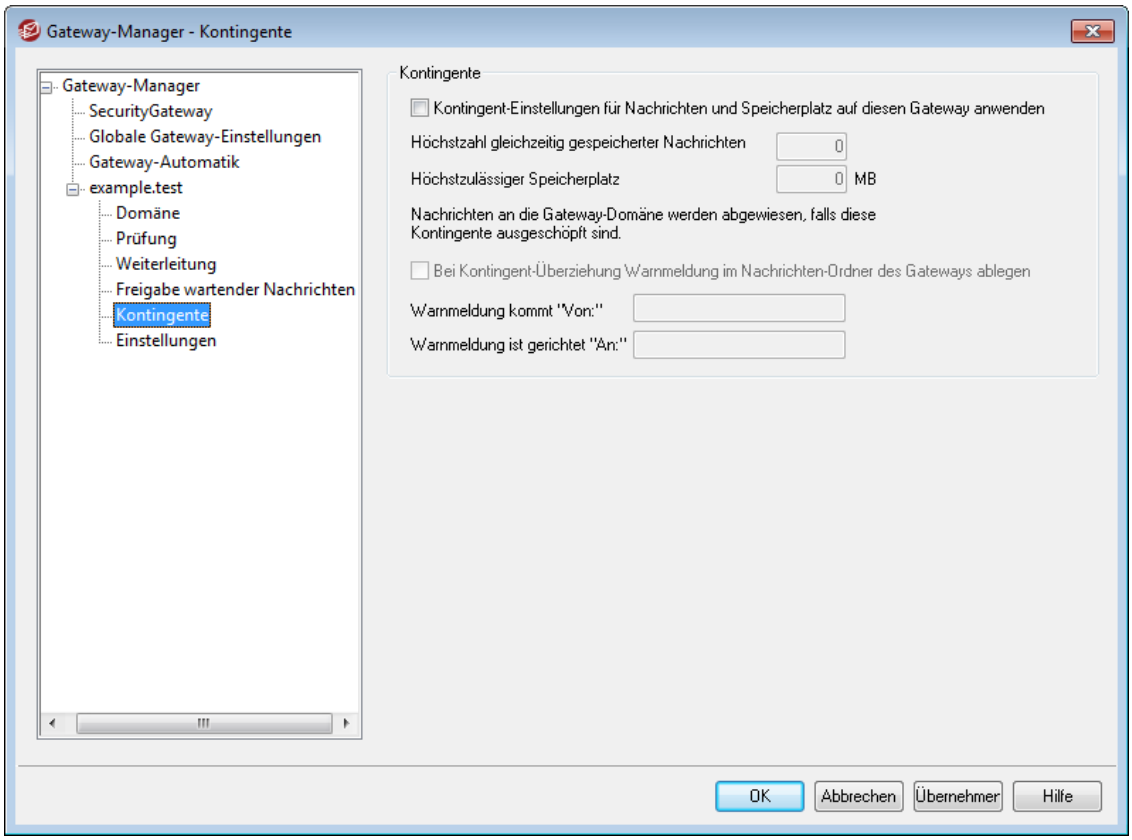
Anforderungen von folgenden IP-Adressen befolgen
Diese Option bewirkt, dass MDaemon ETRN- und ATRN-Befehle von den IP-Adressen in der nebenstehenden Adressliste befolgt.

Anforderungen von folgenden IP-Adressen ignorieren
Diese Option bewirkt, dass MDaemon ETRN- und ATRN-Befehle von den IP-Adressen in der nebenstehenden Adressliste ignoriert.

Neue IP hinzufügen
Um eine neue IP-Adresse in die Liste einzufügen, müssen die IP-Adresse in dieses Feld eingetragen und dann *Hinzufügen* angeklickt werden.

Entfernen
Ein Klick auf dieses Steuerelement entfernt den ausgewählten Eintrag aus der Liste der IP-Adressen.

3.3.3.5 Kontingente



Kontingente

Kontingent-Einstellungen für Nachrichten und Speicherplatz auf diesen Gateway anwenden
Falls Obergrenzen für den Speicherplatz in KB und die Anzahl der Nachrichten, die eine Domäne enthalten darf, definiert werden sollen, muss diese Option aktiviert werden. Entpackte Dateianlagen im Dateiverzeichnis sind der Kontingentierung ebenfalls unterworfen. Nachrichten, die nach Überschreitung des Kontingents angeliefert werden, weist der Server ab.

Höchstzahl gleichzeitig gespeicherter Nachrichten
Dieser Wert gibt die Höchstzahl der Nachrichten an, die MDaemon für diese Gateway-Domäne speichert. Der Wert 0 bewirkt, dass die Zahl der Nachrichten nicht begrenzt wird.

Höchstzulässiger Speicherplatz
Hier wird die Obergrenze für den Speicherplatz angegeben, den der Gateway belegen darf. Nach Überschreiten dieses Kontingents werden weitere

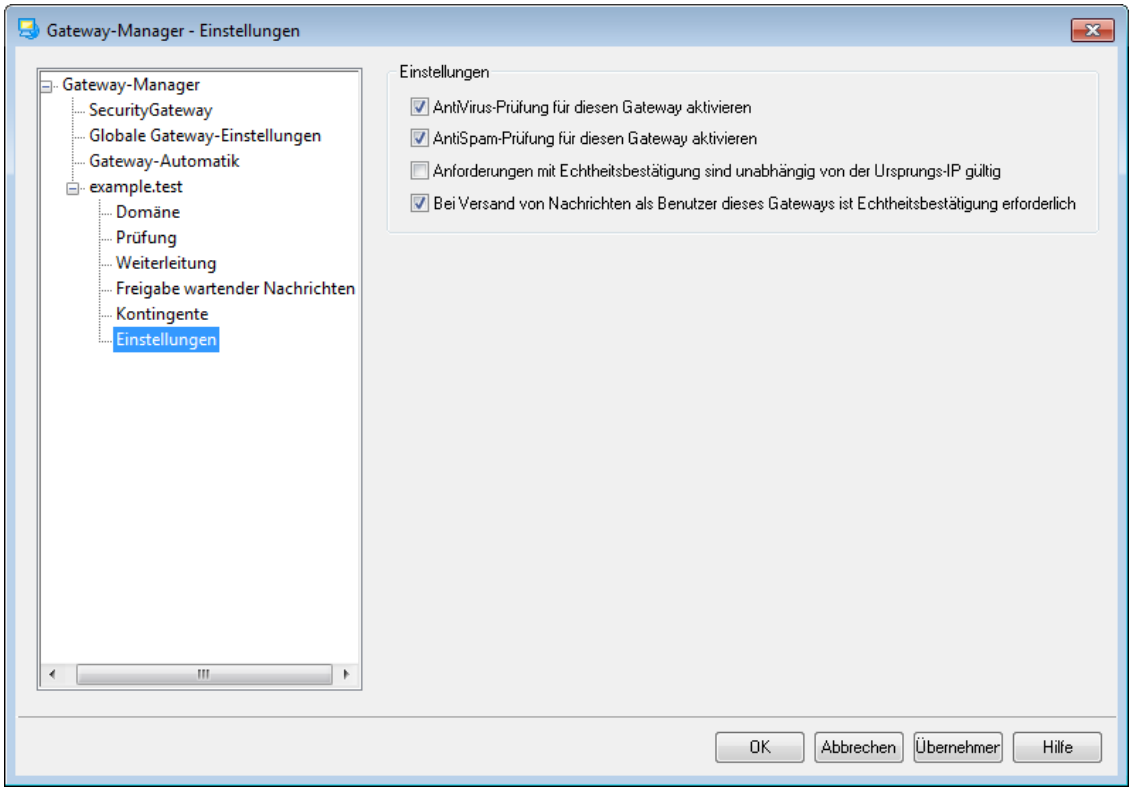
Nachrichten abgewiesen. Der Wert 0 bewirkt, dass der zulässige Speicherplatz nicht beschränkt wird.

Bei Kontingent-Überziehung Warnmeldung im Nachrichten-Ordner des Gateways ablegen
Wenn die Postzustellung an eine Domäne das Speicherplatzkontingent oder die Höchstzahl der Nachrichten überziehen würde, wird eine entsprechende Warnmeldung in den Nachrichten-Ordner des Gateways eingestellt. Absender und Empfänger der Warnmeldung können mithilfe der beiden folgenden Optionen definiert werden.

Warnmeldung kommt "Von:"
Hier wird der Absender für die Warnmeldung wegen Kontingentüberschreitung eingetragen.

Warnmeldung ist gerichtet "An:"
Hier wird der Empfänger für die Warnmeldung wegen Kontingentüberschreitung eingetragen.

3.3.3.6 Einstellungen



Optionen

AntiVirus-Prüfung für diesen Gateway aktivieren
Falls Sie auf Ihrem System die optionalen Leistungsmerkmale von MDaemon AntiVirus 648 nutzen und die Nachrichten dieses Domänen-Gateways mit seiner Hilfe prüfen lassen wollen, aktivieren Sie diese Option. Ist diese Option abgeschaltet, so prüft MDaemon AntiVirus die Nachrichten dieses Gateways nicht.

AntiSpam-Prüfung für diesen Gateway aktivieren
Um die Einstellungen des Spam-Filters auf die Nachrichten dieses Domänen-Gateways anzuwenden, muss diese Option aktiv sein. Ist sie abgeschaltet, sind die Nachrichten von der Prüfung durch den Spam-Filter ausgenommen.

Anforderungen mit Echtheitsbestätigung sind unabhängig von der Ursprungs-IP gültig
Diese Option bewirkt, dass Befehle in echtheitsbestätigten Verbindungen unabhängig von der IP-Adresse, von der sie ausgehen, immer befolgt werden. Ist diese Option abgeschaltet, so werden nur Befehle von den IP-Adressen ausgeführt, die im Abschnitt Zugriff weiter unten erfasst sind.

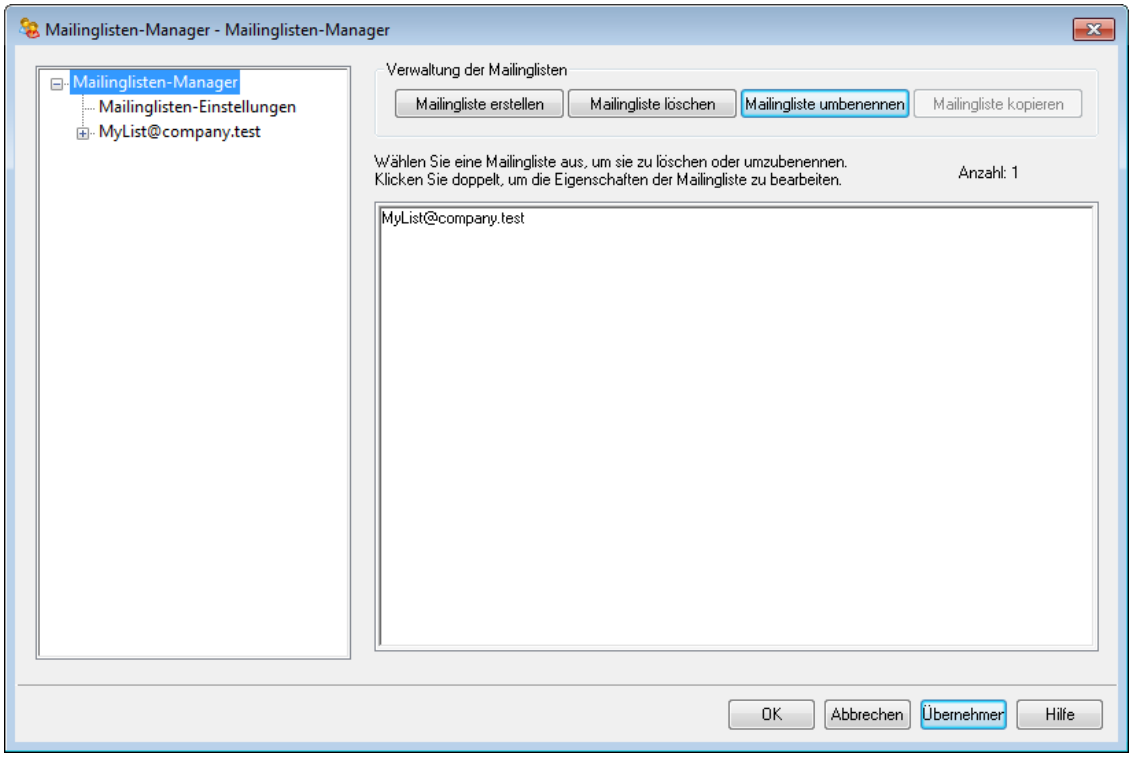
Bei Versand von Nachrichten als Benutzer dieses Gateways ist Echtheitsbestätigung erforderlich
Diese Option bewirkt, dass zum Versand aller Nachrichten, die angeblich aus dieser Domäne stammen sollen, Echtheitsbestätigung erforderlich ist. Nachrichten können dann nur zugestellt werden, wenn die Echtheitsbestätigung erfolgreich durchlaufen wurde oder die IP-Adresse der Gegenstelle eine Vertraute IP-Adresse ist. Andernfalls werden die Nachrichten abgewiesen. Diese Einstellung ist grundsätzlich aktiv.

Werden neue Domänen-Gateways eingerichtet, so wird diese Option auch für sie per Voreinstellung aktiviert. Soll die Option bei neuen Domänen-Gateways nicht per Vorgabe aktiv sein, so kann dies durch Bearbeiten des folgenden Eintrags in der Datei `MDaemon.ini` erreicht werden:

```
[Special]
GatewaySendersMustAuth=No (Voreinstellung ist "Yes", Ja)
```

3.4 Mailinglisten-Manager

Mailinglisten werden manchmal auch E-Mail-Gruppen, Diskussionsgruppen oder Verteilerlisten genannt. Sie gestatten es, Gruppen von Benutzern per E-Mail gemeinsam so zu erreichen, wie wenn diese Gruppen sich ein gemeinsames Postfach teilen würden. Alle Listenmitglieder erhalten Kopien aller E-Mail-Nachrichten, die an eine Mailingliste gerichtet sind. Listen können lokale und externe Empfängeradressen enthalten. Sie können öffentlich oder privat und moderiert oder offen geführt sein. Ihre Inhalte können als Digest 289 oder als normale Einzelnachrichten versendet werden. Darüber hinaus stehen zahlreiche Leistungsmerkmale zur Verfügung.



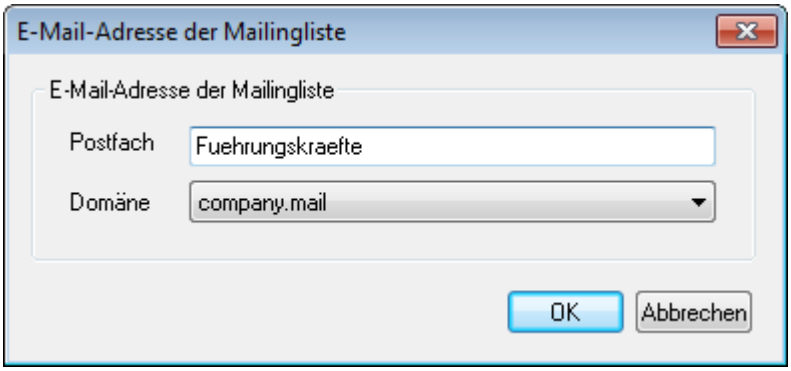
Sie können Ihre Mailinglisten mithilfe des Mailinglisten-Managers verwalten. Sie erreichen den Mailinglisten-Manager über das Menü Einstellungen » Mailinglisten-Manager....

Verwaltung der Mailinglisten

Der Navigationsbereich im linken Teil dieses Konfigurationsdialog enthält für jede Mailingliste einen eigenen Eintrag. Über diesen Eintrag erreichen Sie die einzelnen Abschnitte des Konfigurationsdialogs mit den Einstellungen für die jeweilige Mailingliste. Über den Navigationsbereich erhalten Sie außerdem Zugriff auf die Mailinglisten-Einstellungen 272, von wo aus Sie verschiedene systemweite Einstellungen vornehmen können. Im rechten Teil dieses Konfigurationsdialogs finden Sie Steuerelemente, um Listen zu erstellen, zu löschen und umzubenennen. Um die Einstellungen einer Mailingliste zu bearbeiten, können Sie durch einen Doppelklick auf die Mailingliste den Editor für Mailinglisten aufrufen.

Mailingliste erstellen

Um eine neue Mailingliste zu erstellen, klicken Sie auf das Steuerelement **Mailingliste erstellen**. Es wird der Konfigurationsdialog E-Mail-Adresse der Mailingliste aufgerufen. Tragen Sie in das Feld Postfach den Postfachnamen der Mailingliste ein, beispielsweise "MeineListe", und wählen Sie im Dropdown-Menü Domäne die Domäne aus, zu der die Mailingliste gehören soll, beispielsweise "company.mail". Beide Bestandteile ergeben zusammen die E-Mail-Adresse der Liste (im Beispiel "MeineListe@company.mail"). Nachrichten, die an diese E-Mail-Adresse gerichtet sind, werden an alle Mitglieder der Mailingliste übermittelt, wobei die Einstellungen der jeweiligen Mailingliste für die Art der Übermittlung maßgeblich sind. Um die Erstellung der Mailingliste abzuschließen, klicken Sie auf **OK**. Nachdem Sie die Liste erstellt haben, können Sie durch einen Doppelklick auf ihren Eintrag die Einstellungen der Liste und ihre Mitglieder bearbeiten. **Beachte**: Die Namen der Mailinglisten dürfen die Zeichen ! und | nicht enthalten.



Mailingliste löschen
Um eine Mailingliste zu löschen, wählen Sie den Eintrag der Mailingliste aus, klicken Sie auf **Mailingliste löschen**, und bestätigen Sie die Sicherheitsabfrage.

Mailingliste umbenennen
Um eine Mailingliste umzubenennen, wählen Sie den Eintrag der Mailingliste aus, und klicken Sie auf **Mailingliste umbenennen**. Es öffnet sich der Konfigurationsdialog E-Mail-Adresse der Mailingliste. Nehmen Sie dort die gewünschten Änderungen vor, und klicken Sie zum Abschluss auf **OK**.

Mailingliste kopieren
Um eine neue Mailingliste anzulegen und dabei die Einstellungen aus einer anderen Mailingliste zu übernehmen, wählen Sie die gewünschte Ursprungsmailingliste in der Liste aus, und klicken Sie auf **Mailingliste kopieren**. Geben Sie dann den Postfachnamen und die Domäne für die neue Mailingliste an.

Bearbeiten einer bestehenden Mailingliste

Um eine Mailingliste zu konfigurieren, klicken Sie doppelt auf ihren Eintrag im Mailinglisten-Manager. Wählen Sie danach im Navigationsbereich im linken Teil des Fensters den gewünschten Abschnitt aus, dessen Einstellungen Sie bearbeiten wollen:

Mitglieder 275
Einstellungen 278
Kopfzeilen 281
Mitgliedschaft 284
Erinnerungen 288
Moderation 292
Digest 289
Routing 294
Benachrichtigungen 290
Zusatzdateien 296
Öffentlicher Ordner 298
Active Directory 299
ODBC 302

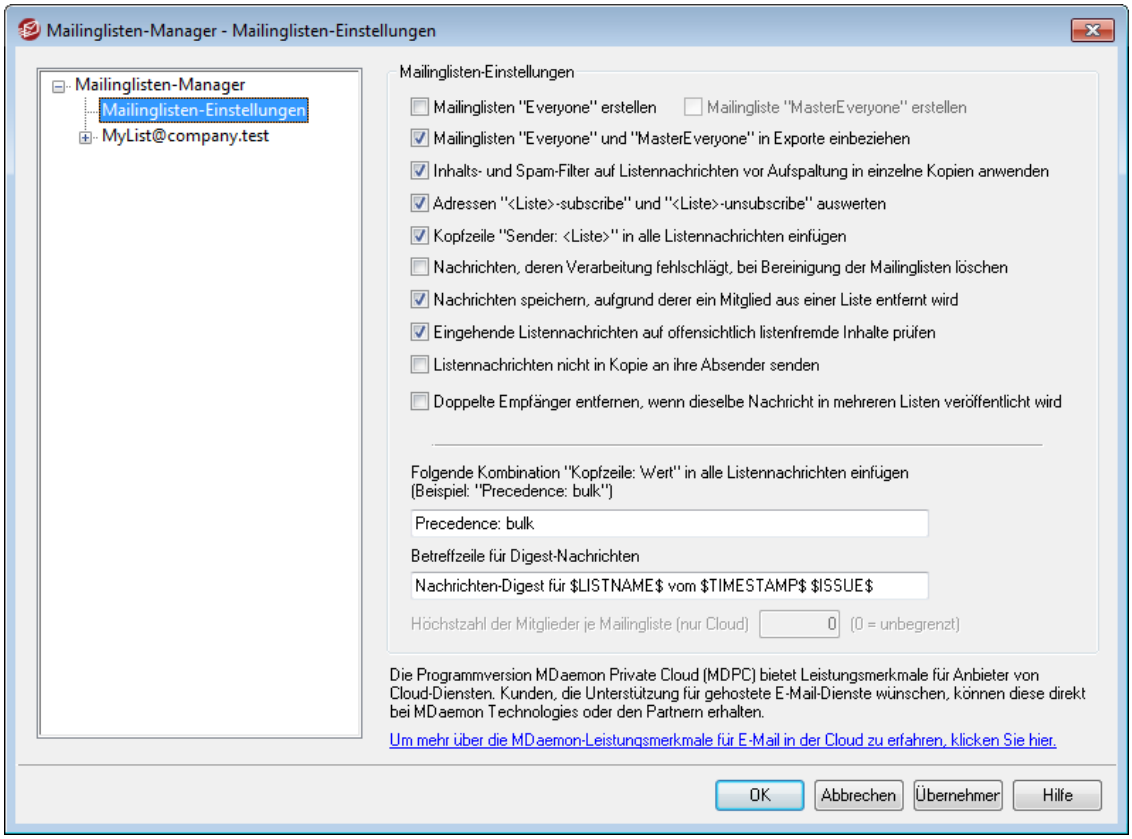
Mailinglisten-Einstellungen

Um verschiedene systemweite Einstellungen für Mailinglisten zu bearbeiten, klicken Sie im linken Teil des Fensters auf **Mailinglisten-Einstellungen**. Sie rufen dadurch den Konfigurationsdialog Mailinglisten-Einstellungen 272 auf.

Siehe auch:

[Mailinglisten-Einstellungen](#) 272

3.4.1 Mailinglisten-Einstellungen



Mailinglisten-Einstellungen

Mailinglisten "Everyone" erstellen
Diese Option bewirkt, dass Mailinglisten des Typs "Everyone" ("Alle Benutzer") für alle Domänen auf dem MDaemon-Server erstellt werden (z.B. "everyone@example.com"). Die Option erstellt eine solche Mailingliste für jede Domäne. Mithilfe der Mailinglisten können Sie allen Benutzern der Domäne eine E-Mail-Nachricht senden, indem Sie sie an "everyone@<Domäne>" adressieren. Private Benutzerkonten 760 sind in den Mailinglisten des Typs "Everyone" nicht enthalten. Die Option ist per Voreinstellung abgeschaltet.

Mailingliste "MasterEveryone" erstellen
Diese Option bewirkt die Erstellung der Mailingliste "MasterEveryone". Diese Mailingliste enthält die Benutzer in allem Domänen, die auch in den Mailinglisten "Everyone" der einzelnen Domänen enthalten sind. Die Option ist per Voreinstellung abgeschaltet.

Mailinglisten "Everyone" und "MasterEveryone" in Exportfunktionen einbeziehen
Per Voreinstellung werden die Mailinglisten "Everyone" und "MasterEveryone" mit exportiert, wenn Sie mithilfe der Option "Benutzerkonten » Export" Mailinglisten exportieren. Falls Sie diese besonderen Listen nicht in die exportierten Mailinglisten aufnehmen wollen, deaktivieren Sie diese Option.

Inhalts- & Spam-Filter auf Listennachrichten vor Aufspaltung in einzelne Kopien anwenden
Falls im Abschnitt Routing[294] des Mailinglisten-Editors die Option *Listennachrichten an jedes Mitglied einzeln zustellen* aktiv ist, bewirkt diese Option, dass die Regeln der Inhalts- und Spam-Filter auf die Listennachrichten angewendet werden, bevor sie in gesonderte Nachrichten aufgespalten und den Listenmitgliedern zugestellt werden

Adressen "<Liste>-subscribe" und "<Liste>-unsubscribe" auswerten
Ist diese Option aktiv, so erkennt MDaemon Adressen, die nach diesem Format aufgebaut sind, immer als gültige E-Mail-Adressen, so lange die zugehörige Mailingliste besteht. Besteht beispielsweise eine Mailingliste mit dem Namen `MeineListe@example.com`, so können Benutzer die Liste abonnieren und abbestellen, indem sie an `MeineListe-Subscribe@example.com` und `MeineListe-Subscribe@example.com` Nachrichten senden. Der Inhalt der Betreffzeilen und des Nachrichtentextes ist belanglos. MDaemon fügt, solange diese Option aktiv ist, die folgende Zeile in die Listennachrichten ein:

```
List-Unsubscribe: <mailto:<Liste>-Unsubscribe@example.com>
```

Manche Mailclients werten diese Zeile aus und stellen den Benutzern daraufhin automatisch ein Steuerelement "Abbestellen" zur Verfügung.

Sie können diese Einstellung für einzelne Mailinglisten übergehen, indem Sie im Konfigurationsdialog Moderation[292] des Mailinglisten-Editors die Optionen zu den **URLs für die Mailingliste** entsprechend konfigurieren.

Kopfzeile "Sender: <Liste>" in alle Listennachrichten einfügen
Diese Option fügt den Listennachrichten die Kopfzeile `Sender` hinzu.

Nachrichten, deren Verarbeitung fehlschlägt, bei Bereinigung der Mailinglisten löschen
Diese Option bewirkt, dass MDaemon alle Listennachrichten ohne auswertbaren Adressen löscht.

Nachrichten speichern, aufgrund derer ein Mitglied aus einer Liste entfernt wird
MDaemon prüft zurück geleitete Listennachrichten, um die Adressen solcher Mitglieder aus der Liste zu entfernen, die nicht für die Nachrichtenzustellung erreichbar sind. Diese Option bewirkt die Aufbewahrung solcher Nachrichten, die zur Löschung eines Mitglieds aus der Liste geführt haben. Nähere Informationen hierzu finden Sie in der Beschreibung der Option *E-Mail-Adressen aus der Liste entfernen, falls die Zustellung an Sie fehlschlägt...* im Abschnitt Einstellungen[278].

Eingehende Listennachrichten auf offensichtlich listenfremde Inhalte prüfen
Diese Option bewirkt, dass MDaemon Nachrichten an Mailinglisten abweist, von denen MDaemon feststellt, dass sie nicht an die Liste sondern an das Systemkonto hätten gerichtet sein müssen. Benutzer können beispielsweise eine Mailingliste bestellen und abbestellen, indem Sie die Befehle Subscribe (Bestellen) und Unsubscribe (Abbestellen) an den Beginn einer E-Mail-Nachricht stellen und diese Nachricht an das Systemkonto senden (z.B. "mdaemon@example.com"). Stattdessen versuchen Benutzer häufig irrtümlich, solche Nachrichten an die Mailingliste selbst zu richten. Diese Option verhindert, dass solche Nachrichten in der Mailingliste veröffentlicht werden.

Listennachrichten nicht in Kopie an ihre Absender senden
Diese Option bewirkt, dass Absender von Nachrichten, die an Mailinglisten gerichtet sind, keine Kopien ihrer eigenen Nachrichten über die Mailinglisten erhalten. Diese Option ist per Voreinstellung abgeschaltet.

Doppelte Empfänger entfernen, wenn dieselbe Nachricht in mehreren Listen veröffentlicht wird
Ist diese Option aktiv, und ist eine einzelne Nachricht an mehrere Mailinglisten gerichtet, so stellt MDaemon an alle Empfänger, die in mehr als einer dieser Mailinglisten Mitglieder[275] sind, nur eine Kopie dieser Nachricht zu. Ein Beispiel hierzu: Falls der Benutzer `frank@example.net` Mitglied in den Mailinglisten `Liste-A@example.com` und `Liste-B@example.com` ist und eine eingehende Nachricht an beide Mailinglisten gerichtet ist, erhält der Benutzer insgesamt nur eine Kopie dieser Nachricht, und nicht etwa eine Kopie je Mailingliste. Diese Option wirkt nur auf Mailinglisten selbst. Wäre die Nachricht im Beispiel neben den beiden Mailinglisten auch an die E-Mail-Adresse des Benutzers selbst gerichtet, so würde der Benutzer die Nachricht in zwei, nicht aber drei Ausfertigungen erhalten. Diese Option ist per Voreinstellung abgeschaltet.

Die Nutzung dieser Option empfiehlt sich in der Regel nicht. Benutzer verwalten und nutzen die Mailinglisten auf ganz unterschiedliche Weise, und es ist nicht vorhersagbar, in welcher von mehreren Listen die Nachricht zugestellt wird, falls doppelte Nachrichten in dieser Weise unterdrückt werden. Die Option kann daher den Benutzern unnötige Schwierigkeiten bereiten. Sie kann insbesondere die Verfolgung von Diskussionsfäden und die Nutzung der IMAP-Filter[736] zum Sortieren von Nachrichten in bestimmte Ordner erschweren.

Folgende Kombination "Kopfzeile: Wert" in alle Listennachrichten einfügen
Mithilfe dieser Option können Sie eine feste Kombination aus Kopfzeile und Wert (etwa "Precedence: bulk") in alle Listennachrichten eintragen.

Betreffzeile für Digest-Nachrichten
Mithilfe dieser Option können Sie die Betreffzeile anpassen, die MDaemon in Digest-Nachrichten[289] für Mailinglisten einsetzt. Per Voreinstellung wird die Betreffzeile gebildet aus der Vorlage "`Nachrichten-Digest für $LISTNAME$ vom $TIMESTAMP$ Ausgabe $ISSUE$`". Die Makros werden umgesetzt in den Namen der Mailingliste, den Zeitpunkt der Erstellung des Digests und die Nummer der Ausgabe.

Höchstzahl der Mitglieder je Mailingliste (nur Cloud) [x] (0=unbegrenzt)
Mithilfe dieser Option können Sie die Höchstzahl zulässiger Mitglieder je Mailingliste für diese Domäne begrenzen.

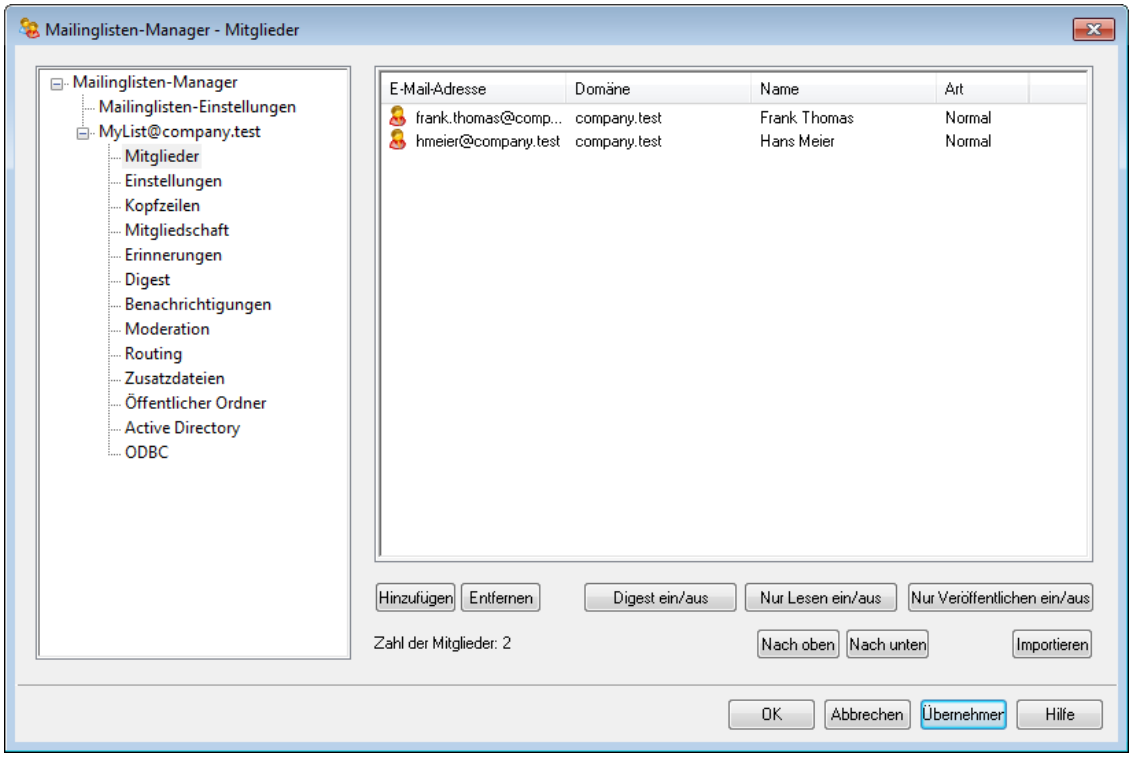
MDaemon Private Cloud verfügbar. Es steht auch eine entsprechende, systemweit wirksame Option im Abschnitt Einstellungen[272] des Mailinglisten-Managers zur Verfügung.

Siehe auch:

Mailinglisten-Manager[269]

3.4.2 Mailinglisten-Editor

3.4.2.1 Mitglieder



In diesem Abschnitt werden E-Mail-Adressen und Namen aller Listenmitglieder angezeigt. In jedem Eintrag erscheint auch der Typ der Mitgliedschaft: normal, Digest, Nur-Lesen oder Nur Veröffentlichen.

Hinzufügen
Durch Anklicken dieses Steuerelements fügen Sie der Mitglieder-Liste neue Mitglieder hinzu 277.

Entfernen
Um ein Mitglied aus der Liste zu entfernen, wählen Sie seinen Eintrag aus, und klicken Sie danach auf dieses Steuerelement.

Digest ein/aus
Durch Auswahl eines Mitglieds und Anklicken dieses Steuerelements kann seine Mitgliedschaft auf Digest 289 umgestellt werden. Um zur normalen Mitgliedschaft zurückzukehren, klicken Sie erneut auf das Steuerelement.

Nur-Lesen ein/aus
Hiermit wird das ausgewählte Mitglied auf "Nur-Lesen" gesetzt. Es kann Nachrichten empfangen, aber in der Mailingliste nichts veröffentlichen. Um zur normalen Mitgliedschaft zurückzukehren, klicken Sie erneut auf das Steuerelement.

Nach oben/Nach unten
Mithilfe dieser Steuerelemente können Sie ein Listenmitglied oder mehrere Listenmitglieder an eine andere Stelle in der Liste verschieben. Wählen Sie dazu die Listenmitglieder aus, und klicken Sie danach auf diese Steuerelemente. Sie können die Liste auch durch Anklicken einer Spaltenüberschrift sortieren.

Beachte: Wenn Sie die Liste durch Anklicken einer Spaltenüberschrift sortieren, so ersetzt diese Sortierung eine manuelle Sortierung, die Sie mithilfe der Steuerelemente Nach oben/Nach unten vorher etwa vorgenommen haben.

Nur Veröffentlichen ein/aus
Hiermit wird das ausgewählte Mitglied auf "Nur Veröffentlichen" gesetzt, Es kann Nachrichten an die Liste senden, empfängt aber nichts, was in der Liste veröffentlicht wurde. Um zur normalen Mitgliedschaft zurückzukehren, klicken Sie erneut auf das Steuerelement.

Importieren
Durch Anklicken dieses Steuerelements können Sie eine Mitgliederliste aus einer Textdatei importieren, deren einzelne Felder durch Kommata voneinander getrennt sind (kommagetrennte Datei). Jeder Eintrag muss auf einer eigenen Zeile stehen, deren einzelne Felder durch Kommata getrennt sind. Außerdem muss die erste Zeile der Datei (der Feldraster) die Namen der Felder und ihre Reihenfolge auf den folgenden Zeilen angeben. Ein Feld muss die Bezeichnung "**Email**" tragen und die E-Mail-Adressen enthalten. Es stehen auch zwei wahlfreie Felder zur Verfügung: "**FullName**" und "**Type**". **FullName** kann die Klartextnamen der Mitglieder enthalten. **Type** kann die Werte "**read only" (Nur Lesen)**, "**post only" (Nur Veröffentlichen)**, "**digest" (Digest)** oder **"normal" (Normal)** enthalten. Der Importvorgang berücksichtigt nur diese Felder und lässt alle anderen unbeachtet. Die Feldnamen dürfen nicht in andere Sprachen übersetzt werden.

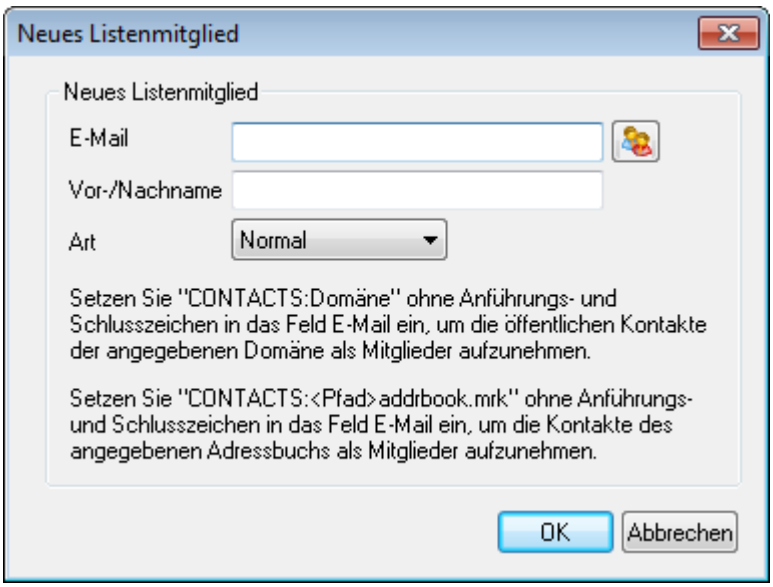
Ein Beispiel hierzu:

```
"Email", "FullName", "Type", "Address", "telephone"
"user01@altn.com", "Michael Mason", "Digest", "123 Street",
"519.555.0100"
```

MDaemon versendet an Mitglieder, die so importiert wurden, keine Begrüßungsnachricht (falls eine solche definiert ist), und es wird beim Import keine Prüfung auf bereits vorhandene Mitglieder durchgeführt.

Zahl der Mitglieder
Die Gesamtzahl der Mitglieder der bearbeiteten Mailingliste wird in dieser Zeile am unteren Ende des Konfigurationsdialogs angezeigt.

Hinzufügen neuer Mitglieder



Neues Listenmitglied

E-Mail
Tragen Sie hier die E-Mail-Adresse des neuen Mitglieds ein. Sie können eine Adresse in das Textfeld eintragen oder durch Anklicken des Benutzer-Symbols die Benutzerkonten und Gruppen durchsuchen und die Benutzerkonten und Gruppen auswählen, die Sie hinzufügen wollen. Die Adressen der Mitglieder dürfen die Zeichen "!" und "|" nicht enthalten.

Falls Sie alle Benutzerkonten einer bestimmten Domäne oder alle Benutzer aus einer bestimmten Benutzergruppe zur Liste hinzufügen wollen, können Sie dazu als E-Mail-Adresse die besonderen Makros **ALL_USERS:<Domäne>** oder **GROUP:<Gruppe>** hier eintragen; Sie müssen die E-Mail-Adressen nicht einzeln hinzufügen. So hat beispielsweise das Hinzufügen von `ALL_USERS:example.com` als Listenmitglied dieselbe Wirkung wie das einzelne Hinzufügen jedes Benutzerkontos aus der Domäne `example.com`. Das Hinzufügen von `ALL_USERS:example.com` als Listenmitglied hat dieselbe Wirkung wie das Hinzufügen jedes einzelnen Benutzerkontos der Domäne `example.com`.

Sie können das besondere Makro **CONTACTS:<Domäne>** dazu verwenden, die öffentlichen Kontakte 122 der jeweiligen Domäne als Listenmitglieder einzutragen. Ein Beispiel hierzu: `CONTACTS:example.com`.

Vor-/Nachname
Tragen Sie hier den vollständigen Namen des Mitglieds ein. Falls im Konfigurationsdialog Kopfzeilen 281 die Option *Inhalt der Kopfzeile "To:" (An:)*

ersetzen durch: Name des Mitglieds gesetzt ist, erscheint dieser Name im Feld "An:".

Art
Mithilfe dieses Dropdown-Menüs legen Sie die Art der Mitgliedschaft fest. Es stehen folgende Optionen zur Auswahl:

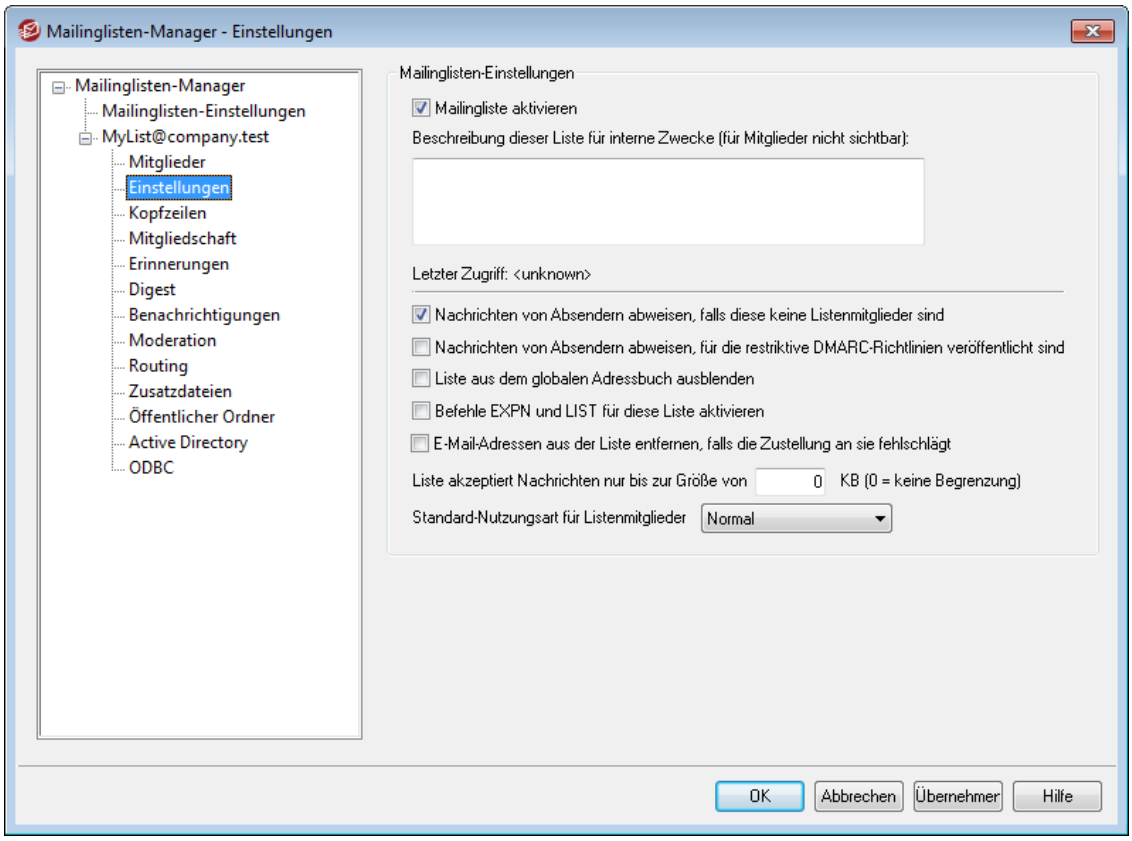
Normal — Das Mitglied kann Listennachrichten normal senden und empfangen.

Digest — Das Mitglied kann Listennachrichten senden und empfangen, wobei die empfangenen Nachrichten immer im Digest-Format geliefert werden.

Nur Lesen — Das Mitglied kann Nachrichten aus der Liste empfangen, aber keine Nachrichten an die Liste senden.

Nur Veröffentlichen — Das Mitglied kann Nachrichten an die Liste senden, aber keine Nachrichten von der Liste empfangen.

3.4.2.2 Einstellungen



Mailinglisten-Einstellungen

Mailingliste aktivieren
Um die Mailingliste vorübergehend zu deaktivieren, deaktivieren Sie dieses Kontrollkästchen. Während die Liste deaktiviert ist, werden alle Nachrichten, die über SMTP für die Liste eingehen oder durch sie versandt werden, mit einem vorübergehenden Fehler 451 abgewiesen.

Beschreibung dieser Liste für interne Zwecke (für Mitglieder nicht sichtbar)
Sie können in dieses Feld eine Beschreibung der Liste für interne Zwecke eintragen. Diese Beschreibung dient nur der Verwaltung der Liste; sie wird den Mitgliedern nicht angezeigt und erscheint nicht in den Kopfzeilen.

Letzter Zugriff
Hier erscheint der Zeitpunkt, zu dem der letzte Zugriff auf die Mailingliste erfolgt ist. Hierdurch lassen sich Mailinglisten einfach erkennen, die selten oder gar nicht mehr genutzt werden.

Nachrichten von Absendern abweisen, falls diese keine Listenmitglieder sind
Diese Option bewirkt, dass die Mailingliste als "private Liste" betrieben wird. Es können dann nur Mitglieder der Liste über die Liste Nachrichten versenden; Nachrichten aller anderen Absender werden abgewiesen.

Nachrichten von Absendern abweisen, für die restriktive DMARC-Richtlinien veröffentlicht sind
Diese Option bewirkt, dass für die Liste eingehende Nachrichten abgewiesen werden, falls für ihre Absenderdomäne restriktive DMARC 538-Richtlinien veröffentlicht sind (z.B. p=quarantine oder p=reject). Diese Option wird üblicherweise nicht benötigt, wenn die Option "*...E-Mail-Adresse im Absenderfeld 'From' ersetzen...*" im Abschnitt Kopfzeilen 281 aktiv ist.

Sind sowohl diese Option wie auch die Option "*...E-Mail-Adresse im Absenderfeld 'From:' ersetzen...* 281" deaktiviert, dann ist damit zu rechnen, dass Server von Empfängern der Listennachrichten diese Nachrichten abweisen. In manchen Fällen können die Empfänger auch automatisch aus der Mailingliste entfernt werden 280. Sie sollten daher sicherstellen, dass wenigstens eine der beiden genannten Optionen aktiv ist.

Liste aus dem globalen Adressbuch ausblenden
Diese Option bewirkt, dass die Mailingliste aus den über Webmail und LDAP bereit gestellten öffentlichen Adressbüchern ausgeblendet wird.

Befehle EXPN und LIST für diese Liste aktivieren
Per Voreinstellung befolgt MDaemon die Befehle EXPN und LIST nicht bei Mailinglisten, damit die Mitgliederlisten der Mailinglisten geheim bleiben. Falls Sie diese Option aktivieren, übermittelt MDaemon während Nachrichten-Verbindungen die Mitgliederinformationen als Antwort auf die Befehle EXPN und LIST.

E-Mail-Adressen aus der Liste entfernen, falls die Zustellung an sie fehlschlägt
Diese Option bewirkt, dass MDaemon E-Mail-Adressen automatisch aus der Mitgliederliste entfernt, wenn die Zustellung an diese Adressen mit einem dauerhaften Fehler endgültig fehlgeschlagen ist. MDaemon entfernt die Adressen auch dann, wenn eine Nachricht die Funktionen zur wiederholten Zustellung 864 durchläuft und aus der Wiederholungs-Warteschlange gelöscht wird, ohne dass die Zustellung zuvor erfolgreich war.

Die Option *E-Mail-Adressen aus der Liste entfernen, falls die Zustellung an sie fehlschlägt...* soll dann Abhilfe schaffen, wenn der Mailserver des Empfängers die Nachrichten abweist. Diese Option wirkt nur dann, wenn die Option *Listennachrichten mit gesondertem RCPT-Befehl für jedes Mitglied zustellen* im Abschnitt Routing 294 aktiv ist. Falls Sie abgehende Listennachrichten über einen Smarthost leiten, finden Sie nähere Informationen weiter unten im Abschnitt Erweiterte Bereinigung von Mailinglisten 280.

Liste akzeptiert Nachrichten nur bis zur Größe von [xx] KB (0=keine Begrenzung)
Diese Option begrenzt die Größe der Nachrichten, die über die Mailingliste versandt werden dürfen. Nachrichten, deren Größe diese Grenze überschreitet, werden abgewiesen.

Standard-Nutzungsart für Listenmitglieder
Aus diesem Dropdown-Menü können Sie die Standard-Nutzungsart für neue Mitglieder dieser Mailingliste auswählen. Sie können die Nutzungsart für bestehende Mitglieder jederzeit im Abschnitt Mitglieder 275 ändern. Es stehen folgende vier Nutzungsarten zur Verfügung:

Normal — Das Mitglied kann Listennachrichten normal senden und empfangen.

Digest — Das Mitglied kann Listennachrichten senden und empfangen, wobei die empfangenen Nachrichten immer im Digest-Format geliefert werden.

Nur Lesen — Das Mitglied kann Nachrichten aus der Liste empfangen, aber keine Nachrichten an die Liste senden.

Nur Veröffentlichen — Das Mitglied kann Nachrichten an die Liste senden, aber keine Nachrichten von der Liste empfangen.

Erweiterte Bereinigung von Mailinglisten

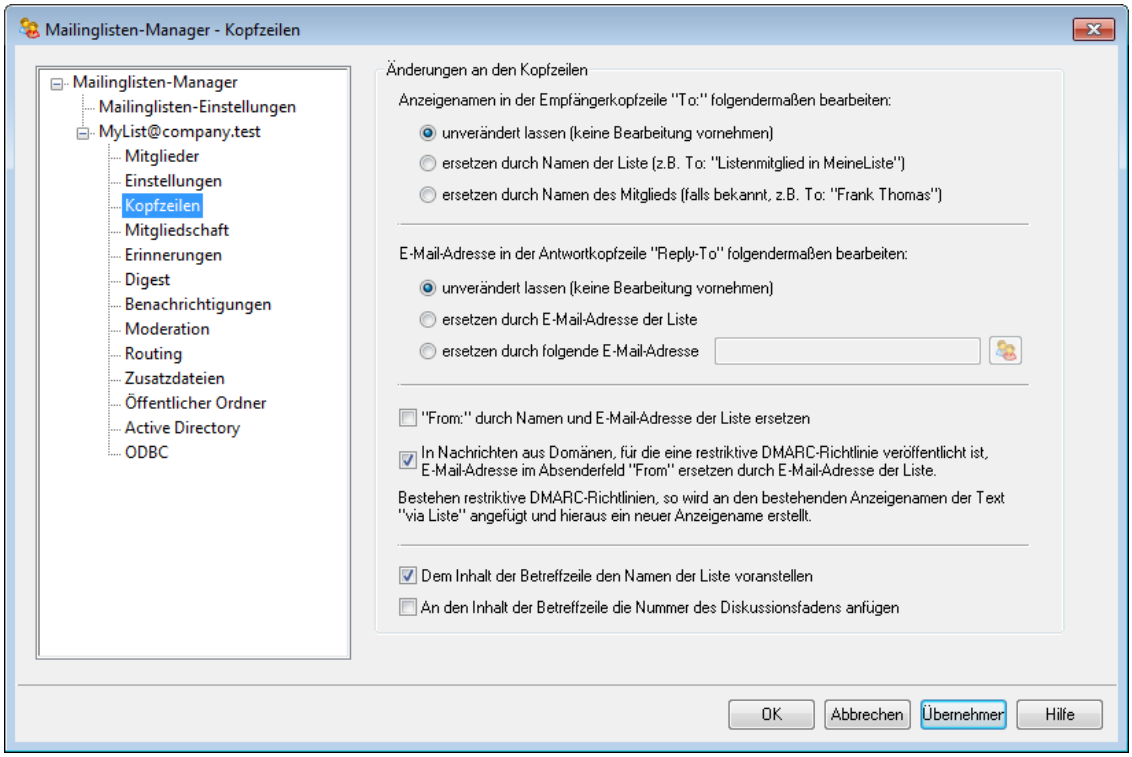
Ist die Option *E-Mail-Adressen aus der Liste entfernen, falls die Zustellung an sie fehlschlägt...* aktiv, und ist als Antwortpfad für die Nachrichten einer Liste ein lokales Postfach angegeben (siehe SMTP-"Bounce"-Adresse der Liste im Konfigurationsdialog Benachrichtigungen 290), so versucht MDaemon jeden Tag um Mitternacht, problematische Adressen aus den zurück geleiteten Nachrichten auszuwerten und unerreichbare Mitglieder aus der Liste zu löschen. Diese Funktion sortiert ungültige Adressen aus Mailinglisten noch effizienter aus, und zwar besonders dann, wenn die Listennachrichten nicht direkt zugestellt sondern geroutet werden.

Im Konfigurationsdialog Mailinglisten-Einstellungen 272 finden Sie zwei Einstellungen, die sich auf diese Funktion beziehen. Die Option *Nachrichten, deren Verarbeitung fehlschlägt, bei Bereinigung der Mailinglisten löschen* bewirkt, dass zurück geleitete Nachrichten, die keine auswertbare Adresse enthalten, gelöscht werden. Die Option *Nachrichten speichern, aufgrund derer ein Mitglied aus einer Liste entfernt wird* bewirkt, dass alle Nachrichten, die zur Löschung eines Listenmitglieds führen, aufbewahrt werden.

Wird die E-Mail-Adresse eines lokalen Benutzers als *SMTP-"Bounce"-Adresse für diese Liste* 290 eingetragen, so kann dies dazu führen, dass die E-Mail-Nachrichten dieses Benutzers gelöscht werden. Ob dieser Fall wirklich eintritt, hängt von den Einstellungen zur Bereinigung der Listen aus dem Konfigurationsdialog Mailinglisten-Einstellungen 272 ab.

Schlägt eine Zustellung einer Nachricht für eine bestimmte Adresse mit einem Fehler 5xx fehl, so wird die Adresse, bei der dieser Fehler aufgetreten ist, in die Datei `BadAddress.txt` im Protokoll-Verzeichnis aufgenommen. Anhand der Einträge der Datei lassen sich beispielsweise ungültige E-Mail-Adressen aus Mailinglisten schneller finden als durch eine Suche in den Protokollen über abgehende SMTP-Verbindungen. Diese Datei wird jeden Tag um Mitternacht automatisch gelöscht; es wird so verhindert, dass sie übermäßig groß wird.

3.4.2.3 Kopfzeilen



Änderungen an den Kopfzeilen

Anzeigenamen in der Empfängerkopfzeile "To:" folgendermaßen bearbeiten: Hiermit wird festgelegt, welchen Text MDaemon in den Anzeigenamen zur E-Mail-Adresse (auch Klarnamenfeld oder Namensfeld genannt) der Listennachrichten einfügen soll, wenn MDaemon eine an die Liste gerichtete Nachricht erhält.

unverändert lassen (keine Bearbeitung vornehmen) - Wird diese Option ausgewählt, ändert MDaemon den Anzeigenamen nicht, und das Feld mit der Adresse erscheint genau so, wie es der Absender eingegeben hat.

ersetzen durch Namen der Liste - Hiermit wird der Anzeigename durch den Namen der Liste und den Zusatz "Listenmitglied" ersetzt. Lautet der Name der Liste beispielsweise "Meine-Familie", so wird der Anzeigename geändert in "Listenmitglied in Meine-Familie".

ersetzen durch Namen des Mitglieds (falls bekannt) - Ist diese Option ausgewählt, erscheint im Anzeigenamen die Adresse des jeweiligen Nachrichtenempfängers, falls sie bekannt ist.

Der Mitgliedsname lässt sich nur dann auswählen, falls im Abschnitt Routing 294 die *Option Listennachrichten an jedes Mitglied einzeln zustellen* aktiv ist. Ist dort hingegen *Listennachrichten mit gesondertem RCPT-Befehl für jedes Mitglied zustellen* ausgewählt, verwendet MDaemon hier standardmäßig den *Listennamen*.

E-Mail-Adresse in der Antwortkopfzeile "Reply-To" folgendermaßen bearbeiten:
Diese Option bestimmt, welche E-Mail-Adresse in die Kopfzeile Reply-To: (Antwort an:) der einzelnen Listennachrichten eingetragen wird.

unverändert lassen (keine Bearbeitung vornehmen)
Aktivieren Sie diese Option, um die Kopfzeile Reply-To: unverändert zu lassen. Der Wert, der in der Nachricht an die Mailingliste ursprünglich enthalten war, bleibt erhalten. Diese Option empfiehlt sich, wenn direkte Antworten auf Listennachrichten nicht über die Mailingliste an alle Listenmitglieder sondern direkt an den Absender der Ursprungsnachricht gesendet werden sollen.

ersetzen durch E-Mail-Adresse der Liste
Aktivieren Sie diese Option, falls Antworten auf Listennachrichten nicht an den Absender der Ursprungsnachricht sondern an die Mailingliste selbst gerichtet werden sollen. Diese Option empfiehlt sich, wenn Sie die Liste als Diskussionsgruppe verwenden wollen, in der Antworten in der Regel an alle Mitglieder gehen sollen.

ersetzen durch folgende E-Mail-Adresse
Aktivieren Sie diese Option, falls sie Antworten auf Listennachrichten an eine bestimmte E-Mail-Adresse richten wollen. Geben Sie dazu die gewünschte E-Mail-Adresse ein, oder wählen Sie sie nach Anklicken des Symbols für die Benutzerkonten aus der Liste der in MDaemon bestehenden Benutzerkonten aus. Sie können diese Option beispielsweise einsetzen, um die Mailingliste für einen Newsletter zu verwenden, bei dem Antworten immer eine bestimmte Kontaktadresse erreichen sollen.

"From:" durch Namen und E-Mail-Adresse der Liste ersetzen
Diese Option bewirkt, dass der Inhalt der Absenderkopfzeile "From:" durch den Namen und die E-Mail-Adresse der Mailingliste ersetzt wird.

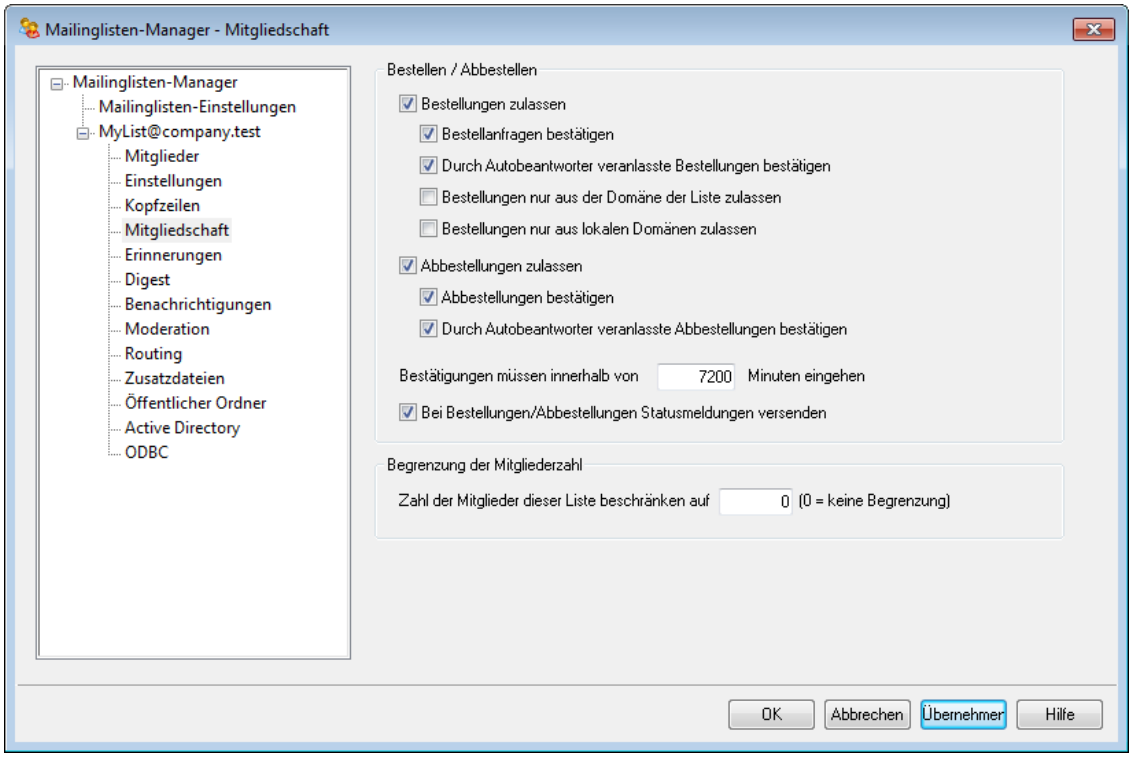
In Nachrichten aus Domänen, für die eine restriktive DMARC-Richtlinie veröffentlicht ist, E-Mail-Adresse im Absenderfeld "From" ersetzen durch E-Mail-Adresse der Liste
Diese Option ist per Voreinstellung aktiv. Sie ersetzt in eingehenden Listennachrichten die E-Mail-Adresse des Absenders in der Absenderkopfzeile From: (Von:) durch die E-Mail-Adresse der Mailingliste, bevor die Nachricht über die Mailingliste zugestellt wird. Diese Ersetzung wird nur vorgenommen, falls für die Domäne des Absenders der Listennachricht eine restriktive DMARC[538]-Richtlinie veröffentlicht ist (etwa p=quarantine oder p=reject). Diese Vorgehensweise verhindert, dass die Listennachrichten durch andere Server abgewiesen werden, die solche restriktiven DMARC-Policies befolgen. Neben der Änderung an der E-Mail-Adresse in der Kopfzeile From wird auch der Anzeigename geändert, indem ihm "via Listenname" angefügt wird; hierdurch wird deutlich, dass die Nachricht auf Veranlassung des Absenders durch die Mailingliste versandt wurde. Enthält die Nachricht keine Kopfzeile Reply-To:, und ist die Liste nicht so konfiguriert, dass die Kopfzeile Reply-To: bearbeitet wird, so wird bei jeder Änderung der Kopfzeile From: der ursprüngliche Inhalt der Kopfzeile From: in die Kopfzeile Reply-To: übernommen.

Sie sollten diese Option nicht deaktivieren, wenn Sie sich über die Folgen nicht vollständig im Klaren sind und sich dann bewusst dafür entschieden haben, auf dieses Leistungsmerkmal zu verzichten. Falls Sie diese Option deaktivieren, dann ist damit zu rechnen, dass Server von Empfängern der Listennachrichten diese Nachrichten abweisen. In manchen Fällen können die Empfänger auch automatisch aus der Mailingliste entfernt werden[280]. Sie können statt dieser Option auch die Option *Nachrichten von Absendern abweisen, für die restriktive DMARC-Richtlinien veröffentlicht sind*[278] aktivieren; dann werden eingehende Listennachrichten von Absenderdomänen mit restriktiven DMARC-Richtlinien abgewiesen.

Dem Inhalt der Betreffzeile den Namen der Liste voranstellen
Diese Option bewirkt, dass MDaemon den Namen der Mailingliste in eckige Klammern setzt und am Beginn der Betreffzeile in alle Listennachrichten einfügt (z.B. [MeineListe]). Diese Option ist per Voreinstellung aktiv.

An den Inhalt der Betreffzeile die Nummer des Diskussionsfadens anfügen
Diese Option bewirkt, dass an das Ende der Betreffzeile der Listennachrichten die Nummer des jeweiligen Diskussionsfadens gesetzt wird. Die Nummern werden dabei in geschweifte Klammern gesetzt. Sind die Diskussionsfadennummern vorhanden, so können die Listennachrichten im Posteingang durch Sortieren nach Betreff zugleich chronologisch sortiert werden. Diese Option ist per Voreinstellung abgeschaltet.

3.4.2.4 Mitgliedschaft



Bestellen / Abbestellen

Bestellungen zulassen
Mit dieser Option wird festgelegt, ob neue Mitglieder die Liste bestellen können, indem sie eine entsprechende Anforderung an MDaemon senden. Bestellungen sind durch Steuernachrichten besonderen Inhalts oder über Autobeantworter möglich. Nähere Informationen hierzu finden Sie im Abschnitt Mailinglisten bestellen 286.

Bestellanfragen bestätigen
Mit dieser Option prüft MDaemon die Bestellung nachzuprüfen. MDaemon erstellt dazu einen eindeutigen Kode für die Bestellung und sendet ihn in einer entsprechenden Nachricht an das neue Mitglied. Dieses muss auf die Nachricht antworten, bevor MDaemon den Benutzer in die Mailingliste einträgt. Die Bestätigungen müssen innerhalb einer bestimmten Frist eingehen; die Benutzer müssen daher in der weiter unten festgelegten Frist auf die Nachrichten geantwortet haben. **Beachte:** Sie finden den Inhalt der Bestätigungsnachricht in der Datei `SubConf.dat` im Verzeichnis "`MDaemon\app\`".

Durch Autobeantworter veranlasste Bestellungen bestätigen
Soll sich die Bestätigung auch auf solche Bestellungen erstrecken, die über die Funktion *Absender der folgenden Mailingliste hinzufügen* durch einen Autobeantworter 724 veranlasst wurden, so muss diese Option gesetzt sein. Wie bei der Option oben erstellt MDaemon einen eindeutigen Kode und versendet ihn an das neue Mitglied. Auch hier muss die Bestätigung in der unten festgelegten Frist eingehen.

Bestellungen nur aus der Domäne der Liste zulassen
Diese Option bewirkt, dass Benutzer der Mailingliste nur dann beitreten können, wenn sie zu derselben Domäne gehören wie die Mailingliste selbst. Ein Beispiel hierzu: Für die Mailingliste "MyList@example.com" können bei aktivierter Option nur Benutzer aus der Domäne "example.com" die Mailingliste bestellen.

Bestellungen nur aus lokalen Domänen zulassen
Diese Option bewirkt, dass Benutzer der Mailingliste nur dann beitreten können, wenn sie zu einer der Domänen gehören, die auf demselben Server gehostet sind, auf dem auch die Mailingliste gehostet wird.

Abbestellen

Abbestellungen zulassen
Hiermit wird festgelegt, ob Benutzer eine Mailingliste durch eine Nachricht an MDaemon abbestellen können. Abbestellungen sind durch Steuernachrichten besonderen Inhalts oder über Autobeantworter möglich. Nähere Informationen hierzu finden Sie im Abschnitt Mailinglisten bestellen 286.

Abbestellungen bestätigen
Mit dieser Option prüft MDaemon die Abbestellung nach. Diese Prüfung funktioniert genauso wie die oben beschriebene Prüfung von Bestellungen. MDaemon erstellt dazu einen eindeutigen Kode für die Abbestellung und sendet ihn in einer entsprechenden Nachricht an das Mitglied. Dieses muss auf die Nachricht antworten, bevor MDaemon den Benutzer aus der Mailingliste entfernt. Die Bestätigungen müssen innerhalb einer bestimmten Frist eingehen; die Benutzer müssen daher in der weiter unten festgelegten Frist auf die Nachrichten geantwortet haben.**Beachte:** Sie finden den Inhalt der Bestätigungsnachricht in der Datei `UnSubConf.dat` im Verzeichnis "`MDaemon\app\`".

Durch Autobeantworter veranlasste Bestellungen bestätigen
Soll sich die Bestätigung auch auf solche Abbestellungen erstrecken, die über die Funktion *Absender aus folgender Mailingliste entfernen* durch einen Autobeantworter 724 veranlasst wurden, so muss diese Option gesetzt sein. Wie bei der Option oben erstellt MDaemon einen eindeutigen Kode und versendet ihn an das Mitglied, das die Liste abbestellen will. Auch hier muss die Bestätigung in der unten festgelegten Frist eingehen. Nach Eingang der Bestätigung entfernt MDaemon das Mitglied aus der Liste.

Bestätigungen müssen innerhalb von [xx] Minuten eingehen
Hier wird die Zeit in Minuten eingetragen, die einem Mitglied für die Bestätigung einer Anforderung zur Bestellung oder Abbestellung der Mailingliste verbleibt. Geht innerhalb dieser Frist keine Antwort auf die Bestätigungsanfrage bei MDaemon ein, so wird die fragliche Adresse nicht in die Liste eingetragen oder aus ihr entfernt. Der Benutzer muss dann die Bestellung oder Abbestellung erneut durchführen. Die Voreinstellung beträgt 7.200 Minuten, also fünf Tage.

Diese Einstellung gilt systemweit für alle Mailinglisten. Sie betrifft nicht nur die gerade bearbeitete Mailingliste.

Bei Bestellungen/Abbestellungen Statusmeldungen versenden
Diese Option bewirkt, dass MDaemon nach erfolgreich abgeschlossenen Bestellungen und Abbestellungen Bestätigungsnachrichten versendet, die den Abschluss des jeweiligen Vorgangs bestätigen.

Begrenzung der Mitgliederzahl

Zahl der Mitglieder dieser Liste beschränken auf [xx] (0=keine Begrenzung)
Diese Option begrenzt die Mitgliederzahl für diese Liste. Der Wert 0 bewirkt, dass die Mitgliederzahl nicht begrenzt wird.

Diese Beschränkung wirkt nur auf Adressen, die über E-Mail mithilfe der Verfahren im Abschnitt *Mailinglisten bestellen* 286 in die Liste eingetragen werden. Sie wirkt nicht auf Adresse, die im Konfigurationsdialog Mitglieder 275 von Hand eingetragen werden, und nicht auf Adressen, die per E-Mail die Liste bestellen und dabei das Listenkennwort 292 verwenden.

Siehe auch:

Mailinglisten bestellen 286
Autobeantworter 724

3.4.2.4.1 Mailinglisten bestellen

Bestellen/Abbestellen über E-Mail-Befehle

Um eine Mailingliste zu bestellen oder abzubestellen, sendet der Benutzer eine Nachricht an `MDaemon` oder einen dafür gültigen Aliasnamen bei der Domäne, zu der die Mailingliste gehört, und setzt den Befehl `Subscribe` oder `Unsubscribe` in die erste Zeile des Nachrichtentextes. Ein Beispiel hierzu: Bei `mdaemon.com` besteht eine Mailingliste namens `MD-Support`. Diese kann durch eine Nachricht an "`mdaemon@mdaemon.com`" bestellt werden, deren erste Zeile des Nachrichtentextes "`SUBSCRIBE MD-Support@mdaemon.com`"enthalten muss. Die Betreffzeile wird nicht ausgewertet und kann leer bleiben.

Umfassende Informationen über Inhalt und Aufbau solcher und anderer Steuernachrichten finden Sie im Abschnitt Fernsteuerung des Servers über E-Mail 888 .

Manche Benutzer versuchen, eine Mailingliste zu bestellen oder abzubestellen, indem sie die entsprechenden Befehle per E-Mail an die Liste selbst, nicht aber an das Systemkonto von MDaemon senden. Solche Nachrichten werden dann in der Liste veröffentlicht, sie bewirken aber weder eine Bestellung noch eine Abbestellung. Die Option *Eingehende Listennachrichten auf offensichtlich listenfremde Inhalte prüfen* im Konfigurationsdialog Einstellungen » Voreinstellungen » System 495 verhindert, dass solche falsch adressierten Nachrichten in der

Mailingliste veröffentlicht werden. Diese Option ist per Voreinstellung aktiv.

Bestellen/Abbestellen über E-Mail-Adressen

Die Option *Adressen "<Liste>-subscribe" und "<Liste>-unsubscribe" auswerten* im Konfigurationsdialog Einstellungen » Mailinglisten-Manager » Mailinglisten-Einstellungen[272] ermöglicht es Benutzern, eine Mailingliste zu bestellen und abzubestellen, indem sie statt den oben unter *Bestellen/Abbestellen über E-Mail-Befehle* beschriebenen Befehlen in E-Mail-Nachrichten besondere E-Mail-Adressen verwenden. Bei Nutzung dieser Methode zur Bestellung und Abbestellung sendet der Benutzer einfach eine Nachricht an die Adresse der Liste und setzt dabei dem Postfachnamen den Text "`-subscribe`" für Bestellungen und "`-unsubscribe`" für Abbestellungen hinzu. Lautet der Name der Liste etwa "`franks-list@example.com`", so kann ein Benutzer die Liste durch Versand einer Nachricht an "`franks-list-subscribe@example.com`" bestellen und durch eine Nachricht an "`franks-list-unsubscribe@example.com`" abbestellen. In beiden Fällen werden Inhalt und Betreff der Nachricht nicht beachtet. Solange diese Funktion aktiv ist, fügt MDaemon die folgende Kopfzeile in alle Listennachrichten ein:

```
List-Unsubscribe: <mailto:<Liste>-Unsubscribe@example.com>
```

Manche Mailclients werten diese Zeile aus und stellen den Benutzern daraufhin automatisch ein Steuerelement "Abbestellen" zur Verfügung.

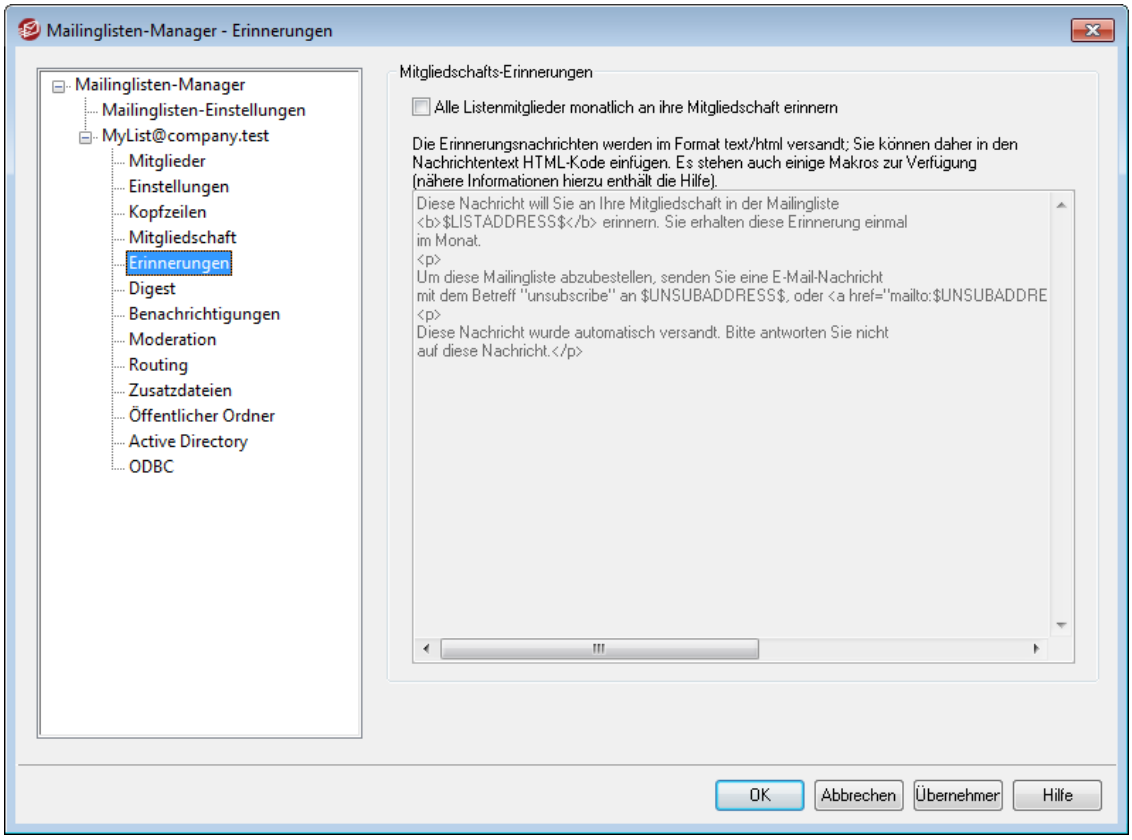
Bestellen/Abbestellen über Autobeantworter

Zum Bestellen und Abbestellen einer Mailingliste können Sie auch Autobeantworter[724] einrichten. Hierzu erstellen Sie Benutzerkonten in MDaemon, die nur den Zweck haben, Adressen, die Nachrichten an diese Benutzerkonten schreiben, mithilfe von Autobeantwortern in Mailinglisten ein- und aus ihnen auszutragen. Hierzu müssen Autobeantworter für jedes Benutzerkonto erstellt werden. Besteht beispielsweise eine Mailingliste "`franks-list@example.com`", so können Sie ein Benutzerkonto mit der Adresse "`franks-list-bestellen@example.com`" erstellen. Sie konfigurieren dann einen Autobeantworter für dieses Benutzerkonto, der alle Absenderadressen eingehender Nachrichten in die Mailingliste "`franks-list@example.com`" einträgt. Wer die Mailingliste bestellen will, schreibt dann einfach eine Nachricht an "`franks-list-bestellen@example.com`". Dies ist eine bequeme Lösung für die Benutzer, da sie sich keine Befehle für die Bestellung und Abbestellung durch E-Mail-Nachrichten merken müssen.

Siehe auch:

Mitgliedschaft[284]
Fernsteuerung des Servers über E-Mail[888]
Autobeantworter[724]
Mailinglisten-Einstellungen[278]

3.4.2.5 Erinnerungen



Mitgliedschafts-Erinnerungen

Alle Listenmitglieder monatlich an ihre Mitgliedschaft erinnern
Diese Option bewirkt, dass der Inhalt des nachfolgenden Textfeldes jeweils am Monatsersten an alle Listenmitglieder als Erinnerung an die Mitgliedschaft in der Mailingliste versandt wird. Die Nachricht wird als text/html versandt; Sie können daher im Text auch HTML-Kode verwenden, falls dies gewünscht ist. Die folgenden Makros sind in der Erinnerungsnachricht verfügbar:

$LISTADDRESS$ - wird ersetzt durch die E-Mail-Adresse der Mailingliste (z.B. MeineListe@example.com)

$LISTNAME$ - wird ersetzt durch den Listennamen selbst (z.B. MeineListe).

$UNSUBADDRESS$ - wird ersetzt durch die Adresse, an die Abbestellungen für die Liste zu richten sind (die E-Mail-Adresse des MDaemon-Systemkontos, z.B. mdaemon@example.com)

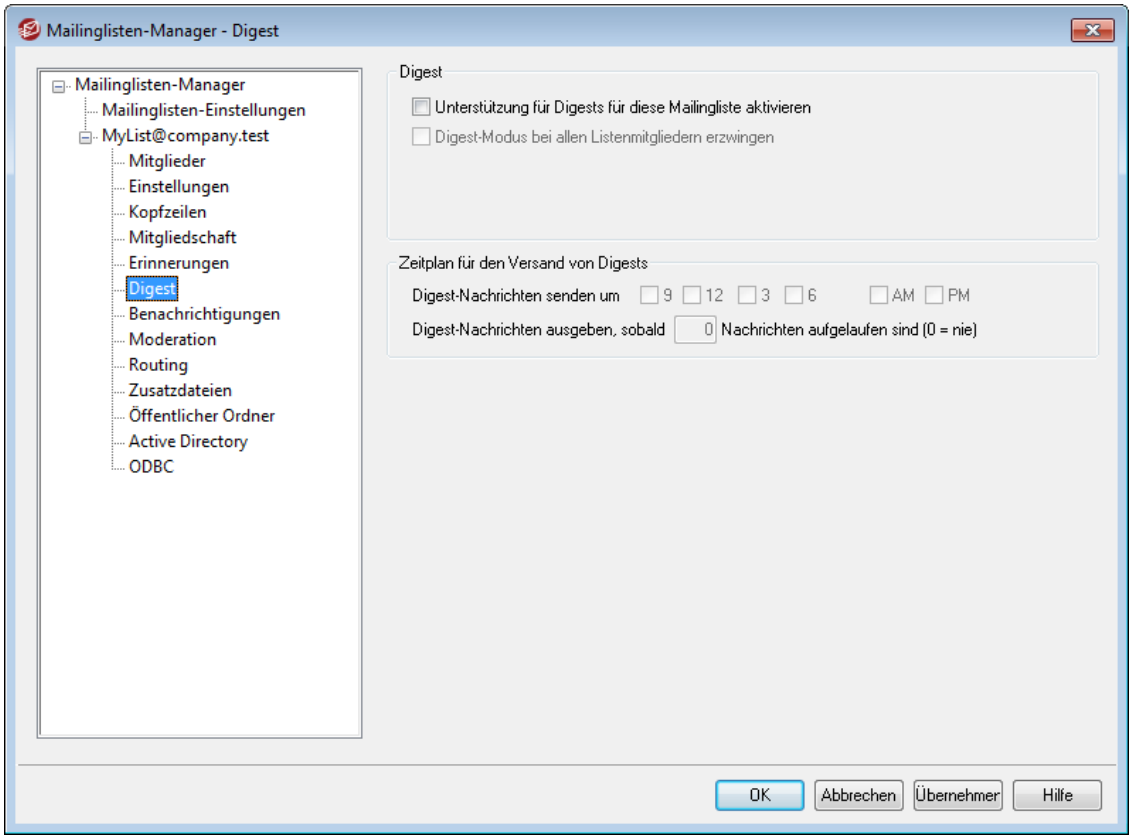
$MEMBERADDRESS$ - wird ersetzt durch die E-Mail-Adresse des Listenmitglieds, das die jeweilige Erinnerungsnachricht erhält (z.B. frank.thomas@example.com)

Falls Sie die Erinnerungsnachrichten an einem anderen Tag des Monats versenden möchten, können Sie den Tag durch Bearbeiten des folgenden Eintrags in der Datei MDaemon.ini ändern:

```
[Special]
ListReminderDay=X
```

An die Stelle des Platzhalters X setzen Sie dabei eine Zahl von 1 bis 28; sie entspricht dem Tag, an dem Sie die Erinnerungen in jedem Monat versenden möchten.

3.4.2.6 Digest



Digest

Unterstützung für Digests für diese Mailingliste aktivieren
Diese Option bestimmt, ob die Mailingliste das Digest-Format unterstützt. Wird Digest unterstützt, so wird eine Kopie jeder Listennachricht archiviert. Mitglieder, die aufgrund des Typs ihrer Mitgliedschaft 275 die Listenpost im Digest-Format empfangen wollen, erhalten diese archivierten Nachrichten in übersichtlichem indiziertem Format. Sie erhalten sie nicht einzeln direkt nach Eingang.

Digest-Modus bei allen Listenmitgliedern erzwingen
Grundsätzlich legen die Mitglieder selbst fest, ob sie Listenpost im Normal- oder Digest-Format erhalten wollen. Mit dieser Option werden alle Mitglieder, unabhängig von ihrer Auswahl, auf den Digest-Modus festgelegt.

Zeitplan für den Versand von Digests

Die folgenden Optionen bestimmen, wie oft und unter welchen Umständen die Digest-Nachrichten an Listenmitglieder versandt werden, die ihre Listenpost im Digest-Format erhalten. Die Optionen wirken unabhängig von einander, so dass jede einzelne für sich den Versand eines Digests auslösen kann.

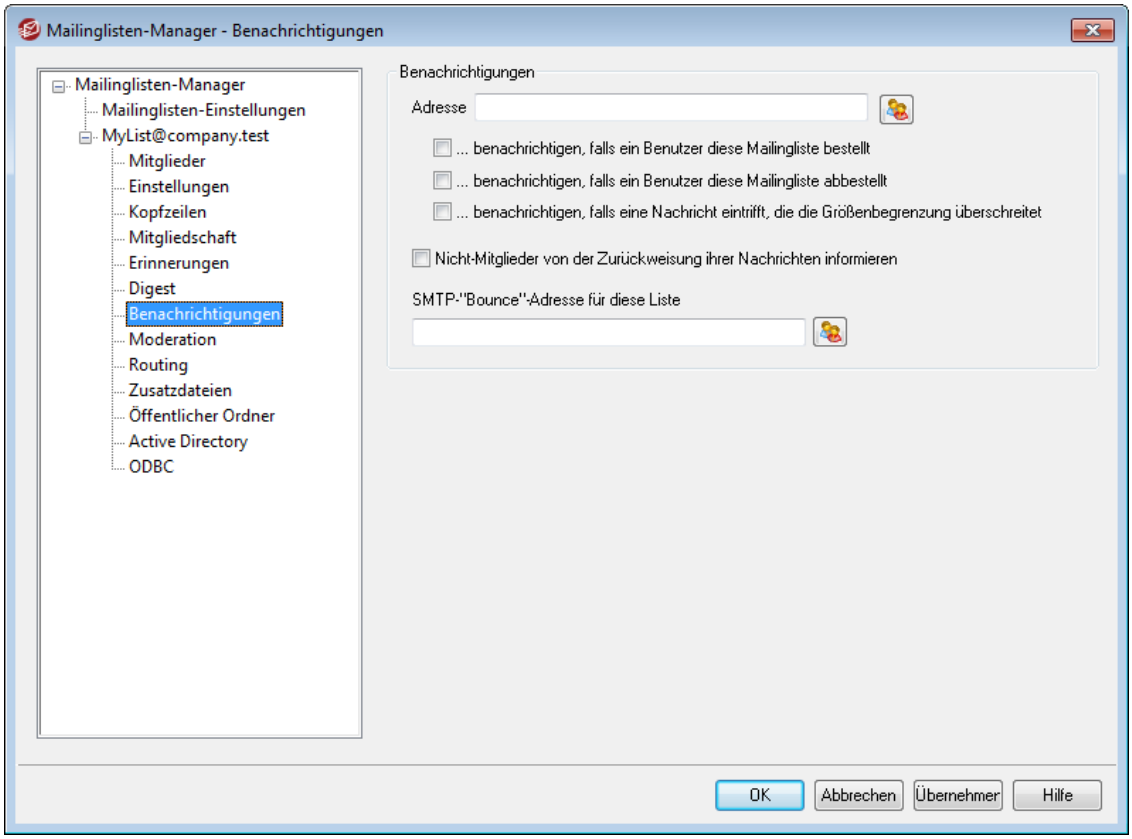
Digest-Nachrichten senden um 9, 12, 3, 6 AM und/oder PM
Diese Option bestimmt, wie oft die Digest-Nachrichten versandt werden. Falls Sie alle Kontrollkästchen in diesem Abschnitt aktivieren, werden die Digest-Nachrichten alle drei Stunden versandt. Zusätzlich können die Nachrichten auch durch die folgenden Optionen versandt werden.

Digest-Nachrichten ausgeben, sobald [xx] Nachrichten aufgelaufen sind (0 = nie)
Diese Option bewirkt, dass eine Digest-Nachricht versandt wird, sobald die hier angegebene Anzahl von Nachrichten in der Liste aufgelaufen ist. Der Wert 0 (der auch die Voreinstellung darstellt) bewirkt, dass diese Option abgeschaltet ist.

Siehe auch:

Mitglieder 275
Fernsteuerung des Servers über E-Mail 888

3.4.2.7 Benachrichtigungen



Benachrichtigungen

Adresse [xx]
Die hier angegebene Adresse wird benachrichtigt, falls die nachfolgend ausgewählten Ereignisse eintreten.

...benachrichtigen, falls ein Benutzer diese Mailingliste bestellt
Die vorher angegebene Adresse wird jedes Mal dann benachrichtigt, wenn ein Benutzer die Mailingliste abonniert.

...benachrichtigen, falls ein Benutzer diese Mailingliste abbestellt
Die Adresse wird benachrichtigt, wenn ein Benutzer die Liste abbestellt.

...benachrichtigen, falls eine Nachricht eintrifft, die die Größenbegrenzung überschreitet
Eine Benachrichtigung erfolgt, wenn ein Benutzer eine Nachricht sendet, die über der Größenbegrenzung liegt. Die Größenbegrenzung wird mithilfe der Option *Liste akzeptiert Nachrichten nur bis zur Größe von [xx] KB* im Konfigurationsdialog Einstellungen 278 festgelegt.

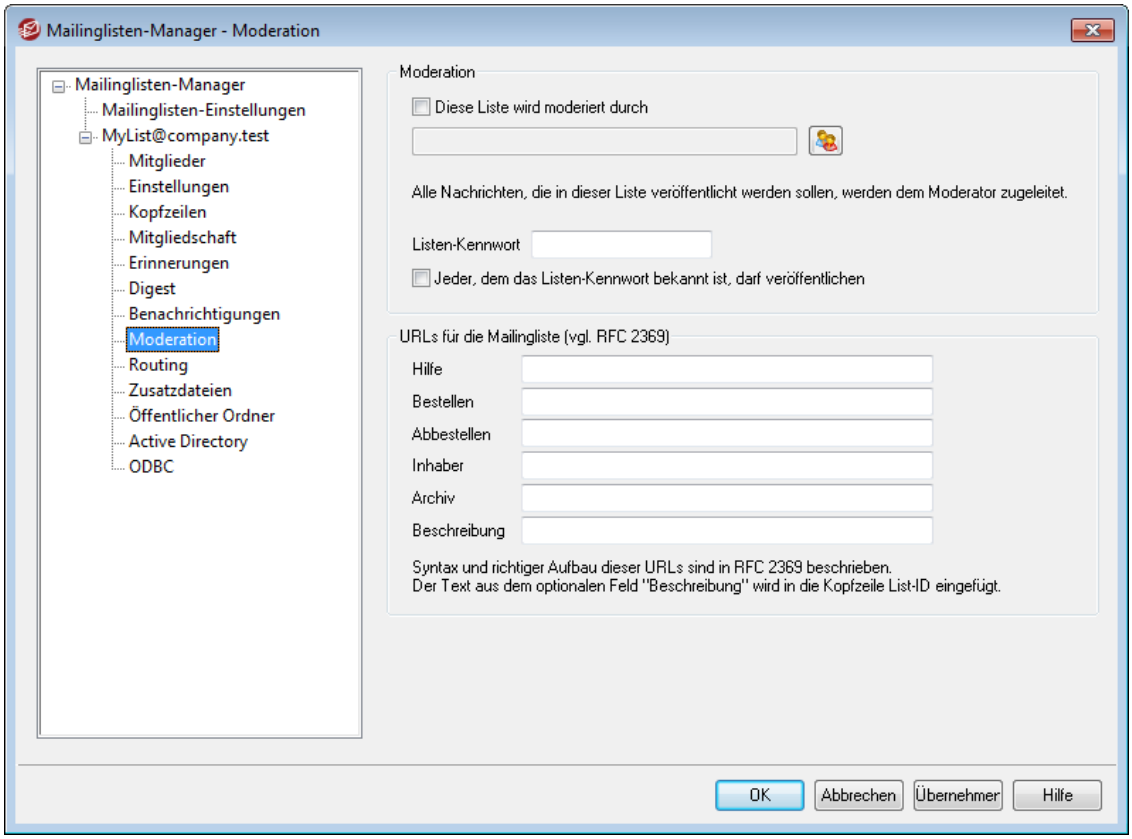
Nicht-Mitglieder von der Zurückweisung ihrer Nachrichten informieren
Sendet ein Benutzer eine Nachricht an eine private Liste, ohne Mitglied zu sein, so wird er von MDaemon informiert, dass die Nachricht zurückgewiesen wurde. Der Benutzer erfährt dabei auch, wie er sich anmelden kann. Listen werden als privat gekennzeichnet, indem die Option *Nur Listenmitglieder dürfen in dieser Liste veröffentlichen* im Konfigurationsdialog Einstellungen 278 aktiviert wird.

Zurücklaufende Nachrichten

SMTP-"Bounce"-Adresse für diese Liste
Hier wird eine Adresse angegeben, die unzustellbare Nachrichten erhält, wenn diese an die Liste zurückgehen. In einer Mailingliste von 100 Teilnehmern kann es beispielsweise 10 – 20 Benutzer geben, die wegen Adressänderungen, gestörter Server o.ä. nicht erreichbar sind, sodass Nachrichten an diese Benutzer zur Liste zurückkommen. Das SMTP-System erstellt Benachrichtigungen mit weiteren Informationen über solche unerreichbaren Adressen und leitet sie an den Absender zurück. Der Empfänger für solche Benachrichtigungen kann hier zentral bestimmt werden. Wird kein Empfänger angegeben, dann versendet MDaemon die Listennachrichten so, dass es keine Rückläufer geben kann. Diese Adresse soll nicht die Adresse der Mailingliste selbst sein.

Wird die E-Mail-Adresse eines lokalen Benutzers als *SMTP-"Bounce"-Adresse für diese Liste* eingetragen, so kann dies dazu führen, dass die E-Mail-Nachrichten dieses Benutzers gelöscht werden. Ob dieser Fall wirklich eintritt, hängt von den Einstellungen zur Bereinigung der Listen aus dem Konfigurationsdialog Mailinglisten-Einstellungen 272 ab. Tragen Sie daher die Adresse eines lokalen Benutzers als Bounce-Adresse nur ein, wenn Sie eine Fehlfunktion ausschließen können. Nähere Informationen finden Sie im Abschnitt Erweiterte Bereinigung von Mailinglisten 280.

3.4.2.8 Moderation



Moderation

Diese Liste wird moderiert durch
Ist diese Option gesetzt, so wird die Liste von dem angegebenen Benutzer moderiert. Bei moderierten Listen werden alle Nachrichten der Mitglieder erst dem Moderator zugeleitet; er darf als einziger Nachrichten in der Liste veröffentlichen.

Listen-Kennwort
Sie können in dieses Textfeld ein Kennwort für die Liste eintragen. Dieses Kennwort kann zusammen mit der Option *Jeder, dem das Listenkennwort bekannt ist, darf veröffentlichen* weiter unten eingesetzt werden, und mithilfe des Kennworts kann die Höchstzahl der Mitglieder, die im Konfigurationsdialog Mitgliedschaft 284 konfiguriert wird, übergangen werden. Das Kennwort eröffnet auch den Zugang zu mehreren Funktionen, die im Abschnitt *Fernsteuerung des Servers über E-Mail* 888 näher beschrieben sind.

Jeder, dem das Listen-Kennwort bekannt ist, darf veröffentlichen
Ist ein Kennwort für die Liste vergeben, und ist diese Option aktiv, so kann jeder veröffentlichen, indem er das Kennwort an den Beginn der Nachricht setzt, die er an die Liste sendet. Auf diese Weise können auch in moderierten Listen Benutzer Nachrichten veröffentlichen, obwohl sie nicht Moderatoren sind.

URLs für die Mailingliste (vgl. RFC 2369)

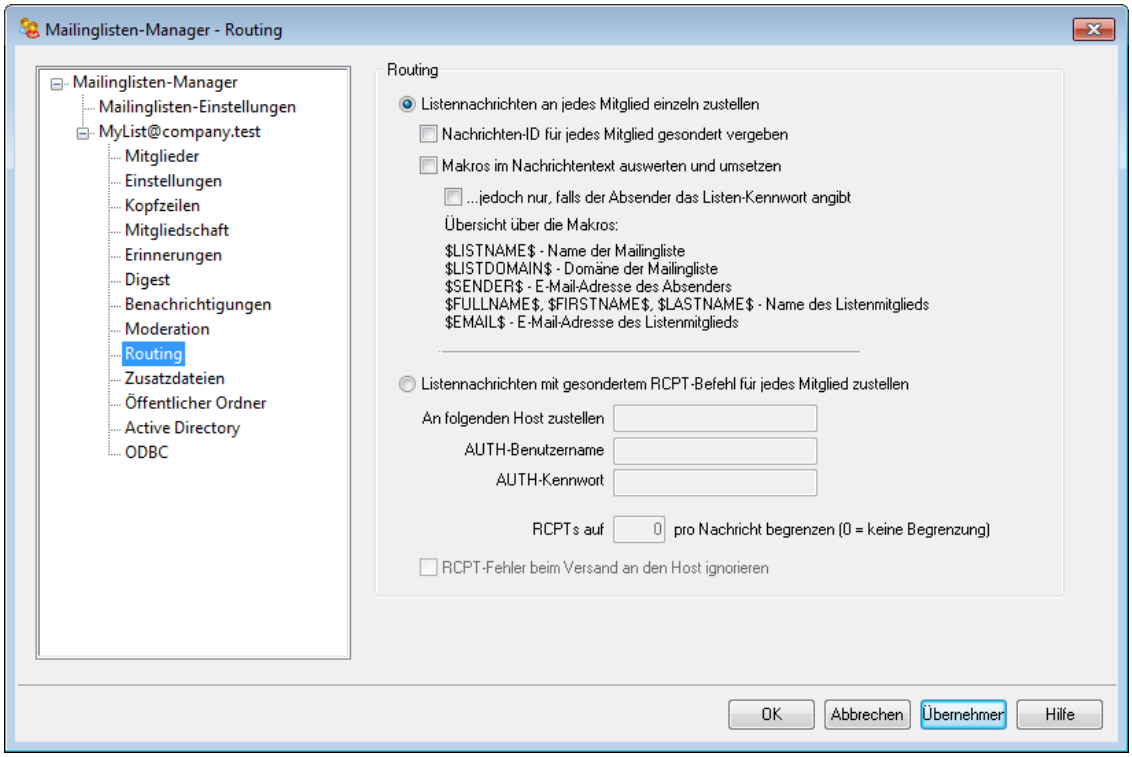
MDaemon kann in Listennachrichten alle sechs Kopfzeilen einfügen, die in RFC 2369 (*Die Verwendung von URLs als Meta-Syntax für wesentliche Befehle in Mailinglisten und ihre Übermittlung in Kopfzeilen von Nachrichten*) beschrieben sind. Die Kopfzeilen sind: **List-Help** (Hilfe), **List-Subscribe** (Bestellen), **List-**

Unsubscribe (Abbestellen), **List-Post** (Veröffentlichen), **List-Owner** (Inhaber) und **List-Archive** (Archiv). Falls Sie eine oder mehrere dieser Kopfzeilen in die Listennachrichten einfügen lassen wollen, tragen Sie in die zugehörigen Felder die gewünschten Inhalte ein. Das Format der Inhalte muss dem in RFC 2369 beschriebenen Format entsprechen (z.B. `<mailto:liste@example.com?subject=Hilfe>`). Das über die vorstehende Verknüpfung erreichbare Dokument, das derzeit nur in englischer Sprache verfügbar ist, enthält für die Kopfzeilen auch Beispiele. MDaemon ändert die Inhalte nicht; liegen sie nicht im richtigen Format vor, so bleiben sie daher wirkungslos.

Beschreibung (wird in die Kopfzeile List-ID: eingefügt)
In dieses Feld können Sie eine kurze Beschreibung der Mailingliste eintragen. Diese Beschreibung wird in die Kopfzeile `List-ID:` aller über die Liste versandten Nachrichten eingefügt. Die Beschreibung und die Kennung der Mailingliste werden in die Kopfzeile aufgenommen (z.B. `List-ID: "Franks persönliche Mailingliste" <MeineListe.example.com>`). Die Kennung entspricht der E-Mail-Adresse der Mailingliste, in der jedoch das Zeichen @ durch das Zeichen . ersetzt wird; diese Änderung ist erforderlich, um die Spezifikation für Listen-IDs einzuhalten. Falls Sie die *Beschreibung* leer lassen, enthält die Kopfzeile `List-ID:` nur die Kennung der Mailingliste (z.B. `List-ID: <MeineListe.example.com>`). Enthält eine für die Mailingliste eingehende Nachricht bereits eine Kopfzeile List-ID:, so ersetzt MDaemon diese bestehende Kopfzeile durch die eigene Kopfzeile für die zugehörige Liste.

Die Kopfzeilen List-Subscribe und List-Unsubscribe sind per Voreinstellung in allen Listennachrichten vorhanden, solange die Option Adressen "*<Liste>-subscribe" und "<Liste>-unsubscribe*" auswerten im Konfigurationsdialog Mailinglisten-Einstellungen 278 aktiv ist. Falls Sie die entsprechenden Kopfzeilen für die gerade bearbeitete Liste anpassen wollen, tragen Sie die gewünschten Inhalte hier ein. Ist die genannte Option deaktiviert, so werden die Kopfzeilen List-Subscribe und List-Unsubscribe nur dann in die Listennachrichten eingefügt, wenn hier entsprechende Inhalte eingetragen sind.

3.4.2.9 Routing



Routing

Listennachrichten an jedes Mitglied einzeln zustellen
Diese Option bewirkt, dass für alle Nachrichten, die zur Zustellung in einer Mailingliste eingehen, je eine eigene Nachricht für jedes Mitglied erstellt und an das Mitglied versandt wird. Hierdurch werden zahlreiche Einzelnachrichten erstellt; dies kann, abhängig von der Größe der Liste und der Auslastung, die Systemleistung des Servers beeinträchtigen.

Nachrichten-ID für jedes Mitglied gesondert vergeben
MDaemon kann sicherstellen, dass jede nach oben stehender Option erzeugte Einzelnachricht eine eindeutige Nachrichten-ID erhält. Dazu ist diese Option zu setzen. Diese Option ist per Voreinstellung abgeschaltet. Sie sollte nur dann aktiviert werden, wenn die beschriebene Vorgehensweise im jeweiligen Einsatzumfeld erforderlich ist.

Makros im Nachrichtentext auswerten und umsetzen
Diese Option bewirkt, dass in den Listennachrichten bestimmte Makros unterstützt und ausgewertet werden. Wird ein solches Makro gefunden, so ersetzt MDaemon das Makro durch den ihm zugeordneten Inhalt. Diese Ersetzung erfolgt für jede Nachricht gesondert, bevor sie an die einzelnen Listenmitglieder versandt wird.

...jedoch nur, falls der Absender das Listen-Kennwort angibt
Mithilfe dieser Option können Sie die Nutzung der Makros auf Nachrichten solcher Benutzer beschränken, in denen das Listenkennwort 292 angegeben ist. Makros in anderen Nachrichten werden dann nicht ausgewertet. Wenn diese Option deaktiviert ist, können alle Benutzer die Makros verwenden, die auch Nachrichten an die Liste senden dürfen.

Makros:

$LISTNAME$	Der Name der Liste. Er entspricht dem "Postfach"-Teil der vollständigen Adresse der Liste (z.B. "MeineListe" bei MeineListe@example.com).
$LISTDOMAIN$	Die Domäne der Liste (z.B. "example.com" bei MeineListe@example.com).
$SENDER$	Die E-Mail-Adresse des Absenders der Nachricht.
$FULLNAME$ $FIRSTNAME$ $LASTNAME$	Der vollständige Name, der Vorname oder der Nachname des Listenmitglieds, soweit verfügbar.
$EMAIL$	Die E-Mail-Adresse des Listenmitglieds.

Listennachrichten mit gesondertem RCPT-Befehl für jedes Mitglied zustellen
Diese Option bewirkt, dass MDaemon eine einzige Kopie jeder Listennachricht an den unten angegebenen Smart-Host sendet. Es werden keine getrennten Nachrichten für jedes Mitglied versandt. Bei dieser Methode werden während der SMTP-Verbindung an den angegebenen Host mehrere Befehle `RCPT To` übermittelt.

An folgenden Host zustellen
Tragen Sie hier den Smart-Host ein, an den Sie mithilfe mehrerer Befehle RCPT To alle Listennachrichten für die Mitglieder übermitteln wollen.

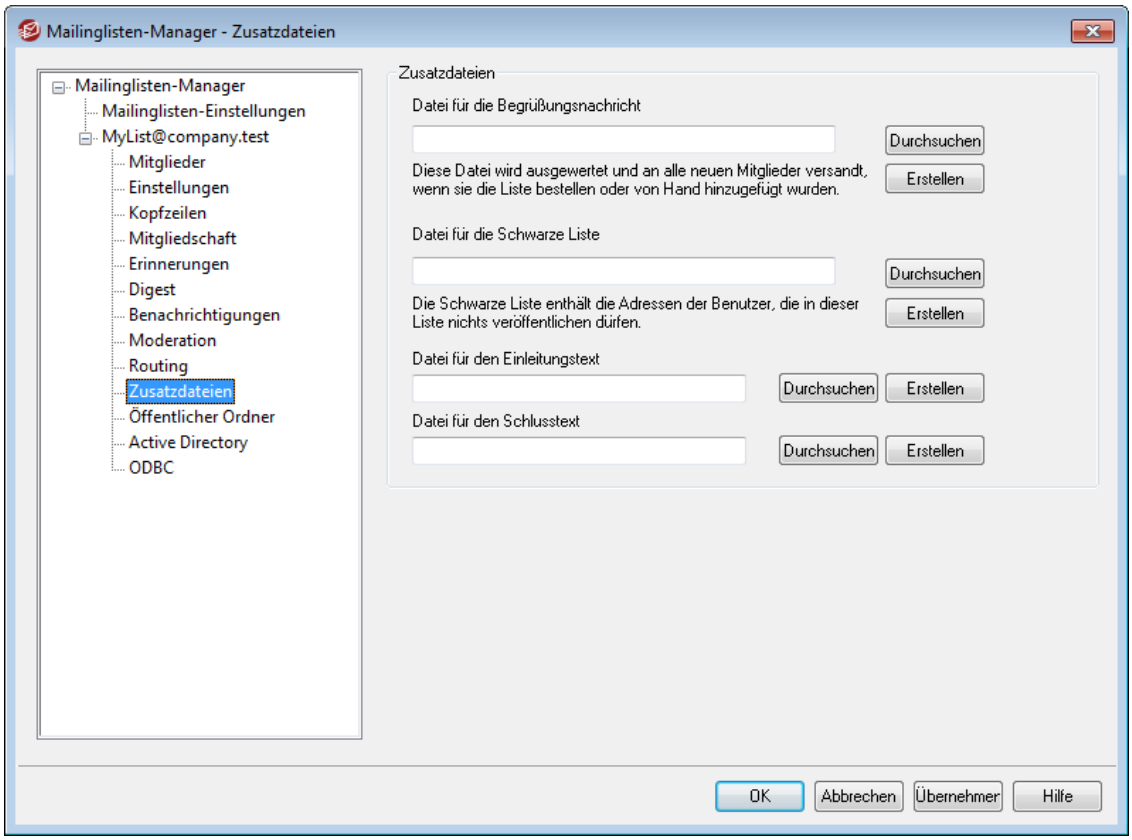
AUTH-Benutzername/Kennwort
Benutzername und Kennwort zur Anmeldung an dem Host, soweit erforderlich.

RCPTs auf [xx] pro Nachricht begrenzen (0=keine Begrenzung)
Manche Server nehmen nur eine bestimmte Anzahl an Empfängern pro Nachricht an. Diese Begrenzung kann hier eingetragen werden, sodass MDaemon zusätzliche Kopien derselben Nachricht erstellt und diese jeweils an weniger Empfänger gleichzeitig richtet. Hiermit wird die Begrenzung bei den Servern unterlaufen. Diese Funktion ist mit der Funktion *Listennachrichten an jedes Mitglied einzeln zustellen* vergleichbar, nur wird die Post hierbei in Empfängergruppen aufgeteilt, und es wird nicht pro Empfänger eine eigene Nachricht erstellt.

RCPT-Fehler beim Versand an den Host ignorieren
Manche Mailserver versenden an bestimmte Domänen keine Post, sodass bei dem Routing nur einer einzigen Nachricht Probleme auftreten können. Ein

Fehler während des Versands würde MDaemon normalerweise veranlassen, die Zustellung insgesamt abzubrechen. Mit dieser Option ignoriert MDaemon hingegen die Fehlermeldungen des Servers während des Versands und stellt damit sicher, dass wenigstens die übrigen Empfänger die Nachrichten erhalten.

3.4.2.10 Zusatzdateien



Zusatzdateien

Datei für die Begrüßungsnachricht
Falls hier eine Datei angegeben ist, wird sie immer dann verarbeitet, wenn neue Mitglieder die Mailingliste bestellt haben. Der Inhalt der Datei wird dann an die neuen Mitglieder versandt. Die folgenden Makros können in der Begrüßungsnachricht für neue Mitglieder benutzt werden:

`$PRIMARYDOMAIN$`	Dieses Makro wird in den Namen der Standard-Domäne von MDaemon umgesetzt; dieser Name wird im Konfigurationsdialog Domänen-Manager 181 bestimmt.
`$PRIMARYIP$`	Dieses Makro wird in die IP-Adresse umgesetzt, die mit der Standard-Domäne von MDaemon verknüpft ist.
`$MACHINENAME$`	Dieses Makro wird in den FQDN umgesetzt, der im Konfigurationsmenü für die Standard-Domäne eingerichtet wird.

`$LISTEMAIL$` Dieses Makro wird in die E-Mail-Adresse der Liste umgesetzt, z.B. `MeineListe@example.com`.

`$LISTNAME$` Dieses Makro wird in den Namen der Mailingliste umgesetzt, z.B. `MeineListe`.

`$LISTDOMAIN$` Dieses Makro wird in den Domänennamen der Mailingliste umgesetzt, z.B. `example.com`.

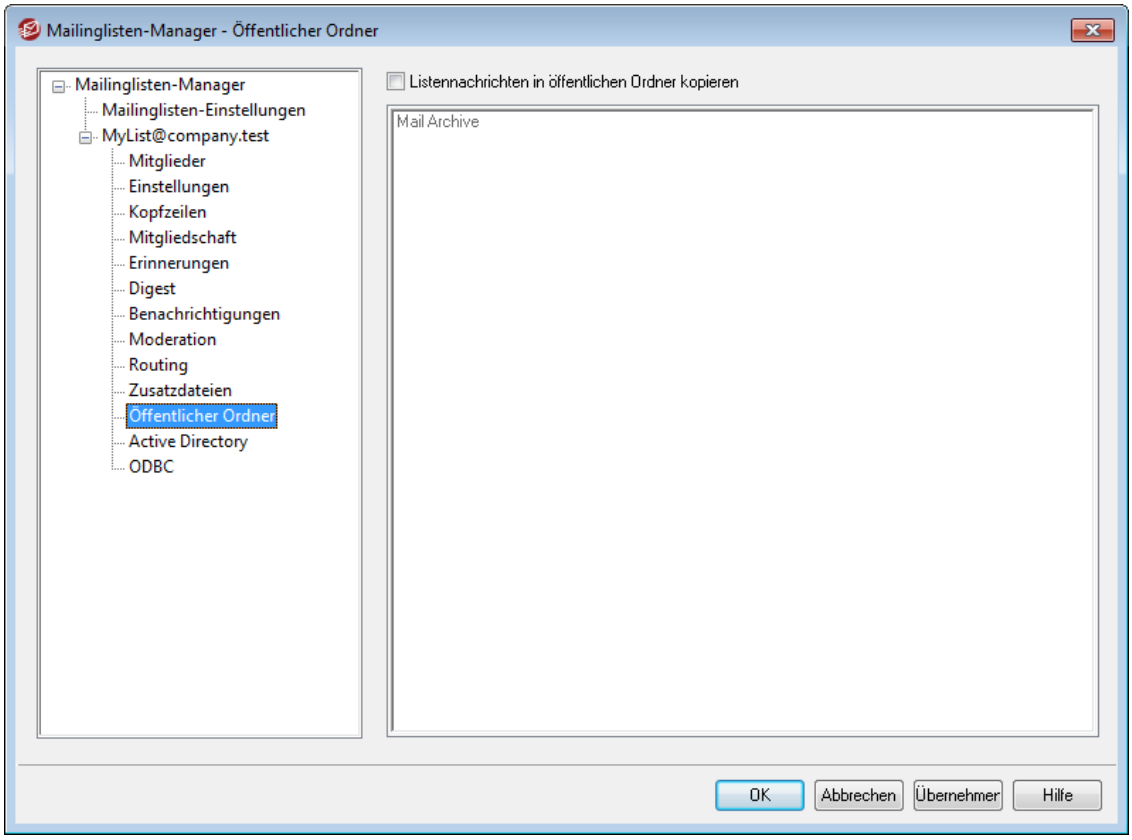
`%SETSUBJECT%` Mithilfe dieses Makros kann in der Begrüßungsnachricht ein abweichender Betreff angegeben werden. Der gewünschte Text kann dabei andere für Listen zugelassene Makros enthalten, wie etwa `$LISTEMAIL$`. Ein Beispiel hierzu: `%SetSubject%=Willkommen in der Mailingliste $LISTNAME$`.

Datei für die Sperrliste
Falls hier eine Datei angegeben ist, wird die Mailingliste für die darin enthaltenen Adressen gesperrt, sodass Nachrichten von diesen die Liste nicht erreichen.

Datei für den Einleitungstext/Schlusstext
Die Inhalte der hier angegebenen Dateien werden den Listennachrichten als Einleitungs- und Schlusstexte hinzugefügt.

Erstellen
Um eine neue Datei zu erstellen, klicken Sie auf das Steuerelement *Erstellen*, das der Datei zugeordnet ist, die Sie anlegen wollen. Geben Sie einen Namen ein, und klicken Sie auf *Öffnen*. Die neu erstellte Datei wird hierdurch in Notepad zur Bearbeitung geöffnet.

3.4.2.11 Öffentlicher Ordner

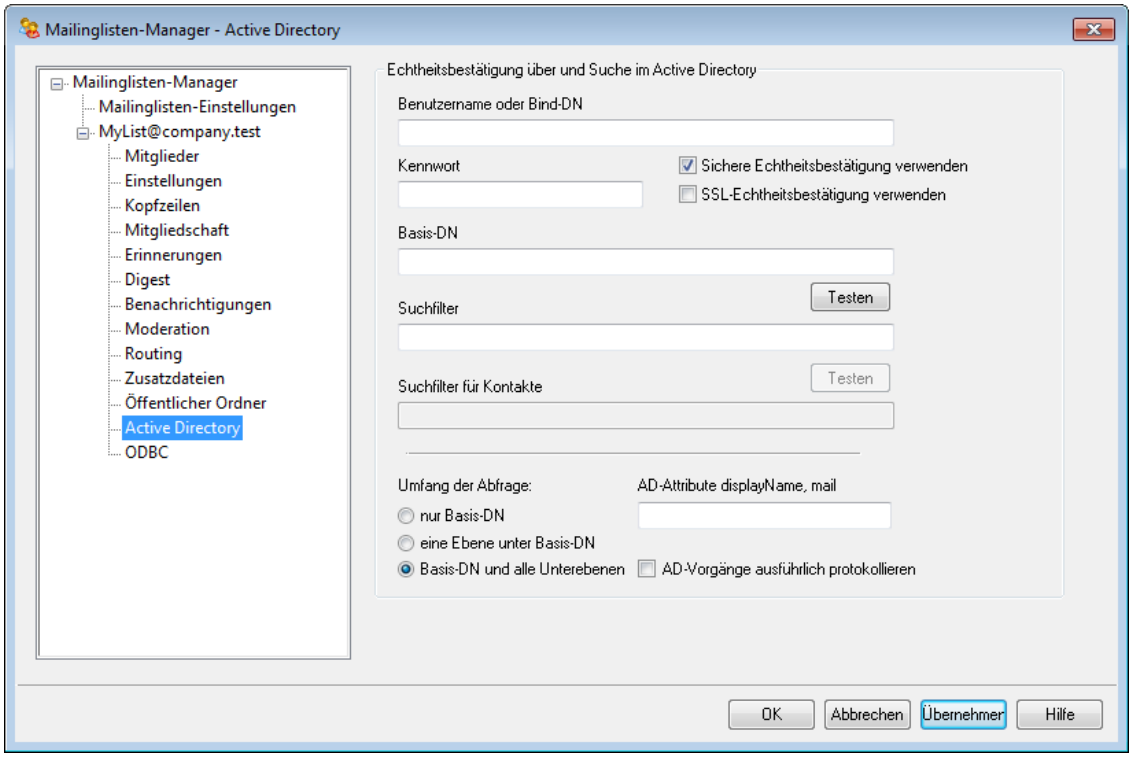


MDaemon unterstützt öffentliche IMAP-Ordner[119] im Zusammenhang mit Mailinglisten. Öffentliche Ordner sind zusätzliche Ordner, die mehreren IMAP-Benutzern zugänglich sind. Sie unterscheiden sich hierin von den privaten IMAP-Ordnern, auf die in der Regel nur ein einzelner Benutzer Zugriff hat. Die Einstellungen in diesem Dialog bewirken, dass alle Nachrichten, die an diese Mailingliste gerichtet sind, automatisch in einen bestehenden öffentlichen Ordner kopiert werden.

Listennachrichten in öffentlichen Ordner kopieren
Diese Option bewirkt, dass die Nachrichten aus der Mailingliste nicht nur an die Listenmitglieder zugestellt, sondern auch in einen öffentlichen IMAP-Ordner kopiert werden.

Wählen Sie einen öffentlichen Ordner aus.
Wählen Sie aus dieser Liste den öffentlichen Ordner aus, in den die Nachrichten aus der Mailingliste kopiert werden sollen.

3.4.2.12 Active Directory



Mithilfe der Optionen in diesem Konfigurationsdialog können Sie die Daten von Listenmitgliedern aus einem Active Directory abrufen.

Echtheitsbestätigung über und Suche im Active Directory

Benutzername oder Bind-DN
Hier wird der Windows-Benutzername oder der eindeutige Gesamtname (englisch "Distinguished Name", kurz DN) angegeben, den MDaemon bei der Verbindung mit dem Active Directory über LDAP verwenden soll. Das Active Directory gestattet die Nutzung eines Windows-Anmeldenamens oder eines Benutzerprinzipalnamens (UPNs) für diese Verbindung.

Wird statt eines Windows-Anmeldenamens ein DN angegeben, so muss die Option "*Sichere Echtheitsbestätigung verwenden*" weiter unten abgeschaltet sein.

Kennwort
Hier wird das Kennwort zu dem DN oder Windows-Anmeldenamen aus dem Feld *Bind-DN* angegeben.

Sichere Echtheitsbestätigung verwenden
Diese Option bewirkt, dass beim Verbindungsaufbau zum Active Directory die sichere Echtheitsbestätigung verwendet wird. Diese Option darf nicht verwendet werden, wenn im Feld *Bind-DN* statt eines Windows-Anmeldenamens ein DN eingetragen ist.

SSL-Echtheitsbestätigung verwenden
Diese Option bewirkt, dass bei Verbindungen zum Active Directory die Echtheitsbestätigung durch eine SSL-Verbindung geschützt sein soll.

Diese Option erfordert einen SSL-Server und eine entsprechende Infrastruktur im Windows-Netzwerk und dem Active Directory. Falls Unsicherheiten bestehen, ob diese Infrastruktur vorhanden ist, und diese Option genutzt werden soll, empfiehlt es sich, diese Fragen mit dem Netzwerkverwalter zu klären.

Attribut für die E-Mail-Adresse
In diesem Feld muss das Attribut angegeben werden, das die E-Mail-Adressen enthält, die für diese Liste genutzt werden sollen. Wird in diesem Feld beispielsweise "`Mail`" angegeben, so müssen alle Benutzerkonten im Active Directory, die als Listenmitglieder behandelt werden sollen, das Attribut "`Mail`" enthalten, und in diesem Attribut muss jeweils eine E-Mail-Adresse eingetragen sein.

Suche im Active Directory

Basis-DN
Hier wird der DN eingetragen. Er stellt den Ausgangspunkt im Verzeichnisbaum (englisch "Directory Information Tree", kurz DIT) dar, von dem aus MDaemon das Active Directory auf Benutzerkonten und Änderungen durchsucht. MDaemon beginnt die Suche grundsätzlich beim Root-DSE, also auf der höchsten Ebene der Active-Directory-Struktur. Wird hier stattdessen ein Ausgangspunkt angegeben, der näher an der Struktur der Benutzerkonten in dem jeweils verwendeten Active-Directory-Verzeichnisbaum liegt, so kann dies die Zeit verringern, die zum Durchsuchen des DIT nach Benutzerkonten und Änderungen benötigt wird. Bleibt das Feld leer, so wird die Voreinstellung `LDAP://rootDSE` verwendet.

Suchfilter
Hier wird der LDAP-Suchfilter eingetragen, der bei der Abfrage des Active Directorys auf Benutzerkonten und Änderungen eingesetzt wird. Mithilfe dieses Filters lassen sich die Benutzerkonten, die in die Überwachung des Active Directorys einbezogen werden sollen, genauer eingrenzen.

Testen
Durch Anklicken dieses Steuerelements können Sie die Einstellungen Ihres Suchfilters testen.

AD-Attribute displayName, mail
Sie müssen in dieses Feld das Attribut eintragen, das die E-Mail-Adressen enthält, die diese Mailingliste nutzen soll. Falls Sie beispielsweise "`Mail`" in dieses Feld eintragen, dann muss das Attribut "`Mail`" für jedes Benutzerkonto im Active Directory gesetzt sein, das Sie als Listenmitglied behandeln wollen. Das Attribut muss jeweils eine E-Mail-Adresse enthalten. Sie können diesem Attribut wahlweise ein Attribut des Active Directory für den vollständigen Namen der Listenmitglieder voranstellen. In diesem Fall müssen Sie beide Attribute durch ein Komma trennen. Ein Beispiel hierzu ist "`displayName, mail`" statt nur "`mail`". Das erste Attribut muss dabei das Attribut im Active Directory sein, das den

vollständigen Namen enthält, das zweite Attribut muss die E-Mail-Adresse enthalten.

Umfang der Abfrage:

Dieser Abschnitt steuert den Umfang, in dem das Active Directory durchsucht wird.

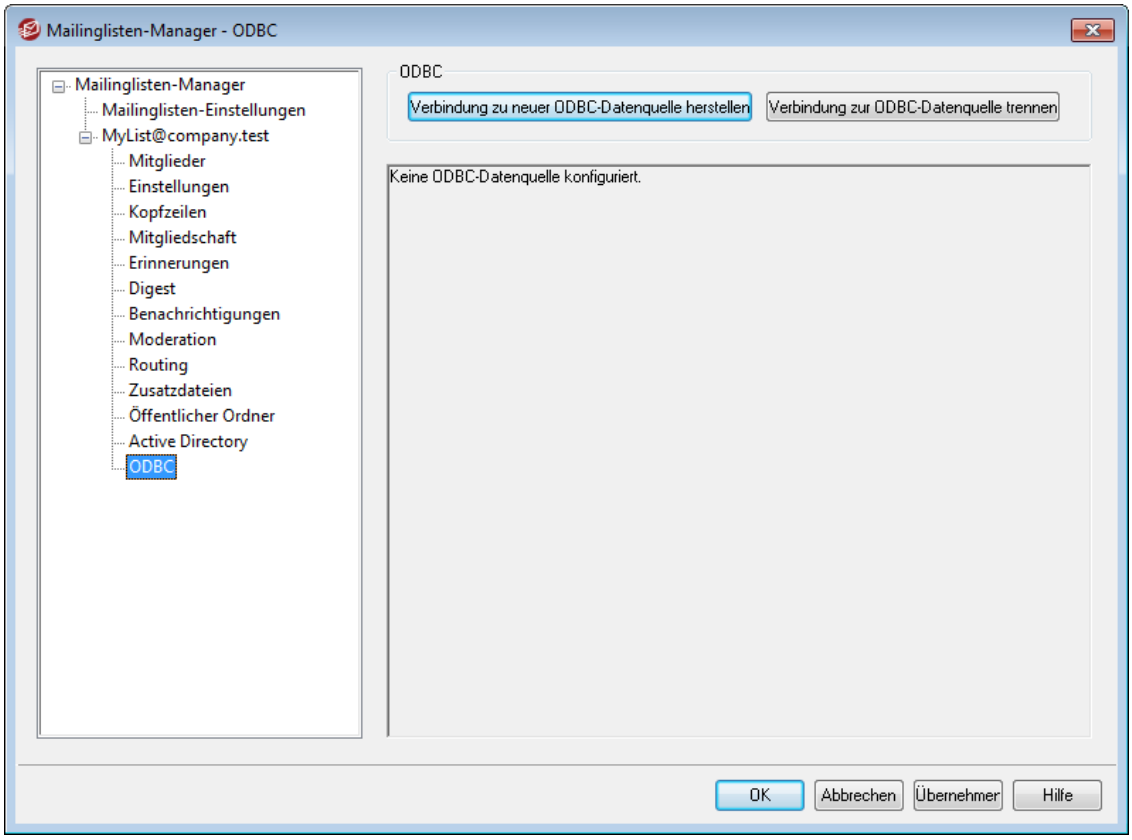
nur Basis-DN
Diese Option bewirkt, dass die Abfragen auf den oben angegebenen Basis-DN begrenzt bleiben. Unterhalb dieser Stelle werden keine Abfragen im Verzeichnisbaum (DIT) durchgeführt.

eine Ebene unter Basis-DN
Diese Option bewirkt, dass die Suche im Verzeichnisbaum des Active Directory auf eine Ebene unter dem oben angegebenen DN erstreckt wird.

Basis-DN und alle Unterebenen
Diese Option bewirkt, dass die Suche von dem angegebenen DN auf alle Unterebenen im Verzeichnisbaum erstreckt wird. Dies ist die Voreinstellung. Gemeinsam mit der Voreinstellung Root-DSE, die weiter oben beschrieben ist, bewirkt sie, dass der gesamte Verzeichnisbaum unterhalb des Root-DSE durchsucht wird.

AD-Vorgänge ausführlich protokollieren
MDaemon protokolliert die Active-Directory-Transaktionen per Voreinstellung ausführlich. Ist ein weniger ausführliches Protokoll über die Active-Directory-Transaktionen gewünscht, so muss diese Option abgeschaltet werden.

3.4.2.13 ODBC



Für die Mitgliederverwaltung der Mailinglisten können Sie eine ODBC-kompatible Datenbank einsetzen. Der Konfigurationsdialog ODBC im Editor für Mailinglisten definiert eine Verbindung zwischen einer Mailingliste und einer Datenbank; dazu können Datenquelle, Tabelle und Feldzuordnungen ausgewählt werden. Trifft eine neue Nachricht für eine Mailingliste ein, so werden automatisch eine oder mehrere SQL-Abfragen durchgeführt und die sich hieraus ergebenden E-Mail-Adressen als Teil der Listenmitglieder behandelt.

Der Liste können auch Mitglieder hinzugefügt werden, indem man diese mithilfe der durch die Datenbank selbst bereitgestellten Werkzeuge der Datenbank hinzufügt.

ODBC

Dieser Abschnitt gibt einen Überblick über die aktuellen ODBC-Einstellungen für diese Mailingliste, insbesondere die Feldzuordnungen für die Datenbank und die SQL-Abfragen, mit deren Hilfe die Berechtigungen der einzelnen Listenmitglieder festgelegt werden (etwa Normal, nur Veröffentlichen, nur Lesen, ergänzend Digest).

Verbindung zu neuer ODBC-Datenquelle herstellen
Ein Klick auf dieses Steuerelement ruft den ODBC-Auswahlassistenten auf, um die System-Datenquelle für diese Mailingliste auszuwählen.

Verbindung zur ODBC-Datenquelle trennen
Durch Anklicken dieses Steuerelements können Sie die Verbindung zu der oben angegebenen ODBC-Datenquelle trennen.

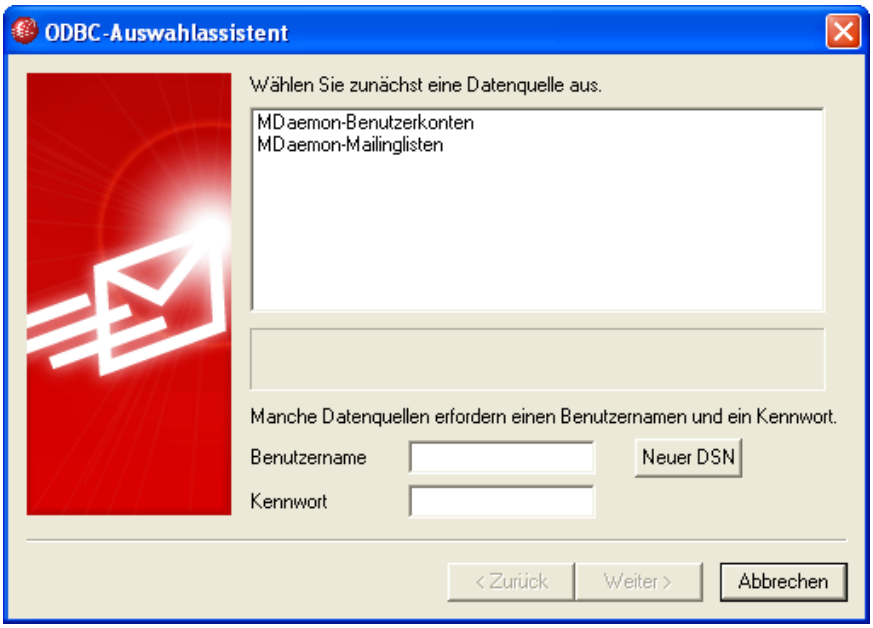
Siehe auch:

Einrichten einer ODBC-Systemdatenquelle für Mailinglisten 303
Erstellen einer neuen Systemdatenquelle 305

3.4.2.13.1 Einrichten einer ODBC-Datenquelle

Um eine ODBC-Datenquelle in Verbindung mit einer Mailingliste zu verwenden, gehen Sie folgendermaßen vor:

1. Klicken Sie im Konfigurationsdialog ODBC 302 des Editors für Mailinglisten auf **Verbindung zu neuer ODBC-Datenquelle herstellen,** um den ODBC-Auswahlassistenten aufzurufen.

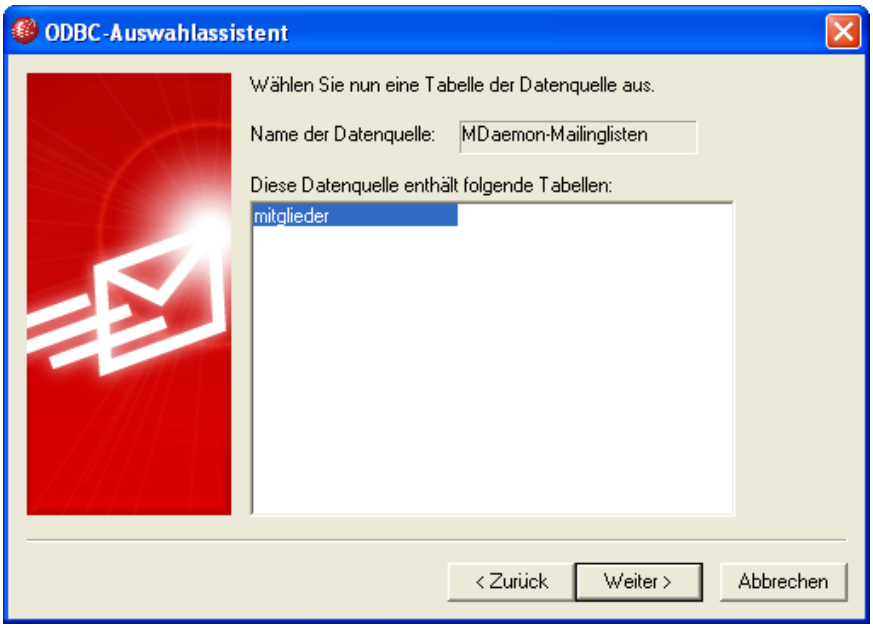


2. Wählen Sie die **Datenquelle**, die Sie für Ihre Benutzerdatenbank nutzen wollen. Falls keine kompatible Datenquelle in der Liste erscheint, klicken Sie auf **Neuer DSN**, und folgen Sie dann den Anweisungen unter **Erstellen einer neuen ODBC-Datenquelle** 305.

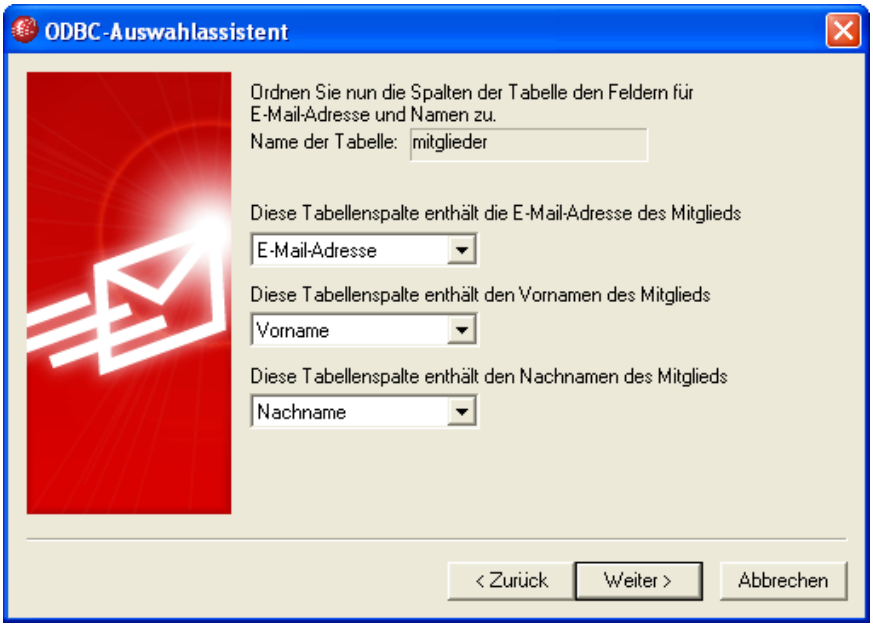
3. Falls erforderlich, geben Sie **Benutzernamen** und **Kennwort** für die Datenquelle ein.

4. Klicken Sie auf **Weiter**.

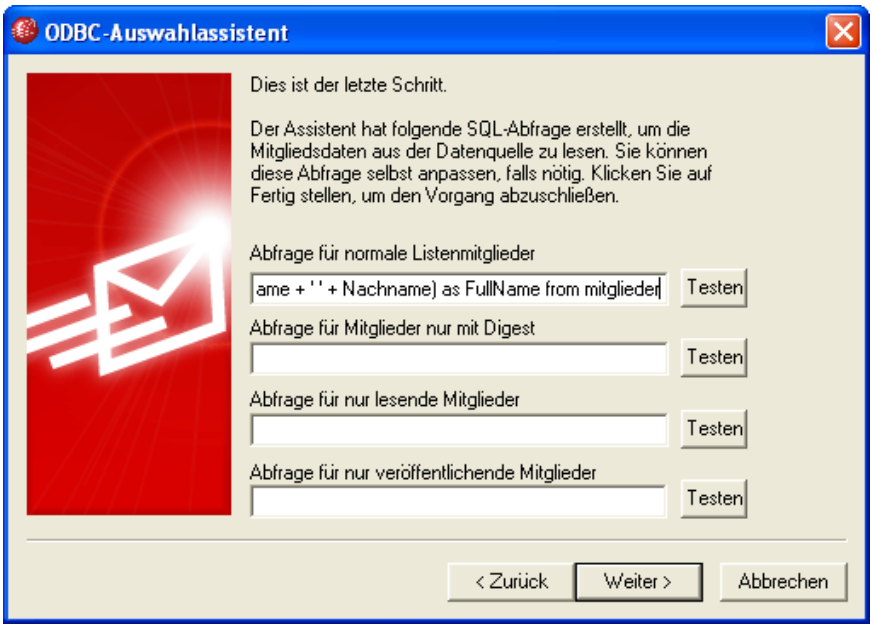
5. Die Datenquelle muss mindestens eine Tabelle mit Spalten für E-Mail-Adressen und Namen enthalten. Falls die Datenquelle wenigstens eine geeignete Tabelle enthält, wählen Sie die gewünschte Tabelle, und klicken Sie auf **Weiter.** Andernfalls klicken Sie auf **Abbrechen,** um den ODBC-Auswahlassistenten zu verlassen. Sie müssen dann zunächst mithilfe Ihrer Datenbank-Anwendung die nötige Tabelle in der Datenbank erstellen, bevor Sie die Verbindung zur Datenquelle herstellen können.



6. Ordnen Sie mithilfe der Auswahlmenüs die Spalten der Tabelle den Datenfeldern **E-Mail-Adresse**, **Vorname** und **Nachname**zu. Klicken Sie dann auf **Weiter**.



7. Der ODBC-Auswahlassistent erstellt auf der Grundlage der in **Schritt 6** vorgenommenen Einstellungen eine SQL-Abfrage. MDaemon verwendet diese Abfrage, um die Mitgliedsdaten der Liste aus der Datenbank zu lesen. Die Abfragen können von Hand nachbearbeitet werden, falls dies gewünscht ist. Sie können auch andere Abfragekriterien enthalten und dadurch weitere Parameter der Mitglieder steuern, etwa die Berechtigung nur zum Lesen oder nur zum Veröffentlichen sowie den Digest-Modus. Neben jedem Abfragefeld steht ein Steuerelement zum **Testen** dieser Abfrage zur Verfügung. Die erstellten Abfragen lassen sich hiermit einfach und schnell daraufhin überprüfen, ob sie wirklich die gewünschten Daten aus der Datenbank abfragen können. Wenn Sie die Konfiguration abgeschlossen haben, klicken Sie auf **Weiter**.



8. Klicken Sie auf **Fertig stellen**.

Siehe auch:

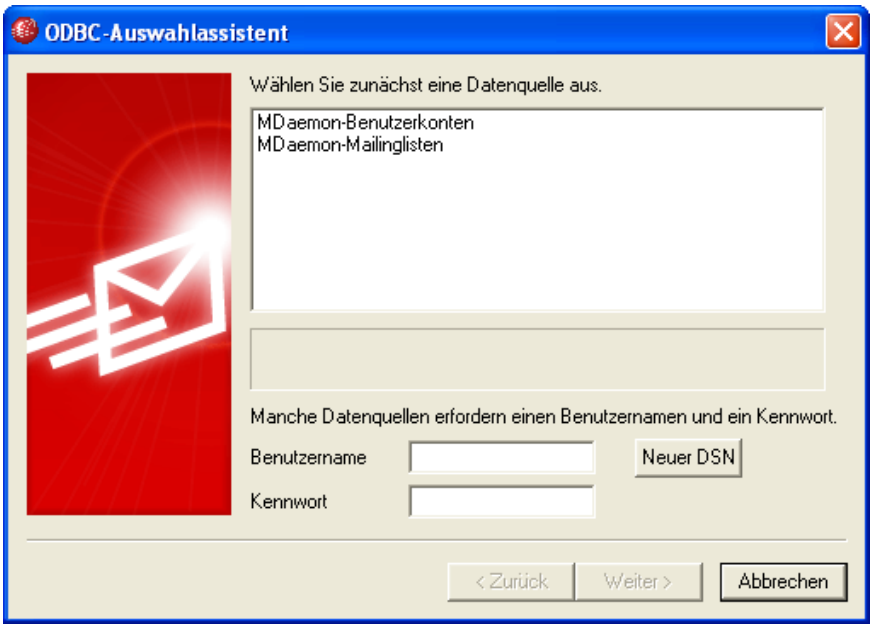
Editor für Mailinglisten » ODBC 302
Erstellen einer neuen ODBC-Datenquelle 305

3.4.2.13.2 Erstellen einer neuen ODBC-Datenquelle

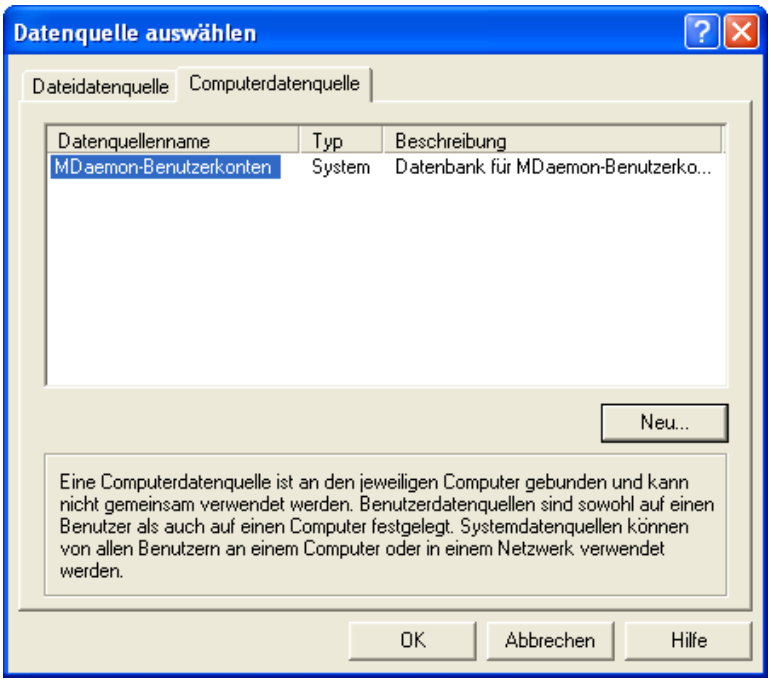
Um eine neue ODBC-Systemdatenquelle für die Nutzung durch eine Mailingliste zu erstellen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Konfigurationsdialog ODBC 302 des Editors für Mailinglisten auf **Verbindung zu neuer ODBC-Datenquelle herstellen,** um den ODBC-Auswahlassistenten aufzurufen.

2. Klicken Sie auf **Neuer DSN**, um den Dialog zur Auswahl einer Datenquelle aufzurufen.

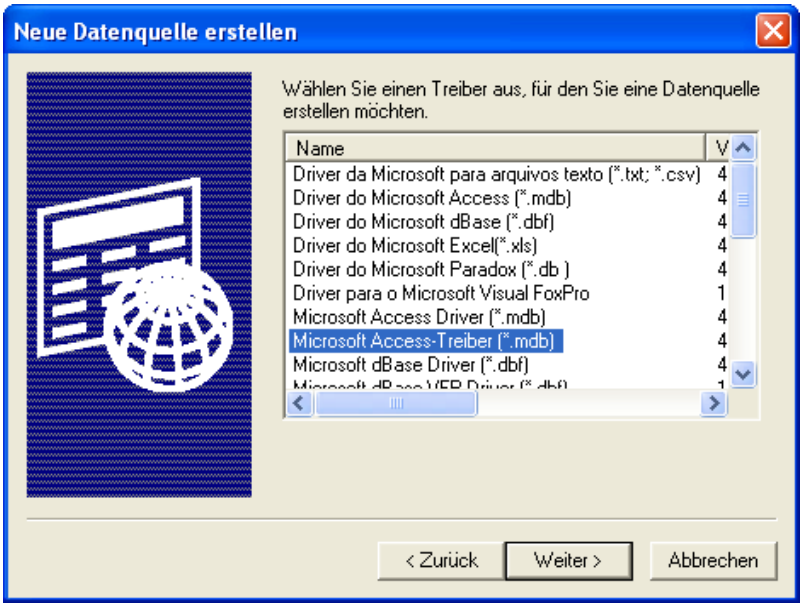


3. Wechseln Sie auf die Registerkarte **Computerdatenquelle**, und klicken Sie auf **Neu...**, um den Dialog Neue Datenquelle erstellen aufzurufen.

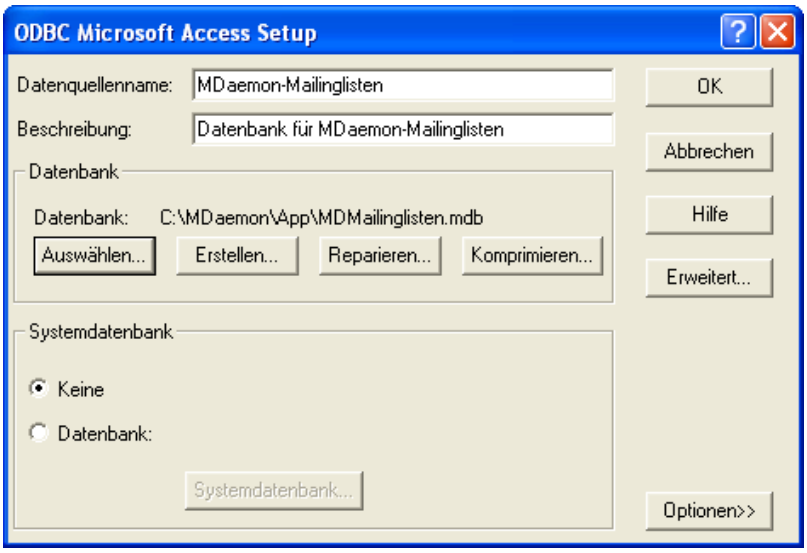


4. Wählen Sie **Systemdatenquelle**, und klicken Sie auf **Weiter.**

5. Wählen Sie den **Datenbanktreiber**, den Sie zur Erstellung der Datenquelle nutzen wollen, und klicken Sie auf **Weiter**



6. Klicken Sie auf **Fertig stellen**, um den Konfigurationsdialog für den Datenbanktreiber aufzurufen. Das Erscheinungsbild dieses Konfigurationsdialogs hängt von dem ausgewählten Treiber ab (unten wird beispielhaft der Dialog für Microsoft Access gezeigt).



7. Bestimmen Sie einen **Datenquellennamen** für Ihre neue Datenquelle, und tragen Sie alle anderen Informationen ein, die der Datenbanktreiber abfragt (beispielsweise für Erstellung und Auswahl einer Datenbank, Auswahl eines Verzeichnisses oder Servers usw.).

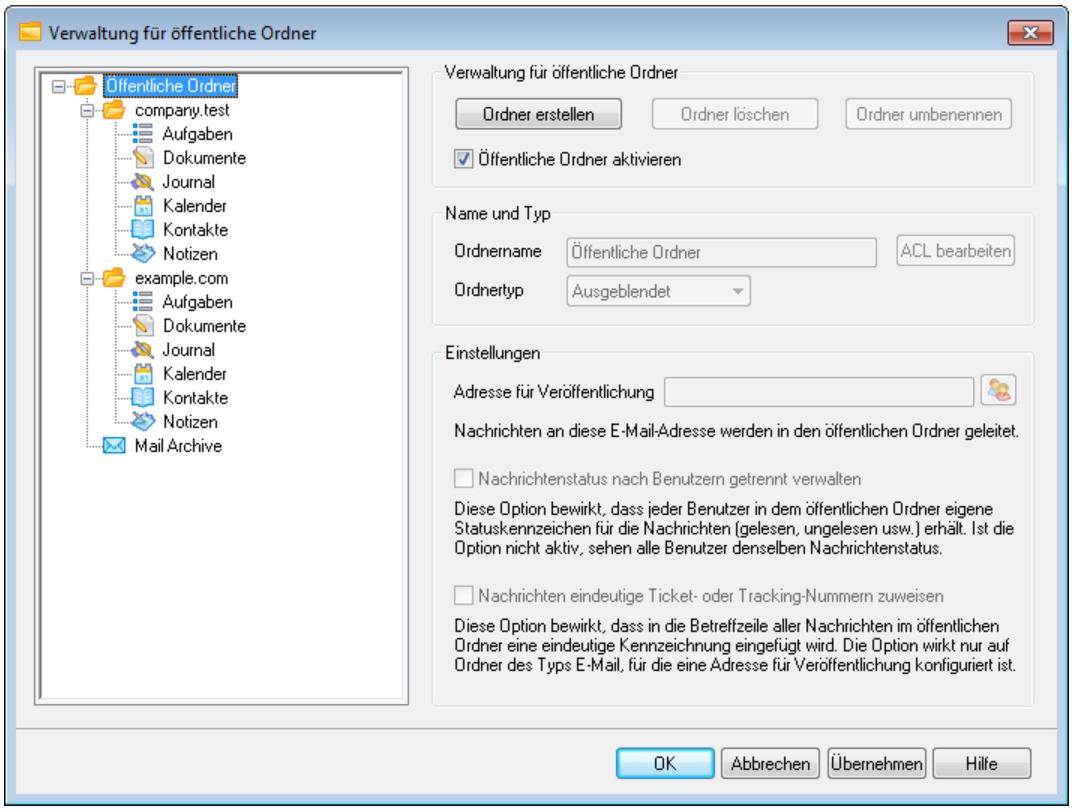
8. Klicken Sie auf **OK**, um den Dialog des Datenbanktreibers zu schließen.

9. Klicken Sie auf **OK**, um den Dialog zur Auswahl einer Datenquelle zu schließen.

Siehe auch:

ODBC - Mailinglisten 302
Einrichten einer ODBC-Datenquelle für eine Mailingliste 303

3.5 Verwaltung für öffentliche Ordner

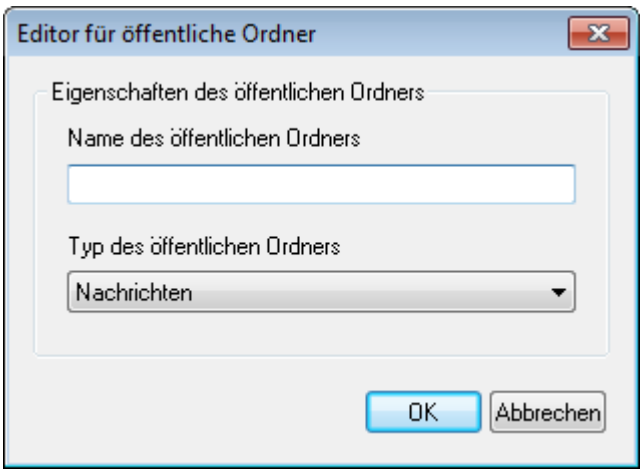


Mithilfe dieses Konfigurationsdialogs können Sie Ihre öffentlichen Ordner[119] verwalten. Sie erreichen die Verwaltung für öffentliche Ordner über "Einstellungen » Verwaltung für öffentliche Ordner...".

Verwaltung für öffentliche Ordner

Ordner erstellen

Um einen neuen öffentlichen Ordner erstellen, wählen Sie in der Ordnerliste den Ordner aus, unter dem Sie den Ordner erstellen wollen, und klicken Sie danach auf *Ordner erstellen*. Geben Sie einen Namen für den öffentlichen Ordner ein, wählen Sie den Typ des öffentlichen Ordners aus, und klicken Sie danach auf *OK*.



Ordner löschen
Um einen öffentlichen Ordner zu löschen, wählen Sie in der Ordnerliste den gewünschten Ordner aus, und klicken Sie danach auf *Ordner löschen*.

Ordner umbenennen
Um einen öffentlichen Ordner umzubenennen, wählen Sie in der Ordnerliste den gewünschten Ordner aus, und klicken Sie danach auf *Ordner umbenennen*. Geben Sie den neuen Namen ein, und klicken Sie danach auf *OK*.

Öffentliche Ordner aktivieren
Diese Option gewährt den Benutzern den Zugriff auf öffentliche Ordner. Die Benutzer, die auf einen öffentlichen Ordner zugreifen dürfen, und den Umfang der Rechte, die sie dabei haben, können Sie festlegen, indem Sie den gewünschten Order auswählen und danach das Steuerelement *ACL bearbeiten* anklicken.

Name und Typ

Ordnername
In diesem Textfeld wird der Name des Ordners angezeigt, den Sie in der Ordnerliste ausgewählt haben. Die folgenden Optionen und Einstellungen beziehen sich auf den hier angezeigten Ordner.

Ordnertyp
Mithilfe dieses Auswahlmenüs legen Sie fest, welche Elemente der Ordner enthält, und welchen Typ erhält. Es stehen insbesondere Nachrichten, Kontakte und Kalender zur Verfügung.

ACL bearbeiten
Wählen Sie einen Ordner aus der Ordnerliste aus, und klicken Sie danach auf dieses Steuerelement, um die Zugriffskontrollliste 311 für diesen Ordner zu bearbeiten. Mithilfe der Zugriffskontrollliste (sie wird nach der englischen Bezeichnung Access Control List auch als ACL abgekürzt) können Sie die Benutzer oder Benutzergruppen bestimmen, die auf den Ordner zugreifen können, und Sie können den Umfang der jeweiligen Zugriffsrechte festlegen.

Einstellungen

Adresse für Veröffentlichung
Sie können hier eine lokale E-Mail-Adresse eintragen oder ein bestimmtes MDaemon-Benutzerkonto auswählen. Die Adresse oder das Bentutzerkonto werden mit dem öffentlichen Ordner verknüpft. Nachrichten, die an die hier angegebene *Adresse für Veröffentlichung* gerichtet sind, werden automatisch in den öffentlichen Ordner geleitet. Es können allerdings nur solche Benutzer Nachrichten an diese Adresse senden, die für den öffentlichen Ordner das Zugriffsrecht Veröffentlichen ("post") haben.

Nachrichtenstatus nach Benutzern getrennt verwalten
Diese Option bewirkt, dass der Nachrichtenstatus für diesen Ordner nach Benutzern getrennt und nicht systemweit einheitlich verwaltet wird. Der Nachrichtenstatus bezieht sich insbesondere auf die Kennzeichnungen ("Flags") gelesen, ungelesen, beantwortet und weitergeleitet. Ist diese Option aktiv, so sieht jeder Benutzer des öffentlichen Ordners eigene Statuskennzeichen, die sich ausschließlich aus seinem Zugriff auf den Ordner ergeben. Ein Benutzer, der beispielsweise eine Nachricht selbst noch nicht gelesen hat, sieht sie als "ungelesen", wohingegen ein anderer Benutzer desselben Ordners, der die

Nachricht bereits gelesen hat, sie als "gelesen" sieht. Ist diese Option nicht aktiv, so sehen alle Benutzer denselben Nachrichtenstatus; hat beispielsweise nur ein einziger Benutzer des Ordners eine Nachricht gelesen, so sehen alle anderen Benutzer die Nachricht ebenfalls als "gelesen".

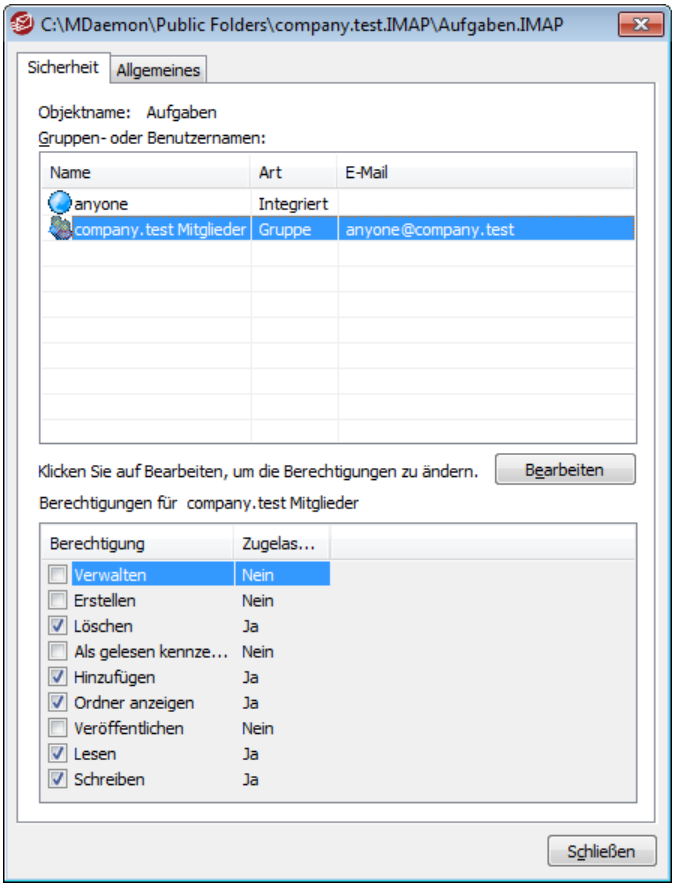
Nachrichten eindeutige Ticket- oder Tracking-Nummern zuweisen
Diese Option bewirkt, dass der öffentliche Ordner als Ordner für Ticketnachrichten arbeitet. MDaemon fügt der Betreffzeile jeder Nachricht, die an die *Adresse für Veröffentlichung* für den Ordner gerichtet ist, den *Ordnernamen* und eine eindeutige Kennzeichnung hinzu. In abgehenden Nachrichten, in denen diese besonders aufgebaute Betreffzeile enthalten ist, ändert MDaemon die Absenderadresse in die Adresse für Veröffentlichung; darüber hinaus kopiert MDaemon eine Kopie der abgehenden Nachricht in den Unterordner "Beantwortet" des öffentlichen Ordners. Alle eingehenden Nachrichten, in denen diese besonders aufgebaute Betreffzeile enthalten ist, werden automatisch in den öffentlichen Ordner umgeleitet, und zwar unabhängig davon, an welche Adresse sie gerichtet waren.

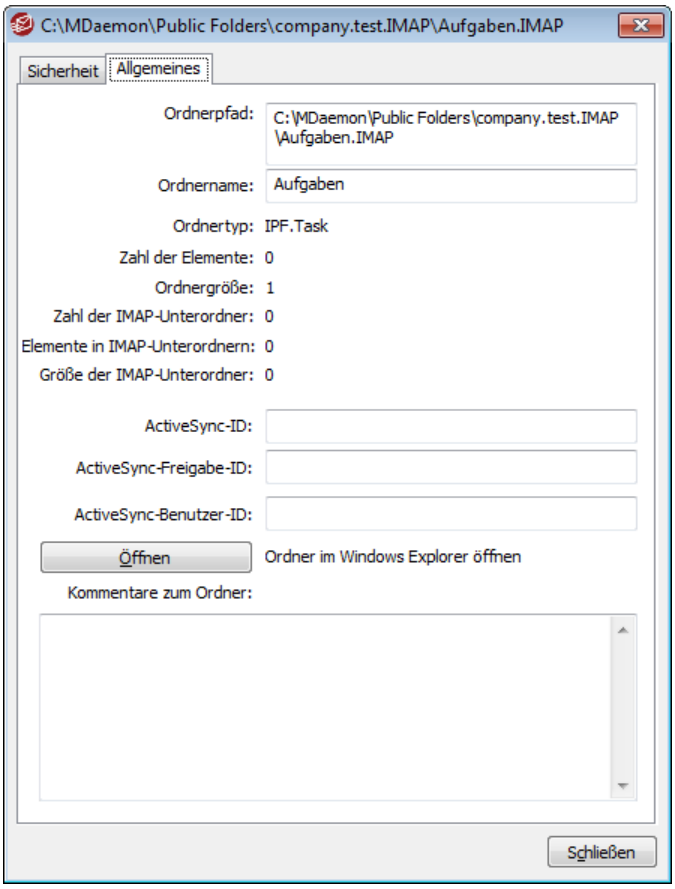
Siehe auch:

Zugriffskontrollliste (ACL) 311
Öffentliche Ordner - Übersicht 119
Öffentliche & Freigegebene Ordner 122
Benutzerkonten-Editor » Freigegebene Ordner 742
Mailingliste » Öffentliche Ordner 298

3.5.1 Zugriffskontrollliste (ACL)

Die Zugriffskontrollliste (nach der englischen Bezeichnung Access Control List auch als ACL abgekürzt) bestimmt, welche Benutzer und Gruppen welche Zugriffsrechte für öffentliche und freigegebene Ordner 119 haben. Die Zugriffskontrollliste ist erreichbar über das Steuerelement *ACL bearbeiten* im Konfigurationsdialog für die Verwaltung öffentlicher Ordner 309 sowie über das Steuerelement *Zugriffskontrollliste bearbeiten* im Abschnitt Freigegebene Ordner 742 des Benutzerkonten-Editors.





Sicherheit

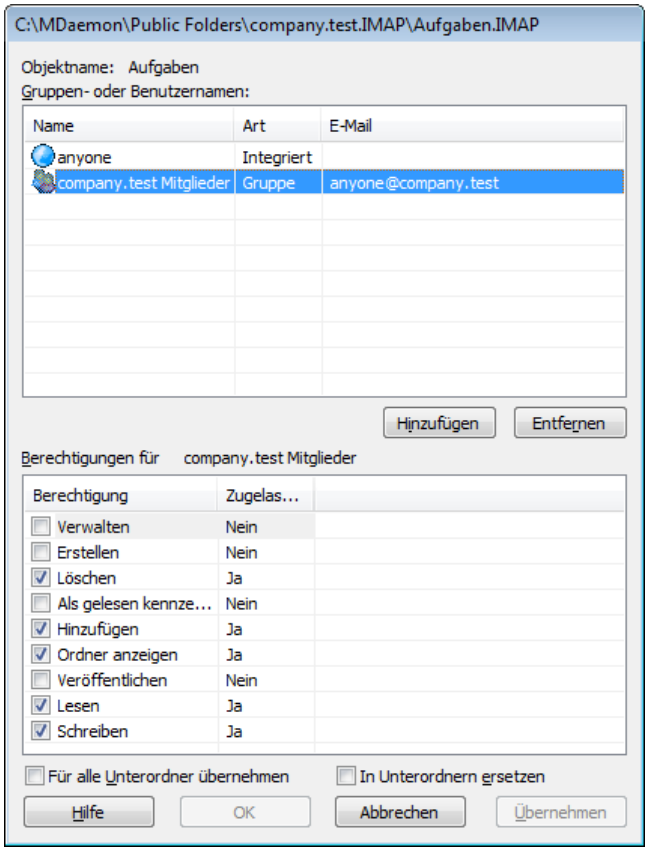
Diese Registerkarte zeigt die Gruppen und Benutzer mit Zugriffsrechten für den Ordner und die Berechtigungen, die ihnen eingeräumt sind. Um die Berechtigungen 314 eines Benutzers oder einer Gruppe einzusehen, klicken Sie auf den Benutzer oder die Gruppe. Um die Berechtigungen zu bearbeiten, klicken Sie auf **Bearbeiten** 313.

Allgemeines

Diese Registerkarte zeigt die Eigenschaften des Ordners, insbesondere Ordnerpfad, Ordnernamen, Ordnertyp und weitere Daten zum Ordner.

Bearbeiten der Zugriffskontrolllisten

Um die Berechtigungen zu bearbeiten, klicken Sie auf der Registerkarte Sicherheit auf **Bearbeiten**. Es öffnet sich der Editor für Zugriffskontrolllisten, in dem Sie die Berechtigungen bearbeiten können.



Objektname
Hier erscheint der Name des Objekts oder Ordners, auf den sich die Berechtigungen beziehen.

Gruppen- oder Benutzernamen
Hier erscheinen die Gruppen und Benutzer, denen Berechtigungen eingeräumt sind. Um die Berechtigungen für eine Gruppe oder einen Benutzer einzusehen, klicken Sie auf den Benutzer oder die Gruppe. Die Berechtigungen erscheinen dann im Abschnitt *Berechtigungen für <Gruppe oder Benutzer>* weiter unten.

Wollen Sie einer Gruppe oder einem Benutzer Berechtigungen einräumen, so aktivieren Sie die Kontrollkästchen für alle gewünschten Berechtigungen.

Hinzufügen
Um einer Gruppe oder einem Benutzer Berechtigungen einzuräumen, der in der Liste noch nicht aufgeführt ist, klicken Sie auf **Hinzufügen**315.

Entfernen
Um eine Gruppe oder einen Benutzer zu entfernen, wählen Sie den betreffenden Eintrag in der Liste aus, und klicken Sie auf **Entfernen**.

Berechtigungen für <Gruppe oder Benutzer>
Um der oben ausgewählten Gruppe oder dem oben ausgewählten Benutzer Berechtigungen einzuräumen, aktivieren Sie das Kontrollkästchen neben jeder gewünschten Berechtigung.

Sie können die folgenden Berechtigungen einräumen:

Verwalten – Der Benutzer darf die Zugriffskontrollliste des Ordners bearbeiten.

Erstellen – Der Benutzer darf in dem Ordner Unterordner anlegen.

Löschen – Der Benutzer darf Elemente aus dem Ordner löschen.

Als gelesen kennzeichnen – Der Benutzer darf den Status der Nachrichten in dem Ordner zwischen gelesen und ungelesen wechseln.

Hinzufügen – Der Benutzer darf Elemente in dem Ordner erweitern und in den Ordner kopieren.

Ordner anzeigen – Der Benutzer sieht den Ordner in seiner persönlichen Liste der IMAP-Ordner.

Veröffentlichen – Der Benutzer darf Nachrichten direkt an den Ordner senden, falls der Ordner so konfiguriert ist, dass er dies zulässt.

Lesen – Der Benutzer darf den Ordner öffnen und seinen Inhalt einsehen.

Schreiben – Der Benutzer darf Kennzeichnungen (Flags) für die Nachrichten in dem Ordner bearbeiten.

Für alle Unterordner übernehmen
Diese Option überträgt die für den gerade bearbeiteten Ordner festgelegten Berechtigungen auch auf alle Unterordner, die der Ordner zum Zeitpunkt der Bearbeitung enthält. Die Berechtigungen für alle Gruppen und Benutzer des gerade bearbeiteten Benutzers werden den Zugriffskontrolllisten der Unterordner hinzugefügt. Bestehen im Unterordner bereits Berechtigungen für die Gruppen und Benutzer, die auch für den gerade bearbeiteten Ordner Berechtigungen haben, dann werden diese bestehenden Berechtigungen im Unterordner ersetzt. Berechtigungen anderer Gruppen und Benutzer, die für die Unterordner etwa bereits bestehen, werden nicht gelöscht.

Ein Beispiel hierzu:

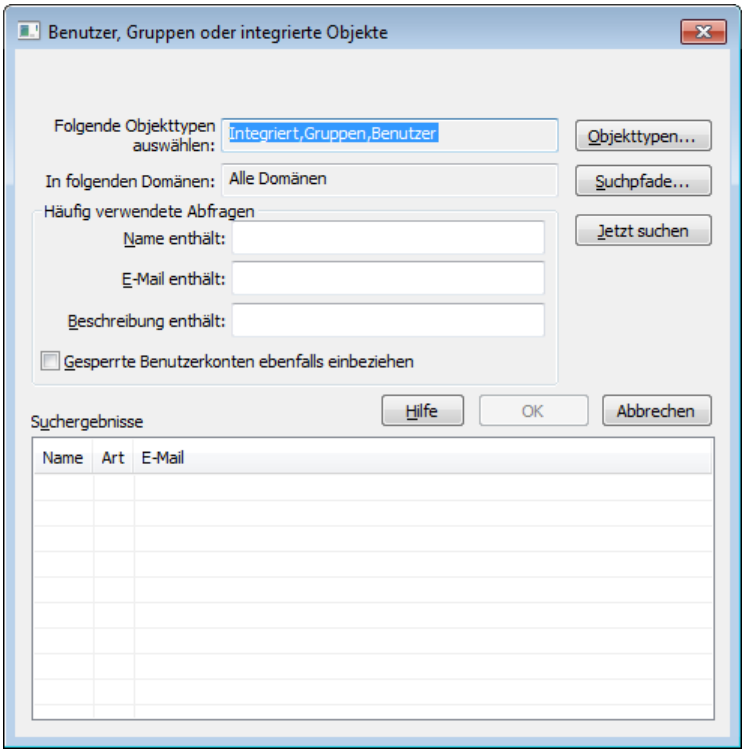
Für den gerade bearbeiteten Ordner bestehen bestimmte Berechtigungen für `Benutzer_A` und `Benutzer_B`. In einem Unterordner des gerade bearbeiteten Ordners bestehen Berechtigungen für `Benutzer_B` und `Benutzer_C`. Diese

Option fügt die Berechtigungen für `Benutzer_A` auch dem Unterordner hinzu und ersetzt die Berechtigungen für den `Benutzer_B` für den Unterordner durch die Berechtigungen des gerade bearbeiteten Ordners. Sie lässt die Berechtigungen für `Benutzer_C` unverändert. Für den Unterordner bestehen danach Berechtigungen für `Benutzer_A`, `Benutzer_B` und `Benutzer_C`.

In Unterordnern ersetzen
Diese Option bewirkt, dass die Berechtigungen aller Unterordner durch die Berechtigungen des gerade bearbeiteten Ordners ersetzt werden. Die Berechtigungen der Unterordner entsprechen dann dem gerade bearbeiteten Ordner.

Hinzufügen einer Gruppe oder eines Benutzers

Um der Zugriffskontrollliste Gruppen und Benutzer hinzuzufügen, klicken Sie im Editor für Zugriffskontrolllisten auf **Hinzufügen**. Es öffnet sich der Konfigurationsdialog zum Hinzufügen von Gruppen und Benutzern, in dem Sie nach Gruppen und Benutzern suchen und sie hinzufügen können.



Folgende Objekttypen auswählen
Um die Objekttypen auszuwählen, die Sie nach Gruppen und Benutzern durchsuchen wollen, klicken Sie auf **Objekttypen...**. Sie können wählen zwischen Integriert, Gruppen und Benutzern.

In folgenden Suchpfaden auswählen
Um die Domänen auszuwählen, die Sie durchsuchen wollen, klicken Sie auf **Suchpfade...**.Sie können alle oder einzelne MDaemon-Domänen auswählen.

Häufig verwendete Abfragen
Sie können die Felder in diesem Abschnitt verwenden, um den Umfang der Suche zu beschränken. Sie können nach Inhalten aus dem Namen des Benutzers, der E-Mail-Adresse und der Beschreibung[714] des Benutzerkontos suchen. Wenn Sie diese Felder leer lassen, ergibt die Suche alle Gruppen und Benutzer, die in den oben ausgewählten Objekttypen und Suchpfaden enthalten sind.

Gesperrte Benutzerkonten ebenfalls einbeziehen
Diese Option bewirkt, dass auch gesperrte Benutzerkonten[714] in die Suche einbezogen werden.

Jetzt suchen
Um die Suche auszuführen, geben Sie alle gewünschten Suchkriterien an, und klicken Sie danach auf **Jetzt suchen**.

Suchergebnisse
Nachdem die Suche abgeschlossen ist, können Sie in diesem Abschnitt alle gewünschten Gruppen und Benutzer auswählen. Um die ausgewählten Gruppen und Benutzer der Zugriffskontrollliste hinzuzufügen, klicken Sie danach auf **OK**.

Die Berechtigungen werden mithilfe der in MDaemon enthaltenen Leistungsmerkmale für Zugriffskontrolllisten (ACL) gesteuert. ACL ist eine Erweiterung des Internet Message Access Protocols (IMAP4), die das Erstellen eigener Zugriffskontrolllisten für alle IMAP-Nachrichtenordner gestattet. Sie können damit anderen Benutzern, die über Benutzerkonten auf demselben Server verfügen, Zugriff auf Ihre Ordner gestatten. Falls Ihr E-Mail-Client keine Zugriffskontrolllisten unterstützt, können Sie die Berechtigungen mithilfe dieses Konfigurationsdialogs bearbeiten.

ACL wird ausführlich in RFC 2086 beschrieben. Sie erhalten dieses Dokument in englischer Sprache unter http://www.rfc-editor.org/rfc/rfc2086.txt.

Siehe auch:

Verwaltung für öffentliche Ordner[309]
Übersicht über die öffentlichen Ordner[119]
Öffentliche & Freigegebene Ordner[122]
Benutzerkonten-Editor » Freigegebene Ordner[742]
Mailinglisten » Öffentlicher Ordner[298]

3.6 Web- & IM-Dienste

3.6.1 Webmail

3.6.1.1 Übersicht

MDaemon Webmail gehört zum Lieferumfang von MDaemon. Webmail ist eine webgestützte E-Mail-Lösung, die den Benutzern alle E-Mail-Funktionen innerhalb ihres bevorzugten Web-Browsers bietet. Webmail kann sich gegen herkömmliche Mailclients mühelos behaupten und bietet den Benutzern den zusätzlichen Vorteil, dass sie von überall auf ihre E-Mail zugreifen können; sie brauchen nur eine Internet- oder Netzwerkverbindung. Alle E-Mail-Ordner, Kontakte, Kalender und sonstigen Elemente der Benutzer liegen auf dem Server, sodass die Benutzer immer genauso Zugriff haben, wie wenn sie im Büro selbst wären.

Webmail bietet auch den Systemverwaltern zahlreiche Vorteile. Die Konfiguration und Wartung einzelner E-Mail-Clients für die Arbeitsplätze entfällt, da Webmail nicht an den Arbeitsplatz oder den Rechner gebunden ist. Die gesamte Konfiguration kann zentral über den Server erledigt werden, eine gesonderte Konfiguration der einzelnen Clients entfällt. Die Grafiken und HTML-Seiten, die Webmail anzeigt, lassen sich an eigene Bedürfnisse und die der Kunden anpassen. Die können Benutzer ihre Benutzerkonten weitgehend selbst verwalten können und damit den Systemverwalter entlasten. Welche Berechtigung die einzelnen Benutzer haben sollen, legt der Systemverwalter fest.

Schließlich bietet Webmail auch den Benutzern über die Verfügbarkeit eines webgestützten Clients hinaus noch einige Vorteile. Ihnen stehen umfassende E-Mail-Funktionen überall dort zur Verfügung, wo sie Zugriff auf einen Browser haben. Die Benutzeroberfläche beherrscht annähernd 30 Sprachen. Persönliche und globale Adressbücher stehen ebenso zur Verfügung wie Ordner zur Aufbewahrung der Post, Filter, Versand und Empfang von Dateianlagen, verschiedene Designs für die Benutzeroberfläche, Designs für mobile Endgeräte, Kalenderfunktionen, Groupware-Funktionen, ein integrierter Instant Messenger, den die Benutzer herunterladen können, und vieles mehr.

Kalender & Terminplanung

MDaemon ist mit einem umfassenden System zur Onlinezusammenarbeit ausgestattet. Die Benutzer können in Webmail sehr einfach Termine ansetzen, Treffen planen und mit Adressbüchern arbeiten. Terminserien werden umfassend unterstützt, und Termine können mithilfe umfangreicher Datenfelder eingehend beschrieben werden. Die Kontakte, Kalender, Notizen und Aufgaben werden in den Postverzeichnissen der einzelnen Benutzer in IMAP-Ordnern abgelegt. Die Benutzer können über Webmail auf diese persönlichen Ordner zugreifen und bestimmen, welche anderen Benutzer ebenfalls Zugriff auf die Ordner erhalten sollen. Alle Webmail-Designs, und insbesondere LookOut, verfügen über Vorlagen, die Kontakte, Kalender und Aufgaben logisch strukturiert und ansprechend darstellen.

Die Einbindung des Terminplaners in MDaemon bringt noch weitere Vorteile, etwa durch Benachrichtigungen über Treffen per E-Mail, und Termine, die von den Benutzern oder anderen Personen angesetzt werden können. Ein Benutzer, für den ein anderer einen Termin angesetzt hat, erhält darüber eine Nachricht per E-Mail, die eine Zusammenfassung der Termindaten enthält. Jeder als Teilnehmer an einem Termin eingetragene Benutzer erhält eine eigene Einladung per E-Mail, aus der Datum, Uhrzeit, Treffpunkt, Beschreibung und die Teilnehmerliste hervorgehen. Teilnehmer, bei denen ein solches Treffen eine Terminkollision verursacht, werden hiervon ebenfalls gesondert verständigt. Der Benutzer, der den Termin angesetzt

hat, erhält eine Zusammenfassung mit Beschreibung und Teilnehmerliste, aus der auch Terminkollisionen ersichtlich sind.

Der Kalender unterstützt auch den Internet-Calendar-Standard (iCalendar oder iCal), den auch bei Microsoft Outlook und andere iCalendar-kompatible E-Mail-Clients verwenden. Der Kalender kann iCalendar-Daten, die an die Benutzer des Systems gerichtet sind, erkennen und deren Kalender entsprechend aktualisieren. Öffnet ein Benutzer eine iCalendar-Dateianlage in Webmail, so übernimmt Webmail die darin enthaltenen Termindaten in den Terminkalender des Benutzers. Benutzer, die einen Termin eintragen, können E-Mail-Adressen angeben, an die iCalendar-kompatible Nachrichten versandt werden sollen. Diese Funktion kann durch die Benutzer selbst konfiguriert werden.

MDaemon Instant Messenger

MDaemon ist mit dem MDaemon Instant Messenger (MDIM) ausgestattet. MDIM das sichere Instant-Messaging-System von MDaemon und eine Anwendung für den Infobereich (früher Systray), die schnellen Zugriff auf die wichtigsten E-Mail-Funktionen von Webmail bietet. Jeder Benutzer von Webmail kann MDIM selbst laden und auf dem lokalen Rechner installieren. Schon vor der Installation ist MDIM dabei speziell für den anfordernden Benutzer konfiguriert, sodass der Benutzer nur noch wenige Einstellungen selbst vornehmen muss.

MDIM läuft im Hintergrund und überwacht die Benutzerkonten durch direkte Kommunikation mit dem Webmail-Server. Es ist daher nicht mehr notwendig, ein Browserfenster zu öffnen oder offen zu halten, um den Posteingang auf neue Nachrichten zu überprüfen. MDIM prüft, ob neue Post eingetroffen ist, und benachrichtigt den Benutzer durch Abspielen einer Klangdatei oder durch eine Bildschirmmeldung. MDIM zeigt dem Benutzer auch eine Liste seiner Ordner sowie Anzahl und Status der Nachrichten, die diese Ordner enthalten (neu, ungelesen und gelesen). MDIM kann auch den Browser des Benutzers starten und einen bestimmten Ordner direkt aufrufen.

MDIM enthält auch ein voll ausgestattetes Instant-Messaging-System. Die Benutzer können eine Kontaktliste mit anderen MDIM-Benutzern einsehen, aus der auch deren Status (online, abwesend, offline) ersichtlich ist. Sie können mit einem oder mehreren anderen eine Konferenz beginnen, den eigenen Status festlegen und im Verlaufsordner vorangegangene Konferenzen betrachten.

Weitere Informationen zu MDIM enthält das integrierte Hilfesystem.

Das Instant-Messaging-System des MDaemon Instant Messengers

MDIM enthält einen Client für das Instant Messaging (IM), der den XMPP-Server 372 von MDaemon nutzt. Die Benutzer, die diesen Client nutzen, können, je nach Auswahl durch den Administrator, ihrer MDIM-Kontaktliste die Benutzer der eigenen Domäne und der anderen auf dem Server gehosteten Domänen hinzufügen und mit ihnen per Instant Messaging kommunizieren. Sie können den eigenen Online-Status setzen, den Status der Kontakte einsehen, Emoticons nutzen, die Textfarbe ändern, Dateien übermitteln, die Klangsignale für Benachrichtigungen setzen und andere Voreinstellungen bearbeiten. Es sind auch Gruppenunterhaltungen möglich, an denen sich mehrere Kontakte gleichzeitig beteiligen. Die Leistungsmerkmale für das Instant Messaging sind über das Kontextmenü für das Symbol im Systray und über das MDIM-Fenster erreichbar.

Das IM-System des MDaemon Instant Messengers unterstützt auch Skripte und erlaubt damit anderen Programmen die direkte Interaktion. Ein solches Programm kann direkt Nachrichten an andere MDIM-Benutzer senden, indem es im Verzeichnis

MDaemon\WorldClient\ Signaldateien (englisch Semaphore-Dateien, Dateiendung SEM) anlegt. Das Format dieser SEM-Dateien stellt sich wie folgt dar:

`To: user1@example.com`	E-Mail-Adresse des MDIM-Benutzers.
`From: user2@example.com`	E-Mail-Adresse des Absenders der Instant Message.
`<Leerzeile>`	
`Text der Instant Message.`	Hier wird der Nachrichtentext für die Instant Message eingetragen.

Der Name der SEM-Datei muss mit den Zeichen "IM-" beginnen und danach eine eindeutige Zahl enthalten, z.B. "IM-0001.SEM". Anwendungen sollten außerdem eine dazu passende Datei "IM-0001.LCK" anlegen, um die entsprechende SEM-Datei zu sperren. Sobald die SEM-Datei fertig erstellt wurde, ist die LCK-Datei zu löschen, damit die SEM-Datei verarbeitet werden kann. MDaemon versendet nach dieser Methode Instant-Messages mit Terminerinnerungen.

Der Inhaltsfilter verfügt über eine Aktion, um eine Instant-Message zu versenden, wobei dieselbe Skriptverarbeitung zum Einsatz kommt. Regeln, die die Aktion nutzen, können die Makros des Inhaltsfilters auch in der IM verwenden. Beispielsweise kann eine Regel dazu benutzt werden, eine Instant-Message mit folgendem Inhalt zu versenden:

```
Sie haben eine Nachricht von $SENDER$ erhalten.
Betreff: $SUBJECT$
```

Mit diese Regel lässt sich eine effiziente Methode verwirklichen, Benachrichtigungen über neue Nachrichten durch MDIM zu geben.

Bei vielen Systemverwaltern bestehen Vorbehalte gegen die Verwendung eines Instant-Messaging-Systems, die meist in fehlender zentraler Kontrolle und der Tatsache, dass sich bei herkömmlichen IM-Clients der Nachrichtenverkehr nicht überwachen lässt, begründet sind. Das Instant-Messaging-System für MDIM wurde daher mit dem Ziel entwickelt, diese Unzulänglichkeiten zu überwinden. Zunächst arbeitet dieses System nicht auf Basis direkter Verbindungen zwischen den Nachrichten austauschenden Gegenstellen ("Peer-to-Peer") – zwischen den einzelnen MDIM-Clients besteht zu keinem Zeitpunkt eine Direktverbindung. Außerdem kann der Systemverwalter von MDaemon ein zentrales Protokoll über alle Instant Messages einsehen, da jede IM über den Server läuft. Zur Sicherheit des Unternehmens und seiner Angestellten kann daher ein lückenloses Protokoll über alle IM-Transaktionen erstellt werden. Dieses wird in der Datei XMPPServer-<Datum>.log im Verzeichnis MDaemon\LOGS\ abgelegt.

Instant Messaging wird auf Domänenebene bereit gestellt und gesteuert. Die Optionen, Instant Messaging zu aktivieren und zu sperren und um festzulegen, ob das Instant-Messaging protokolliert werden soll, befindet sich im Abschnitt MDIM 331 des Konfigurationsdialogs für Webmail (Einstellungen » Web- & IM-Dienste » Webmail » MDIM). Der Domänen-Manager 190 enthält einen ähnlichen Konfigurationsdialog, mit dessen Hilfe die Leistungsmerkmale nach Domänen getrennt gesteuert werden können.

Skins für den MDaemon Instant Messenger

Die Benutzeroberfläche des MDIM kann *msstyles*-Skins verarbeiten, die im Internet leicht verfügbar sind. Es liegen bereits mehrere Skins bei. Um einen neuen Skin zu installieren, laden Sie die jeweilige Datei *.msstyles herunter, und legen Sie sie in

dem MDIM-Ordner `\Styles\` in einem Unterordner ab, dessen Name dem Namen des Skins entspricht. Heißt die Datei beispielsweise `Red.msstyles`, so ergibt sich der Pfad "`\.\Styles\Red\Red.msstyles`".

Dropbox-Integration

Dem Konfigurationsdialog Strg+W » Webmail wurde der neue Abschnitt Dropbox hinzugefügt. Sie können in diesem Abschnitt den "App-Key" und das "App-Secret" eingeben und den Text einer Datenschutzerklärung festlegen. Diese Daten sind erforderlich, um die Dropbox-Dienste in Webmail zu integrieren. Sie erhalten den App-Key und das App-Secret, wenn Sie Webmail auf der Dropbox-Website als "App" registrieren. Alt-N kann diese Registrierung, die nur einmal durchgeführt werden muss, nicht für Sie übernehmen. Umfassende Informationen über die Registrierung Ihrer Webmail-Installation als App bei Dropbox können Sie dem Artikel 1166 in der Wissensdatenbank entnehmen.

Sobald App-Key und App-Secret konfiguriert sind, kann Webmail Verbindungen zwischen den Benutzerkonten und Dropbox-Konten herstellen. Sobald sich ein Benutzer das erste Mal in den Designs WorldClient oder LookOut anmeldet, erscheint ein neues Auswahlmenü am unteren Seitenrand. Der Benutzer kann dort zwischen drei Optionen wählen: Anzeigen der Dropbox bei der folgenden Anmeldung, keine Anzeige der Dropbox, und Aufruf der neuen Ansicht Optionen » Cloud-Apps. In der Ansicht Optionen » Cloud-Apps können die Benutzer das Steuerelement Dropbox einrichten anklicken. Hierdurch wird ein OAuth-2.0-Popup geöffnet. Es gibt dem Benutzer Auskunft darüber, mit welchem Dienst er sich verbindet, und welche Berechtigungen Webmail hierfür anfordert. Es stehen auch eine Verknüpfung zur Datenschutzerklärung und das Steuerelement "Mit Dropbox verbinden" zur Verfügung. Durch Anklicken von "Mit Dropbox verbinden" wird der Benutzer auf die Dropbox-Website geleitet. Ist der Benutzer noch nicht bei Dropbox angemeldet, kann er sich hier entweder an seinem Dropbox-Benutzerkonto anmelden oder ein Dropbox-Benutzerkonto erstellen. Nach der Anmeldung fragt Dropbox den Benutzer, ob Webmail die Berechtigung zum Vollzugriff auf sein Dropbox-Konto erhalten darf. Stimmt der Benutzer zu, so wird er zu Webmail zurückgeleitet und informiert, ob die Berechtigung erfolgreich erteilt wurde. Die Berechtigung bleibt eine Woche lang gültig, danach muss der Benutzer die Berechtigung erneuern, und Webmail erhält einen Berechtigungstoken, der wiederum eine Woche lang gültig ist. Ist die Berechtigung erfolgreich erteilt, so zeigt Webmail dem Benutzer für jede Dateianlage ein Dropbox-Symbol an. Durch Anklicken dieses Symbols kann der Benutzer die Dateianlage in den Pfad `/WorldClient_Attachments/` seiner Dropbox speichern.

In den Editorfenstern der Designs WorldClient und LookOut können Benutzer durch Anklicken des Dropbox-Symbols in der Symbolleiste des HTML-Editors (oben links) Dateien aus ihren Dropboxen auswählen. Für dieses Leistungsmerkmal müssen die Benutzer den Zugriff auf ihre Dropbox-Konten nicht über Optionen » Cloud-Apps und OAuth 2.0 einrichten. Nur App-Key und App-Secret sind erforderlich.

Die Dropbox-Integration ist per Voreinstellung abgeschaltet. Sie kann mithilfe des Konfigurationsdialogs Dropbox 336 für alle Benutzer aktiviert werden. Der Administrator kann die Integration auch für einzelne Benutzer durch Hinzufügen des Eintrags `DropboxAccessEnabled=Yes` zur jeweiligen Datei `User.ini` aktivieren.

Ende-zu-Ende-Verschlüsselung von E-Mail-Nachrichten und Dateianlagen

Das Design WorldClient unterstützt die Ende-zu-Ende-Verschlüsselung von E-Mail-Nachrichten und Dateianlagen mithilfe von Virtru. Webmail-Benutzer, die dieses

Leistungsmerkmal nutzen wollen, müssen in das Design Webmail wechseln, dann die Seite Optionen » Verfassen aufsuchen und dort das Kontrollkästchen **Virtru aktivieren** anklicken. Danach wird im Editorfenster zum Verfassen von Nachrichten eine Schaltfläche sichtbar, mit deren Hilfe die Benutzer die Nachrichten vor dem Versand verschlüsseln können. Dieses Leistungsmerkmal ist einfach zu nutzen, und es verlangt vom Benutzer nicht, sich Kennwörter oder Schlüssel zu merken oder sie zu vergeben. Empfänger, die Clients mit Unterstützung für Virtru (hierzu gehört auch Webmail) oder Virtru-Plugins für andere Clients nutzen, können die verschlüsselten Nachrichten regulär öffnen und lesen, ohne hierzu besondere Aktionen ausführen zu müssen. Empfänger, deren Clients Virtru nicht unterstützen, erhalten eine Verknüpfung, mit deren Hilfe sie die Nachrichten in einem besonderen, browsergestützten Leseprogramm lesen können.

Falls Sie die Nutzung der Virtru-Verschlüsselung in Webmail durch Ihre Benutzer unterbinden wollen, öffnen Sie die Datei `Domains.ini` im Verzeichnis `MDaemon\WorldClient`, und fügen Sie ihr den Eintrag `VirtruDisabled=Yes` hinzu.

Nähere Informationen hierzu finden Sie in englischer Sprache unter E-Mail Encryption.

Die Nutzung von Webmail

Starten von Webmail

Es stehen drei mögliche Vorgehensweisen zur Verfügung, um den Webmail-Server zu starten:

1. Führen Sie im Abschnitt Stats im linken Bereich der Benutzeroberfläche von MDaemon einen Rechtsklick auf den Eintrag Webmail aus, und wählen Sie aus dem Kontextmenü den Eintrag Aktivieren/deaktivieren.
2. Klicken Sie auf der Benutzeroberfläche auf "Datei » Webmail-Server aktivieren".
3. Klicken Sie auf der Benutzeroberfläche auf "Einstellungen » Web- & IM-Dienste", und klicken Sie dann im Abschnitt Web-Server auf *Webmail wird unter dem internen Web-Server ausgeführt*.

Anmeldung an Webmail

1. Rufen Sie in Ihrem Browser den URL `http://example.com:WCPortnummer` auf. Die Portnummer wird im Abschnitt Web-Server 322 des Konfigurationsdialogs Webmail konfiguriert. Falls Sie Webmail auf dem Standard-Port für Webanwendungen (Port 80) betreiben, brauchen Sie die Portnummer in der URL für Webmail nicht anzugeben (z.B. `www.example.com` statt `www.example.com:3000`).
2. Geben Sie Benutzernamen und Kennwort zu Ihre MDaemon-Benutzerkonto an.
3. Klicken Sie auf Anmelden.

Ändern der Portnummer von Webmail

1. Klicken Sie in der Menüleiste auf "Einstellungen » Web- & IM-Dienste".
2. Tragen Sie in das Eingabefeld der Option *Webmail-Server überwacht folgenden TCP Port* die gewünschte Portnummer ein.
3. Klicken Sie auf OK.

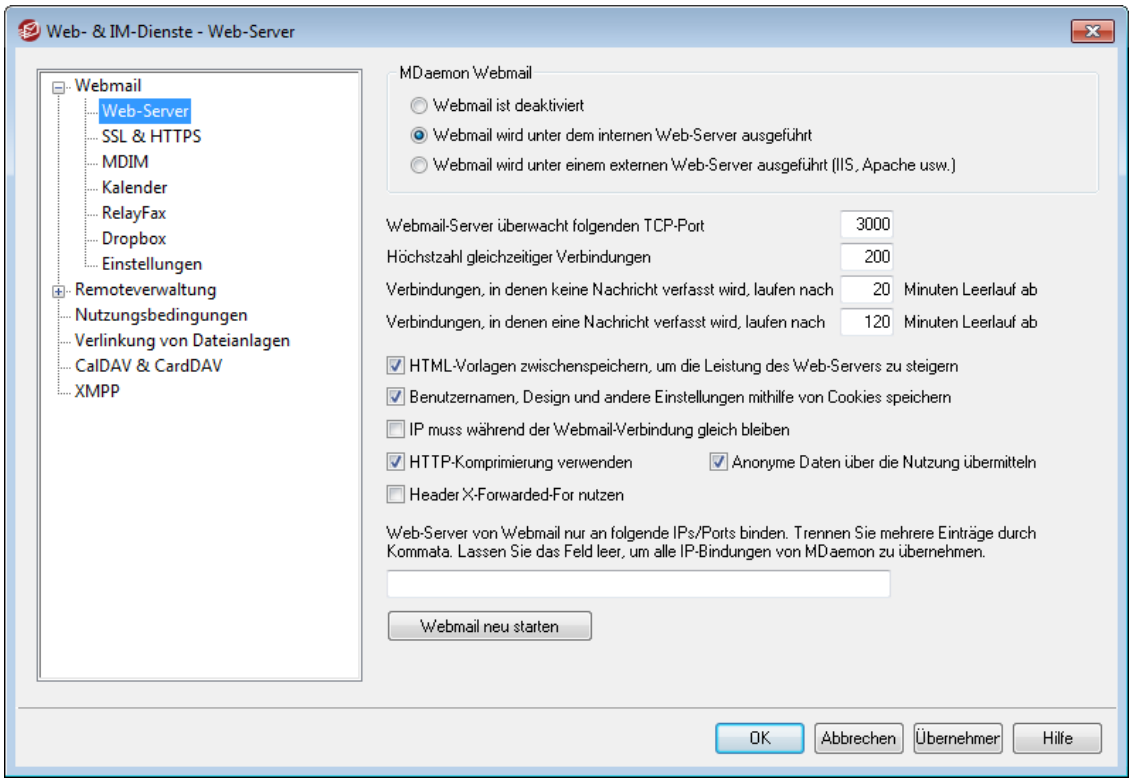
Hilfe für Benutzer von Webmail

Webmail ist mit einer umfassenden Hilfe für die Benutzer ausgestattet. Sie können diese Online-Hilfe direkt aus Webmail aufrufen und erhalten darin Informationen über die Leistungsmerkmale von Webmail, die Ihren Benutzern zur Verfügung stehen.

Weitere Optionen zu den Adressbüchern finden Sie unter:

Webmail » MDIM 331
LDAP 824

3.6.1.2 Web-Server



Dieser Konfigurationsdialog enthält verschiedene Einstellungen, die die Konfiguration für Webmail systemweit und ohne Unterschied für alle Domänen auf dem Server bestimmen.

MDaemon Webmail

Webmail ist deaktiviert
Mit dieser Option wird Webmail abgeschaltet. Webmail lässt sich auch über das Menü Datei sowie über den rechten Abschnitt im Bereich Statistik der Benutzeroberfläche von MDaemon aktivieren und deaktivieren.

Falls Sie das Leistungsmerkmal Verlinkung von Dateianlagen 364 nutzen wollen, muss Webmail aktiv sein.

Webmail wird unter dem internen Web-Server ausgeführt
Diese Option bewirkt, dass Webmail unter dem MDaemon-eigenen Web-Server ausgeführt wird. Webmail lässt sich auch über das Menü Datei sowie über den rechten Abschnitt im Bereich Statistik der Benutzeroberfläche von MDaemon aktivieren und deaktivieren.

Webmail wird unter einem externen Web-Server ausgeführt (IIS, Apache usw.)
Diese Option muss aktiv sein, falls Webmail unter den Internet Information Services (IIS) oder einem sonstigen Web-Server ausgeführt werden, der MDaemon-eigene Web-Server hingegen nicht verwendet werden soll. So lange diese Option aktiv ist, sind bestimmte Menüpunkte in der Benutzeroberfläche nicht zugänglich. Diese gesperrten Menüpunkte beeinflussen Einstellungen, die den Betrieb des externen Web-Servers stören können.

Weitere Informationen hierzu finden Sie unter Einbindung von Webmail in IIS 324.

Webmail-Server überwacht folgenden TCP-Port
Auf dieser Portnummer beantwortet Webmail ankommende Verbindungsversuche.

Höchstzahl gleichzeitiger Verbindungen
Hiermit wird die Höchstzahl der Verbindungen festgelegt, die Webmail gleichzeitig zulässt.

Verbindungen, in denen keine Nachricht verfasst wird, laufen nach [xx] Minuten Leerlauf ab
Wenn ein Benutzer bei Webmail angemeldet ist, aber gerade keine Nachricht verfasst, wird die Verbindung nach der hier angegebenen Leerlaufdauer durch Webmail getrennt.

Verbindungen, in denen eine Nachricht verfasst wird, laufen nach [xx] Minuten Leerlauf ab
Dieser Eintrag legt die höchstzulässige Leerlaufdauer für Sitzungen fest, in denen gerade eine Nachricht verfasst wird. Dieser Timer sollte deutlich höher eingestellt werden als der vorhergehende. Der Leerlauf während der Erstellung einer Nachricht dauert üblicherweise deutlich länger, weil erst beim Absenden der Nachricht, nicht jedoch während des Verfassens, Daten mit dem Server ausgetauscht werden.

HTML-Vorlagen zwischenspeichern, um die Leistung des Web-Servers zu steigern
Diese Option veranlasst Webmail, die Vorlagen im Speicher zu behalten und sie nicht erst bei Bedarf einzulesen. Dies kann die Leistung des Servers erheblich steigern; Änderungen an den Vorlagen erfordern dann aber einen Neustart von Webmail, da sie sonst nicht berücksichtigt werden.

Benutzernamen, Design und andere Einstellungen mithilfe von Cookies speichern
Hiermit kann Webmail den Anmeldenamen, das gewählte Design und einige andere Einstellungen für die Benutzer in einem sog. Cookie auf deren lokalen Rechnern speichern. Für die Benutzer ist damit bereits der Anmeldedialog an ihre individuellen Einstellungen angepasst, sie müssen in ihren Browsern allerdings Cookies zulassen.

IP muss während der Webmail-Verbindung gleich bleiben
Dies ist eine zusätzliche Sicherheitsmaßnahme. Die Einstellung bewirkt, dass eine Webmail-Verbindung mit einem bestimmten Benutzer auf genau die IP-Adresse beschränkt wird, die dem Benutzer bei Verbindungsaufbau zugewiesen war. Eine

Webmail-Verbindung kann somit nicht mehr durch einen Unbefugten "übernommen" werden, da sich dann die IP-Adresse der Gegenstelle ändern würde. Diese Betriebsart erhöht die Sicherheit beträchtlich, kann aber zu Problemen führen, wenn der Benutzer einen Proxy-Server verwendet oder die Internetverbindung über einen Wählzugang herstellt, der die IP-Adressen dynamisch zuweist und nach Verbindungsabbrüchen ändert.

Header X-Forwarded-For nutzen
Diese Option ermöglicht die Nutzung des Headers `X-Forwarded-For`. Dieser Header wird bisweilen durch Proxy-Server hinzugefügt. Diese Option ist per Voreinstellung abgeschaltet. Aktivieren Sie diese Option nur, falls Ihr Proxy-Server diesen Header hinzufügt.

HTTP-Komprimierung verwenden
Diese Option bewirkt, dass in den Webmail-Verbindungen die HTTP-Komprimierung verwendet wird.

Anonyme Daten über die Nutzung übermitteln
Webmail übermittelt per Voreinstellung anonyme und unkritische Daten über die Nutzung. Hierzu gehören das genutzte Betriebssystem, die genutzte Browser-Version und vergleichbare Daten. Die Daten werden durch die MDaemon Technologies Ltd. genutzt, um Webmail zu verbessern. Falls Sie die Übermittlung dieser anonymen Daten über die Nutzung unterbinden wollen, deaktivieren Sie diese Option.

Web-Server von Webmail nur an folgende IPs/Ports binden
Sie können mithilfe dieser Einstellung den Webmail-Serverdienst auf bestimmte IP-Adressen und Ports beschränken. Tragen Sie hierzu die gewünschten IP-Adressen und Ports, durch Kommata getrennt, in das Feld ein. Um einen Port anzugeben, erstellen Sie einen Eintrag im Format "`IP-Adresse:Port`" (beispielsweise `192.0.2.0:80`). Falls Sie einen Port nicht angeben, werden der weiter oben in diesem Konfigurationsdialog angegebenen Standard-TCP-Port und der Standard-HTTPS-Port aus dem Konfigurationsdialog SSL & HTTPS 327 genutzt. Das Zeichen "`*`" bewirkt, dass Webmail auf Verbindungen auf allen Ports reagiert. Der Eintrag "`*,*:80`" veranlasst Webmail beispielsweise, auf allen IP-Adressen die konfigurierten Standard-Ports (per Voreinstellung 3000 und 443) und zusätzlich auf allen IP-Adressen den Port 80 zu überwachen. Falls Sie dieses Feld leer lassen, überwacht Webmail alle IP-Adressen, die Sie für Ihre Domänen 181 konfiguriert haben.

Webmail neu starten
Ein Klick auf dieses Steuerelement startet den Webmail-Serverdienst neu. Beachte: Dieser Neustart ist nach einer Änderung der Portnummer für Webmail nötig, damit Webmail die neue Portnummer übernimmt.

3.6.1.2.1 Die Einbindung von Webmail in die IIS6

Webmail verfügt über einen eigenen Web-Server und benötigt daher die Internet Information Services (IIS) nicht. Webmail unterstützt aber die IIS und kann als ISAPI-DLL in die IIS eingebunden werden. Die folgende Beschreibung, wie Webmail in den IIS6 eingebunden werden kann, ist dem Artikel Nr. 01465 der Wissensdatenbank für MDaemon entnommen, die unter www.mdaemon.com verfügbar ist:

1. Öffnen Sie den Internet-Informationsdienstemanager.
2. Klicken Sie rechts auf **Anwendungspools**.

3. Wählen Sie **Neu/Anwendungspool**.
4. Bennenen Sie den Pool als **Alt-N**, und klicken Sie auf **OK.**
5. Klicken Sie rechts auf **Alt-N**.
6. Klicken Sie auf **Eigenschaften**.
7. Klicken Sie auf die Registerkarte **Leistung**.
8. Deaktivieren Sie die Optionen **Arbeitsprozesse im Leerlauf herunterfahren nach (Minuten):** und **Warteschlange für Kernelanforderung begrenzen auf (Anzahl der Anforderungen)**.
9. Klicken Sie auf die Registerkarte **Identität**.
10. Wählen Sie im Auswahlmenü für das Steuerelement Vordefiniert den Eintrag **Lokales System**.
11. Klicken Sie auf **OK.**
12. Klicken Sie rechts auf **Websites**.
13. Wählen Sie **Neu**.
14. Klicken Sie auf **Website**. (Hierdurch wird ein Assistent gestartet.)
15. Klicken Sie auf **Weiter**.
16. Geben Sie einen Namen für die Site an, etwa **Webmail**.
17. Klicken Sie auf **Weiter**.
18. Klicken Sie erneut auf **Weiter**.
19. Navigieren Sie zum Heimatverzeichnis; in einer Standard-Installation ist dies **C:\MDaemon\WorldClient\HTML**.
20. Klicken Sie auf **Weiter**.
21. Stellen Sie sicher, dass die Berechtigungen **Lesen**, **Skripts ausführen** und **Ausführen** angehakt sind.
22. Klicken Sie auf **Weiter**.
23. Klicken Sie auf **Fertig stellen**.
24. Klicken Sie rechts auf die Website, die Sie soeben erstellt haben **(Webmail)**.
25. Klicken Sie auf **Eigenschaften**.
26. Klicken Sie auf die Registerkarte **Dokumente**.
27. Entfernen Sie alle dort aufgeführten Dokumente.
28. Fügen Sie **WorldClient.dll** hinzu.
29. Klicken Sie die Registerkarte **Basisverzeichnis**.
30. Wählen Sie im Auswahlmenü für die Anwendungspools **Alt-N**.
31. Klicken Sie auf **OK**.
32. Klicken Sie auf **Webdiensterweiterungen**.
33. Aktivieren Sie **Alle unbekannten ISAPI-Erweiterungen**, oder erstellen Sie eine neue Erweiterung für **WorldClient.dll**.

Das Internetdienst-Gästekonto **IUSER_<SERVERNAME>** benötigt für das MDaemon-Verzeichnis und alle seine Unterverzeichnisse die NTFS-Berechtigung **Vollzugriff**.

1. Klicken Sie rechts auf das Verzeichnis von MDaemon (z.B. C:\MDaemon).
2. Klicken Sie auf **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Sicherheit**.
4. Klicken Sie auf **Hinzufügen**.
5. Klicken Sie auf **Erweitert**.
6. Klicken Sie auf **Jetzt suchen**.
7. Wählen Sie **IUSER_<SERVERNAME>** aus (dabei steht anstelle von "<SERVERNAME>" der Name des lokalen Rechners).
8. Klicken Sie auf **OK**.
9. Klicken Sie auf **OK**.
10. Haken Sie das Kontrollkästchen **Vollzugriff** an.
11. Klicken Sie auf **OK**.

Diese Schritte müssen für alle Verzeichnisse wiederholt werden, die MDaemon benutzt.

Um MDaemon nach dem Einrichten des Webs zu aktualisieren oder auf eine neue Version aufzurüsten, verfahren Sie wie folgt:

1. Öffnen Sie den Internet-Informationsdienstemanager.
2. Öffnen Sie die Liste der **Anwendungspools**.
3. Klicken Sie rechts auf **Alt-N**.
4. Klicken Sie auf **Beenden**.
5. Beenden Sie MDaemon.
6. Führen Sie die Installation oder Aktualisierung durch.
7. Starten Sie MDaemon nach Abschluss der Installation.
8. Klicken Sie im Internet-Informationsdienstemanager erneut rechts auf **Alt-N**.
9. Klicken Sie auf **Starten**.

Falls Sie die vorstehend erläuterte Vorgehensweise befolgen, soll dies folgendes bewirken.

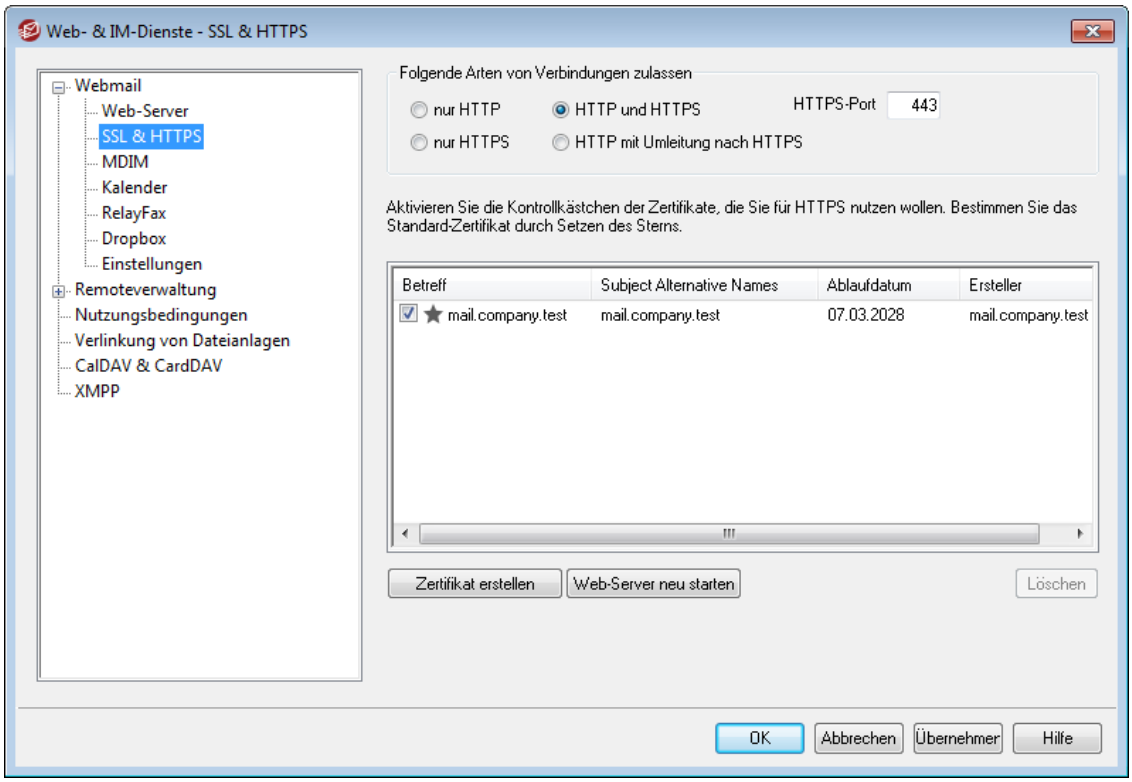
1. Nachdem Sie den **Anwendungspool** beendet haben, erhalten die Benutzer die Meldung **Dienst nicht verfügbar**.
2. Es sollte in der Regel nicht erforderlich sein, das System nach der Aktualisierung von MDaemon neu zu starten.

Die Verwendung von Webmail im Zusammenhang mit dem IIS wird durch den technischen Support nicht unterstützt. Anwender, die Webmail in den IIS einbinden, müssen sich aller Sicherheitsrisiken und der sonstigen Auswirkungen bewusst sein, die das Ausführen von Anwendungen unter dem IIS hat. Es empfiehlt sich dringend, alle Sicherheits-

Patches und –Updates für den IIS zu installieren, bevor Webmail als ISAPI-Erweiterung installiert wird.

Webmail kann nicht aus der Benutzeroberfläche von MDaemon gestartet und gestoppt werden, so lange er in den IIS eingebunden ist. Dies ist nur über die IIS-Verwaltungskonsole möglich.

3.6.1.3 SSL & HTTPS



Der MDaemon-eigene Web-Server unterstützt das Secure-Sockets-Layer-Protokoll (SSL). SSL ist das Standardverfahren für die Sicherung webgestützter Kommunikation zwischen Server und Client. Es stellt Funktionen für die Echtheitsbestätigung des Servers, Datenverschlüsselung und zusätzliche Echtheitsbestätigung für den Client einer TCP/IP-Verbindung zur Verfügung. Da auch alle wichtigen Browser HTTPS (HTTP über SSL) unterstützen, genügt es, ein gültiges digitales Zertifikat auf dem Server zu installieren, damit beim Verbindungsaufbau eines Clients die SSL-Funktionen automatisch genutzt werden.

Die Einstellungen zu den HTTPS-Funktionen von Webmail befinden sich im Menü SSL & HTTPS, das über Einstellungen » Web- & IM-Dienste » Webmail erreichbar ist. Um die Bedienung zu vereinfachen, sind diese Einstellungen auch in dem Konfigurationsdialog "Sicherheit » Sicherheits-Manager » SSL & TLS » Webmail" gespiegelt.

Nähere Informationen über das SSL-Protokoll und die Zertifikate finden Sie unter **SSL & TLS** 577.

Diese Einstellungen wirken auf Webmail nur dann, wenn der MDaemon-eigene Web-Server verwendet wird. Ist Webmail stattdessen in die IIS oder einen anderen Web-Server eingebunden, so bleiben diese Einstellungen wirkungslos. Die Unterstützung für SSL und HTTPS muss in diesem Fall über den verwendeten Web-Server mithilfe seiner Verwaltungswerkzeuge konfiguriert werden.

Folgende Arten von Verbindungen zulassen

nur HTTP
Soll Webmail keine HTTPS-Verbindungen annehmen, so muss diese Option aktiv sein. Es sind dann nur HTTP-Verbindungen zulässig.

HTTP und HTTPS
Diese Option bewirkt, dass Webmail zwar SSL unterstützt, die Webmail-Benutzer jedoch HTTPS nicht zwingend verwenden müssen. Webmail überwacht den weiter unten konfigurierten HTTPS-Port auf eingehende Verbindungen, lässt jedoch auch normale HTTP-Verbindungen auf dem Webmail-Port zu, der im Konfigurationsdialog Web-Server 322 in der Konfiguration von Webmail definiert ist.

nur HTTPS
Diese Option bewirkt, dass Verbindungen zu Webmail ausschließlich über HTTPS hergestellt werden können. Webmail reagiert nur noch auf HTTPS-Verbindungen, nicht aber auf HTTP-Verbindungen, so lange diese Option aktiv ist.

HTTP mit Umleitung nach HTTPS
Diese Option bewirkt, dass HTTP-Verbindungen auf den HTTPS-Port umgeleitet und dann als HTTPS-Verbindungen weiter geführt werden.

HTTPS-Port
Hier wird der TCP-Port eingetragen, den Webmail auf eingehende SSL-Verbindungen überwachen soll. Die Grundeinstellung für den SSL-Port ist 443. Wird dieser SSL-Standardport verwendet, so muss beim Aufruf des URLs von Webmail keine Portnummer angegeben werden (z.B. entspricht "https://example.com" dem URL "https://example.com:443").

Diese Portnummer ist nicht dieselbe, die Webmail im Bereich Web-Server 322 im Konfigurationsdialog für Webmail zugewiesen wurde. Falls HTTP-Verbindungen zu Webmail weiterhin zugelassen sein sollen, müssen sie jenen anderen Port verwenden, sonst ist kein Verbindungsaufbau möglich. HTTPS-Verbindungen müssen hingegen auf dem HTTPS-Port hergestellt werden.

Zertifikat zur Nutzung mit HTTPS/SSL auswählen

In dieser Liste sind Ihre SSL-Zertifikate aufgeführt. Um Zertifikate für die Nutzung durch MDaemon zu aktivieren, aktivieren Sie die zugehörigen Kontrollkästchen. Um ein Zertifikat als Standard-Zertifikat zu bestimmen, klicken Sie auf den Stern neben

dem gewünschten Zertifikat. MDaemon unterstützt die Erweiterung Server Name Identification (SNI) für das Protokoll TLS. Das Leistungsmerkmal SNI (Identifizierung von Servernamen) ermöglicht die Nutzung eines eigenen Zertifikats für jeden einzelnen Hostnamen, der Ihrem Server zugeordnet ist. MDaemon prüft die aktiven Zertifikate und wählt das Zertifikat aus, in dessen Datenfeld Subject Alternative Names der jeweils angeforderte Hostname enthalten ist. (Sie legen diese Subject Alternative Names bei Erstellung des Zertifikats fest.). Falls der Client keinen bestimmten Hostnamen anfordert, oder falls MDaemon kein Zertifikat mit übereinstimmendem Hostnamen findet, nutzt MDaemon das Standard-Zertifikat. Auf der Benutzeroberfläche von MDaemon können Sie ein Zertifikat durch Doppelklick auf seinen Eintrag in der Windows-Zertifikatverwaltung öffnen und seine Eigenschaften einsehen. Diese Funktion steht in der browsergestützten Remoteverwaltung nicht zur Verfügung.

Löschen
Hierdurch wird das in der Liste ausgewählte Zertifikat gelöscht. Vor dem eigentlichen Löschvorgang erscheint ein Dialogfenster mit einer Sicherheitsabfrage, ob der Löschvorgang auch wirklich durchgeführt werden soll.

Zertifikat erstellen

Um ein SSL-Zertifikat zu erstellen, klicken Sie auf das Steuerelement Zertifikat erstellen.

Einzelheiten zu dem Zertifikat

Hostname
Hier wird der Hostname angegeben, zu dem die Benutzer eine Verbindung herstellen (z.B. "wc.example.com").

Name der Organisation/Firma
Hier wird der Name der Organisation oder der Firma eingetragen, die dieses Zertifikat besitzt.

Weitere Hostnamen (mehrere Einträge durch Kommata trennen)
Falls auf Ihrem System weitere Hostnamen konfiguriert sind, zu denen Benutzer

Verbindungen herstellen, so können Sie das Zertifikat auch auf diese Hostnamen erstrecken. Geben Sie hierzu die anderen Hostnamen oder Domänennamen hier ein. Trennen Sie mehrere Einträge durch Kommata. Jokerzeichen sind zulässig, sodass sich "`*.example.com`" auf alle Subdomänen von example.com erstrecken würde (etwa "`wc.example.com`", "`mail.example.com`", usw.).

MDaemon unterstützt die Erweiterung Server Name Identification (SNI) für das Protokoll TLS. Das Leistungsmerkmal SNI (Identifizierung von Servernamen) ermöglicht die Nutzung eines eigenen Zertifikats für jeden einzelnen Hostnamen, der Ihrem Server zugeordnet ist. MDaemon prüft die aktiven Zertifikate und wählt das Zertifikat aus, in dessen Datenfeld Subject Alternative Names der jeweils angeforderte Hostname enthalten ist. Falls der Client keinen bestimmten Hostnamen anfordert, oder falls MDaemon kein Zertifikat mit übereinstimmendem Hostnamen findet, nutzt MDaemon das Standard-Zertifikat.

Länge des Schlüssels
Hier wird die gewünschte Länge des Schlüssels in Bit ausgewählt. Je länger der Schlüssel, desto besser ist der Datenaustausch gesichert. Dabei ist aber zu beachten, dass nicht alle Anwendungsprogramme Schlüssel mit einer Länge von mehr als 512 Bit verarbeiten können.

Hash-Algorithmus
Hier wird der Hash-Algorithmus ausgewählt; mögliche Algorithmen sind SHA1 und SHA2. Per Voreinstellung wird SHA2 genutzt.

Land/Region
Wählen Sie hier das Land oder die Region aus, in der sich dem oder in der sich der Server befindet.

Web-Server neu starten

Ein Klick auf dieses Steuerelement startet den Web-Server neu. Dieser Neustart ist nach jeder Änderung an einem Zertifikat erforderlich; erst danach werden neue Zertifikate genutzt.

Verwaltung Ihres Zertifikats mithilfe von Let's Encrypt

Let's Encrypt ist eine Zertifizierungsstelle (auch Certificate Authority, kurz CA), die mithilfe eines automatisierten Verfahrens unentgeltlich Zertifikate zur Verfügung stellt. Dieses Verfahren soll die derzeit noch weit verbreiteten und komplexen Verfahren der manuellen Erstellung, Echtheitsprüfung, Signatur, Installation und Verlängerung von Zertifikaten für die Sicherung von Websites ablösen.

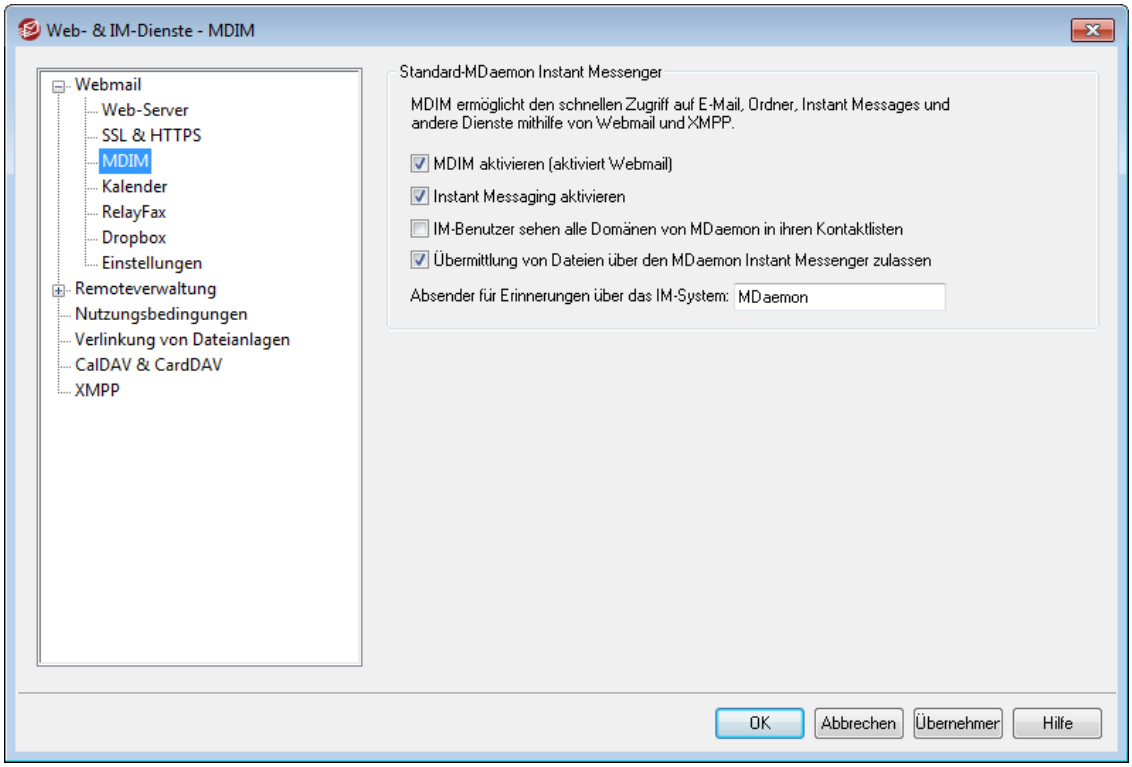
Um dieses Verfahren zu unterstützen, steht Ihnen der Konfigurationsdialog Let's Encrypt 596 zur Verfügung. Mithilfe dieses Konfigurationsdialog wird das automatische Verfahren zur Verwaltung eines Zertifikats unterstützt, das Let's Encrypt bereitstellt. Sie können hier ein PowerShell-Skript einfach konfigurieren und ausführen, das im Verzeichnis "`MDaemon\LetsEncrypt`" abgelegt ist. Wenn Sie dieses Skript ausführen, wird hierdurch das System für Let's Encrypt eingerichtet, und insbesondere werden die für die erfolgreiche Abwicklung der http-01-Challenge

erforderlichen Dateien in das HTTP-Verzeichnis von Webmail kopiert. Das Skript nutzt als Domäne für das Zertifikat den SMTP-Hostnamen[184] der Standard-Domäne[181] und fügt etwa konfigurierte *Weitere Hostnamen* ein, ruft das Zertifikat ab, importiert es in Windows, und konfiguriert MDaemon so, dass das Zertifikat für MDaemon, Webmail und die Remoteverwaltung genutzt wird. Darüber hinaus erstellt das Skript im Verzeichnis "`MDaemon\Logs\`" die Protokolldatei `LetsEncrypt.log`. Diese Protokolldatei wird immer dann, wenn das Skript ausgeführt wird, gelöscht und neu erstellt. Sie beinhaltet Datum und Uhrzeit, wann das Skript ausgeführt wurde. Falls Sie eine *E-Mail-Adresse des Administrators für Benachrichtigungen* angegeben haben, werden im Fehlerfall Benachrichtigungen an diese Adresse versandt. Nähere Informationen finden Sie im Abschnitt Let's Encrypt[596].

Siehe auch:

SSL & TLS[577]
Erstellen und Verwenden von SSL-Zertifikaten[902]

3.6.1.4 MDIM



Dieser Konfigurationsdialog steuert die Standard-Einstellungen, die für den MDaemon Instant Messenger (MDIM)[318] in neu erstellten Domänen genutzt werden. Für einzelne Domänen können mithilfe der Konfigurationsdialoge MDIM[190] im Domänen-Manager eigene, abweichende Einstellungen getroffen werden. Die Leistungsmerkmale des MDaemon Instant Messengers können für einzelne Benutzerkonten mithilfe des Konfigurationsdialogs Web-Dienste[720] und für Gruppen von Benutzerkonten mithilfe des Konfigurationsdialogs Gruppen-Eigenschaften[784] aktiviert und deaktiviert werden.

Standard-MDaemon Instant Messenger

MDIM aktivieren (aktiviert Webmail)
Diese Option bewirkt, dass der MDaemon Instant Messenger über Webmail per Voreinstellung zum Herunterladen bereit gestellt wird. Die Benutzer können die Installationsroutine für den MDIM in Webmail auf der Seite Optionen » MDaemon Instant Messenger abrufen. Die Installationsroutine, die die Benutzer dort erhalten, ist für das Benutzerkonto, von dem aus sie abgerufen wird, jeweils schon vorkonfiguriert, sodass die Installation und die Einrichtung vereinfacht sind.

Instant Messaging aktivieren
Per Voreinstellung können Benutzerkonten den MDIM und XMPP-Clients[372] von Drittanbietern nutzen, um mit anderen Benutzern ihrer Domäne Instant Messages auszutauschen. Falls Sie diese Option deaktivieren, ist das Instant Messaging nicht per Voreinstellung verfügbar.

IM-Benutzer sehen alle Domänen von MDaemon in ihren Kontaktlisten
Diese Option bewirkt, dass die Benutzer per Voreinstellung Kontakt aus allen Ihren MDaemon-Domänen in die Kontaktlisten eintragen können. Ist diese Option deaktiviert, so können Benutzer nur Kontakte aus der Domäne hinzufügen, der sie selbst angehören. Ein Beispiel hierzu: Falls Ihre MDaemon-Installation die Domänen example.com und example.org umfasst, können Ihre Benutzer bei aktivierter Option Kontakte aus beiden Domänen für das Instant Messaging nutzen. Ist die Option nicht aktiv, so können Benutzer aus der Domäne example.com nur Benutzer aus der Domäne example.com hinzufügen, und Benutzer aus der Domäne example.org können nur Benutzer aus der Domäne example.org hinzufügen. Der Domänen-Manager[190] enthält eine entsprechende Option, mit deren Hilfe dieses Verhalten nach Domänen getrennt gesteuert werden kann.

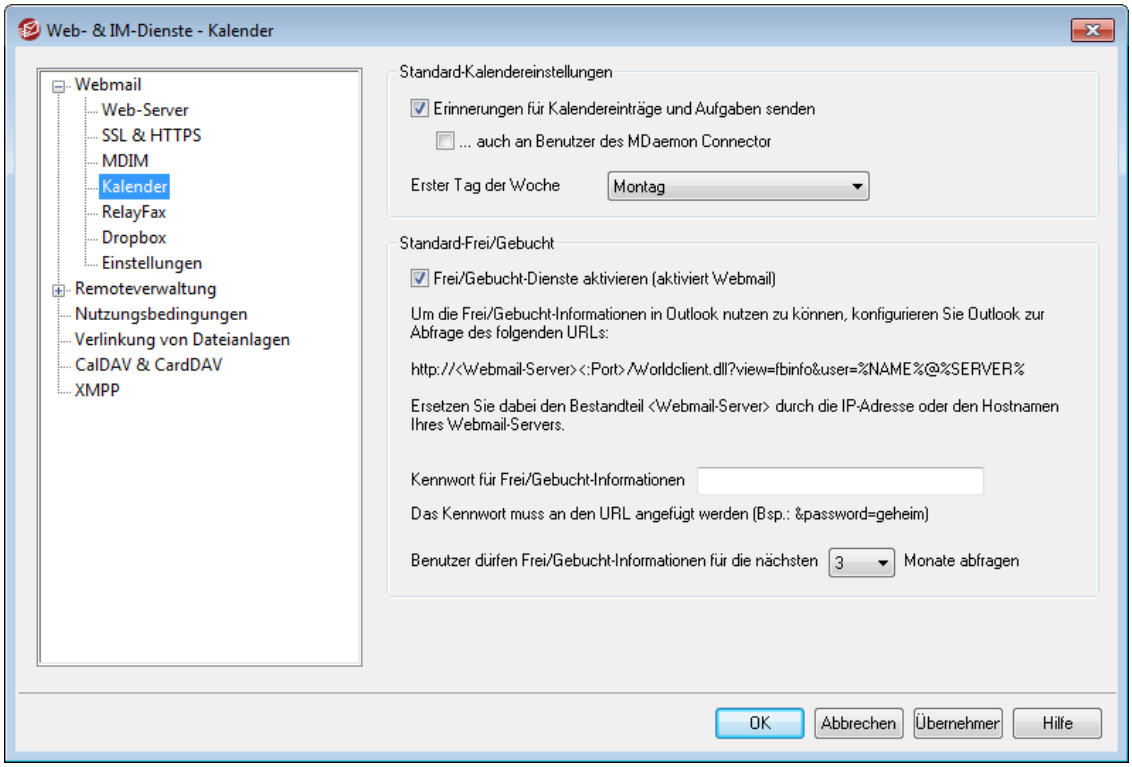
Übermittlung von Dateien über den MDaemon Instant Messenger zulassen
Per Voreinstellung können MDIM-Benutzer an ihre MDIM-Kontakte Dateien übermitteln. Falls Sie nicht wünschen, dass Dateien über den MDIM übermittelt werden können, deaktivieren Sie diese Option.

Absender für Erinnerungen über das IM-System
Wird in den Webmail-Kalender eines Benutzers ein Termin eingetragen, so kann dafür eine Terminerinnerung veranlasst werden, die dem Benutzer zu einer bestimmten Zeit zugesandt wird. Ist das IM-System für die Domäne des Benutzers aktiv, und nutzt der Benutzer MDIM, so wird ihm die Terminerinnerung über MDIM angezeigt. In diesem Textfeld können Sie den Namen festlegen, der als Absendername für die Erinnerung im Feld "Von:" angezeigt wird. Dieses Textfeld enthält die Voreinstellung für neue Domänen. Sie können über den Konfigurationsdialog MDIM[190] im Domänen-Manager[190] für einzelne Domänen abweichende Einstellungen treffen.

Siehe auch:

Domänen-Manager » MDIM[190]
Benutzerkonten-Editor » Web-Dienste[720]
Gruppen-Eigenschaften[784]

3.6.1.5 Kalender



Dieser Konfigurationsdialog steuert die Standard-Einstellungen für die Kalender-Funktionen von MDaemon. Für einzelne Domänen können mithilfe des Konfigurationsdialogs Kalender[192] im Domänen-Manager eigene, abweichende Einstellungen getroffen werden.

Standard-Optionen für Kalender

Erinnerungen für Kalendereinträge und Aufgaben senden
Falls Webmail die Erinnerungsnachrichten für Kalender und Aufgaben über E-Mail und den MDaemon Instant Messenger an die Benutzer senden soll, muss diese Option aktiv sein.

...auch an Benutzer des Outlook Connectors
Falls die Option "*Erinnerungen für Kalendereinträge und Aufgaben senden*" oben aktiv ist, können durch Aktivieren dieser Option die Erinnerungen auch Benutzern des Outlook Connectors gesandt werden.

Erster Tag der Woche
Der aus diesem Rollmenü ausgewählte Wochentag erscheint in den Terminkalendern dieser Domäne als erster Tag der Woche.

Standard-Frei/Gebucht

MDaemon enthält einen Server für Frei/Gebucht-Informationen, mit dessen Hilfe der Organisator einer Besprechung prüfen kann, wann die gewünschten Teilnehmer verfügbar sind. Diese Funktion ist über eine Verknüpfung zur Zeitplanung in der Maske für die Besprechungsplanung in Webmail zugänglich. Die Funktion zeigt die Liste der Besprechungsteilnehmer und eine farbig gekennzeichnete Übersicht über die Kalender der Teilnehmer. Für jeden Teilnehmer wird in einer eigenen Zeile durch Farbkennzeichnung dargestellt, zu

welchen Zeiten er verfügbar ist. Dabei wird nach "belegt", "unter Vorbehalt", "nicht im Büro" und "keine Information" unterschieden. In der Besprechungsplanung kann auch automatisch der nächste verfügbare Termin gesucht werden. Der Server stellt dann den nächstmöglichen Zeitpunkt fest, zu dem alle Teilnehmer verfügbar sind. Anschließend kann eine Besprechungsanfrage an alle Teilnehmer gesendet werden, und die Teilnehmer können zusagen oder ablehnen.

Der Server für die Frei/Gebucht-Informationen, den Webmail bereit stellt, ist auch zu Microsoft Outlook kompatibel. Um den Server zu nutzen, muss in Outlook nur der URL zu dem Frei/Gebucht-Server von Webmail eingetragen werden. Bei Outlook 2002 sind die Einstellungen für die Abfrage von Frei/Gebucht-Informationen beispielsweise über "Extras » Optionen » Kalenderoptionen... » Frei/Gebucht-Optionen..." zugänglich.

In die Maske in Outlook muss folgender URL eingetragen werden:

```
http://<Webmail><:Port>
/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER%
```

Ersetzen Sie dabei "<Webmail>" durch die IP-Adresse oder den Domänennamen Ihres Webmail-Servers und "<:Port>" durch die Portnummer (falls Sie nicht den Standard-Web-Port nutzen). Ein Beispiel:

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%
@%SERVER%
```

Weitere Informationen über die Nutzung von Frei/Gebucht-Informationen bei der Terminplanung enthält die Online-Hilfe von Webmail.

Verwaltung von Frei/Gebucht-Informationen aktivieren
Diese Option schaltet die Funktionen des Frei/Gebucht-Servers für die Benutzer frei.

Kennwort für Frei/Gebucht-Informationen
Soll die Abfrage der Frei/Gebucht-Informationen über Outlook durch ein Kennwort geschützt werden, so muss dieses Kennwort hier eingetragen werden. Die Benutzer müssen dem oben konfigurierten URL in Outlook das Kennwort (im Format "&password=Kennwort") hinzufügen. Ein Beispiel hierzu:

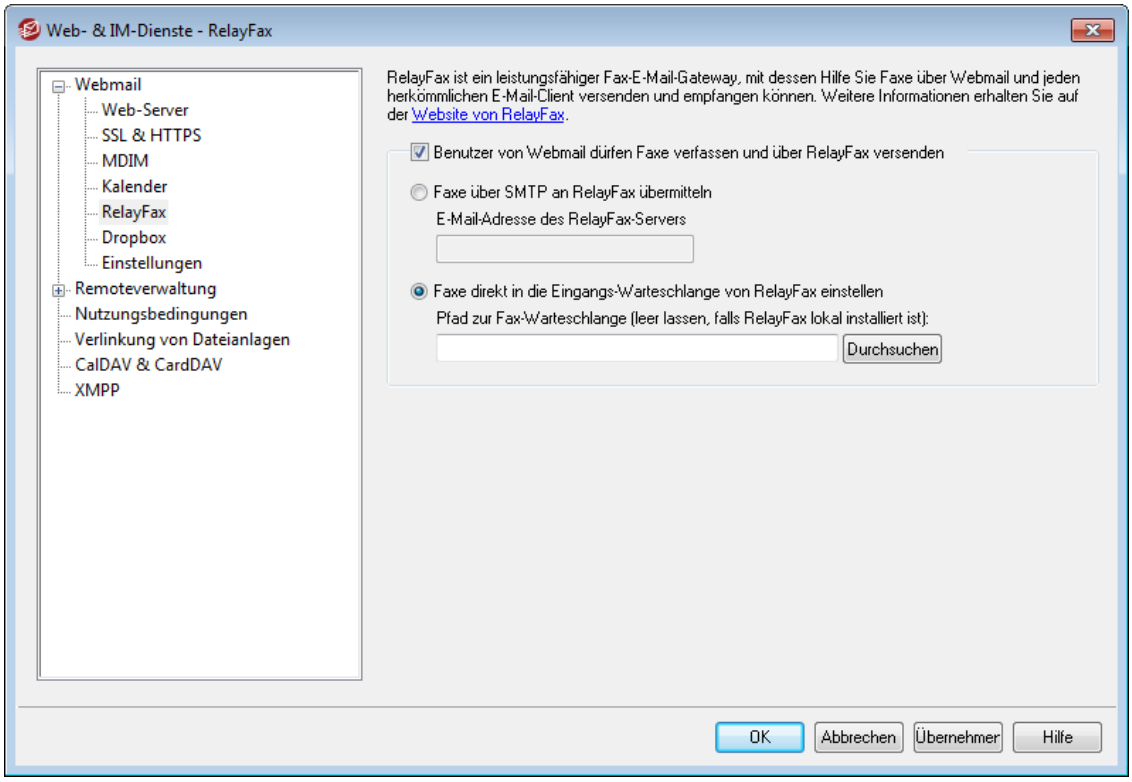
```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME
%@%SERVER%&password=MyFBServerPassword
```

Benutzer dürfen Frei/Gebucht-Informationen für die nächsten [xx] Monate abfragen
Diese Option bestimmt, für welchen Zeitraum die Benutzer Frei/Gebucht-Informationen im Voraus abfragen dürfen.

Siehe auch:

Domänen-Manager » Kalender 192

3.6.1.6 RelayFax



Der RelayFax-Server von MDaemon Technologies schafft einen Übergang zwischen E-Mail und Telefax und umgekehrt. Er lässt sich nahtlos in Webmail einbinden und kann somit allen Benutzern Telefaxdienste zur Verfügung stellen. Benutzer von Webmail erhalten Zugriff auf verschiedene Funktionen, mit denen sie Telefaxe aus WorldClient heraus erstellen und versenden können. Weitere Informationen erhalten Sie auf der Website www.mdaemon.com im Abschnitt RelayFax.

Optionen zur Einbindung von RelayFax

Benutzer von Webmail dürfen Faxe verfassen und über RelayFax versenden
Hiermit wird RelayFax in Webmail eingebunden. Sobald die Option aktiv ist, erscheinen die Verknüpfung "Fax erstellen" und weitere Fax-Funktionen in MDaemon.

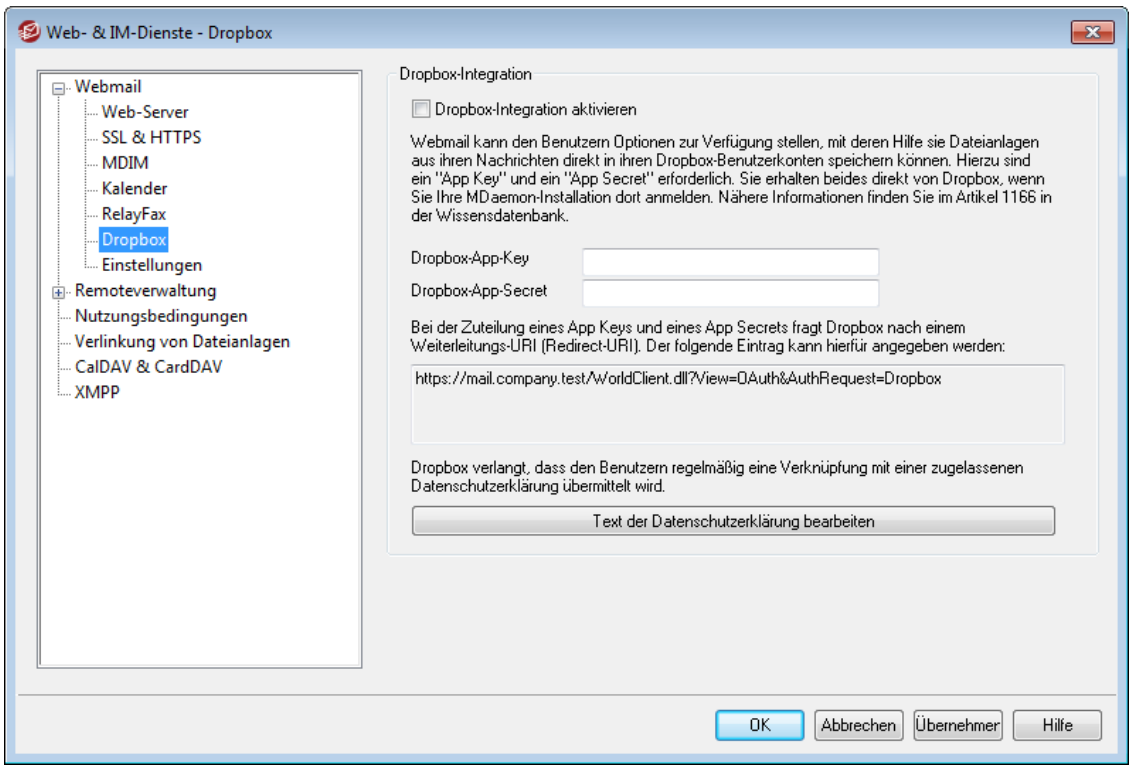
Faxe über SMTP an RelayFax übermitteln
RelayFax überwacht ein bestimmtes Postfach auf eingehende Nachrichten, die per Fax versandt werden sollen. Mit dieser Option verwendet MDaemon den normalen Übertragungsweg über SMTP, um die Nachrichten an das Postfach zu senden. Das ist besonders dann sinnvoll, wenn das Postfach, welches RelayFax überwacht, nicht im lokalen Netzwerk liegt. Liegt hingegen RelayFax ebenfalls im lokalen Netzwerk, so bietet es sich an, dass MDaemon die Nachrichten direkt in die Warteschlange von RelayFax einstellt. Weitere Informationen hierzu finden Sie unten unter *Faxe direkt in die Eingangs-Warteschlange von RelayFax einstellen*.

E-Mail-Adresse des RelayFax-Servers
An die hier angegebene E-Mail-Adresse werden alle per Fax zu versendenden Nachrichten geschickt. Sie muss mit jener Adresse übereinstimmen, die RelayFax auf Nachrichten überwacht.

Faxe direkt in die Eingangs-Warteschlange von RelayFax einstellen
Falls sich RelayFax im lokalen Netzwerk befindet, ist diese Option gegenüber dem Versand per SMTP vorzugswürdig. MDaemon stellt dann Nachrichten für RelayFax direkt in dessen Eingangs-Warteschlange ein, ohne sie per SMTP zu übertragen.

Pfad zur Fax-Warteschlange
Werden RelayFax und MDaemon auf demselben Rechner ausgeführt, so bleibt das Feld für den Pfad leer; ansonsten wird hier der Pfad zu dem Verzeichnis \app\ von RelayFax eingetragen.

3.6.1.7 Dropbox



MDaemon Webmail unterstützt Dropbox direkt. Die Benutzer können daher Dateianlagen in ihren Dropbox-Benutzerkonten speichert, und sie können direkte Verknüpfungen mit Dateien, die in Dropbox-Benutzerkonten gespeichert sind, in abgehende Nachrichten einfügen. Um den Benutzern diese Leistungsmerkmale bereit zu stellen, müssen Sie Ihre Webmail-Installation auf der DBX-Plattform als Dropbox-App registrieren. Diese Registrierung ist unkompliziert; Sie müssen sich lediglich an einem Dropbox-Benutzerkonto anmelden, einen eindeutigen Namen für eine App mit Vollzugriff auf Dropbox ("Full Dropbox") erstellen, den URI für die Umleitung nach Webmail angeben ("Redirect URI") und eine Standardeinstellung ändern. Anschließend müssen Sie den App Key und das App Secret der Dropbox in die entsprechenden Felder des Dropbox-Konfigurationsdialogs in Webmail kopieren. Ihre Benutzer können dann bei der nächsten Anmeldung an Webmail ihre Dropbox-Benutzerkonten mit Webmail verknüpfen. Eine genaue Anleitung für die Erstellung Ihrer Dropbox-App und die Verknüpfung mit Webmail finden Sie im Abschnitt Erstellen und Verknüpfen Ihrer Dropbox-App 338 weiter unten.

Nachdem Sie Ihre Dropbox-App erstellt haben, hat die App zunächst den Status "Entwicklung" ("Development"). In diesem Status können 500 Webmail-Benutzer ihre Dropbox-Benutzerkonten mit der App verknüpfen. Dropbox verlangt jedoch, dass Sie

den Status "Wirkbetrieb" ("Production") binnen zwei Wochen beantragen und erteilt erhalten, nachdem sich 50 Benutzer mit Ihrer Dropbox-App verknüpft haben. Ist dieser Status nach Ablauf der genannten Frist nicht erteilt, dann wird die Verknüpfung weiterer Benutzer mit Ihrer App unterbunden, und zwar unabhängig davon, wie viele Benutzer (0 bis 500) mit Ihrer App verknüpft sind. Solange der Status "Wirkbetrieb" nicht erteilt wurde, funktioniert die Dropbox-Integration zwar weiterhin, aber es können keine weiteren Benutzer ihre Benutzerkonten mit der Dropbox-App verknüpfen. Die Erteilung der Freigabe für den Wirkbetrieb ist ein unkomplizierter Prozess, der sicherstellen soll, dass Ihre App den Richtlinien und Nutzungsbedingungen von Dropbox entspricht. Nähere Informationen hierzu erhalten Sie in englischer Sprache im Abschnitt Production Approval ("Freigabe für den Wirkbetrieb") der Entwicklerrichtlinien für die DBX-Plattform.

Sobald Ihre Webmail-App erstellt und richtig konfiguriert ist, erhalten alle Webmail-Benutzer bei der Anmeldung an Webmail die Möglichkeit, ihre Benutzerkonten mit ihren eigenen Dropbox-Konten zu verknüpfen. Die Benutzer müssen sich dazu an Dropbox anmelden und der App die Berechtigung für den Zugriff auf das Dropbox-Benutzerkonto erteilen. Die Benutzer werden dann mithilfe eines Umleitungs-URIs, der während des Anmeldeverfahrens an Dropbox übermittelt wurde, wieder zu Webmail zurückgeleitet. Aus Sicherheitsgründen muss dieser URI einem der Umleitungs-URIs ("Redirect URIs") entsprechen, die Sie auf der Info-Seite Ihrer App auf Dropbox.com angegeben haben. Nähere Informationen hierzu finden Sie weiter unten. Abschließend tauschen Webmail und Dropbox einen Zugriffskode und einen Zugriffstoken aus, mit deren Hilfe Webmail eine Verbindung zum Dropbox-Benutzerkonto herstellen kann. Diese Verbindung ermöglicht es den Benutzern, Dateianlagen in ihren Dropbox-Benutzerkonten zu speichern. Der Zugriffstoken läuft nach jeweils sieben Tagen ab; die Benutzer müssen daher die Berechtigung zur Nutzung ihrer Dropbox-Benutzerkonten immer wieder neu erteilen. Die Benutzer können auf der Seite Cloud-Apps in Webmail auch die Verknüpfung ihres Benutzerkontos mit ihrer Dropbox manuell trennen, und sie können die Berechtigung manuell neu erteilen.

Dropbox-Integration

Dropbox-Integration aktivieren
Nachdem Sie Ihre Dropbox-App erstellt und mit Webmail verknüpft haben, aktivieren Sie diese Option. Sie gestatten Ihren Webmail-Benutzern damit, ihre Webmail-Benutzerkonten mit ihren Webmail-Benutzerkonten zu verknüpfen. Falls Sie die Dropbox-Integration für einzelne Benutzer aktivieren oder deaktivieren wollen, können Sie den Dateien `User.ini` der einzelnen Benutzer den Eintrag "`DropboxAccessEnabled=Yes` (oder `No`)" hinzufügen.

Dropbox-App-Key und Dropbox-App-Secret
Sie finden den App-Key und das App-Secret auf der Info-Seite Ihrer App auf Dropbox.com. Tragen Sie beide Werte hier ein, um Webmail mit Ihrer Dropbox-App zu verknüpfen.

Umleitungs-URI
Sie müssen auf der Info-Seite Ihrer App auf Dropbox.com einen Umleitungs-URI ("Redirect URI") angeben. MDaemon zeigt in diesem Textfeld automatisch einen URI an, der hierfür nutzbar sein sollte. Sie können wahlweise mehr als einen Umleitungs-URI angeben. Sie können beispielsweise für jede Ihrer Domänen einen eigenen URI und sogar für den localhost einen URI angeben, der dann bei Anmeldungen an Webmail von dem Rechner aus genutzt werden kann, auf dem der Server selbst ausgeführt wird.

Einige Beispiele hierzu:

```
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 lässt Umleitungs-URIs nur zu, wenn sie gesicherte Verbindungen herstellen. Daher muss für Webmail HTTPS 327 aktiv sein.

Text der Datenschutzerklärung bearbeiten
Durch Anklicken dieser Schaltfläche können Sie die Datenschutzerklärung Ihrer Webmail-App bearbeiten. Dropbox verlangt, dass Ihren Benutzern von Zeit zu Zeit eine freigegebene Datenschutzerklärung angezeigt wird. Die Seite **Mit Dropbox verbinden**, die Ihren Benutzern angezeigt wird, enthält daher eine Verknüpfung namens "Datenschutzerklärung", die zu dem Inhalt der hier bearbeiteten Textdatei führt. Die Verknüpfung öffnet ein kleines Fenster, in dem der Text der Datenschutzerklärung angezeigt wird, und sie enthält eine Schaltfläche, mit deren Hilfe die Benutzer die Datenschutzerklärung herunterladen können. Falls Sie den Text der Datenschutzerklärung formatieren wollen, oder falls er Verknüpfungen enthalten soll, fügen Sie den entsprechenden HTML-Kode in die Datenschutzerklärung ein.

Erstellen und Verknüpfen Ihrer Dropbox-App

Die nachfolgende Übersicht erläutert die einzelnen Schritte, die zur Erstellung Ihrer Dropbox-App und zur Verknüpfung mit Webmail erforderlich sind.

1. Rufen Sie in Ihrem Browser die DBX-Plattform auf.
2. Melden Sie sich an Ihrem Dropbox-Benutzerkonto an.
3. Wählen Sie **Dropbox API.**
4. Wählen Sie **Full Dropbox** ("Vollzugriff auf Dropbox").
5. Geben Sie Ihrer App einen eindeutigen Namen.
6. Klicken Sie auf **Create App** ("App erstellen").
7. Klicken Sie auf **Enable additional users** ("weitere Benutzer zulassen"), und klicken Sie dann auf **Okay**.
8. Change **Allow implicit grant** to **Disallow**
9. Geben Sie mindestens einen **Redirect URI** ("Umleitungs-URI") an, und klicken Sie nach Angabe des URIs jeweils auf **Add** ("Hinzufügen"). Die URIs müssen gesicherte Verbindungen mit Ihrem Webmail herstellen (HTTPS muss für Webmail aktiv sein).

   Einige Beispiele hierzu:

   https://mail.company.test/WorldClient.dll?View=OAuth&AuthRequest=Dropbox

   https://localhost/WorldClient.dll?View=OAuth&AuthRequest=Dropbox
10. Lassen Sie die Info-Seite Ihrer App in Ihrem Browser geöffnet, und rufen Sie die Benutzeroberfläche von MDaemon auf.

11. Klicken Sie auf **Einstellungen**.
12. Klicken Sie aufClick **Web- & IM-Dienste**.
13. Klicken Sie im Abschnitt **Webmail** auf **Dropbox**.
14. Kopieren Sie aus Ihrem Browser die Werte **App key** und **App secret** in die entsprechenden Felder des **Dropbox**-Konfigurationsdialogs in MDaemon.
15. Klicken Sie auf **Übernehmen**.
16. Klicken Sie auf **OK**.

Anweisungen für die Verknüpfung von Webmail-Benutzerkonten mit den Dropbox-Benutzerkonten der Webmail-Benutzer finden Sie in der Online-Hilfe von Webmail und im Artikel 1166 der Wissensdatenbank.

3.6.1.8 Google Drive

Diese Seite ist nur in der Webschnittstelle der MDaemon-Remoteverwaltung 350 (MDRA) verfügbar.

Einbindung von Google Drive

MDaemon Webmail kann den Benutzern Optionen anbieten, mit denen sie Dateianlagen aus Nachrichten direkt in ihre Google-Drive-Benutzerkonten speichern können. Sie können außerdem dort gespeicherte Dokumente bearbeiten und verwalten. Um diese Leistungsmerkmale zu aktivieren, sind ein **API-Schlüssel**, eine **Client-ID** und ein **Client-Schlüssel** erforderlich. Diese Daten werden direkt von Google bezogen. Hierzu muss in der Google-API-Konsole eine App erstellt, und es muss Ihre MDaemon-Installation bei Google registriert werden. Eine Komponente dieser App ist die Anmeldung über OAuth 2.0. Sie gestattet Ihren Webmail-Benutzern, sich bei Webmail anzumelden und dann den Zugriff auf ihre Google-Drive-Benutzerkonten durch MDaemon freizugeben. Sobald diese Freigabe erteilt ist, können die Benutzer ihre in Google Drive gespeicherten Ordner und Dateien einsehen. Sie können Dateien auch hochladen, herunterladen, verschieben, kopieren, umbenennen und löschen. Sie können außerdem Dateien nach und aus den lokalen Dokumentordnern kopieren und verschieben. Wenn Benutzer Dokumente bearbeiten wollen, so können Sie die Dokumente in Google Drive betrachten und Änderungen vornehmen, soweit sie in Google Drive die entsprechenden Berechtigungen haben. Die Vorgehensweise zum Einrichten des Google Drive ähnelt der Vorgehensweise bei der Integration von Dropbox 336 und MultiPOP-OAuth 145 in MDaemon.

Einbindung von Google Drive aktivieren
Diese Option aktiviert die Integration von Google Drive. Nähere Informationen hierzu finden Sie im Abschnitt **Erstellen und Verbinden Ihrer App für Google Drive** weiter unten.

API-Schlüssel für Google Drive
Dies ist die eindeutige API-Schlüssel, der Ihrer App bei der Erstellung in der Google-API-Konsole zugewiesen wurde. Nachdem Sie Ihre App erstellt haben, kopieren Sie den API-Schlüssel, und fügen Sie ihn hier ein.

Client-ID für Google Drive
Dies ist die eindeutige Client-ID, die App bei der Erstellung in der Google-API-Konsole zugewiesen wurde. Nachdem Sie Ihre App erstellt haben, kopieren Sie die Client-ID, und fügen Sie sie hier ein.

Client-Schlüssel für Google Drive
Dies ist der eindeutige Client-Schlüssel, der auch als "Client Secret" bezeichnet wird, und der Ihrer App bei der Erstellung in der Google-API-Konsole zugewiesen wurde. Nachdem Sie Ihre App erstellt haben, kopieren Sie den Client-Schlüssel, und fügen Sie ihn hier ein.

Redirect URI
Beim Erstellen Ihrer App für Google Drive müssen Sie einen Redirect-URI angeben. Dieser Redirect-URI wird auch als Weiterleitungs-URI oder Umleitungs-URI bezeichnet. Der Redirect-URI, der als Beispiel angezeigt wird, ist ein Beispiel, das aus dem SMTP-Hostnamen[184] der Standard-Domäne[181] erstellt wird. Er sollte für die Benutzer dieser Domäne bei der Anmeldung an Webmail nutzbar sein. Sie sollten auch für alle anderen MDaemon-Domänen, die Ihre Benutzer für die Anmeldung an Webmail möglicherweise verwenden, solche Redirect-URIs erstellen. Ein Beispiel hierzu: "`https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive`" würde für alle Benutzer funktionieren, die sich über die Domäne mail.example.com an Webmail anmelden. Nähere Informationen hierzu finden Sie im Abschnitt **Erstellen und Verbinden Ihrer App für Google Drive** weiter unten.

Text der Datenschutzerklärung bearbeiten
Die Integration des Google Drive erfordert, dass Sie Ihren Benutzern in regelmäßigen Abständen eine Verknüpfung zeigen, unter der sie eine genehmigte Datenschutzerklärung einsehen können. Mithilfe dieser Schaltfläche können Sie Ihre Datenschutzerklärung bearbeiten.

Erstellen und Verbinden Ihrer App für Google Drive

Sie finden nachfolgend die einzelnen Bedienschritte für die Erstellung Ihrer App für Google Drive.

Um eine Google-App zu erstellen, die Ihren Benutzern den Zugriff auf ihre Google-Drive-Benutzerkonten von der Webmail-Seite **Dokumente** aus gestattet, gehen Sie folgendermaßen vor:

1. Melden Sie sich an der MDaemon-Remoteverwaltung[350] an, und rufen Sie die Seite Google Drive auf. Sie finden diese Seite unter Hauptmenü » Webmail-Einstellungen. Aktivieren Sie dort die Option **Einbindung von Google Drive aktivieren**.
2. Wechseln Sie in einen gesonderten Browser-Tab. Melden Sie sich dort an Ihrem Google-Benutzerkonto an, und rufen Sie die Google-API-Konsole auf.
3. Falls Sie sich in der Projektliste befinden, klicken Sie auf **NEUES PROJEKT**. Falls Sie sich auf der Seite Ressourcen verwalten befinden, klicken Sie auf **(+) PROJEKT ERSTELLEN**.
4. Geben Sie einen **Projektnamen** ein, z.B. "Google Drive für MDaemon". Falls Sie die Projekt-ID ändern wollen, klicken Sie auf **BEARBEITEN**. Sie können die Projekt-ID auch unverändert lassen. **Beachte:** Die Projekt-ID kann nach der Erstellung des Projekts nicht mehr geändert werden.

5. Falls Sie über eine Organisationsressource verfügen, wählen Sie diese im Feld **Speicherort** aus. Andernfalls belassen Sie den Eintrag "Keine Organisation".
6. Nachdem das Projekt geladen wurde, klicken Sie auf **+ APIS UND DIENSTE AKTIVIEREN**.
7. Tragen Sie in das Suchfeld "Google Drive" ein, wählen Sie **Google Drive API** aus, und klicken Sie auf **Aktivieren**.
8. Klicken Sie im Navigationsbereich links im Abschnitt **APIs und Dienste** auf **Anmeldedaten**.
9. Klicken Sie am oberen Seitenrand auf **+ ANMELDEDATEN ERSTELLEN**, und wählen Sie im Dropdownmenü den Eintrag **API-Schlüssel**.
10. Kopieren Sie den Schlüssel aus dem Feld **Mein API-Schlüssel** in die Zwischenablage (hierfür steht eine Schaltfläche neben dem Eintrag zur Verfügung).
11. Wechseln Sie in den Browser-Tab, in dem die MDaemon-Remoteverwaltung angezeigt wird, und fügen Sie den API-Schlüssel in das Feld **API-Schlüssel für Google Drive** ein. Falls Sie diesen Vorgang später ausführen wollen, können Sie den API-Schlüssel auch anderweit speichern.
12. Wechseln Sie zurück in den Browser-Tab, in dem die Google-API-Konsole angezeigt wird. Klicken Sie dort im Navigationsbereich links im Abschnitt **API und Dienste** auf **OAuth-Zustimmungsbildschirm**.
13. Wählen Sie im Abschnitt Under User Type den Eintrag **Extern** aus, und klicken Sie auf **ERSTELLEN**. **Beachte:** Falls Sie über eine Organisationsressource verfügen, sowie in Abhängigkeit von dem Veröffentlichungsstatus Ihrer App, kann die Option **Intern** vorzugswürdig sein. Nähere Informationen hierzu finden Sie im Abschnitt Veröffentlichungsstatus 342 weiter unten.
14. Geben Sie den **Anwendungsnamen** ein (z.B. Google Drive für Webmail). Geben Sie eine **Nutzersupport-E-Mail** ein, an die sich die Benutzer wenden können, und geben Sie unter **Kontaktdaten des Entwicklers** eine E-Mail-Adresse ein, an die sich Google bei Änderungen an Ihrem Projekt wenden kann. Weitere Angaben müssen Sie auf dieser Seite für die Erstellung der App nicht machen. Je nach Ihrer Organisation oder Ihren Prüfvorschriften können Sie aber noch das Anwendungslogo und Verknüpfungen zu Ihren Nutzungsbedingungen 363 und der Datenschutzerklärung Ihres Unternehmens hinzufügen. Die Felder für die **Anwendungsdomänen** und die Liste autorisierter Domänen werden automatisch ausgefüllt, wenn Sie in einem späteren Schritt die *Redirect-URIs* hinzufügen. **Beachte:** Diese Informationen werden für den Zustimmungsbildschirm verwendet, den Ihre Benutzer dann angezeigt erhalten, wenn sie MultiPOP für den Zugriff auf Google Drive berechtigen.
15. Klicken Sie auf **SPEICHERN UND FORTFAHREN**.
16. Klicken Sie auf **BEREICHE HINZUFÜGEN ODER ENTFERNEN**, und kopieren Sie die nachfolgend aufgeführten URIs in das Eingabefeld im Abschnitt "Bereiche manuell hinzufügen". Sie können alle URIs gleichzeitig kopieren. Klicken Sie danach auf **ZUR TABELLE HINZUFÜGEN**.

```
https://www.googleapis.com/auth/userinfo.email
https://www.googleapis.com/auth/drive.file
https://www.googleapis.com/auth/documents
```

```
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/spreadsheets
```

17. Klicken Sie auf **SPEICHERN UND FORTFAHREN**.
18. Klicken Sie im Abschnitt Testnutzer auf **ADD USERS** (Benutzer hinzufügen), und geben Sie jedes Google-Drive-Benutzerkonto ein auf das über MDaemon zugegriffen werden soll. Klicken Sie danach auf **HINZUFÜGEN** (beachten Sie auch die Hinweise zum Veröffentlichungsstatus 342 Ihrer App weiter unten).
19. Klicken Sie auf **SPEICHERN UND FORTFAHREN**.
20. Klicken Sie im Abschnitt Fazit am Ende der Seite auf **ZURÜCK ZUM DASHBOARD**.
21. Klicken Sie im Navigationsbereich links auf **Anmeldedaten**, und klicken Sie danach auf **(+) ANMELDEDATEN ERSTELLEN**. Wählen Sie die Option **OAuth-Client-ID**.
22. Wählen Sie im Dropdownmenü "Anwendungstyp" den Eintrag **Webanwendung** aus, und klicken Sie danach im Abschnitt "Autorisierte Weiterleitungs-URIs", click **+ URI HINZUFÜGEN**. Geben Sie den Weiterleitungs-URI ein. Der Redirect-URI, der auf der Seite Google Drive als Beispiel angezeigt wird, ist ein Beispiel, das aus dem SMTP-Hostnamen 184 der Standard-Domäne 181 erstellt wird. Er sollte für die Benutzer dieser Domäne bei der Anmeldung an Webmail nutzbar sein. Sie sollten auch für alle anderen MDaemon-Domänen, die Ihre Benutzer für die Anmeldung an Webmail möglicherweise verwenden, solche Redirect-URIs erstellen. Ein Beispiel hierzu: "`https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive`" würde für alle Benutzer funktionieren, die sich über die Domäne mail.example.com an Webmail anmelden. Falls bei Ihnen beispielsweise auch eine Domäne "mail.company.test" gehostet wird, dann würde auch ein Redirect-URI für diese Domäne benötigt, also beispielsweise "`https://mail.company.test/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive`".
23. Klicken Sie auf **ERSTELLEN**.
24. Kopieren Sie die Daten aus den Feldern **Client-ID** und **Clientschlüssel** in die Felder für die Client-ID und den Client-Schlüssel in Ihrem Konfigurationsdialog Google Drive. Sie können hier auch den API-Schlüssel für Google Drive eintragen, falls Sie das zuvor nicht schon erledigt haben.

Veröffentlichungsstatus — Diese Anleitung bezieht sich auf die Erstellung einer Google-App mit dem Veröffentlichungsstatus "**Test**". Dieser Status erfordert das Hinzufügen jedes einzelnen Google-Benutzerkontos, auf dessen Google Drive von Webmail aus zugegriffen werden soll. Die Höchstgrenze sind hierbei 100 Benutzer. Wenn Ihre Benutzer in Webmail dazu aufgefordert werden, MDaemon die Berechtigung zum Zugriff auf Google Drive zu erteilen, erscheint eine

Warnmeldung. Sie fordert den Benutzer dazu auf, zu bestätigen, dass Testzugriff auf das Projekt besteht und dass die Risiken verstanden werden, die mit dem Zugriff einer ungeprüften App auf die Daten verbunden sind. Die eingeräumte Berechtigung verfällt nach sieben Tagen; alle Benutzer müssen daher einmal wöchentlich den Zugriff auf Google Drive erneut gestatten.

Um diese Einschränkungen und Anforderungen außer Kraft zu setzen, müssen Sie den Status der App auf "**In Produktion**" setzen. Sie müssen dazu unter Umständen einen Prüfprozess durchlaufen. Nähere Informationen über die Prüfung von Apps und den Veröffentlichungsstatus finden Sie in folgenden Artikeln, die Google in englischer Sprache veröffentlicht hat: Erstellen Ihres OAuth-Zustimmungsbildschirms und FAQ zur Prüfung der Authentifizierungs-API.

Berechtigung für Google Drive in Webmail erteilen

Nachdem die App für Google Drive erstellt und die Optionen auf der Seite Google Drive in MDaemon nach der vorstehenden Anleitung konfiguriert wurden, müssen alle Benutzer, die über Webmail auf ihre Google-Drive-Benutzerkonten zugreifen wollen, hierzu die entsprechende Berechtigung erteilen. Hierzu müssen die Benutzer folgendermaßen vorgehen:

1. An Webmail anmelden
2. Das Symbol **Optionen** in der oberen rechten Bildschirmecke anklicken, und danach **Cloud-Apps** anklicken.
3. **Google Drive einrichten** anklicken. Hierdurch öffnet sich eine **OAuth-2.0-Seite**.
4. **Verknüpfung mit Google Drive herstellen** anklicken.
5. Falls der Benutzer noch nicht angemeldet ist, fordert Google Drive zur Anmeldung oder zur Auswahl eines Benutzerkontos auf.
6. Es kann eine Warnmeldung angezeigt werden, dass Google die App nicht überprüft hat, und dass Zugriff auf eine App gewährt wird, die noch getestet wird, sowie dass der Vorgang nur fortgesetzt werden soll, wenn sich der Benutzer sicher ist, dass der Entwickler der App bekannt ist. Diese Warnmeldung muss mit **Fortfahren** bestätigt werden.
7. Die Leistungsmerkmale von Google Drive auswählen, die in Webmail zur Verfügung stehen sollen. Anschließend **Fortsetzen** anklicken.
8. Es erscheint ein abschließender Hinweis, dass MDaemon jetzt mit Google Drive verbunden ist. Das Fenster kann nun geschlossen werden.
9. Der Zugriff auf Google Drive über die Seite **Dokumente** in Webmail ist jetzt möglich.

Siehe auch:

MultiPOP-OAuth 145
Dropbox-Integration 336

3.6.1.9 Kategorien

In der MDaemon-Remoteverwaltung finden Sie die Optionen zu den Kategorien unter **Hauptmenü » Webmail-Einstellungen » Kategorien**.

Webmail unterstützt in den Designs LookOut und WorldClient Kategorien für E-Mail-Nachrichten. Benutzer können der Nachrichten-Übersicht die Spalte Kategorien hinzufügen. Sie müssen hierzu auf der Seite "**Optionen » Spalten**" den Eintrag "**Kategorien**" aktivieren.

Um Nachrichten den Kategorien zuzuweisen, werden zunächst die betroffenen Nachrichten in der Nachrichtenliste ausgewählt. Danach wird per Rechtsklick auf den ausgewählten Nachrichten das Kontextmenü aufgerufen, und hier werden die Kategorien ausgewählt. Sie können auch eine Nachricht öffnen und die Kategorie dann mithilfe der entsprechenden Option in der Symbolleiste zuweisen.

Kategorien

Auf der Seite Kategorien der MDaemon-Remoteverwaltung können Sie die Domänen-Kategorien konfigurieren. Die Domänen-Kategorien stellen eine vorgegebene Liste von Kategorien dar, die den Benutzern in Webmail angezeigt wird, die sie aber weder bearbeiten noch löschen können. Sie können auf dieser Seite außerdem die Liste der voreingestellten persönlichen Kategorien erstellen, die neuen Benutzern angezeigt wird.

Domänen-Kategorien

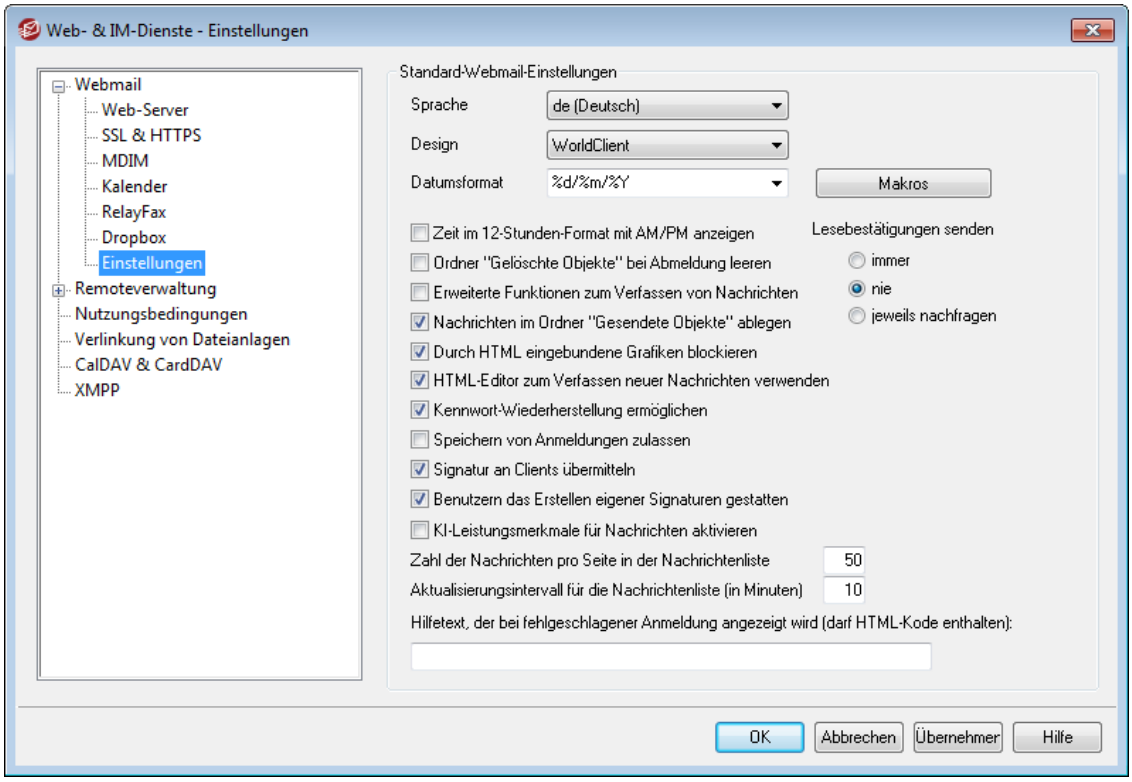
Domänen-Kategorien sind vorgegebene Kategorien, die Ihre Benutzer weder neu anordnen noch bearbeiten oder löschen können. Ist die Option *Domänen-Kategorien aktivieren* aktiv, so erscheinen diese Kategorien am Anfang der Liste der Kategorien, die Ihren Benutzern angezeigt wird. Als Administrator können Sie auf dieser Seite die Domänen-Kategorien neu anordnen, bearbeiten und löschen, und Sie können neue Domänen-Kategorien hinzufügen.

Persönliche Kategorien

In diesem Abschnitt erscheint die Liste der voreingestellten persönlichen Kategorien. Diese Liste wird in die Benutzerkonten der Webmail-Benutzer kopiert. Die Benutzer können die persönlichen Kategorien selbständig verwalten. Sie können die Kategorien neu anordnen, bearbeiten und löschen, und sie können neue Kategorien hinzufügen. Falls auf Ihrem Server auch Domänen-Kategorien aktiv sind, erscheinen diese Domänen-Kategorien aber stets am Anfang der Liste der Kategorien, und die Benutzer können die Domänen-Kategorien weder bearbeiten noch doppelt anlegen. Persönliche Kategorien, die mit Domänen-Kategorien namensgleich sind, werden ausgeblendet. Falls Sie persönliche Kategorien nicht zulassen wollen, deaktivieren Sie die Option **Benutzer dürfen persönliche Kategorien bearbeiten**. In diesem Fall werden nur die Domänen-Kategorien angezeigt. Ist auch die Option **Domänen-Kategorien aktivieren** deaktiviert, dann stehen den Benutzern die Leistungsmerkmale für Kategorien nicht zur Verfügung.

Nähere Informationen über die Dateien, in denen die Kategorien und ihre Übersetzungen verwaltet werden, finden Sie in der Datei `MDaemon\WorldClient\CustomCategories.txt`.

3.6.1.10 Einstellungen



Dieser Konfigurationsdialog legt die Standard-Einstellungen für den Konfigurationsdialog Webmail-Einstellungen 194 im Domänen-Manager fest. Diese Einstellungen bestimmen in vielen Bereichen, wie die Leistungsmerkmale durch Webmail-Benutzer nach ihrer Anmeldung an Webmail zunächst genutzt werden können. Die Benutzer selbst können über die Seiten im Menü Optionen in Webmail viele dieser Einstellungen an ihre Wünsche und Anforderungen anpassen.

Standard-Webmail-Einstellungen

Sprache
Durch Auswahl aus diesem Rollmenü wird die Sprache festgelegt, in der die Benutzeroberfläche von Webmail bei der ersten Anmeldung eines Benutzers an der ausgewählten Domäne erscheint. Die Benutzer können dann ihre bevorzugte Sprache über die Einstellungen von Webmail selbst auswählen.

Design
Aus diesem Rollmenü wird das Standard-Design ausgewählt, das Webmail bei der ersten Anmeldung eines Benutzers anzeigt. Die Benutzer können dann das von ihnen bevorzugte Design über die Einstellungen von Webmail auf der Seite Optionen » Benutzeranpassung selbst auswählen.

Datumsformat
Dieses Textfeld definiert das Datumsformat für die Benutzer von Webmail. Über das Steuerelement *Makros* wird eine Liste aller Makros angezeigt, die in diesem Textfeld zulässig sind. Nachfolgend sind alle diese Makros aufgeführt:

%A — Name des Wochentags

%B — Name des Monats

%d — Tag (wird als "01-31" angezeigt)

%m — Monat (wird als "01-12" angezeigt)

%y — Jahreszahl zweistellig

%Y — Jahreszahl vierstellig

In Webmail wird so beispielsweise "`%Y-%m-%d`" in die Datumsanzeige "`2011-12-15`" umgesetzt.

Makros
Ein Klick auf dieses Steuerelement zeigt ein Hilfefenster mit allen Makros an, die für das oben beschriebene Feld *Datumsformat* zulässig sind.

Lesebestätigungen senden
Diese Option bestimmt das Verhalten von Webmail in den Fällen, in denen eingehende Nachrichten eine Anforderung nach einer Lesebestätigung enthalten.

immer
Diese Option bewirkt, dass MDaemon dem Absender eine Bestätigung darüber sendet, dass die Nachricht gelesen wurde. Der Webmail-Benutzer, der die Nachricht erhalten hat, erhält dabei keine Information darüber, dass eine Lesebestätigung verlangt oder versandt wurde.

nie
Diese Option bewirkt, dass Webmail die Anforderungen nach Lesebestätigungen ignoriert.

jeweils nachfragen
Diese Option bewirkt, dass der Webmail-Benutzer jeweils gefragt wird, ob er eine Lesebestätigung versenden will. Die Abfrage erscheint, wenn der Benutzer eine Nachricht öffnet, die eine Anforderung nach einer Lesebestätigung enthält.

Zeit im 12-Stunden-Format mit AM/PM anzeigen
Diese Option bewirkt, dass die Uhrzeit in Webmail im 12-Stunden-Format mit den Zusätzen AM und PM angezeigt wird. So lange diese Option nicht aktiv ist, zeigt Webmail die Zeit im 24-Stunden-Format an. Die Benutzer können diese Einstellung über die Option "*Uhrzeit im 12-Stunden-Format mit AM/PM anzeigen*" auf der Seite Optionen » Kalender in Webmail selbst ändern.

Ordner "Gelöschte Objekte" bei Abmeldung leeren
Diese Option bewirkt, dass der Ordner *Gelöschte Objekte* eines Benutzers bei dessen Abmeldung aus Webmail geleert wird. Die Benutzer können diese Einstellung über die Einstellungen von Webmail selbst ändern.

Erweiterte Funktionen zum Verfassen von Nachrichten
Mit dieser Einstellung stehen den Benutzern beim Verfassen neuer Nachrichten erweiterte Möglichkeiten zur Verfügung. So lange diese Funktion nicht aktiv ist, wird lediglich das normale Fenster zum Verfassen neuer Nachrichten geöffnet. Die Benutzer können diese Einstellung über die Seite Optionen » E-Mail verfassen in Webmail selbst ändern.

Nachrichten im Ordner "Gesendete Objekte" ablegen
Diese Option bewirkt, dass eine Kopie jeder gesendeten Nachricht in dem Ordner *Gesendete Objekte* des jeweiligen Benutzerkontos abgelegt wird. Die Benutzer

können diese Einstellung über die Seite Optionen » E-Mail verfassen in WorldClient selbst ändern.

Durch HTML eingebundene Grafiken blockieren
Diese Option verhindert, dass Grafikdateien, die in E-Mail-Nachrichten im HTML-Format eingebunden sind und auf externen Servern liegen, in Webmail automatisch angezeigt werden. Will der Benutzer diese Grafiken sehen, so muss er eine Informationsleiste anklicken, die im Browserfenster oberhalb der Nachricht erscheint. Diese Funktion dient der Verhinderung von Spam-Nachrichten, da viele Spam-Nachrichten Grafiken mit besonderen URLs enthalten, die die E-Mail-Adresse des Benutzers, der die Nachricht betrachtet, identifizieren. Wird eine solche Grafik von dem externen Server abgerufen, so erhält der Spammer hierdurch die Bestätigung, dass die zugehörige E-Mail-Adresse gültig ist und gelesen wird. Die Option ist per Voreinstellung aktiv.

Nachrichten in neuem Browserfenster verfassen
Diese Option bewirkt, dass zum Verfassen von Nachrichten ein neues Browserfenster geöffnet wird, und dass die Editorfunktionen nicht im Hauptfenster dargestellt werden. Falls Sie nicht wünschen, dass ein gesondertes Fenster geöffnet wird, deaktivieren Sie diese Option. Die Benutzer können diese Einstellung über die Einstellungen zum Verfassen neuer Nachrichten in Webmail selbst ändern.

HTML-Editor zum Verfassen neuer Nachrichten verwenden
Diese Option erlaubt es den Benutzern, Nachrichten im Rich-Text-Format (HTML) zu verfassen. Die Benutzer können diese Einstellung über die Seite Optionen » E-Mail verfassen in Webmail selbst ändern.

Kennwort-Wiederherstellung ermöglichen
Diese Option ermöglicht solchen Benutzer der Domäne die Kennwort-Wiederherstellung, die über die Berechtigung zum Bearbeiten ihres Kennworts 720 verfügen. Diese Benutzer können in Webmail eine alternative E-Mail-Adresse hinterlegen und sich an diese E-Mail-Adresse eine Verknüpfung zum Zurücksetzen ihres Kennworts senden lassen, falls sie ihr Kennwort einmal vergessen sollten. Um dieses Leistungsmerkmal einzurichten, müssen die berechtigen Benutzer im Konfigurationsdialog Optionen » Sicherheit in Webmail die alternative E-Mail-Adresse und ihr Kennwort angeben. Benutzern, die sich danach mit einem falschen Kennwort an Webmail anzumelden versuchen, wird die Verknüpfung "Haben Sie Ihr Kennwort vergessen?" angezeigt. Nach Anklicken dieser Verknüpfung werden sie aufgefordert, die alternative E-Mail-Adresse für die Kennwort-Wiederherstellung einzugeben, die sie zuvor in Webmail eingetragen haben. Geben sie die Adresse richtig ein, so sendet Webmail an die Adresse eine Nachricht mit einer Verknüpfung zu der Seite, auf der die Benutzer ein neues Kennwort festlegen können. Dieses Leistungsmerkmal ist per Voreinstellung abgeschaltet.

Sie können dieses Leistungsmerkmal nach Benutzern getrennt aktivieren. Hierzu bearbeiten Sie den folgenden Eintrag in der Datei `User.ini` für die betroffenen Benutzer (z.B. `\Users\example.com\frank\WC\user.ini`):

```
[User]
EnablePasswordRecovery=Yes (Ja, oder "=No", Nein, um dieses
Leistungsmerkmal für den gerade bearbeiteten Benutzer zu
deaktivieren.)
```

Speichern von Anmeldungen bei Zwei-Faktor-Authentifizierung zulassen (auch für Remoteverwaltung)
Wird bei einer Anmeldung an Webmail oder an der Remoteverwaltung die Zwei-Faktor-Authentifizierung genutzt, so erscheint per Voreinstellung eine Option zum Speichern der Anmeldung auf der Abfrageseite für die Zwei-Faktor-Authentifizierung. Aktiviert der Benutzer diese Option, so wird für eine gewisse Zeit (siehe hierzu "*Speichern von Anmeldungen zulassen*" weiter unten) der zweite Faktor bei der Anmeldung nicht mehr abgefragt. Falls Sie diese Speicherung der Anmeldung nicht zulassen und stattdessen die Abfrage des zweiten Faktors bei jeder Anmeldung erzwingen wollen, deaktivieren Sie diese Option. **Beachte:** Diese Option steht nur in der Webschnittstelle der MDaemon-Remoteverwaltung (MDRA) 350 zur Verfügung.

Speichern von Anmeldungen zulassen
Diese Option ermöglicht es den Webmail-Benutzer, ihre Anmeldung für eine bestimmte Zeit zu speichern. Ist sie aktiv, und stellen die Benutzer eine Verbindung über den https 327-Port her, so erscheint auf der Anmeldeseite von MDaemon Webmail die Option *Anmeldung beibehalten*. Aktivieren die Benutzer diese Option vor der Anmeldung, dann wird ihre Anmeldung auf dem gerade genutzten Endgerät gespeichert. Rufen die Benutzer danach Webmail erneut von demselben Endgerät aus auf, so werden sie automatisch angemeldet und müssen Benutzernamen und Kennwort nicht eingeben. Diese Anmeldung wird beibehalten, bis sie sich manuell von Webmail abmelden oder der Token für die Speicherung der Anmeldung verfällt.

Per Voreinstellung werden Anmeldungen für 30 Tage gespeichert, und danach müssen sich die Benutzer erneut anmelden. Sie können diesen Zeitraum mithilfe der Option *Speichern von Anmeldungen zurücksetzen* auf der Webschnittstelle der MDaemon-Remoteverwaltung 350 verlängern. Sie können den Zeitraum auch ändern durch Bearbeiten des Eintrags `RememberUserExpiration=30` key im Abschnitt `[Default:Settings]` der Datei `Domains.ini`. Sie finden diese Datei im Verzeichnis `\MDaemon\WorldClient\`. Sie können den Zeitraum auf höchstens 365 Tage setzen. **Beachte**: Für die Zwei-Faktor-Authentifizierung 720 besteht eine eigene Einstellung. Sie finden diese Einstellung, den Eintrag `TwoFactorAuthRememberUserExpiration=30`, im Abschnitt `[Default:Settings]` der Datei `Domains.ini`. Sie finden diese Datei im Verzeichnis `\MDaemon\WorldClient\`. Sobald der Zeitraum für die Zwei-Faktor-Authentifizierung abgelaufen ist, müssen sich die Benutzer erneut mithilfe der Zwei-Faktor-Authentifizierung anmelden, und zwar auch dann, wenn die Speicherdauer für die Anmeldung zu diesem Zeitpunkt noch nicht abgelaufen ist.

Die Option *Speichern von Anmeldungen zulassen* ist per Voreinstellung abgeschaltet. Sie wirkt auf alle Ihre Domänen. Falls Sie diese Einstellung für einzelne Domänen abweichend konfigurieren wollen, können Sie hierzu im Abschnitt Webmail 194 des Domänen-Managers auf der Desktop-Benutzeroberfläche von MDaemon die Einstellung *Speichern von Anmeldungen zulassen* für die betreffenden Domänen konfigurieren.

Die Funktion *Anmeldung beibehalten* ermöglicht es Benutzern, die Anmeldung auch auf mehreren Endgeräten zu speichern. Insbesondere aus diesem Grund sollten die Benutzer angewiesen werden, diese Funktion nicht in öffentlichen Netzen zu nutzen. Darüber hinaus steht in der MDaemon-Remoteverwaltung die Funktion *Speichern von*

Anmeldungen zurücksetzen zur Verfügung, mit deren Hilfe Sie, beispielsweise bei Verdacht auf unerlaubte Zugriffe, die gespeicherten Anmeldungen aller Benutzer zurücksetzen können, damit sich die Benutzer erneut anmelden müssen.

Signatur an Clients übermitteln
Diese Option bewirkt, dass die Standard-Client-Signatur 140 an die Webmail-Benutzer übermittelt werden. In Webmail wird hierdurch eine Signature mit dem Namen "System" erstellt. Sie ist über die Seite **Optionen » E-Mail verfassen** erreichbar. Die Benutzer können diese Signaturen automatisch in Entwürfe für neue Nachrichten übernehmen lassen. Falls Sie die Client-Signatur für einzelne Domänen getrennt anpassen oder aktivieren und deaktivieren wollen, können Sie hierzu die Optionen in den Abschnitten Client-Signaturen 206 und Webmail 194 des Domänen-Managers verwenden.

Benutzern das Erstellen eigener Signaturen gestatten
Diese Option gestattet es Ihren Benutzern, eigene benutzerdefinierte Signaturen in Webmail zu erstellen. Die Benutzer können dann entscheiden, welche Signatur beim Verfassen von Nachrichten automatisch in den Entwurf übernommen werden soll. Falls Sie benutzerdefinierte Signaturen nicht zulassen, aber die Option *Signatur an Clients übermitteln* oben aktiv ist, können die Benutzer nur die dadurch vorgegebene Client-Signatur 140 (in Webmail die Signatur "System") automatisch in die Entwürfe für neue Nachrichten einfügen lassen. Die Optionen für die Signaturen sind in Webmail erreichbar über **Optionen » E-Mail verfassen**.

Benutzern das Bearbeiten der Anzeigenamen für ihre Aliasnamen gestatten
Diese Option gestattet es Ihren Benutzern, die Anzeigenamen aller Aliasnamen zu bearbeiten, die mit ihren Benutzerkonten verbunden sind. Um die Aliasnamen zu bearbeiten, müssen die Benutzer im Webmail-Design Pro im Abschnitt Einstellungen » E-Mail verfassen die Option *Anzeigenamen für Aliasnamen bearbeiten* aufrufen. Diese Option ist per Voreinstellung abgeschaltet. **Beachte:** Diese Option steht nur in der Webschnittstelle der MDaemon-Remoteverwaltung (MDRA) 350 zur Verfügung.

Zahl der Nachrichten pro Seite in der Nachrichtenliste
Diese Option steuert, wie viele Nachrichten auf jeder Seite der Nachrichtenliste für die einzelnen Nachrichten-Ordner erscheinen. Enthält ein Ordner mehr Nachrichten, als hier angegeben sind, so erscheinen über und unter der Nachrichtenliste Steuerelemente, mit denen der Benutzer die nun mehrseitige Nachrichtenliste durchblättern kann. Die Benutzer können diese Einstellung in Webmail selbst ändern.

Aktualisierungsintervall für die Nachrichtenliste (in Minuten)
Hier wird der Zeitabstand in Minuten festgelegt, nach dem Webmail die Nachrichtenliste automatisch aktualisiert. Die Benutzer können diese Einstellung auf der Seite Optionen » Benutzeranpassung in Webmail selbst ändern.

Hilfetext, der bei fehlgeschlagener Anmeldung angezeigt wird (darf HTML-Kode enthalten)
In diesem Textfeld können Sie einen Text (entweder als reinen Text oder im HTML-Format) angeben, den Webmail im Anmeldedialog anzeigt, falls bei der Anmeldung eines Benutzers ein Fehler auftritt. Der Text erscheint unter dem

folgenden Text: *"Ihre Anmeldedaten sind ungültig. Bitte versuchen Sie es erneut. Falls Sie Unterstützung benötigen, wenden Sie sich bitte an den Administrator Ihres E-Mail-Systems."*. Sie können in diesem Text Ihren Benutzern beispielsweise eine Verknüpfung zu einer anderen Seite anbieten oder Kontaktdaten für eine Stelle anzeigen, an die sich die Benutzer im Fall von Fehlern bei der Anmeldung an WorldClient wenden können.

Anpassung der Ordner für freigegebene und gesperrte Absender

Sie können verschiedene Leistungsmerkmale in Webmail anpassen, indem Sie bestimmte Dateien im Verzeichnis `MDaemon\WorldClient\` bearbeiten:

Sie können die Ordner für freigegebene und gesperrte Absender per Voreinstellung vor den Benutzern von Webmail verbergen. Hierzu öffnen Sie die Datei `MDaemon\WorldClient\Domains.ini`, und ändern Sie im Abschnitt `[Default:UserDefaults]` die Einträge "`HideWhiteListFolder=`" oder "`HideBlackListFolder=`" von "`No`" in "`Yes`". Sie können diese Ordner auch vor einzelnen Benutzern verbergen, indem Sie die gleich lautenden Einträge im Abschnitt `[User]` der Dateien `User.ini` für die betroffenen Benutzer bearbeiten.

Siehe auch:

Domänen-Manager » Webmail-Einstellungen 194

3.6.1.11 Branding

Mithilfe der Optionen auf der Seite Branding der Remoteverwaltung 350 von MDaemon können Sie die Grafiken konfigurieren, die auf der Anmeldeseite und oberhalb der Navigationsleiste von Webmail erscheinen.

Um die voreingestellten Grafiken durch Ihre eigenen, benutzerdefinierten Grafiken zu ersetzen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Seite Anpassung auf **Benutzerdefinierte Grafiken nutzen**.
2. Wählen Sie im Abschnitt Auswahl der Grafik für den Anmeldedialog je nach dem verwendeten Browser die Option **Datei auswählen** oder **Durchsuchen,** und wählen Sie dann die Datei aus, die Sie hochladen wollen. In diesem Abschnitt wird auch die Standard-Größe für die Grafik für den Anmeldedialog angezeigt.
3. Klicken Sie auf **Benutzerdefinierte Grafik hochladen**.
4. Wiederholen Sie die Schritte 2 und 3, um eine Grafik für die Navigationsleiste und den invertierten Navigationsbereich hochzuladen.

Nach dem Hochladen der Grafikdateien erscheinen sie an den jeweils vorgesehenen Stellen anstelle der mit Webmail ausgelieferten Standard-Grafikdateien.

3.6.2 Remoteverwaltung

Die Remoteverwaltung von MDaemon ist eine Webschnittstelle, die Ihnen die Fernwartung von MDaemon mithilfe eines Webbrowsers gestattet. Die Remoteverwaltung ist als Serveranwendung dafür ausgelegt, auf demselben Rechner im Hintergrund ausgeführt zu werden, auf dem auch MDaemon installiert ist. Der Zugriff auf die Remoteverwaltung ist durch einen Webbrowser möglich, indem dort

der URL und die Portnummer eingegeben werden, die der Remoteverwaltung zugewiesen sind (z.B. `www.example.com:1000`). Nach der Benutzeranmeldung erhält der Benutzer Zugriff auf die verschiedenen Einstellungen von MDaemon. Art und Umfang der Einstellungen, auf die der Benutzer Zugriff erhält, richten sich nach seiner Zugriffsberechtigung. Es sind drei Zugriffsberechtigungen zu unterscheiden, die einem Benutzer in der Remoteverwaltung zugewiesen werden können: Global, Domäne und Benutzer.

Globale Administratoren — Die Einstellungen für diese Benutzer in MDaemon sehen den globalen Zugriff vor. Global bedeutet dabei, dass diese Benutzer jede beliebige Einstellung und Funktion von MDaemon, die über die Remoteverwaltung zugänglich ist, einsehen und bearbeiten können. Globale Administratoren können Benutzer, Domänen und Mailinglisten hinzufügen, bearbeiten und löschen. Sie können die INI-Dateien eines Programms bearbeiten, Kennwörter verwalten und viele weitere Funktionen nutzen; sie haben den uneingeschränkten Zugriff als Systemverwalter.

Domänen-Administratoren — Sie sind den Globalen Administratoren vergleichbar und haben ebenfalls Zugriff auf Benutzer und Einstellungen, die mithilfe der Remoteverwaltung zugänglich sind. Die Administratorrechte der Domänen-Administratoren sind aber auf die Domäne oder Domänen beschränkt, für die sie die Rechte von Domänen-Administratoren erhalten haben. Sie sind außerdem auf die Rechte beschränkt, den Benutzerkonten der Domänen-Administratoren im Abschnitt Web-Dienste 720 zugewiesen sind. Domänen-Administratoren erhalten ihre Administratorrechte und die Zuweisung zu den Domänen, für die sie diese Rechte haben, über die Remoteverwaltung entweder durch einen Globalen Administrator oder durch einen anderen Domänen-Administrator mit Administratorrechten für die betroffenen Domänen.

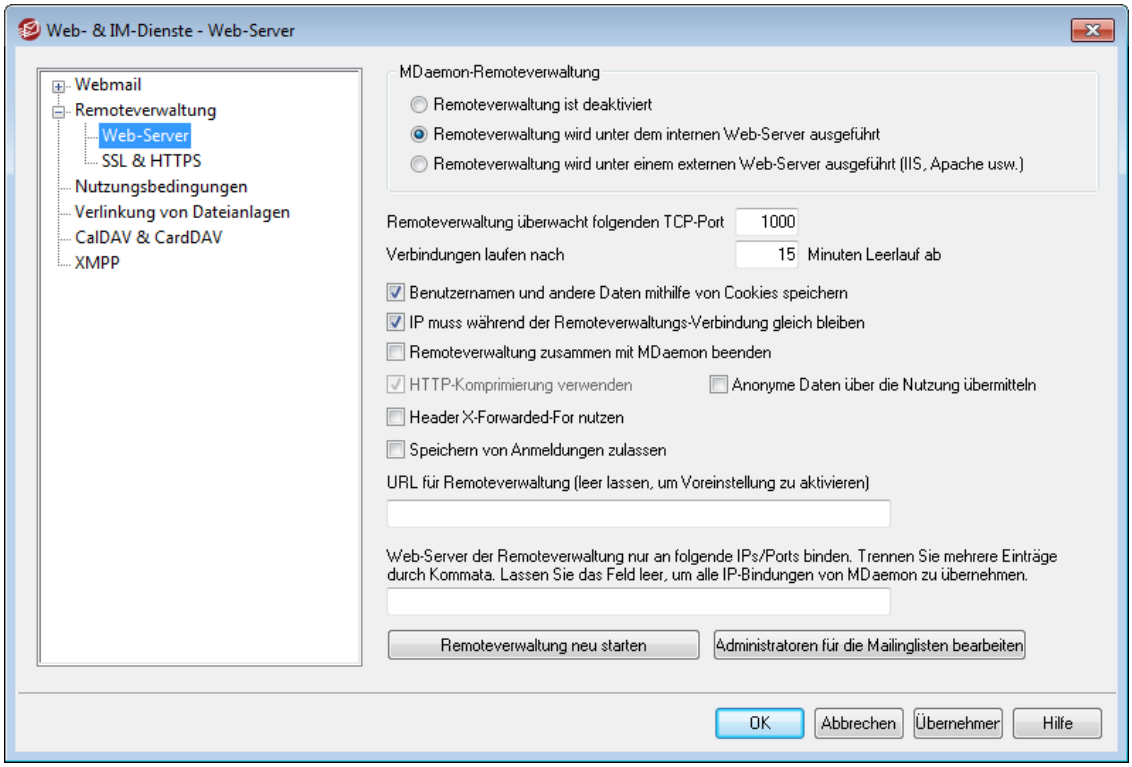
Benutzer — Diese Berechtigungsstufe ist die am meisten eingeschränkte. Sie erlaubt es normalen MDaemon-Benutzern beispielsweise, sich bei der Remoteverwaltung anzumelden und die Einstellungen ihres eigenen Benutzerkontos einzusehen. Außerdem können sie dann ihre MultiPOP-Einträge, Nachrichten-Filter, Autobeantworter und anderes bearbeiten. Die Art und Anzahl der Einstellungen, die ein Benutzer selbst bearbeiten darf, hängt von der Berechtigung ab, die jedem einzelnen Benutzer durch den Benutzerkonten-Manager in MDaemon erteilt werden kann.

Benutzer mit Zugriffsrechten sowohl für Webmail als auch für die Remoteverwaltung können die Remoteverwaltung aus Webmail heraus aufrufen. Wird im dem Menü "Optionen" der Menüpunkt "Erweiterte Einstellungen" ausgewählt, so öffnet sich die Remoteverwaltung in einem neuen Browserfenster.

Siehe auch:

Remoteverwaltung » Web-Server 352
Remoteverwaltung » HTTPS 355
Vorlagen-Manager » Web-Dienste 795
Benutzerkonten-Editor » Web-Dienste 720
Die Einbindung der Remoteverwaltung in die IIS 359

3.6.2.1 Web-Server



MDaemon-Remoteverwaltung

Remoteverwaltung ist deaktiviert
Mit dieser Option wird die Remoteverwaltung abgeschaltet. Die Remoteverwaltung lässt sich auch über das Menü Datei sowie über den rechten Abschnitt im Bereich Statistik der Benutzeroberfläche von MDaemon aktivieren und deaktivieren.

Remoteverwaltung wird unter dem internen Web-Server ausgeführt
Diese Option bewirkt, dass die Remoteverwaltung unter dem MDaemon-eigenen Web-Server ausgeführt wird. Die Remoteverwaltung lässt sich auch über das Menü Datei sowie über den rechten Abschnitt im Bereich Statistik der Benutzeroberfläche von MDaemon aktivieren und deaktivieren.

Remoteverwaltung wird unter einem externen Web-Server ausgeführt (IIS, Apache usw.)
Diese Option muss aktiv sein, falls die Remoteverwaltung unter den Internet Information Services (IIS) oder einem sonstigen Web-Server ausgeführt werden, der MDaemon-eigene Web-Server hingegen nicht verwendet werden soll. So lange diese Option aktiv ist, sind bestimmte Menüpunkte in der Benutzeroberfläche nicht zugänglich. Diese gesperrten Menüpunkte beeinflussen Einstellungen, die den Betrieb des externen Web-Servers stören können.

Weitere Informationen hierzu finden Sie unter Einbindung der Remoteverwaltung in IIS 359.

Remoteverwaltung überwacht folgenden TCP-Port
Auf dieser Portnummer beantwortet die Remoteverwaltung ankommende Verbindungsversuche.

Verbindungen laufen nach [xx] Minuten Leerlauf ab
Wenn ein Benutzer bei der Remoteverwaltung angemeldet ist, wird die Verbindung nach der hier angegebenen Leerlaufdauer durch die Remoteverwaltung getrennt. Die Voreinstellung beträgt 15 Minuten.

Verschiedene Einstellungen

Benutzernamen und andere Daten mithilfe von Cookies speichern
Per Voreinstellung nutzt die Benutzeroberfläche der Remoteverwaltung Cookies, sodass die Browser der Benutzer die Benutzernamen und weitere Parameter für die Anmeldungen speichern können. Falls Sie die Nutzung von Cookies nicht zulassen wollen, deaktivieren Sie diese Option. Diese Option passt die Anmeldung besser an die Bedürfnisse der Benutzer an; sie funktioniert aber nur, wenn die Benutzer in ihren Browsern Cookies zulassen.

IP muss während der Remoteverwaltungs-Verbindung gleich bleiben
Dies ist eine zusätzliche Sicherheitsmaßnahme. Die Einstellung bewirkt, dass eine Verbindung mit der Remoteverwaltung mit einem bestimmten Benutzer auf genau die IP-Adresse beschränkt wird, die dem Benutzer bei Verbindungsaufbau zugewiesen war. Eine Verbindung mit der Remoteverwaltung kann somit nicht mehr durch einen Unbefugten "übernommen" werden, da sich dann die IP-Adresse der Gegenstelle ändern würde. Diese Betriebsart erhöht die Sicherheit beträchtlich, kann aber zu Problemen führen, wenn der Benutzer einen Proxy-Server verwendet oder die Internetverbindung über einen Zugang mit dynamischer Adresszuweisung herstellt, der die IP-Adressen dynamisch zuweist und nach Verbindungsabbrüchen ändert.

Remoteverwaltung zusammen mit MDaemon beenden
Diese Option bewirkt, dass die Remoteverwaltung beendet wird, sobald MDaemon beendet wird. Ist diese Option abgeschaltet, so wird die Remoteverwaltung auch nach Beendigung von MDaemon im Hintergrund ausgeführt.

HTTP-Komprimierung verwenden
Diese Option bewirkt, dass in den Verbindungen mit der Remoteverwaltung die HTTP-Komprimierung verwendet wird.

Anonyme Daten über die Nutzung übermitteln
Der Webclient der MDaemon-Remoteverwaltung übermittelt per Voreinstellung anonyme und unkritische Daten über die Nutzung. Hierzu gehören das genutzte Betriebssystem, die genutzte Browser-Version und vergleichbare Daten. Die Daten werden durch die MDaemon Technologies Ltd. genutzt, um die Remoteverwaltung zu verbessern. Falls Sie die Übermittlung dieser anonymen Daten über die Nutzung unterbinden wollen, deaktivieren Sie diese Option.

Header X-Forwarded-For nutzen
Diese Option ermöglicht die Nutzung des Headers `X-Forwarded-For`. Dieser Header wird bisweilen durch Proxy-Server hinzugefügt. Diese Option ist per Voreinstellung abgeschaltet. Aktivieren Sie diese Option nur, falls Ihr Proxy-Server diesen Header hinzufügt.

Speichern von Anmeldungen zulassen
Diese Option ermöglicht es den Benutzern der MDaemon-Remoteverwaltung, ihre Anmeldungen für eine bestimmte Zeit zu speichern. Ist sie aktiv, und stellen die Benutzer eine Verbindung über den https 355-Port her, so erscheint auf der Anmeldeseite der MDaemon-Remoteverwaltung die Option *Anmeldung*

beibehalten. Aktivieren die Benutzer diese Option vor der Anmeldung, dann wird ihre Anmeldung auf dem gerade genutzten Endgerät gespeichert. Rufen die Benutzer danach die Remoteverwaltung erneut von demselben Endgerät aus auf, so werden sie automatisch angemeldet und müssen Benutzernamen und Kennwort nicht eingeben. Diese Anmeldung wird beibehalten, bis sie sich manuell von der Remoteverwaltung abmelden oder der Token für die Speicherung der Anmeldung verfällt. Per Voreinstellung werden Anmeldungen für 30 Tage gespeichert, und danach müssen sich die Benutzer erneut anmelden. Falls Sie diesen Zeitraum verlängern wollen, können sie hierzu in der Webschnittstelle der MDaemon-Remoteverwaltung die Option *Token für gespeicherte Anmeldungen laufen nach folgender Anzahl Tagen ab* verwenden.

Sie können den Zeitraum auch ändern, indem Sie im Abschnitt `[Default:Settings]` der Datei `Domains.ini` den Eintrag `RememberUserExpiration=30` bearbeiten. Sie finden die Datei im Verzeichnis `\MDaemon\WorldClient\` folder. Sie können den Zeitraum auf höchstens 365 Tage setzen. **Beachte**: Für die Zwei-Faktor-Authentifizierung 720 besteht eine eigene Einstellung. Sie finden diese Einstellung, den Eintrag `TwoFactorAuthRememberUserExpiration=30`, im Abschnitt `[Default:Settings]` der Datei `Domains.ini`. Sie finden diese Datei im Verzeichnis `\MDaemon\WorldClient\`. Sobald der Zeitraum für die Zwei-Faktor-Authentifizierung abgelaufen ist, müssen sich die Benutzer erneut mithilfe der Zwei-Faktor-Authentifizierung anmelden, und zwar auch dann, wenn die Speicherdauer für die Anmeldung zu diesem Zeitpunkt noch nicht abgelaufen ist.

Die Option *Speichern von Anmeldungen zulassen* ist per Voreinstellung abgeschaltet.

Die Funktion *Anmeldung beibehalten* ermöglicht es Benutzern, die Anmeldung auch auf mehreren Endgeräten zu speichern. Insbesondere aus diesem Grund sollten die Benutzer angewiesen werden, diese Funktion nicht in öffentlichen Netzen zu nutzen. Darüber hinaus steht in der MDaemon-Remoteverwaltung die Funktion *Speichern von Anmeldungen zurücksetzen* zur Verfügung, mit deren Hilfe Sie, beispielsweise bei Verdacht auf unerlaubte Zugriffe, die gespeicherten Anmeldungen aller Benutzer zurücksetzen können, damit sich die Benutzer erneut anmelden müssen.

URL für Remoteverwaltung
Der Menüpunkt Erweiterte Einstellungen in Webmail, mit dessen Hilfe entsprechend berechtigte Benutzer ihre Konten-Einstellungen bearbeiten können, verweist auf den hier angegebenen URL. Dieses Feld bleibt leer, wenn die Remoteverwaltung unter dem MDaemon-eigenen Web-Server ausgeführt wird. Der URL für die Remoteverwaltung muss bei Nutzung eines anderen Web-Servers, wie etwa der IIS, und in Fällen, in denen die Remoteverwaltung über einen anderen URL oder eine andere IP-Adresse zugänglich ist, in dieses Feld eingetragen werden.

Web-Server der Remoteverwaltung nur an folgende IPs binden
Soll der Serverdienst der Remoteverwaltung nur bestimmte IP-Adressen bedienen, so sind diese Adressen durch Kommata getrennt hier einzutragen. Solange das Feld leer bleibt, spricht die Remoteverwaltung auf ankommende Verbindungen auf allen IP-Adressen an, die den Domänen 181 zugewiesen sind.

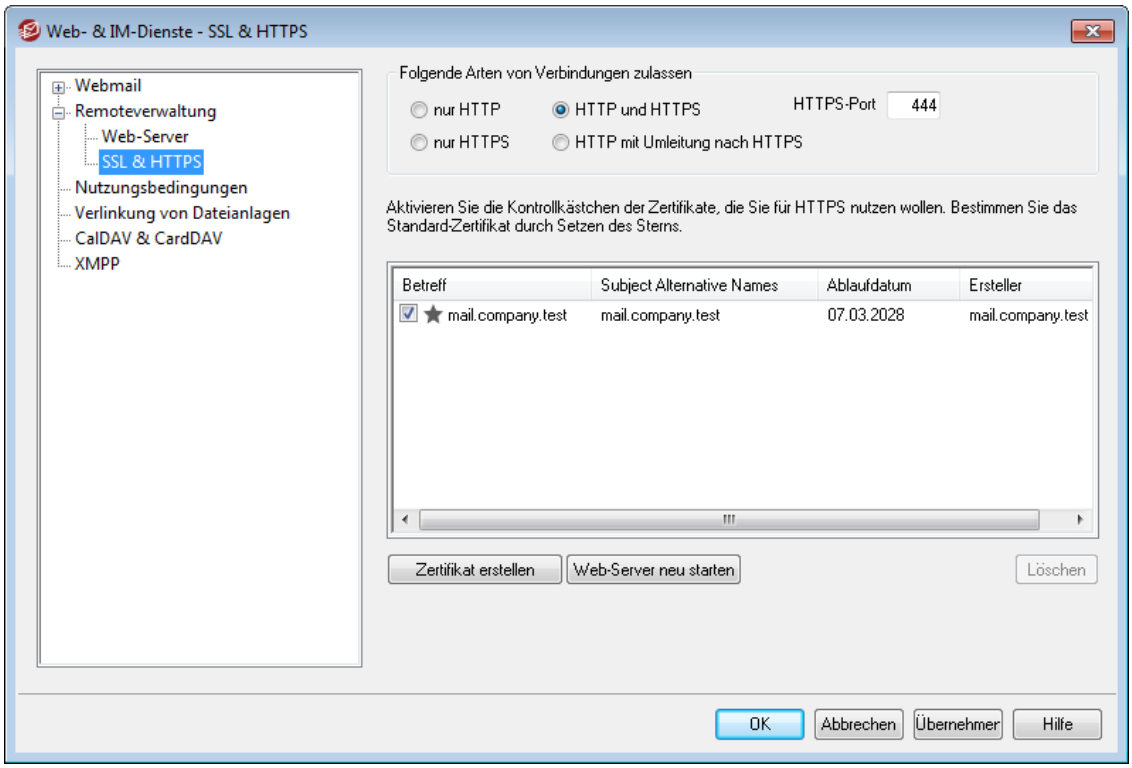
Remoteverwaltung neu starten (erforderlich nach Änderungen an Port- oder IIS-Einstellung)
Ein Klick auf dieses Steuerelement startet den Serverdienst der Remoteverwaltung neu. Beachte: Dieser Neustart ist nach einer Änderung der Portnummer für die Remoteverwaltung nötig, damit die Remoteverwaltung die neue Portnummer übernimmt.

Administratoren für die Mailinglisten bearbeiten
Um die Datendatei mit den Administratoren der Mailinglisten in einem Texteditor zu öffnen und nötigenfalls zu bearbeiten, klicken Sie auf dieses Steuerelement.

Siehe auch:

Remoteverwaltung 350
Remoteverwaltung » HTTPS 355
Die Einbindung der Remoteverwaltung in die IIS 359
Vorlagen-Manager » Web-Dienste 795
Benutzerkonten-Editor » Web-Dienste 720

3.6.2.2 SSL & HTTPS



Der MDaemon-eigene Web-Server unterstützt das Secure-Sockets-Layer-Protokoll (SSL). SSL ist das Standardverfahren für die Sicherung webgestützter Kommunikation zwischen Server und Client. Es stellt Funktionen für die Echtheitsbestätigung des Servers, Datenverschlüsselung und zusätzliche Echtheitsbestätigung für den Client einer TCP/IP-Verbindung zur Verfügung. Da auch alle wichtigen Browser HTTPS (HTTP über SSL) unterstützen, genügt es, ein gültiges digitales Zertifikat auf dem Server zu installieren, damit beim Verbindungsaufbau eines Clients die SSL-Funktionen automatisch genutzt werden.

Die Einstellungen zu den HTTPS-Funktionen von WorldClient befinden sich im Menü SSL & HTTPS, das über Einstellungen » Web- & IM-Dienste » Remoteverwaltung erreichbar ist. Um die Bedienung zu vereinfachen, sind diese Einstellungen auch in dem Konfigurationsdialog "Sicherheit » Sicherheits-Einstellungen » SSL & TLS » Remoteverwaltung" gespiegelt.

Nähere Informationen über das SSL-Protokoll und die Zertifikate finden Sie unter **SSL & TLS** 577.

Diese Einstellungen wirken auf die Remoteverwaltung nur dann, wenn der MDaemon-eigene Web-Server verwendet wird. Ist die Remoteverwaltung stattdessen in die IIS oder einen anderen Web-Server eingebunden, so bleiben diese Einstellungen wirkungslos. Die Unterstützung für SSL und HTTPS muss in diesem Fall über den verwendeten Web-Server mithilfe seiner Verwaltungswerkzeuge konfiguriert werden.

Folgende Arten von Verbindungen zulassen

nur HTTP
Soll die Remoteverwaltung keine HTTPS-Verbindungen annehmen, so muss diese Option aktiv sein. Es sind dann nur HTTP-Verbindungen zulässig.

HTTP und HTTPS
Diese Option bewirkt, dass die Remoteverwaltung zwar SSL unterstützt, die Benutzer der Remoteverwaltung jedoch HTTPS nicht zwingend verwenden müssen. Die Remoteverwaltung überwacht den weiter unten konfigurierten HTTPS-Port auf eingehende Verbindungen, lässt jedoch auch normale HTTP-Verbindungen auf dem Remoteverwaltungs-Port zu, der im Konfigurationsdialog Web-Server 352 in der Konfiguration der Remoteverwaltung definiert ist.

nur HTTPS
Diese Option bewirkt, dass Verbindungen zur Remoteverwaltung ausschließlich über HTTPS hergestellt werden können. Die Remoteverwaltung reagiert nur noch auf HTTPS-Verbindungen, nicht aber auf HTTP-Verbindungen, so lange diese Option aktiv ist.

HTTP mit Umleitung nach HTTPS
Diese Option bewirkt, dass HTTP-Verbindungen auf den HTTPS-Port umgeleitet und dann als HTTPS-Verbindungen weiter geführt werden.

HTTPS-Port
Hier wird der TCP-Port eingetragen, den die Remoteverwaltung auf eingehende SSL-Verbindungen überwachen soll. Die Grundeinstellung für den SSL-Port ist 444. Wird dieser SSL-Standardport verwendet, so muss beim Aufruf des URLs für die Remoteverwaltung keine Portnummer angegeben werden (z.B. entspricht "https://example.com" dem URL "https://example.com:444").

Diese Portnummer ist nicht dieselbe, die der Remoteverwaltung im Bereich Web-Server 352 im Konfigurationsdialog für die Remoteverwaltung zugewiesen

wurde. Falls HTTP-Verbindungen zur Remoteverwaltung weiterhin zugelassen sein sollen, müssen sie jenen anderen Port verwenden, sonst ist kein Verbindungsaufbau möglich. HTTPS-Verbindungen müssen hingegen auf dem HTTPS-Port hergestellt werden.

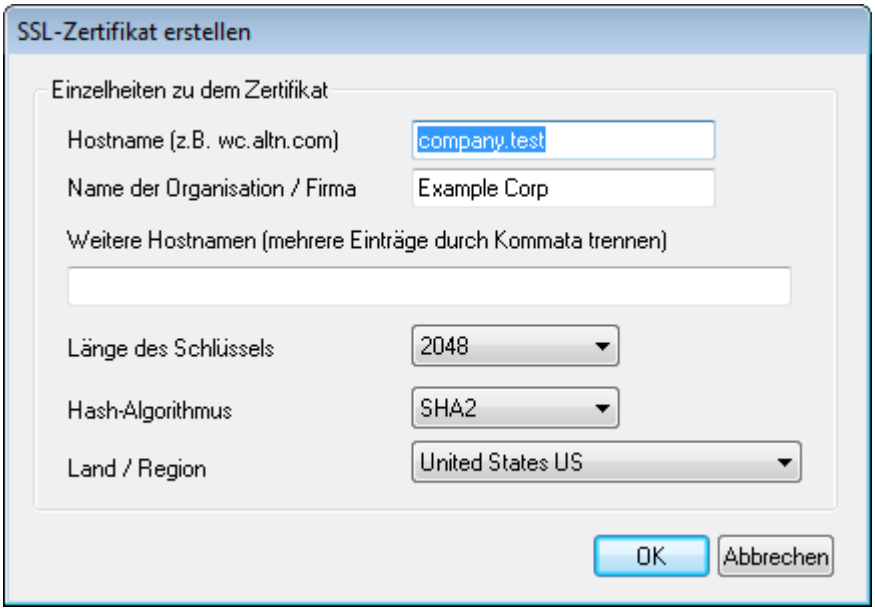
Zertifikat zur Nutzung mit HTTPS/SSL auswählen

In dieser Liste sind Ihre SSL-Zertifikate aufgeführt. Um Zertifikate für die Nutzung durch MDaemon zu aktivieren, aktivieren Sie die zugehörigen Kontrollkästchen. Um ein Zertifikat als Standard-Zertifikat zu bestimmen, klicken Sie auf den Stern neben dem gewünschten Zertifikat. MDaemon unterstützt die Erweiterung Server Name Identification (SNI) für das Protokoll TLS. Das Leistungsmerkmal SNI (Identifizierung von Servernamen) ermöglicht die Nutzung eines eigenen Zertifikats für jeden einzelnen Hostnamen, der Ihrem Server zugeordnet ist. MDaemon prüft die aktiven Zertifikate und wählt das Zertifikat aus, in dessen Datenfeld Subject Alternative Names der jeweils angeforderte Hostname enthalten ist. (Sie legen diese Subject Alternative Names bei Erstellung des Zertifikats fest.). Falls der Client keinen bestimmten Hostnamen anfordert, oder falls MDaemon kein Zertifikat mit übereinstimmendem Hostnamen findet, nutzt MDaemon das Standard-Zertifikat. Auf der Benutzeroberfläche von MDaemon können Sie ein Zertifikat durch Doppelklick auf seinen Eintrag in der Windows-Zertifikatverwaltung öffnen und seine Eigenschaften einsehen. Diese Funktion steht in der browsergestützten Remoteverwaltung nicht zur Verfügung.

Löschen
Hierdurch wird das in der Liste ausgewählte Zertifikat gelöscht. Vor dem eigentlichen Löschvorgang erscheint ein Dialogfenster mit einer Sicherheitsabfrage, ob der Löschvorgang auch wirklich durchgeführt werden soll.

Zertifikat erstellen

Um ein SSL-Zertifikat zu erstellen, klicken Sie auf das Steuerelement Zertifikat erstellen.



Hostname

Hier wird der Hostname angegeben, zu dem die Benutzer eine Verbindung herstellen (z.B. "wc.example.com").

Name der Organisation/Firma
Hier wird der Name der Organisation oder der Firma eingetragen, die dieses Zertifikat besitzt.

Weitere Hostnamen (mehrere Einträge durch Kommata trennen)
MDaemon unterstützt derzeit noch nicht mehrere Zertifikate für verschiedene Domänen; alle Domänen müssen sich dasselbe Zertifikat teilen. Falls noch weitere Hostnamen vorhanden sind, zu denen die Benutzer Verbindungen herstellen dürfen, und falls sich das Zertifikat auch auf diese Hostnamen erstrecken soll, so müssen sie hier eingetragen werden. Mehrere Einträge werden durch Kommata getrennt. Jokerzeichen sind zulässig, sodass sich "*.example.com" auf alle Subdomänen von example.com erstrecken würde (etwa "`wc.example.com`", "`mail.example.com`", usw.).

Länge des Schlüssels
Hier wird die gewünschte Länge des Schlüssels in Bit ausgewählt. Je länger der Schlüssel, desto besser ist der Datenaustausch gesichert. Dabei ist aber zu beachten, dass nicht alle Anwendungsprogramme Schlüssel mit einer Länge von mehr als 512 Bit verarbeiten können.

Hash-Algorithmus
Hier wird der Hash-Algorithmus ausgewählt; mögliche Algorithmen sind SHA1 und SHA2. Per Voreinstellung wird SHA2 genutzt.

Land/Region
Wählen Sie hier das Land oder die Region aus, in der sich dem oder in der sich der Server befindet.

Web-Server neu starten

Ein Klick auf dieses Steuerelement startet den Web-Server neu. Dieser Neustart ist nach jeder Änderung an einem Zertifikat erforderlich; erst danach werden neue Zertifikate genutzt.

Verwaltung Ihres Zertifikats mithilfe von Let's Encrypt

Let's Encrypt ist eine Zertifizierungsstelle (auch Certificate Authority, kurz CA), die mithilfe eines automatisierten Verfahrens unentgeltlich Zertifikate zur Verfügung stellt. Dieses Verfahren soll die derzeit noch weit verbreiteten und komplexen Verfahren der manuellen Erstellung, Echtheitsprüfung, Signatur, Installation und Verlängerung von Zertifikaten für die Sicherung von Websites ablösen.

Um dieses Verfahren zu unterstützen, steht Ihnen der Konfigurationsdialog Let's Encrypt 596 zur Verfügung. Mithilfe dieses Konfigurationsdialog wird das automatische Verfahren zur Verwaltung eines Zertifikats unterstützt, das Let's Encrypt bereitstellt. Sie können hier ein PowerShell-Skript einfach konfigurieren und ausführen, das im Verzeichnis "`MDaemon\LetsEncrypt`" abgelegt ist. Wenn Sie dieses Skript ausführen, wird hierdurch das System für Let's Encrypt eingerichtet, und insbesondere werden die für die erfolgreiche Abwicklung der http-01-Challenge erforderlichen Dateien in das HTTP-Verzeichnis von Webmail kopiert. Das Skript nutzt als Domäne für das Zertifikat den SMTP-Hostnamen 184 der Standard-

Domäne[181] und fügt etwa konfigurierte *Weitere Hostnamen* ein, ruft das Zertifikat ab, importiert es in Windows, und konfiguriert MDaemon so, dass das Zertifikat für MDaemon, Webmail und die Remoteverwaltung genutzt wird. Darüber hinaus erstellt das Skript im Verzeichnis "`MDaemon\Logs\`" die Protokolldatei `LetsEncrypt.log`. Diese Protokolldatei wird immer dann, wenn das Skript ausgeführt wird, gelöscht und neu erstellt. Sie beinhaltet Datum und Uhrzeit, wann das Skript ausgeführt wurde. Falls Sie eine *E-Mail-Adresse des Administrators für Benachrichtigungen* angegeben haben, werden im Fehlerfall Benachrichtigungen an diese Adresse versandt. Nähere Informationen finden Sie im Abschnitt Let's Encrypt[596].

Nähere Informationen über SSL und Zertifikate erhalten Sie unter:

Die Einbindung der Remoteverwaltung in die IIS[359]
SSL & TLS[577]
Erstellen und Nutzung von SSL-Zertifikaten[902]

Nähere Informationen über die Remoteverwaltung erhalten Sie unter:

Fernwartung[350]
Remoteverwaltung » Web-Server[352]
Vorlagen-Manager » Web-Dienste[795]
Benutzerkonten-Editor » Web-Dienste[720]

3.6.2.3 Die Einbindung der Remoteverwaltung in die IIS

MDaemon ist mit einem eigenen Web-Server ausgestattet und benötigt daher zum Betrieb der Remoteverwaltung die Internet Information Services (IIS) nicht. Die Remoteverwaltung unterstützt jedoch die IIS und kann daher als ISAPI-DLL arbeiten.

Gehen Sie folgendermaßen vor, um die Remoteverwaltung unter IIS 5 auszuführen:

1. Beenden Sie die Remoteverwaltung. Sie können dazu nach Rechtsklick auf dem Eintrag Remoteverwaltung im Abschnitt *Server* im linken Bereich der Benutzeroberfläche von MDaemon das Kontextmenü aufrufen und dann **Aktivieren/deaktivieren** anklicken.

2. Öffnen Sie den Internet-Informationsdienstemanager (**Start→Systemsteuerung→Verwaltung→Internet-Informationsdienstemanager**).

3. Klicken Sie rechts auf **Standard-Website**, und wählen Sie dann **Neu→Virtuelles Verzeichnis**.

4. Folgen Sie dem Assistenten, der Sie durch die Schritte zur Erstellung eines Virtuellen Verzeichnisses leitet. Die nachfolgenden Namen und Pfade können in den Assistenten eingegeben werden; Sie müssen sie jedoch an Ihre bestehende MDaemon-Installation und den Speicherpfad der Remoteverwaltung anpassen.

   a. Alias: "`WebAdmin`". Klicken Sie auf **Weiter**.
   b. Pfad: "`c:\mdaemon\webadmin\templates`". Klicken Sie auf **Weiter**.
   c. Klicken Sie auf **Weiter**.
   d. Klicken Sie auf **Fertig stellen**.

5. Setzen Sie die Ausführberechtigungen auf **nur Skripts**.
6. Setzen Sie den Anwendungsschutz auf **Niedrig(IIS-Prozess)**.
7. Klicken Sie auf der Registerkarte Virtuelles Verzeichnis im Abschnitt Anwendungseinstellungen auf **Konfiguration**.
8. Klicken Sie auf der Registerkarte **Zuordnungen** auf **Hinzufügen**.
9. Tragen Sie in das Feld **Ausführbare Datei** Pfad und Dateinamen nach folgendem Muster ein: "`c:\mdaemon\webadmin\templates\WebAdmin.dll`". Beachte: Dieses Feld darf keine Leerzeichen enthalten. Falls der verwendete Pfadname Leerzeichen enthält, muss er in das Namensformat 8.3 umgewandelt werden. Die Datei- und Verzeichnisnamen im Namensformat 8.3 können über den Befehl `dir /x` angezeigt werden.
10. Tragen Sie in das Feld **Erweiterung** "`.wdm`" ein, und wählen Sie das Steuerelement für **Alle Verben**.
11. Haken Sie das Kontrollkästchen **Skriptmodul** an.
12. Klicken Sie auf **OK**.
13. Sie können, falls gewünscht, alle anderen Anwendungserweiterungen aus der Liste entfernen. Klicken Sie danach auf **OK**.
14. Fügen Sie auf der Registerkarte **Dokumente** `login.wdm` als Standardinhaltsseite hinzu, und entfernen Sie alle anderen Einträge aus der Liste.
15. Rufen Sie in MDaemon den Konfigurationsdialog **Einstellungen→Web-- & IM-Dienste→Remoteverwaltung** auf, und klicken Sie auf **Remoteverwaltung wird unter einem externen Web-Server ausgeführt**.
16. Geben Sie als **URL für Remoteverwaltung** "`/WebAdmin/login.wdm`" ein.
17. Klicken Sie auf **OK**.

Gehen Sie folgendermaßen vor, um die Remoteverwaltung unter IIS 6 auszuführen:

Legen Sie einen neuen Anwendungspool für die Remoteverwaltung an:

1. Beenden Sie die Remoteverwaltung. Sie können dazu nach Rechtsklick auf dem Eintrag Remoteverwaltung im Abschnitt *Server* im linken Bereich der Benutzeroberfläche von MDaemon das Kontextmenü aufrufen und dann **Aktivieren/Deaktivieren** anklicken.
2. Öffnen Sie den Internet-Informationsdienstemanager (**Start→Systemsteuerung→Verwaltung→Internet-Informationsdienstemanager**).
3. Klicken Sie rechts auf **Anwendungspools**.
4. Klicken Sie auf **Neu→Anwendungspool**.

5. Tragen Sie in das Feld Anwendungspoolkennung "Alt-N" ein, und klicken Sie auf **OK**.
6. Klicken Sie rechts auf **Alt-N**.
7. Klicken Sie auf **Eigenschaften**.
8. Klicken Sie auf die Registerkarte **Leistung**.
9. Deaktivieren Sie "**Arbeitsprozesse im Leerlauf herunterfahren nach (Minuten)**" und "**Warteschlange für Kernelanforderung begrenzen**".
10. Klicken Sie auf die Registerkarte **Identität**.
11. Wählen Sie aus dem Rollmenü für das Steuerelement Vordefiniert den Eintrag **Lokales System**.
12. Klicken Sie auf **OK**.

Erstellen Sie ein Virtuelles Verzeichnis für die Remoteverwaltung:

1. Öffnen Sie den Internet-Informationsdienstemanager (**Start→Systemsteuerung→Verwaltung→Internet-Informationsdienstemanager**).
2. Klicken Sie rechts auf Ihre Website, und wählen Sie dann Neu/Virtuelles Verzeichnis.
3. Geben Sie einen Aliasnamen für das Virtuelle Verzeichnis an (z.B. "WebAdmin").
4. Geben Sie im Feld Pfad den vollständigen Pfad zum "Template"-Verzeichnis der Remoteverwaltung an - z.B."C:\Programme\Alt-N Technologies\WebAdmin\Templates".
5. Lassen Sie die Optionen Lesen und Skripts ausführen angehakt.
6. Schließen Sie den Assistenten ab, und klicken Sie rechts auf das Virtuelle Verzeichnis, das erstellt wurde.
7. Klicken Sie auf Eigenschaften.
8. Ändern Sie auf der Registerkarte Basisverzeichnis den Anwendungspool in "Alt-N".
9. Klicken Sie auf Konfiguration.
10. Klicken Sie auf Hinzufügen, um eine ISAPI-Anwendungserweiterungszuordnung hinzuzufügen.
11. Tragen Sie in das Feld Ausführbare Datei den Pfad zur WebAdmin-DLL nach folgenden Muster ein: "C:\Programme\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll".
12. Tragen Sie in das Feld Erweiterung ".wdm" ein.
13. Aktivieren Sie die Kontrollkästchen **Skriptmodul** und **Verifizieren, dass Datei existiert**.

14. Klicken Sie auf **OK**.
15. Sie können, falls gewünscht, alle anderen Anwendungserweiterungen aus der Liste entfernen. Klicken Sie danach auf **OK**.
16. Klicken Sie auf die Registerkarte **Dokumente.**
17. Stellen Sie sicher, dass die Option **Standardinhaltsseite aktivieren** aktiv ist.
18. Stellen Sie sicher, dass in der Liste nur "`login.wdm`" erscheint.
19. Klicken Sie auf **Ok**, und verlassen Sie den Dialog Eigenschaften des Virtuellen Verzeichnisses.

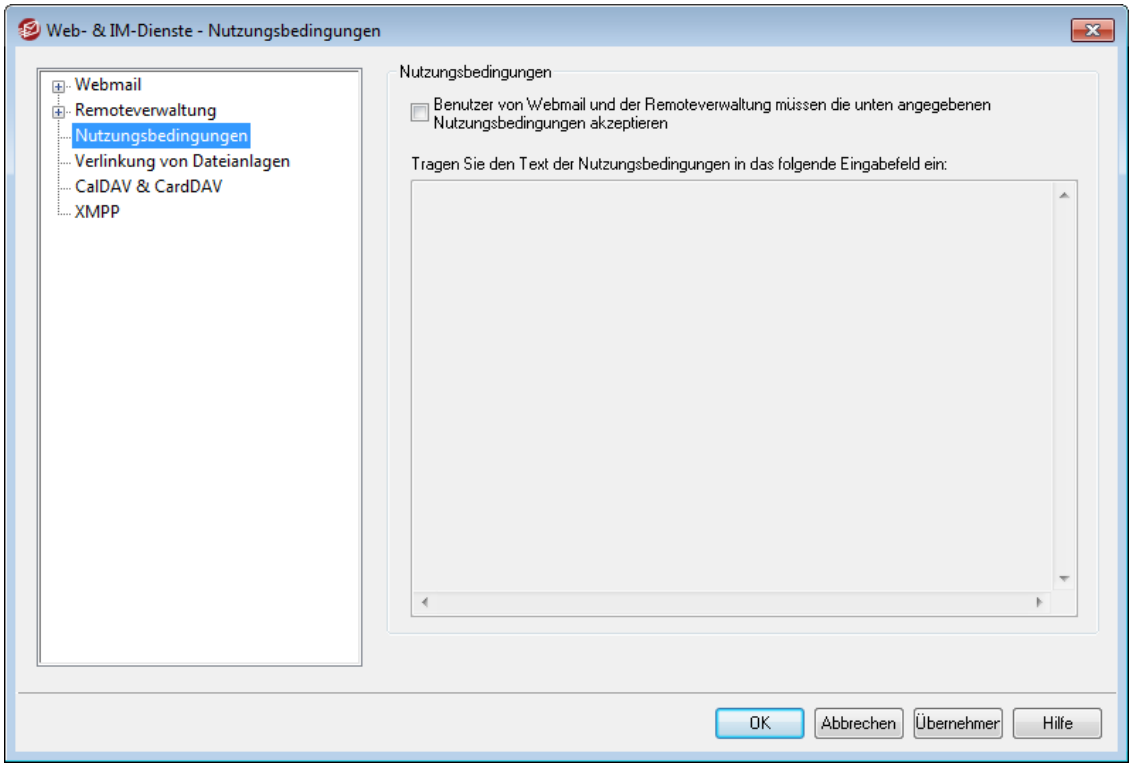
Nehmen Sie `.WDM` in die Liste der zugelassenen Webdiensterweiterungen auf:

1. Klicken Sie auf den Ordner **Webdiensterweiterungen** (in der IIS-Verwaltungskonsole).
2. Klicken Sie auf **Neue Webdiensterweiterung**.
3. Tragen Sie in das Feld Erweiterungsname "`WebAdmin`" ein.
4. Klicken Sie auf **Hinzufügen**, und navigieren Sie dann zu der WebAdmin-ISAPI-Erweiterung. Ein Beispiel für den Pfad:
   `C:\Programme\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll`.
5. Klicken Sie auf **Erweiterungsstatus auf "Zugelassen" setzen**.
6. Klicken Sie auf **OK**.
7. Rufen Sie in MDaemon den Konfigurationsdialog **Einstellungen→Web- & IM-Dienste→Remoteverwaltung** auf, und klicken Sie auf **Remoteverwaltung wird unter einem externen Web-Server ausgeführt**.
8. Geben Sie als **URL für Remoteverwaltung** "`/WebAdmin/login.wdm`" ein.
9. Klicken Sie auf **OK**.

Nähere Informationen über die Remoteverwaltung erhalten Sie unter:

Remoteverwaltung 350
Remoteverwaltung » Web-Server 352
Remoteverwaltung » HTTPS 355
Vorlagen-Manager » Web-Dienste 795
Benutzerkonten-Editor » Web-Dienste 720

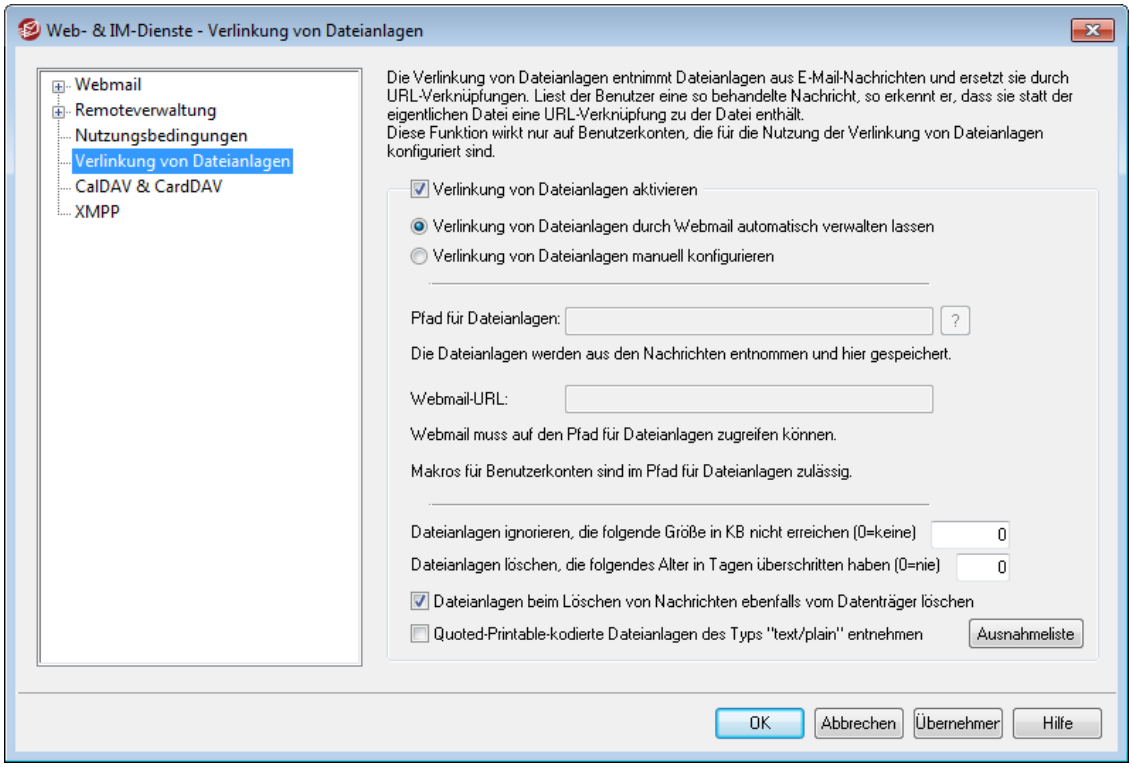
3.6.3 Nutzungsbedingungen



Benutzer von Webmail und der Remoteverwaltung müssen die unten angegebenen Nutzungsbedingungen akzeptieren

Mithilfe dieser Option können Sie erzwingen, dass die Benutzer von Webmail und der Remoteverwaltung bei jeder Anmeldung bestimmten Nutzungsbedingungen zustimmen. Ohne diese Zustimmung ist die Anmeldung nicht möglich, wenn diese Option aktiv ist. Tragen Sie den Text der Nutzungsbedingungen in das Eingabefeld unter dieser Option ein.

3.6.4 Verlinkung von Dateianlagen



Die Verlinkung von Dateianlagen (Einstellungen » Web- & IM-Services » Verlinkung von Dateianlagen) ist ein Leistungsmerkmal, mit dessen Hilfe MDaemon alle Dateianlagen aus eingehenden E-Mail-Nachrichten entnehmen, sie an einem festgelegten Speicherort ablegen und dann in die Nachrichten, aus denen die Dateianlagen entnommen wurden, URL-Verknüpfungen mit den entnommenen Dateien einfügen kann. Die Empfänger können die Dateianlagen durch Anklicken der Verknüpfungen herunterladen. Hierdurch kann die Geschwindigkeit der Nachrichtenverarbeitung erheblich gesteigert werden, was sich insbesondere auswirkt, wenn die Benutzer Nachrichten abrufen oder ihre Nachrichten-Ordner synchronisieren, da umfangreiche Dateianlagen dann in den Nachrichten nicht mehr enthalten sind. Auch die Sicherheit und der Schutz für die Benutzer werden verbessert, da die Dateianlagen an einem zentralen Speicherort abgelegt werden und dort durch den Administrator überwacht werden können. Sie werden nicht mehr automatisch durch die Mailclients abgerufen und dort womöglich noch automatisch ausgeführt. Falls Sie die Option "*Verlinkung von Dateianlagen durch Webmail automatisch verwalten lassen*" nutzen, werden die Speicherorte für die Dateianlagen und die Webmail-URLs automatisch verwaltet. Falls Sie die Verlinkung von Dateianlagen manuell konfigurieren, können Sie von Hand festlegen, wo die Dateien gespeichert werden, und Sie können mithilfe besonderer Makros diesen Speicherort auch dynamisch bestimmen. Die Verlinkung von Dateianlagen arbeitet nur, falls sie in diesem Konfigurationsdialog systemweit aktiviert ist, und falls jedes einzelne Benutzerkonto, das dieses Leistungsmerkmal nutzen soll, im Abschnitt Dateianlagen[734] des Benutzerkonten-Editors entsprechend eingerichtet ist. In demselben Abschnitt steht auch eine Option zur Verfügung, mit deren Hilfe die Verlinkung von Dateianlagen auch auf abgehende Nachrichten angewendet werden kann. Aus abgehenden Nachrichten des Benutzerkontos werden, wenn diese Option aktiv ist, die Dateianlagen ebenfalls entnommen und durch Verknüpfungen mit den gespeicherten Dateien ersetzt. Die Verknüpfungen, die MDaemon in die Nachrichten einfügt, enthalten in allen Fällen nicht die eigentlichen Dateipfade; sie enthalten stattdessen je eine eineindeutige Kennung ("GUID"), mit deren Hilfe der Server die

Dateianlage dem eigentlichen Speicherpfad zuordnet. Die Zuordnungstabelle für die GUIDs wird in der Datei `AttachmentLinking.dat` gespeichert.

Die Verlinkung von Dateianlagen versucht, die Dateinamen aus den MIME-Kopfzeilen zu verwenden, falls solche vorhanden sind. Sind die Dateinamen länger als 50 Zeichen, so werden nur die letzten 50 Zeichen genutzt. Enthalten die Dateinamen keine Dateiendung, so wird die Endung "`.att`" hinzugefügt.

Per Voreinstellung fügt die Verlinkung von Dateianlagen in bestimmte Nachrichten einen Hinweis darauf ein, dass MDaemon bestimmte Dateien durch Verknüpfungen ersetzt hat. Falls Sie diesen Hinweistext ändern wollen, fügen Sie der Datei `MDaemon.ini` im Verzeichnis \app\ den folgenden Eintrag hinzu, und starten Sie dann MDaemon neu:

```
[AttachmentLinking]
HeaderText=Hier benutzerdefinierten Hinweistext
eintragen.
```

Verlinkung von Dateianlagen aktivieren
Mithilfe dieser Option können Sie die Verlinkung von Dateianlagen für alle Benutzerkonten aktivieren, die im Abschnitt Dateianlagen[734] des Benutzerkonten-Editors auf die Nutzung dieses Leistungsmerkmals konfiguriert sind. Sobald Sie diese systemweit gültige Option aktivieren, erscheint eine Abfrage, ob Sie die zugehörige Benutzerkonten-abhängige Option für alle MDaemon-Benutzerkonten aktivieren wollen. Falls Sie hierauf mit "Ja" antworten, wird das Leistungsmerkmal für alle Benutzerkonten aktiviert, und die entsprechende Option in der Vorlage "Neue Benutzerkonten"[808] wird ebenfalls aktiviert. Falls Sie hierauf mit "Nein" antworten, wird das Leistungsmerkmal zwar systemweit zur Nutzung freigegeben, die einzelnen Benutzerkonten nutzen das Leistungsmerkmal jedoch nicht automatisch. Sie müssen das Leistungsmerkmal dann für jedes gewünschte Benutzerkonto gesondert aktivieren. Solange die Verlinkung von Dateianlagen aktiv ist, muss auch der Webmail-Server aktiv bleiben.

Verlinkung von Dateianlagen durch Webmail automatisch verwalten lassen
Diese Option ist per Voreinstellung aktiv, wenn die Verlinkung von Dateianlagen aktiv ist. Sie bewirkt, dass Webmail die Verlinkung von Dateianlagen automatisch verwaltet. Entnommene Dateianlagen werden im Pfad "`...\MDaemon\Attachments\$DOMAIN$\$MAILBOX$\`" gespeichert.

Verlinkung von Dateianlagen manuell konfigurieren
Mithilfe dieser Option können Sie das Verzeichnis selbst bestimmen, in dem die entnommenen Dateianlagen abgelegt werden. Sie müssen bei Nutzung dieser Option sowohl den Pfad für die Dateianlagen als auch den URL für Webmail von Hand eintragen.

Pfad für Dateianlagen
In dieses Textfeld können Sie das Verzeichnis eintragen, in dem die entnommenen Dateianlagen abgelegt werden sollen. Sie können entweder einen festen Verzeichnispfad eintragen, oder Sie können den Pfad mithilfe der Makros für Vorlagen[791] und Skripte[836] dynamisch gestalten. Ein Beispiel hierzu: Der Eintrag "`$ROOTDIR$\Attachments\$DOMAIN$\`" legt

alle Dateianlagen in einem Unterverzeichnis ab, dessen Name der Domäne entspricht, zu der der jeweilige Benutzer gehört. Dieses Verzeichnis liegt wiederum im Unterverzeichnis "Attachments" unter dem Hauptverzeichnis von MDaemon (meist C:\MDaemon\). Für den Benutzer "user1@example.com" würde sich in diesem Beispiel ergeben, dass die entnommenen Dateianlagen in dem Unterverzeichnis "C:\MDaemon\Attachments\example.com\" abgelegt werden. Sie können die Verzeichnispfade noch weiter verzweigen, indem Sie das Makro "$MAILBOX$" an den vorstehenden Beispiel-URL anhängen. Hieraus ergibt sich für den Beispiel-Benutzer ein Unterverzeichnis namens "user1" unter dem Verzeichnis "\example.com\". Der vollständige neue Verzeichnispfad lautet dann "C:\MDaemon\Attachments\example.com\user1\".

Webmail-URL
Tragen Sie hier den URL für Webmail ein (z.B. "http://mail.example.com:3000/WorldClient.dll"). MDaemon nutzt diesen URL für die Erstellung der Verknüpfungen mit den entnommenen Dateianlagen, die in die einzelnen Nachrichten eingefügt werden.

Dateianlagen ignorieren, die folgende Größe in KB nicht erreichen (0 = keine)
Die hier in KB angegebene Größe ist die untere Grenze, ab der Dateianlagen erst aus Nachrichten entnommen werden. Mithilfe dieser Option können Sie verhindern, dass kleinere Dateien entnommen werden. Um alle Dateianlagen, unabhängig von einer Mindestgröße, zu entnehmen, setzen Sie diesen Wert auf "0".

Dateianlagen löschen, die folgendes Alter in Tagen überschritten haben (0 = nie)
Mithilfe dieser Option können Sie die Speicherdauer für die Dateianlagen auf eine bestimmte Anzahl Tage begrenzen. Während der täglichen Bereinigungsvorgänge löscht MDaemon alle gespeicherten Dateianlagen, die das hier angegebene Höchstalter überschritten haben, und die im Standard-Verzeichnis für Dateianlagen oder einem Unterverzeichnis dieses Standard-Verzeichnisses gespeichert sind. Das Standard-Verzeichnis ist "<HauptverzeichnisMDaemon>\Attachments\...". Falls Sie ein anderes Verzeichnis festgelegt haben, in dem die Dateianlagen gespeichert werden, dann werden sie von dort nicht gelöscht. Diese Option ist per Voreinstellung abgeschaltet (Wert "0").

Dateianlagen beim Löschen von Nachrichten ebenfalls vom Datenträger löschen
Diese Option bewirkt, dass entnommene Dateianlagen immer dann vom Server gelöscht werden, wenn die Nachricht, mit der sie verknüpft sind, ebenfalls gelöscht wird.

Ist diese Option aktiv, und ruft ein Benutzer seine E-Mail-Nachrichten über einen POP3-Client ab, der nicht so eingerichtet ist, dass er die Nachrichten auf dem Server belässt, so gehen alle entnommenen Dateianlagen für den Benutzer unwiderruflich verloren. Ist diese Option nicht aktiv, so gehen zwar keine Dateianlagen verloren, aber mit der Zeit belegen veraltete und von den ursprünglichen Empfängern nicht mehr benötigte Dateianlagen immer mehr Speicherplatz auf dem Server. Nahezu alle POP3-Clients

haben die Möglichkeit, die Nachrichten nach dem Abruf nicht vom Server zu löschen.

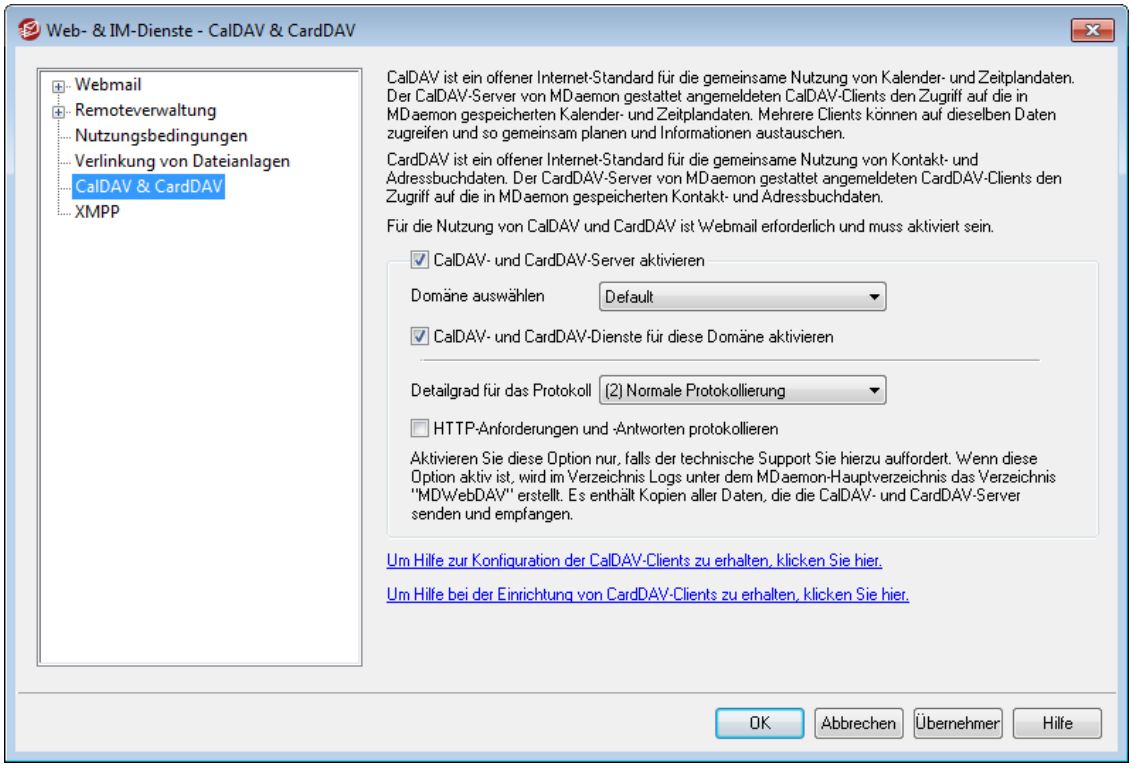
Quoted-Printable-kodierte Dateianlagen des Typs “text/plain” entnehmen
Per Voreinstellung werden quoted-printable-kodierte Dateianlagen des Typs `text/plain` nicht entnommen. Um Dateianlagen dieses Typs ebenfalls automatisch entnehmen zu lassen, aktivieren Sie diese Option.

Ausnahmeliste
Durch Anklicken dieses Steuerelements öffnen Sie die Ausnahmeliste für die Verlinkung von Dateianlagen. In diese Liste tragen Sie alle Dateinamen ein, die nicht aus den Nachrichten entnommen werden sollen. Per Voreinstellung ist `Winmail.dat` bereits eingetragen.

Siehe auch:

Vorlage "Neue Benutzerkonten" 789
Benutzerkonten-Editor » Dateianlagen 734
Makros für Vorlagen 791
Makros für Skripte 836

3.6.5 CalDAV & CardDAV



CalDAV ist ein Internet-Standard zur Verwaltung und Freigabe zur gemeinsamen Nutzung von Kalendern und Zeitplanungsdaten. MDaemon unterstützt CalDAV und ermöglicht es so Ihren Benutzerkonten, mithilfe aller Clients, die CalDAV unterstützen, auf ihre persönlichen Kalender und Aufgaben zuzugreifen und sie zu verwalten. Die Benutzer können, je nach ihren Berechtigungen 311, auch auf öffentliche 309 und freigegebene 742 Kalender und Aufgaben zugreifen. CardDAV ist

ein Standard für den Zugriff auf Kontakte und Adressbuchdaten. Der CardDAV-Server von MDaemon gestattet es echtheitsbestätigten CardDAV-Clients, auf die in MDaemon gespeicherten Kontaktdaten zuzugreifen.

CalDAV- und CardDAV-Server aktivieren
Die Unterstützung für CalDAV und CardDAV ist per Voreinstellung aktiv. Beide Dienste erfordern jedoch Webmail und können daher nur genutzt werden, wenn Webmail aktiv ist322. Falls Sie die Nutzung von CalDAV und CardDAV nicht ermöglichen wollen, deaktivieren Sie diese Option. Um CalDAV und CardDAV für einzelne Domänen zu aktivieren und zu deaktivieren, nutzen Sie die Optionen weiter unten.

Ändern der CalDAV- und CardDAV-Standardeinstellung für alle Domänen
Per Voreinstellung ist in der Option *Domäne auswählen* der Eintrag *Default* aktiv. Er bewirkt, dass CalDAV und CardDAV für alle MDaemon-Domänen unterstützt werden. Um die Voreinstellung zu ändern, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Dropdown-Liste *Domäne auswählen* den Eintrag **Default**.
2. Falls Sie CalDAV und CardDAV für alle Domänen aktivieren wollen, aktivieren Sie das Kontrollkästchen **CalDAV- und CardDAV-Dienste für diese Domäne aktivieren**. Falls Sie die CalDAV- und CardDAV-Dienste per Voreinstellung für alle Domänen deaktivieren wollen, deaktivieren Sie dieses Kontrollkästchen.
3. Klicken Sie auf **OK**.

Aktivieren und Deaktivieren von CalDAV und CardDAV für einzelne Domänen
Um die *Standard-Einstellung* für CalDAV und CardDAV für einzelne Domänen zu übergehen, gehen Sie folgendermaßen vor:

1. Wählen Sie die gewünschte Domäne in der Dropdown-Liste *Domäne auswählen*.
2. Falls Sie CalDAV und CardDAV für die ausgewählte Domäne aktivieren wollen, aktivieren Sie das Kontrollkästchen **CalDAV- und CardDAV-Dienste für diese Domäne aktivieren**. Falls Sie die CalDAV- und CardDAV-Dienste für die ausgewählte Domäne deaktivieren wollen, deaktivieren Sie dieses Kontrollkästchen.
3. Klicken Sie auf **OK**.

Protokollierung

Detailgrad für das Protokoll
Mithilfe dieses Dropdown-Menüs können Sie den Detailgrad festlegen, in dem die CalDAV- und CardDAV-Aktivitäten protokolliert werden. Es stehen sechs Detailgrade zur Verfügung: 1 Debug-Protokollierung, 2 Normale Protokollierung (dies ist die Voreinstellung), 3 Nur Warnungen und Fehler, 4 Nur Fehler, 5 Nur schwer wiegende Fehler und 6 Keine Protokollierung. Diese Einstellung wirkt immer global und kann nicht für einzelne Domänen abweichend getroffen werden.

HTTP-Anforderungen und -Antworten protokollieren
Ist diese Option aktiv, so erstellt MDaemon im Verzeichnis logs ein Unterverzeichnis `MDWebDAV`. In diesem Unterverzeichnis werden alle Daten protokolliert, die der CalDAV- und der CalDAV-Sever senden und empfangen. Im

Normalfall wird diese Option nur zur Fehlersuche eingesetzt. Sie sollte daher nur aktiviert werden, wenn der technische Support hierzu auffordert.

Konfigurieren der CalDAV-Clients

Um Clients zu konfigurieren, die RFC 6764 (Auffinden von Diensten für Kalendererweiterungen zu WebDAV [CalDAV] und vCard-Erweiterungen für WebDAV [CardDAV]) unterstützen, sind üblicherweise nur Servername, Benutzername und Kennwort erforderlich. Sie können DNS-Einträge einrichten, die die Clients auf den richtigen URL hinweisen. Stehen solche DNS-Einträge nicht zur Verfügung, so können die Benutzer bestimmte "allgemein bekannte URLs" im Client eingeben. Diese sind aufgebaut nach dem Muster `/.well-known/caldav`. Ein Beispiel hierzu: `http://example.com:3000/.well-known/caldav`. Der in Webmail integrierte Webserver unterstützt die allgemein bekannten URLs.

Clients, die das automatische Auffinden der CalDAV-Dienste nicht unterstützten, benötigen einen vollständigen URL, um auf die Dienste zugreifen zu können. Zu diesen Clients gehört beispielsweise Mozilla Thunderbird mit dem Kalenderplugin Lightning. Die CalDAV-URLs von MDaemon sind nach folgendem Muster aufgebaut:

Kalender und Aufgaben
Standard-Kalender oder -Aufgabenliste des Benutzers:

`http://[Host]/webdav/calendar`
(z.B. `http://example.com:3000/webdav/calendar`)

`http://[Host]/webdav/tasklist`
(z.B. `http://example.com/webdav/tasklist`)

Benutzerdefinierter Kalender oder benutzerdefinierte Aufgabenliste des Benutzers:

`http://[Host]/webdav/calendar/[Kalendername]`
(z.B. `http://example.com/webdav/calendar/personal`)

`http://[Host]/webdav/tasklist/[Name der Aufgabenliste]`
(z.B. `http://example.com/webdav/tasklist/todo`)

Benutzerdefinierter Kalender oder benutzerdefinierte Aufgabenliste des Benutzers in einem Unterordner:

`http://[Host]/webdav/calendar/[folder]/[Kalendername]`
(z.B. `http://example.com/webdav/calendar/meine-daten/persoenlich`)

`http://[Host]/webdav/tasklist/[folder]/[Name der Aufgabenliste]`
(z.B. `http://example.com/webdav/tasklist/meine-daten/todo`)

Zur gemeinsamen Nutzung freigegebene Kalender und Aufgaben
Standard-Kalender oder -Aufgabenliste eines anderen Benutzers:

`http://[Host]/webdav/calendars/[Domäne]/[Benutzer]`
(z.B. `http://example.com/webdav/calendars/example.net/frank`)

`http://[Host]/webdav/tasks/[Domäne]/[Benutzer]`
(z.B. `http://example.com/webdav/tasks/example.net/frank`)

Benutzerdefinierter Kalender oder benutzerdefinierte Aufgabenliste eines anderen Benutzers:

`http://[Host]/webdav/calendars/[Domäne]/[Benutzer]/[Kalendername]`
(z.B. `http://example.com/webdav/calendars/example.net/frank/personal`)

`http://[Host]/webdav/tasks/[Domäne]/[Benutzer]/[Name der Aufgabenliste]`
(z.B. `http://example.com/webdav/tasks/example.net/frank/todo`)

Öffentliche Kalender und Aufgabenlisten
Standard-Kalender oder -Aufgabenliste der Domäne:

`http://[Host]/webdav/public-calendars/[Domäne]`
(z.B. `http://example.com/webdav/public-calendars/example.com`)

`http://[Host]/webdav/public-tasks/[Domäne]`
(z.B. `http://example.com/webdav/public-tasks/example.com`)

Kalender oder Aufgabenliste auf obersdter Ebene der Hierarchie der öffentlichen Ordner:

`http://[Host]/webdav/public-calendars/[Kalendername]`
(z.B. `http://example.com/webdav/public-calendars/urlaub`)

`http://[Host]/webdav/public-tasks/[Name der Aufgabenliste]`
(z.B. `http://example.com/webdav/public-tasks/projekte`)

Bei der Erprobung des Clients OutlookDAV sind besondere Vorsichtsmaßnahmen erforderlich. Auf Systemen, auf denen mehrere MAPI-Profile vorhanden sind, wurde bei diesem Client beobachtet, dass er für alle Kalendereinträge, die der Server an ihn übermittelt, Löschbefehle an den Server sendet. OutlookDAV unterstützt nur das Standard-MAPI-Profil.

Nähere Informationen zur Einrichtung von CalDAV-Clients sind in englischer Sprache in der MDaemon-Wissensdatenbank verfügbar. Um die entsprechenden Artikel zu finden, suchen Sie nach dem Stichwort "CalDav".

Konfigurieren der CardDAV Clients

Um Clients zu konfigurieren, die RFC 6764 (Auffinden von Diensten für Kalendererweiterungen zu WebDAV [CalDAV] und vCard-Erweiterungen für WebDAV [CardDAV]) unterstützen, sind üblicherweise nur Servername, Benutzername und Kennwort erforderlich. Das Apple-Adressbuch und iOS unterstützen diesen Standard. Sie können DNS-Einträge einrichten, die die Clients auf den richtigen URL hinweisen. Stehen solche DNS-Einträge nicht zur Verfügung, so können die Benutzer bestimmte "allgemein bekannte URLs" im Client eingeben. Diese sind aufgebaut nach dem Muster `/.well-known/carddav`. Ein Beispiel hierzu: `http://example.com:3000/.well-known/carddav`. Der in Webmail integrierte Webserver unterstützt die allgemein bekannten URLs. Clients, die das automatische Auffinden der CardDAV-Dienste nicht unterstützten, benötigen einen vollständigen URL, um auf die Dienste zugreifen zu können.

Bekannte CardDAV-Clients sind Apple Kontakte (Bestandteil von Mac OS X), Apple iOS (iPhone) und Mozilla Thunderbird mithilfe des Plugins SOGO.

Beachte: Bis einschließlich OS X 10.11 (El Capitan) unterstützt die Anwendung Apple Kontakte nur einen einzigen Ordner oder eine einzige Kontaktsammlung. Erkennt der CardDAV-Server, dass Apple Kontakte eine Verbindung herstellt, so übermittelt er nur den Standard-Kontaktordner des gerade angemeldeten Benutzers. In OS X 10.11 (El Capitan) besteht außerdem ein bekannter Fehler, der verhindert, dass ein CardDAV-Benutzerkonto über die Ansicht "Erweitert" des Konfigurationsdialogs hinzugefügt wird.

Zugriff auf Adressbücher
Das Verzeichnis "addressbook" verweist auf das eigene Standard-Adressbuch des jeweiligen Benutzers.

`http://[Host]/webdav/addressbook` - Standardkontaktordner des angemeldeten Benutzers

`http://[Host]/webdav/addressbook/freunde` - Kontaktordner "freunde" des angemeldeten Benutzers

`http://[Host]/webdav/addressbook/ordner/persoenlich` - Kontaktordner "persoenlich" im Ordner "ordner" des angemeldeten Benutzers

Zugriff auf freigegebene, gemeinsam genutzte Ordner eines anderen Benutzers, für die der gerade angemeldete Benutzer zugriffsberechtigt ist
Das Verzeichnis "contacts" verweist auf die freigegebenen Kontaktordner.

`http://[Host]/webdav/contacts/example.com/benutzer2` - Standardkontaktordner des Benutzers benutzer2@company.test

`http://[Host]/webdav/contacts/example.com/benutzer2/meinordner` - Kontaktordner "meinordner" des Benutzers benutzer2@company.test

Zugriff auf öffentliche Ordner, für die der gerade angemeldete Benutzer zugriffsberechtigt ist
Das Verzeichnis "public-contacts" verweist auf die öffentlichen Kontaktordner.

`http://[Host]/webdav/public-contacts/example.com` - Standardkontaktordner der Domäne example.com

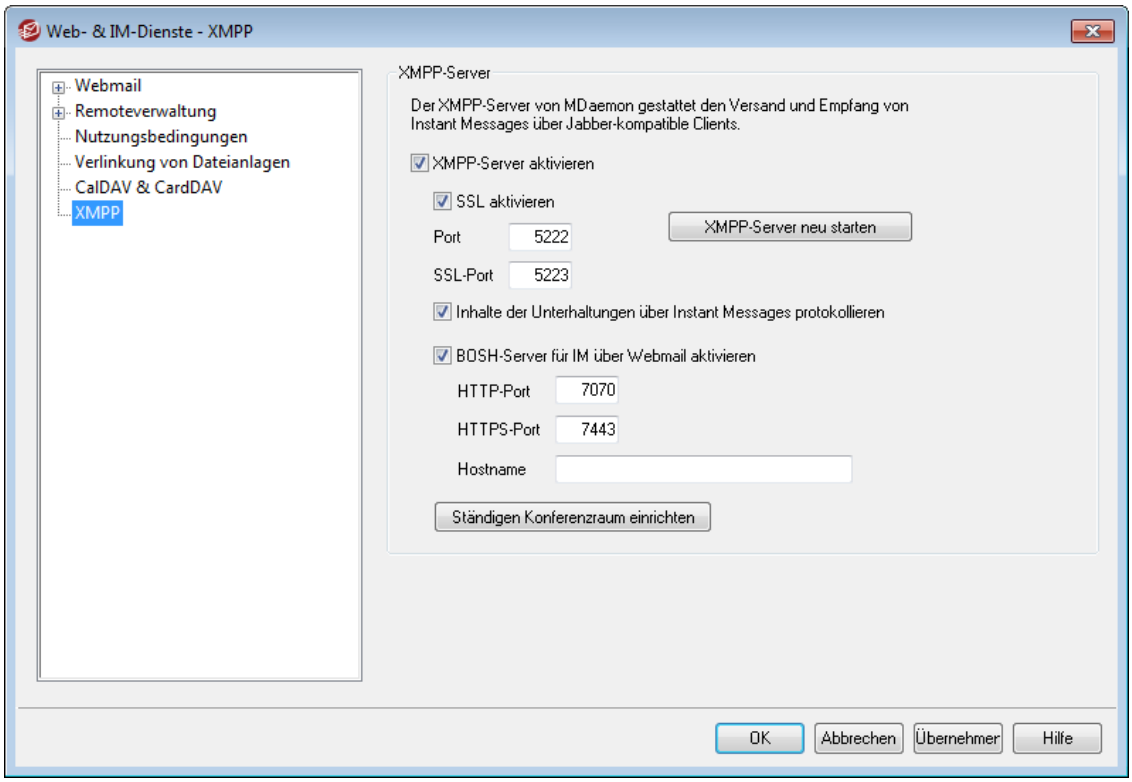
`http://[Host]/webdav/public-contacts/ordnername` - Kontaktordner "ordnername" auf der obersten Ebene der Verzeichnisstruktur der öffentlichen Ordner

Bei der Erprobung des Clients OutlookDAV sind besondere Vorsichtsmaßnahmen erforderlich. Auf Systemen, auf denen mehrere MAPI-Profile vorhanden sind, wurde bei diesem Client beobachtet, dass er für alle Elemente, die der Server

an ihn übermittelt, Löschbefehle an den Server sendet. OutlookDAV unterstützt nur das Standard-MAPI-Profil.

Nähere Informationen zur Einrichtung von CardDAV-Clients sind in englischer Sprache in der MDaemon-Wissensdatenbank verfügbar. Um die entsprechenden Artikel zu finden, suchen Sie nach dem Stichwort "CardDav".

3.6.6 XMPP



MDaemon ist mit einem Server für das Extensible Messaging and Presence Protocol (XMPP) ausgestattet; solche Server werden bisweilen auch als Jabber-Server bezeichnet. Über diesen Server können die Benutzer mithilfe des MDaemon Instant Messengers 318 und von XMPP-Clients, die Drittanbieter bereit stellen, Instant Messages senden und empfangen. Zu diesen XMPP-Clients gehören Pidgin, Gajim, Swift und viele andere. Solche Clients sind für die meisten Betriebssysteme und Plattformen für mobile Endgeräte verfügbar.

Der XMPP-Server wird als Windows-Dienst installiert. Per Voreinstellung nutzt er die Ports 5222 (SSL über STARTTLS) und 5223 (gesonderter SSL-Port). Der XMPP-Server nutzt die SSL-Konfiguration von MDaemon, falls SSL in MDaemon aktiv ist. Manche XMPP-Clients nutzen DNS-Einträge des Typs SRV, um die Hostnamen der Server automatisch zu ermitteln. Nähere Informationen hierzu finden Sie in englischer Sprache unter http://wiki.xmpp.org/web/SRV_Records.

Die Benutzer melden sich in ihren XMPP-Clients mit Ihrer E-Mail-Adressen und Kennwörtern an. Bei manchen Clients ist es erforderlich, die E-Mail-Adresse für die Anmeldung in ihre Bestandteile zu zerlegen. Ein Beispiel hierzu: Bei Nutzung einer E-

Mail-Adresse wie "frank@example.com" ist es bei manchen Clients erforderlich, "frank" als Anmeldenamen oder Benutzernamen und "example.com" als Domäne einzutragen.

Für Chats, an denen mehrere Benutzer oder Gruppen von Benutzern beteiligt sind, stellen die Clients üblicherweise "Chaträume" oder "Konferenzräume" zur Verfügung. Um einen Chat mit einer Benutzergruppe zu beginnen, erstellen Sie einen Chatraum oder Konferenzraum, und geben Sie diesem Raum einen Namen. Danach laden sie die gewünschten Benutzer in den Raum ein. Die meisten Clients verlangen keine Servernamen für solche Räume; es genügt vielmehr, den Räumen einen Namen zuzuweisen. Sollte aber ein Servername für einen Raum erforderlich sein, können Sie hierfür das Muster "conference.<Ihre Domäne>" nutzen (beispielsweise conference.example.com). Einige wenige Clients verlangen, dass der Name des Raums und der Servername in einem Eintrag zusammengefasst werden. Hierfür können Sie das Muster "konferenzraum@conference.<Ihre Domäne>" nutzen (beispielsweise Raum01@conference.example.com).

Manche Clients, wie etwa Pidgin, unterstützen die Suche nach Benutzern. Hiermit können die Benutzer auf dem Server anhand von Namen und E-Mail-Adressen nach anderen Benutzern suchen und sie dann einfach in die Kontaktlisten aufnehmen. Üblicherweise muss hierfür kein Servername oder eine besondere Information, wo die Suche durchgeführt werden soll, angegeben werden. Falls der verwendete Client für die Suche einen Servernamen verlangt, können Sie das Muster "search.<Ihre Domäne>" nutzen (beispielsweise search.example.com). Bei der Suche ist das Zeichen % als Jokerzeichen zulässig. So können Sie beispielsweise in das Feld für die E-Mail-Adresse "%@example.com" eintragen, und Sie erhalten eine Liste aller Benutzer, deren E-Mail-Adressen auf "@example.com" enden.

XMPP-Server

XMPP-Server aktivieren
Mithilfe dieser Option aktivieren Sie den XMPP-Server. Um das Instant Messaging selbst zuzulassen, müssen Sie außerdem die Option **Instant Messaging aktivieren** im Konfigurationsdialog WCIM 331 aktivieren.

SSL aktivieren
Diese Option aktiviert die Unterstützung von SSL durch den XMPP-Server. SSL-Verbindungen müssen dann über den weiter unten konfigurierten *SSL-Port* hergestellt werden. **Beachte:** Diese Option wirkt auch auf den weiter unten konfigurierten BOSH-Server und seine Option *HTTPS-Port*.

Port
Diesen Port nutzt der XMPP-Server für Verbindungen mit SSL über STARTTLS. Die Voreinstellung lautet 5222.

SSL-Port
Diesen Port nutzt der XMPP-Server als gesonderten Port für direkte SSL-Verbindungen. Die Voreinstellung lautet 5223.

XMPP-Server neu starten
Um den XMPP-Server neu zu starten, klicken Sie auf diese Schaltfläche.

Inhalte der Unterhaltungen über Instant Messages protokollieren
Per Voreinstellung werden die Inhalte aller über Instant Messages geführten Unterhaltungen in Dateien protokolliert, deren Namen nach dem Schema

`XMPPServer-<Datum>.log` gebildet werden. Diese Dateien werden im Verzeichnis `MDaemon\Logs\` gespeichert. Falls Sie diese Protokollierung nicht wünschen, deaktivieren Sie diese Option.

BOSH-Server für IM über Webmail aktivieren
Mithilfe dieser Option aktivieren Sie den BOSH-Server. Er ermöglicht das Instant Messaging in MDaemon Webmail selbst.

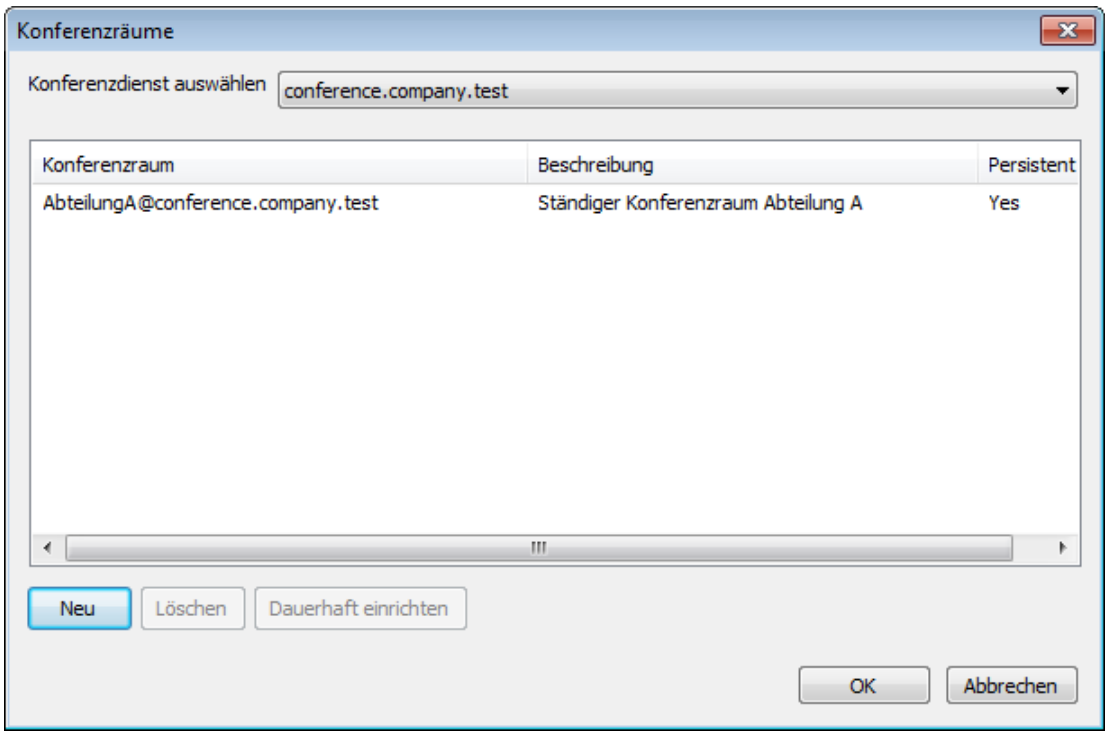
HTTP-Port
Per Voreinstellung nutzt der BOSH-Server den HTTP-Port 7070.

HTTPS-Port
Ist die Option *SSL aktivieren* weiter oben aktiv, so nutzt der BOSH-Server diesen HTTPS-Port. Per Voreinstellung nutzt der BOSH-Server den Port 7443.

Hostname
Mithilfe dieser Option können Sie einen Hostnamen angeben, falls dies erforderlich ist.

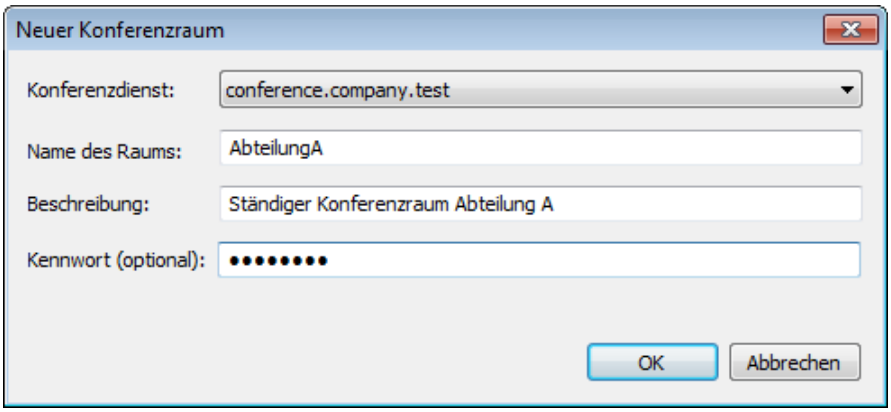
Ständige Konferenzräume konfigurieren

Durch Anklicken dieser Schaltfläche rufen Sie den Konfigurationsdialog für Konferenzräume auf. Legt ein Benutzer einen Konferenzraum an, so wird dieser Konferenzraum per Voreinstellung wieder gelöscht, sobald die letzte Person den Konferenzraum verlassen hat. Mithilfe der folgenden Optionen können Sie Konferenzräume aber auch als ständige Konferenzräume anlegen. Solche Konferenzräume bleiben auch dann bestehen, wenn sie leer sind. Sie können Konferenzräume auch löschen und bestehende, vorübergehende Konferenzräume in ständige Konferenzräume umstellen.



Konferenzdienst auswählen
In diesem Auswahlfeld wählen Sie die Domäne aus. Es erscheinen dann die Konferenzräume dieser Domäne in der Liste.

Neu
Um einen ständigen Konferenzraum einzurichten, klicken Sie auf diese Schaltfläche.



Konferenzdienst auswählen
In diesem Auswahlfeld wählen Sie die Domäne aus, zu der der Konferenzraum gehören soll.

Name des Raums
Geben Sie hier den Namen des Konferenzraums an. Der Name darf keine Leerzeichen enthalten.

Beschreibung
Geben Sie hier die Beschreibung für den Konferenzraum an. Die Beschreibung wird den Benutzern angezeigt, wenn sie diesen Konferenzraum betreten.

Kennwort (optional)
Falls Sie den Konferenzraum durch ein Kennwort sichern wollen, geben Sie das Kennwort hier an. Benutzer, die den Konferenzraum betreten wollen, müssen dieses Kennwort angeben.

Löschen
Um einen Konferenzraum zu löschen, wählen Sie den Konferenzraum aus, und klicken Sie dann auf diese Schaltfläche.

Dauerhaft einrichten
Um einen temporären Konferenzraum in einen ständigen Konferenzraum umzustellen, wählen Sie den Konferenzraum in der Liste aus, und klicken Sie danach auf diese Schaltfäche.

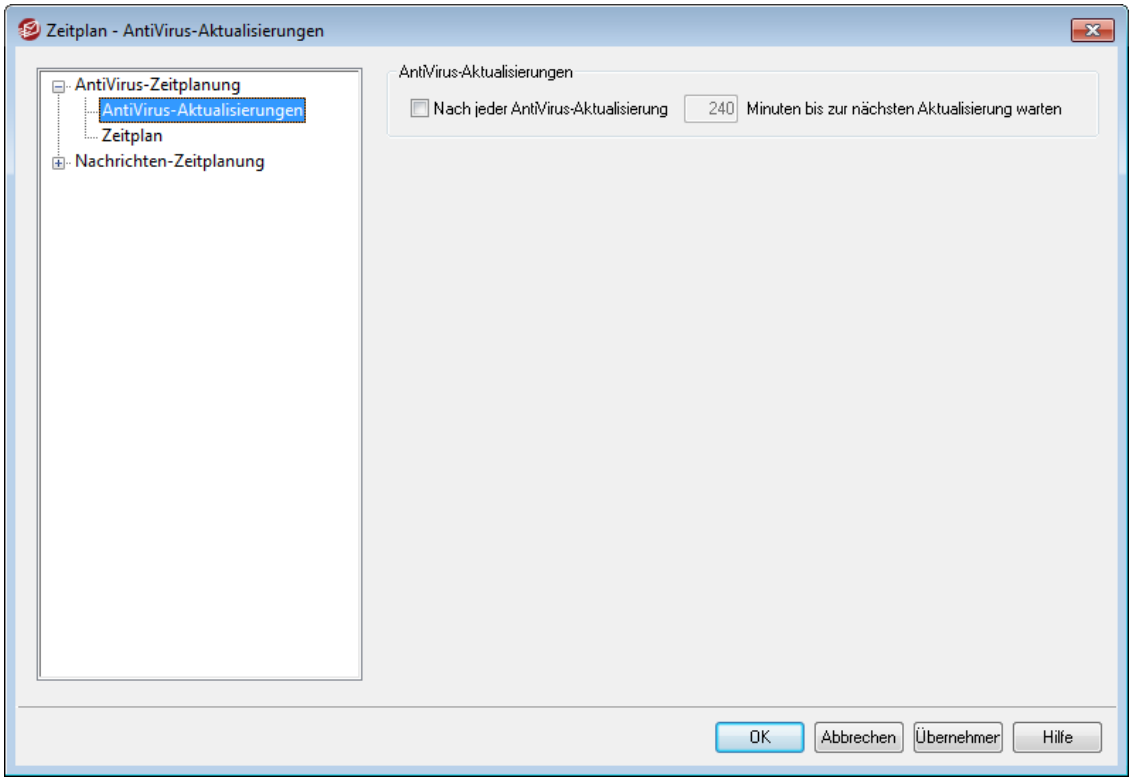
Siehe auch:

Webmail » MDIM 331

3.7 Zeitplan

3.7.1 AntiVirus-Zeitplanung

3.7.1.1 AntiVirus-Aktualisierungen



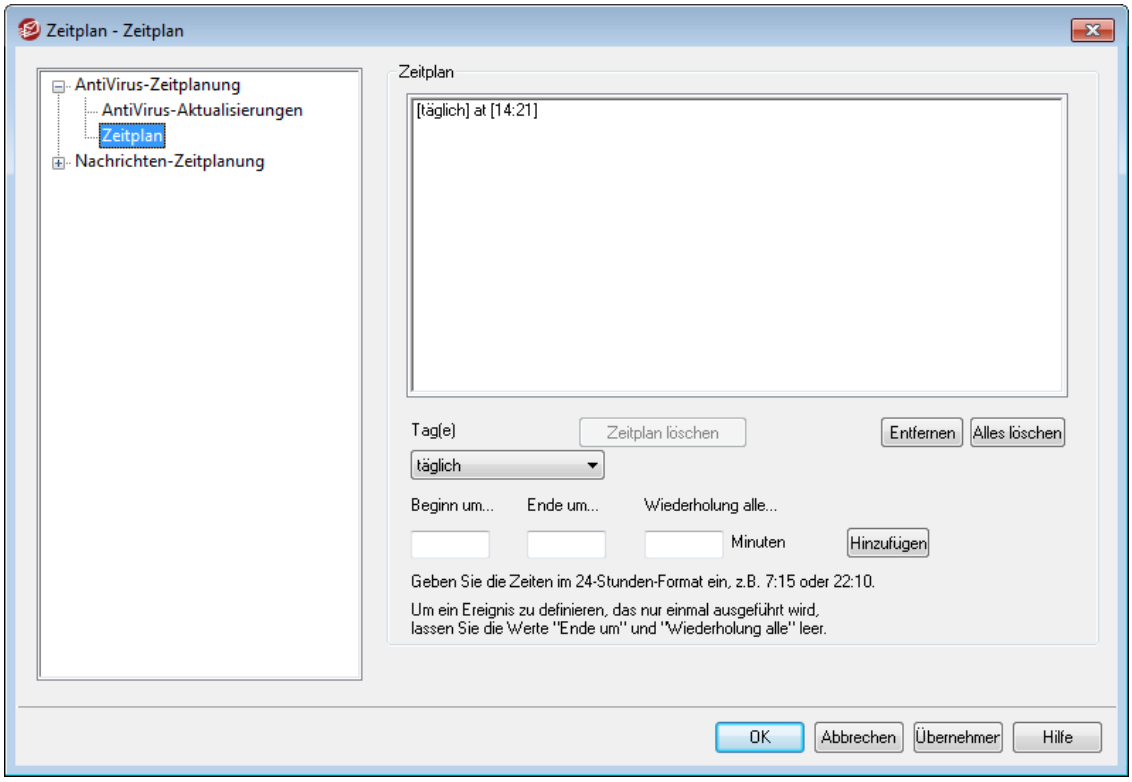
AntiVirus-Aktualisierungen

Nach jeder AntiVirus-Aktualisierung [xx] Minuten bis zur nächsten Aktualisierung warten
Diese Option bestimmt, wie lange AntiVirus nach der jeweils letzten Prüfung auf die Verfügbarkeit neuer Virensignaturen warten muss, bevor AntiVirus erneut nach neuen Virensignaturen sucht. Die Zeitdauer wird in Minuten angegeben. Sie beginnt mit Abschluss der jeweils letzten Suche nach neuen Virensignaturen, und zwar unabhängig davon, ob diese Suche durch den Zeitplan gesteuert oder manuell durchgeführt wurde. Aktualisierungen, die automatisch aufgrund eines Zeitplans oder manuell durch den Benutzer durchgeführt werden, haben Vorrang vor dieser Einstellung und lassen die Zeitdauer wieder neu beginnen. Ein Beispiel hierzu: Beträgt der hier eingetragene Wert 240 Minuten, und lösen Sie schon nach 100 Minuten eine erneute Suche nach neuen Virensignaturen aus, so wird durch diese Suche der Zähler wieder auf 240 Minuten zurückgesetzt.

Siehe auch:

Zeitplan 377
AntiVirus 671
AntiVirus-Aktualisierung 675

3.7.1.2 Zeitplan



Im Zeitplan für AntiVirus-Aktualisierungen können Sie bestimmte Zeiten festlegen, zu denen nach AntiVirus-Aktualisierungen gesucht werden soll. Sie erreichen den Zeitplan über Einstellungen » Zeitplan » AntiVirus-Aktualisierungen » Zeitplan.

Zeitplan

Entfernen
Um einen Eintrag aus der Liste zu entfernen, wählen Sie den Eintrag aus, und klicken Sie dann auf dieses Steuerelement.

Alles löschen
Dieses Steuerelement entfernt alle Einträge aus dem Zeitplan.

Erstellen geplanter Ereignisse

Tag(e)
Um ein neues Ereignis in dem Zeitplan zu planen, wählen Sie zunächst den Tag oder die Tage aus, an denen das Ereignis ausgeführt werden soll. Sie können folgende Auswahl treffen: täglich, Wochentage (Montag bis Freitag), Wochenenden (Samstag und Sonntag), oder einzelne Wochentage.

Beginn um...
Geben Sie hier die Uhrzeit ein, zu der die Suche nach Aktualisierungen beginnen soll. Die Zeit muss im 24-Stunden-Format zwischen 00:00 und 23:59 Uhr eingegeben werden. Soll das Ereignis nur einmal zu dem angegebenen Zeitpunkt ausgeführt werden und sich nicht wiederholen, so ist dies die einzige Zeitangabe, die Sie machen müssen (lassen Sie dann die Optionen *Beginn um...* und *Wiederholung alle...* leer).

Ende um...
Geben Sie hier die Uhrzeit ein, zu der die Suche nach Aktualisierungen enden soll. Die Zeit muss im 24-Stunden-Format zwischen 00:00 und 23:59 Uhr eingegeben werden, und sie muss nach der Zeit liegen, die unter *Beginn um...* eingegeben wurde. Ist beispielsweise unter *Beginn um...* der Wert 10:00 eingetragen, so kann der Wert *Ende um...* zwischen 10:01 und 23:59 liegen. Falls Sie ein einmal auszuführendes Ereignis anlegen wollen, lassen Sie dieses Feld leer.

Wiederholung alle [xx] Minuten
Hier geben Sie das Intervall an, in dem AntiVirus zwischen den unter *Beginn um...* und *Ende um...* angegebenen Zeiten nach Aktualisierungen suchen soll. Falls Sie ein einmal auszuführendes Ereignis anlegen wollen, lassen Sie dieses Feld leer.

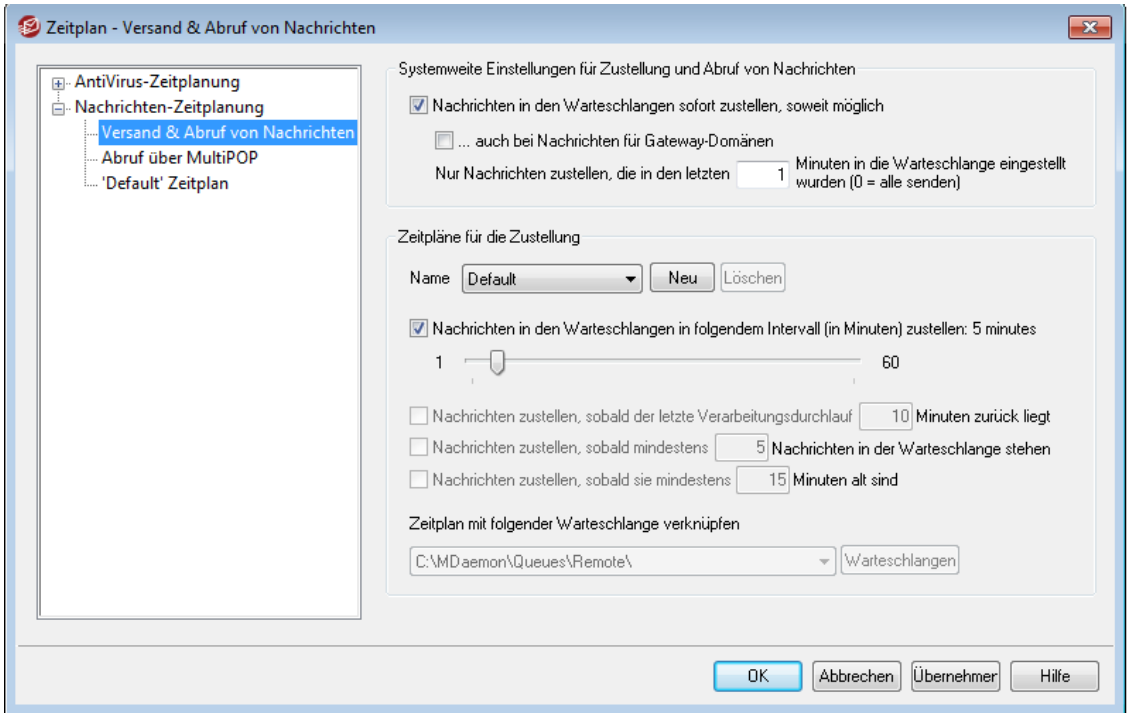
Hinzufügen
Nachdem Sie die gewünschten Daten in die Felder *Tag(e)*, *Beginn um...*, und ggf. *Ende um...* und *Wiederholung alle...* eingetragen haben, klicken Sie auf dieses Steuerelement, um das Ereignis in den Zeitplan einzutragen.

Siehe auch:

AntiVirus 671
AntiVirus-Aktualisierung 675

3.7.2 Nachrichten-Zeitplanung

3.7.2.1 Versand und Abruf von Nachrichten



Sie erreichen die Einstellungen für die Zeitplanung von Ereignissen in MDaemon über Einstellungen » Zeitplan. Hier können Sie die Zeitplanung für die Verarbeitung externer Nachrichten durch MDaemon Ihren Anforderungen entsprechend einfach oder detailgenau vornehmen. Für Empfang und Versand der Nachrichten können Sie entweder mithilfe der Funktionen unter Zeitplan für den Nachrichtenversand 383

einen genauen Zeitplan aufstellen oder ein einfaches Intervall festlegen. Es lassen sich auch Bedingungen für den außerplanmäßigen Versand festlegen, wenn etwa eine gewisse Anzahl Nachrichten seit einer gewissen Zeit auf den Versand wartet. Es können weiter benutzerdefinierte Zeitpläne erstellt und mit Warteschlangen für externe Nachrichten verknüpft werden. Damit lassen sich unterschiedliche Zeitpläne für unterschiedliche Arten von Nachrichten definieren. Denkbar sind etwa getrennte Zeitpläne für große Nachrichten, Nachrichten aus Mailinglisten, Nachrichten von bestimmten Domänen, und vieles mehr.

Sie können mithilfe der Einstellungen im Abschnitt AntiVirus-Aktualisierungen 376 des Konfigurationsdialogs für den Zeitplan bestimmen, wie oft MDaemon nach AntiVirus 648-Aktualisierungen suchen soll.

Mithilfe der Einstellungen in diesem Konfigurationsdialog können Sie steuern, wie oft MDaemon Nachrichten aus den Warteschlangen zustellt. Sie können MDaemon so konfigurieren, dass Nachrichten sofort oder in bestimmten Intervallen oder dann zugestellt werden, wenn eine Mindestanzahl von Nachrichten zur Zustellung aufgelaufen ist. Es stehen auch weitere Optionen zur Verfügung. Falls Sie benutzerdefinierte Zeitpläne erstellen wollen, die Zustellzeiten an bestimmten Tagen vorsehen, nutzen Sie hierzu den entsprechenden Konfigurationsdialog auf der Benutzeroberfläche von MDaemon selbst.

Systemweite Einstellungen für Zustellung und Abruf von Nachrichten

Nachrichten in den Warteschlangen sofort zustellen, soweit möglich
Ist diese Option aktiv, verarbeitet MDaemon jedes Mal dann, wenn eine neue Nachricht an einen externen Empfänger eintrifft und in die Extern-Warteschlange eingestellt wird, alle Nachrichten für externe Empfänger, die innerhalb der Frist eintrafen, die durch die Option *Nur Nachrichten zustellen, die während der letzten [xx] Minuten in die Warteschlange eingestellt wurden* festgelegt wird. Anschließend werden die Nachrichten zugestellt. Der nächste geplante Verarbeitungsdurchlauf oder ein Ereignis, das einen außerplanmäßigen Durchlauf auslöst, werden dann nicht abgewartet.

...auch bei Nachrichten für Gateway-Domänen
Diese Einstellung bewirkt, dass auch Nachrichten an Domänen-Gateways sofort zugestellt werden. Die Einstellung wirkt jedoch nur bei den Gateways, für welche die Einstellung *Gespeicherte Nachrichten bei jedem Verarbeitungsdurchlauf für externe Nachrichten zustellen* aktiv ist. Diese letzte Einstellung ist über den Konfigurationsdialog Gateway 257 des Gateway-Editors zugänglich.

Nur Nachrichten zustellen, die in den letzten [xx] Minuten in die Warteschlange eingestellt wurden (0 = alle senden)
Diese Option bestimmt, wie lange Nachrichten in der Warteschlange stehen, bevor die Option *Nachrichten in den Warteschlangen sofort zustellen, soweit möglich* oben die Zustellung der Nachrichten veranlasst. Tritt die Option oben in Tätigkeit, so stellt MDaemon nicht alle wartenden Nachrichten zu, sondern nur jene, die innerhalb der hier angegebenen Zeit in Minuten in die Warteschlange eingestellt wurden. Die gesamte Warteschlange mit den übrigen Nachrichten wird verarbeitet, wenn ein Verarbeitungsdurchlauf von Hand oder durch den Zeitplan ausgelöst wird. Die Voreinstellung für diese Option beträgt eine Minute. Der Wert 0 bewirkt, dass die gesamte Warteschlange bei jedem Verarbeitungsdurchlauf

abgearbeitet wird; diese Einstellung ist aber deutlich weniger effizient und wird nicht empfohlen.

Die oben beschriebenen Optionen beziehen sich auf den Standard-Zeitplan "Default". Sie sind für benutzerdefinierte Zeitpläne (siehe Option *Name...* unten) nicht verfügbar.

Zeitpläne für die Zustellung

Name...
Aus diesem Rollmenü wählen Sie den Zeitplan aus, den Sie bearbeiten wollen. Der Standard-Zeitplan ("Default") wird immer für die voreingestellte Warteschlange für externe Post sowie für die Post verwendet, die über DomainPOP und MultiPOP abgerufen wurde. Für Systeme, die ihre Internet-Verbindungen als Wählverbindungen herstellen, wird der Standard-Zeitplan auch für LAN-Domänen verwendet, da diese Domänen als externe Domänen definiert sind, die über das lokale Netzwerk ohne Wählverbindung erreichbar sind. Weitere Zeitpläne können mit benutzerdefinierten weiteren Warteschlangen für externe Post verknüpft werden, und Nachrichten können mithilfe des Inhaltsfilters 649 automatisch auf diese benutzerdefinierten Warteschlangen 869 verteilt werden. Nach dem Bearbeiten einer Warteschlange kann der Vorgang durch einen Klick auf OK oder Übernehmen abgeschlossen, oder es kann mit der Bearbeitung weiterer Zeitpläne fortgefahren werden. Wird nach dem Bearbeiten eines Zeitplans unmittelbar ein anderer ausgewählt, so erscheint eine Sicherheitsabfrage, ob die Änderungen gespeichert oder verworfen werden sollen, bevor der andere Zeitplan geladen wird.

Neu
Ein Klick auf dieses Steuerelement legt einen neuen Zeitplan an. Es öffnet sich ein Fenster und fragt den Namen für den Zeitplan ab. Nachdem Sie den Namen vergeben haben, erscheint im Menübaum links ein Eintrag für den neuen Zeitplan für den Nachrichtenversand 383, und Sie können die Zeiteinstellungen und weiteren Optionen für den neuen Zeitplan konfigurieren.

Löschen
Um einen benutzerdefinierten Zeitplan zu löschen, muss der Zeitplan zunächst über das Rollmenü *Name...* ausgewählt werden. Ein Klick auf *Löschen* löscht den Zeitplan sodann. Zuvor wird jedoch eine Sicherheitsabfrage eingeblendet, die den Benutzer fragt, ob er den Zeitplan wirklich löschen will. Wird ein Zeitplan gelöscht, so bleiben etwa mit ihm verknüpfte benutzerdefinierte Warteschlangen für externe Post und Regeln des Inhaltsfilters unberührt. Wird jedoch eine benutzerdefinierte Warteschlange für externe Post gelöscht, so werden auch die mit ihr verknüpften Zeitpläne und Regeln des Inhaltsfilters gelöscht.

Nachrichten in den Warteschlangen in folgendem Intervall (in Minuten) zustellen
Durch Anklicken dieser Option und Verschieben des Zeigers wird das Verarbeitungsintervall für die Postzustellung eingestellt. Es kann zwischen 1 und 60 Minuten betragen. Jeweils nach diesem Zeitablauf verarbeitet MDaemon externe Post, bevor das Intervall neu beginnt. Ist diese Option nicht aktiv, richtet sich die Verarbeitung externer Post nach den übrigen Einstellungen des Zeitplans.

Nachrichten zustellen, sobald der letzte Verarbeitungsdurchlauf [xx] Minuten zurück liegt
Mithilfe dieser Option erfolgt die Verarbeitung externer Post immer nach einer festen Wartezeit nach der Ende des letzten Verarbeitungsdurchlaufs, unabhängig davon, wie der vorhergehende Durchlauf ausgelöst wurde. Anders als bei einer starren Planung mit Wochentag und Uhrzeit oder bei dem oben erläuterten *Intervalltimer* beginnt das Intervall bei dieser Einstellung bei jedem Verarbeitungsdurchlauf, gleich, wie er ausgelöst wurde, von vorn.

Nachrichten zustellen, sobald mindestens [xx] Nachrichten in der Warteschlange stehen
MDaemon löst einen Verarbeitungsdurchlauf immer aus, wenn die Anzahl der Nachrichten in der Extern-Warteschlange den hier angegebenen Wert erreicht oder überschreitet. Diese Durchläufe finden zusätzlich zu den ohnehin geplanten statt.

Nachrichten zustellen, sobald sie mindestens [xx] Minuten alt sind
Ist diese Option aktiv, löst MDaemon immer einen Verarbeitungsdurchlauf aus, wenn eine Nachricht seit der angegebenen Dauer in der Extern-Warteschlange auf den Versand wartet. Diese Durchläufe finden zusätzlich zu den ohnehin geplanten statt.

Warteschlangen

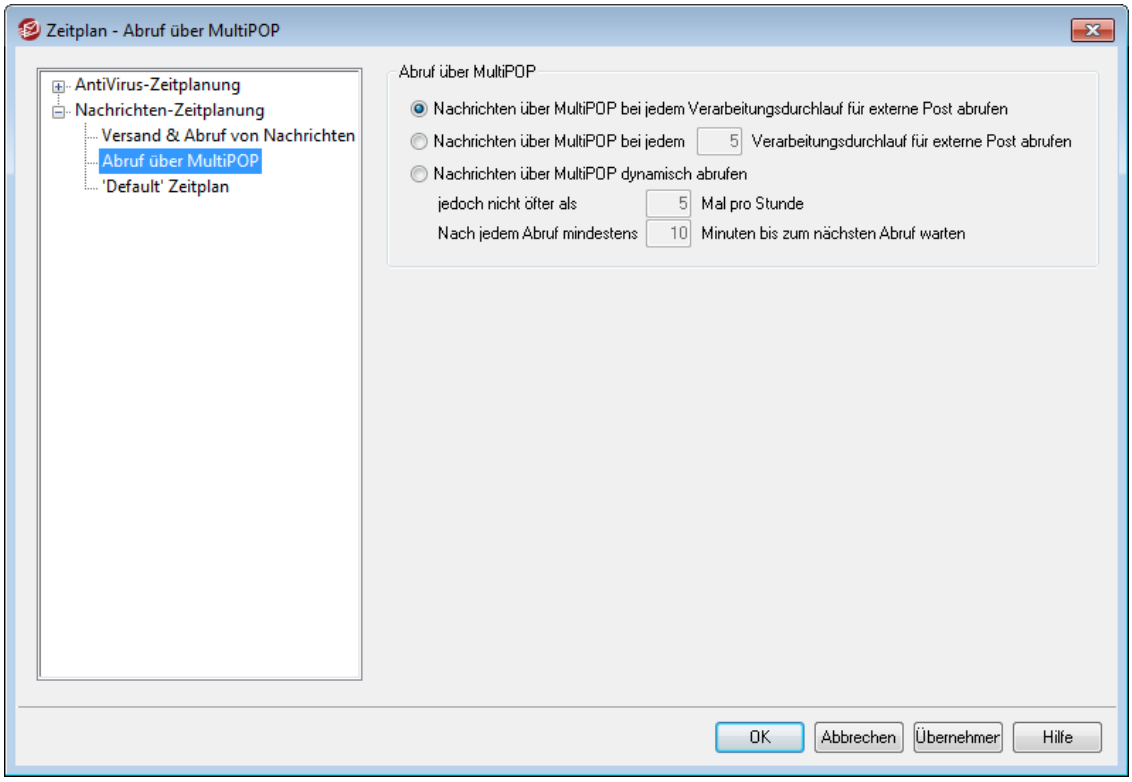
Zeitplan mit folgender Warteschlange verknüpfen
Diese Option bewirkt, dass der ausgewählte Zeitplan mit einer bestimmten benutzerdefinierten Warteschlange für externe Nachrichten verknüpft wird. Mithilfe des Inhaltsfilters lassen sich dann Regeln definieren, die Nachrichten gezielt in die benutzerdefinierte Warteschlange einstellen. Sollen beispielsweise Nachrichten aus Mailinglisten an externe Adressen nur zu bestimmten Zeiten zugestellt werden, so kann für diese Nachrichten eine benutzerdefinierte Warteschlange erstellt werden. Sodann kann eine Regel angelegt werden, die alle diese Nachrichten in die Warteschlange verschiebt, und schließlich wird ein Zeitplan mit den gewünschten Übermittlungszeiten erstellt und mit der Warteschlange verknüpft.

Warteschlangen
Ein Klick auf dieses Steuerelement öffnet den Editor für die Warteschlangen, mit dessen Hilfe benutzerdefinierte Warteschlangen 869 erstellt werden können.

Siehe auch:

Zeitplan für den Nachrichtenversand 383
AntiVirus-Aktualisierungen 376

3.7.2.2 Abruf über MultiPOP



Abruf über MultiPOP

Nachrichten über MultiPOP bei jedem Verarbeitungsdurchlauf für externe Post abrufen
Diese Option veranlasst MDaemon, jedes Mal, wenn externe Post verarbeitet wird, auch Post über MultiPOP 739 abzurufen.

Nachrichten über MultiPOP bei jedem [xx]-ten Verarbeitungsdurchlauf für externe Post abrufen
Mit dieser Option in Verbindung mit einer Zahl im entsprechenden Feld werden Nachrichten über MultiPOP nicht mehr bei jedem Verarbeitungsdurchlauf für externe Nachrichten abgerufen. Die Zahl gibt an, wie oft externe Post verarbeitet wird, bevor der Nachrichtenabruf über MultiPOP statt findet.

Nachrichten über MultiPOP dynamisch abrufen
Diese Option bewirkt den dynamischen Abruf von Post über MultiPOP. Normalerweise werden die Nachrichten über MultiPOP für alle Benutzer, die von dieser Funktion Gebrauch machen, bei jedem Verarbeitungsdurchlauf für externe Post oder in dem gesondert festgelegten Intervall mit abgerufen. Der dynamische Abruf bewirkt, dass Nachrichten über MultiPOP für jeden einzelnen Benutzer erst dann abgerufen werden, wenn dieser Benutzer sein Postfach über POP, IMAP oder Webmail abfragt. Da diese Abfrage den MultiPOP-Abruf aber erst auslöst, erhält der betreffende Benutzer die dann über MultiPOP abgerufenen Nachrichten erst bei seinem nächstfolgenden Zugriff auf sein Postfach. Der Benutzer müsste sein Postfach also zwei Mal abfragen, damit er die neuen MultiPOP-Nachrichten erhält – einmal, um den MultiPOP-Abruf auszulösen, und nochmals, um die dann abgerufenen Nachrichten zu erhalten.

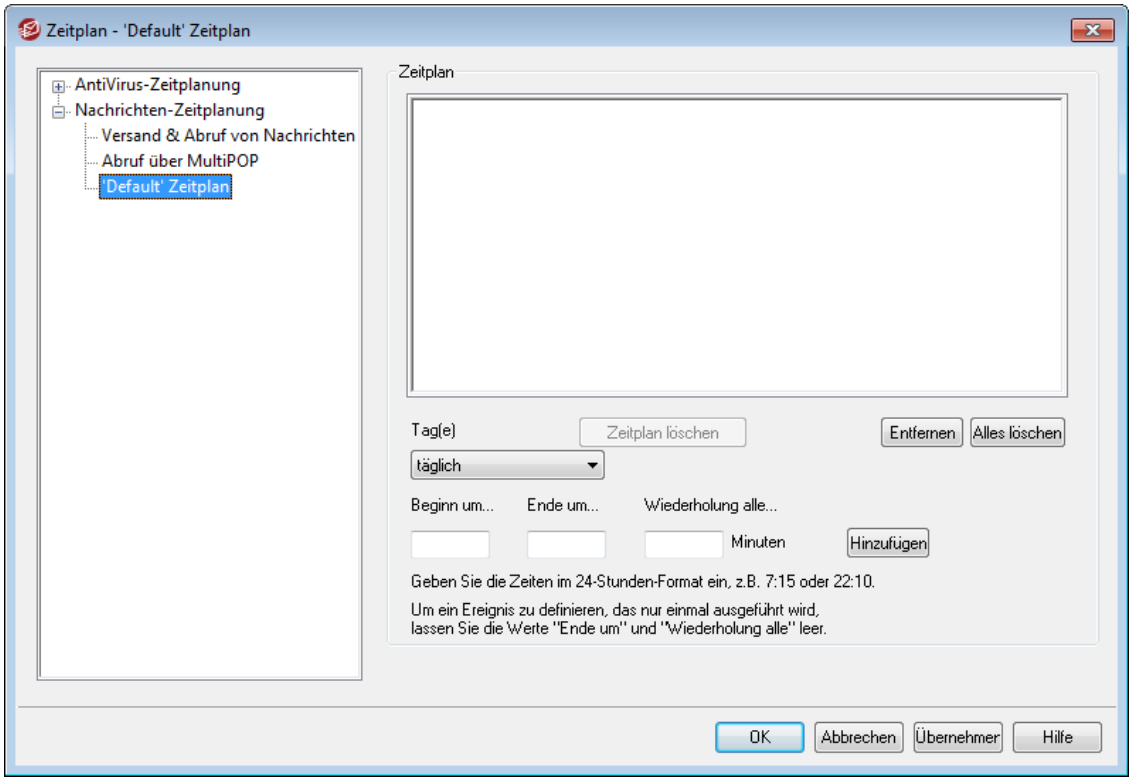
jedoch nicht öfter als [xx] Mal pro Stunde
MultiPOP kann bei intensiver Nutzung die Systemlast beträchtlich erhöhen. Um diesem unerwünschten Effekt vorzubeugen, kann hier eine Höchstgrenze angegeben werden, wie oft pro Stunden MultiPOP-Abfragen für einen Benutzer durchgeführt werden dürfen.

Nach jedem Abruf mindestens [xx] Minuten bis zum nächsten Abruf warten
Auch diese Option dient der Begrenzung der Systemlast auf dem Server; sie steuert, wie oft jeder Benutzer Nachrichten abrufen darf, die über MultiPOP empfangen wurden. Hierzu wird ein Intervall in Minuten festgelegt, während dessen Lauf der Benutzer keine Post über MultiPOP erhalten kann. Geben Sie hier die Zeitdauer in Minuten ein, die Benutzer abwarten müssen, bevor sie Nachrichten wieder über MultiPOP abrufen dürfen

Siehe auch:

MultiPOP 739

3.7.2.3 Zeitplan für den Nachrichtenversand



Für jeden getrennten Zeitplan für den Nachrichtenversand ist im Auswahlmenü *Name* im Konfigurationsdialog Optionen zum Zeitplan für den Nachrichtenversand 378 ein Eintrag vorhanden. Sie können mithilfe der Zeitpläne die Zeiten festlegen, zu denen externe Nachrichten verarbeitet werden. Sie erreichen die einzelnen Zeitpläne über Einstellungen » Zeitplan » Mail Optionen zum Zeitplan für den Nachrichtenversand » 'Name des Zeitplans' Zeitplan.

Zeitplan

Zeitplan löschen
Durch Anklicken dieses Steuerelements löschen Sie den benutzerdefinierten Zeitplan. Nach dem Löschen des Zeitplans wird der zugehörige Eintrag auch aus dem Auswahlmenü *Name* im Konfigurationsdialog Optionen zum Zeitplan für den Nachrichtenversand 378 entfernt. Nach Anklicken des Steuerelements erscheint eine Sicherheitsabfrage, ob die Löschung wirklich gewünscht ist. Sie können nur benutzerdefinierte Zeitpläne löschen, nicht aber den Standard-Zeitplan "Default".

Entfernen
Um einen Eintrag aus der Liste zu entfernen, wählen Sie den Eintrag aus, und klicken Sie dann auf dieses Steuerelement.

Alles löschen
Dieses Steuerelement entfernt alle Einträge aus dem Zeitplan.

Erstellen geplanter Ereignisse

Tag(e)
Um ein neues Ereignis in dem Zeitplan zu planen, wählen Sie zunächst den Tag oder die Tage aus, an denen das Ereignis ausgeführt werden soll. Sie können folgende Auswahl treffen: täglich, Wochentage (Montag bis Freitag), Wochenenden (Samstag und Sonntag), oder einzelne Wochentage.

Beginn um...
Geben Sie hier die Uhrzeit ein, zu der das Ereignis beginnen soll. Die Zeit muss im 24-Stunden-Format zwischen 00:00 und 23:59 Uhr eingegeben werden. Soll das Ereignis nur einmal zu dem angegebenen Zeitpunkt ausgeführt werden und sich nicht wiederholen, so ist dies die einzige Zeitangabe, die Sie machen müssen (lassen Sie dann die Optionen *Beginn um...* und *Wiederholung alle...* leer).

Ende um...
Geben Sie hier die Uhrzeit ein, zu der das Ereignis enden soll. Die Zeit muss im 24-Stunden-Format zwischen 00:00 und 23:59 Uhr eingegeben werden, und sie muss nach der Zeit liegen, die unter *Beginn um...* eingegeben wurde. Ist beispielsweise unter *Beginn um...* der Wert 10:00 eingetragen, so kann der Wert *Ende um...* zwischen 10:01 und 23:59 liegen. Falls Sie ein einmal auszuführendes Ereignis anlegen wollen, lassen Sie dieses Feld leer.

Wiederholung alle [xx] Minuten
Hier geben Sie das Intervall an, in dem das Ereignis zwischen den unter Beginn um... und Ende um... angegebenen Zeiten wiederholt wird. Falls Sie ein einmal auszuführendes Ereignis anlegen wollen, lassen Sie dieses Feld leer.

Hinzufügen
Nachdem Sie die gewünschten Daten in die Felder *Tag(e)*, *Beginn um...*, und ggf. *Ende um...* und *Wiederholung alle...* eingetragen haben, klicken Sie auf dieses Steuerelement, um das Ereignis in den Zeitplan einzutragen.

Je nach Ihren Bedürfnissen können die Optionen zur einfachen Zeitplanung im Konfigurationsdialog Optionen zum Zeitplan für den Nachrichtenversand 378 für Ihre Zwecke ausreichen. Nicht sinnvoll wäre es beispielsweise, einen

> Eintrag für jede Minute eines Tages anzulegen, wenn stattdessen das Intervall einfach auf die Dauer einer Minute konfiguriert werden kann und damit dasselbe Ergebnis erreicht wird. Sollen die Intervalle für externe Nachrichten länger als eine Stunde dauern, oder soll die Verarbeitung nur an bestimmten Wochentagen stattfinden, kann eine Kombination aus dem Intervallzeiger und den sonstigen Einstellungen sinnvoll sein.

Siehe auch:

Optionen zum Zeitplan für den Nachrichtenversand 378
AntiVirus-Aktualisierungen 376
AntiSpam-Aktualisierungen 699

3.8 MDaemon Connector

Das Leistungsmerkmal *MDaemon Connector* (MC) in MDaemon ist ein gesondert zu lizensierendes Leistungsmerkmal, dessen Lizenz von MDaemon Technologies erworben werden kann. MC ermöglicht es den Benutzern, Microsoft Outlook als E-Mail-Client beizubehalten, falls sie dies Wünschen. MC muss hierzu auf den Rechnern der Benutzer installiert sein. MD bietet Groupware-Funktionen und Leistungsmerkmale für die Online-Zusammenarbeit. MC stellt die Verbindung zwischen den Outlook-Clients der Benutzer und ihrem MDaemon-Server her. Die Benutzer können dann die Leistungsmerkmale für E-Mail, Kalender mit Frei/Gebucht-Informationen, Adressbücher, Verteilerliste und Notizen in Microsoft Outlook verwenden.

Ist die Unterstützung für den MC aktiv, so sind die Konfigurationsdialoge für den MDaemon Connector über die Menüleiste von MDaemon unter `Einstellungen » MDaemon Connector` erreichbar. Mithilfe dieser Konfigurationsdialoge können Sie MC konfigurieren und bestimmten Benutzerkonten die Berechtigung erteilen, MC zu nutzen.

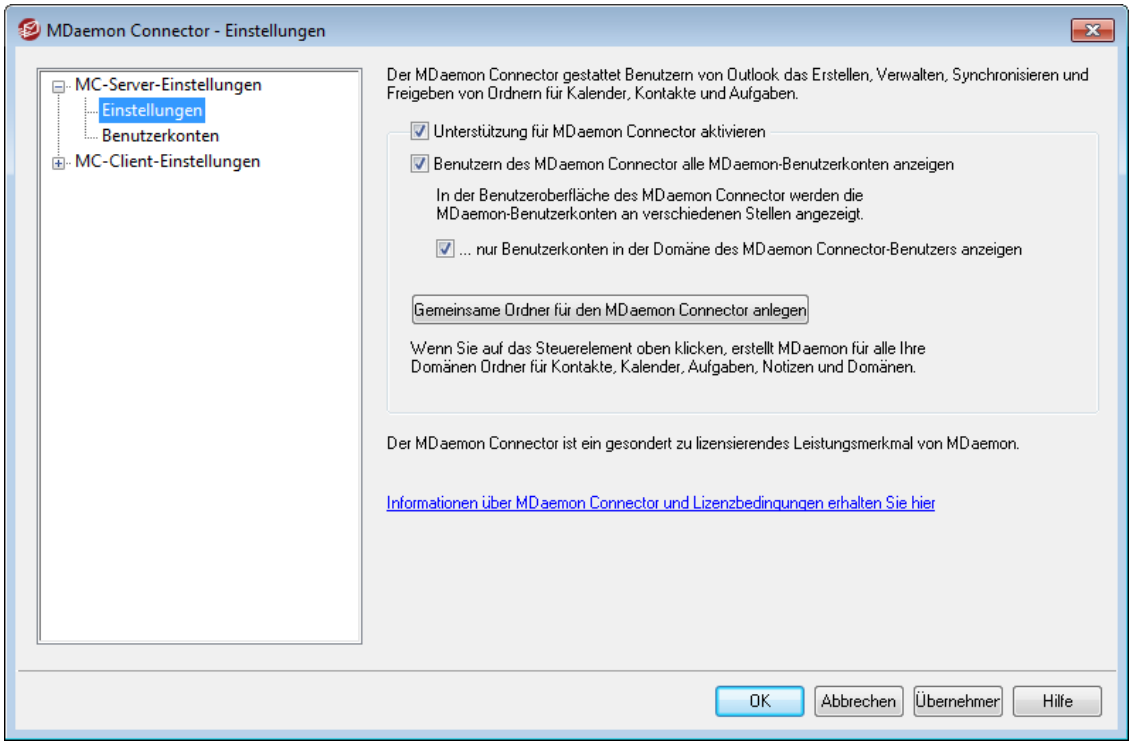
Nähere Informationen über den MDaemon Connector und den Erwerb einer Lizenz finden Sie auf der Seite MDaemon Connector der Website www.mdaemon.com.

Siehe auch:

MC-Server-Einstellungen » Einstellungen 386
MC-Server-Einstellungen » Benutzerkonten 387
MC-Client-Einstellungen 388

3.8.1 MC-Server-Einstellungen

3.8.1.1 Einstellungen



MDaemon Connector

Unterstützung für MDaemon- Connector aktivieren
Diese Option aktiviert das Leistungsmerkmal MDaemon Connector (MC). Die Benutzer können die Funktionen des MDaemon Connectors erst nutzen, wenn diese Option aktiv ist.

Benutzern des MDaemon Connectors alle MDaemon-Benutzerkonten anzeigen
Diese Option bewirkt, dass alle für den MDaemon Connector freigeschalteten Benutzerkonten im Abschnitt für Berechtigungen angezeigt werden, der Teil des MDaemon-Connector-Plugins für Microsoft Outlook ist. Bei Verwendung des MDaemon-Connector-Plugins zur gemeinsamen Nutzung von Outlook-Elementen können die MDaemon-Connector-Benutzer aus dieser Liste jene Benutzerkonten auswählen, denen sie Berechtigungen zuweisen wollen. Ist diese Option abgeschaltet, so bleibt die Benutzerliste im Abschnitt Berechtigungen des MDaemon-Connector-Plugins leer, und die Benutzer müssen die E-Mail-Adressen der gewünschten anderen Benutzerkonten von Hand eintragen. Ein Benutzerkonto darf seine Outlook-Elemente nur dann zur gemeinsamen Nutzung freigeben, wenn es für den MDaemon Connector freigeschaltet ist. Trägt ein Benutzer die Adresse eines nicht freigeschalteten Benutzerkontos in den MDaemon Connector ein, so werden die Outlook-Elemente erst dann für die gemeinsame Nutzung mit diesem anderen Benutzerkonto freigegeben, wenn es, ggf. auch später, auf dem Server auch für den MDaemon Connector freigeschaltet wird.

...nur Benutzerkonten in der Domäne des MDaemon-Connector-Benutzers anzeigen
Diese Option ist nur verfügbar, wenn die oben beschriebene Option *Benutzern des MDaemon-Connectors alle MDaemon-Benutzerkonten anzeigen* aktiv ist. Soll ein Benutzer im Abschnitt Berechtigungen des MDaemon-Connector-

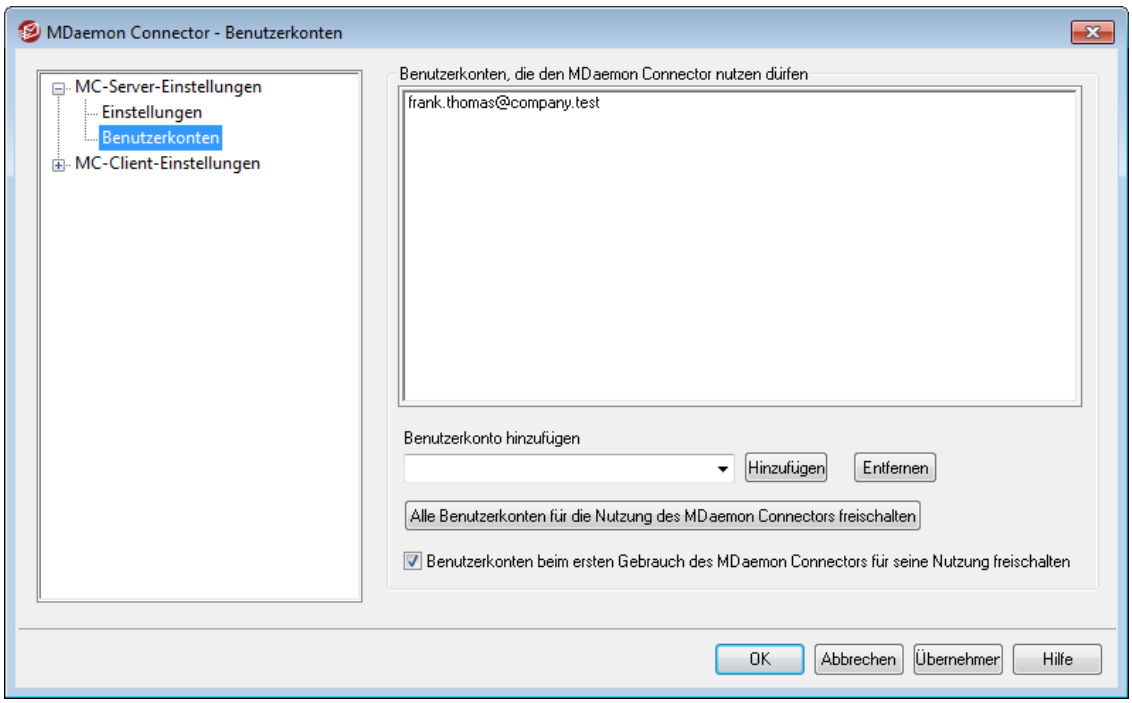
Plugins nur solche Benutzerkonten sehen, die seiner eigenen Domäne angehören und für den MDaemon Connector freigeschaltet sind, so muss diese Option aktiviert werden. Für den MDaemon Connector freigeschaltete Benutzerkonten anderer Domänen erscheinen dann in der Liste nicht, auch wenn sie selbst zur Nutzung des MDaemon Connectors berechtigt sind.

Gemeinsame Ordner für den MDaemon Connector anlegen
Ein Klick auf dieses Steuerelement bewirkt, dass MDaemon einen Standardsatz Ordner für den MDaemon Connector für jede Domäne anlegt. Dabei werden folgende Ordner angelegt: Kontakte, Termine, Journal, Aufgaben und Notizen.

Siehe auch:

MC-Server-Einstellungen » Benutzerkonten 387
MC-Client-Einstellungen 388

3.8.1.2 Benutzerkonten



Benutzerkonten, die den MDaemon Connector nutzen dürfen

In dieser Liste sind die MDaemon-Benutzerkonten aufgeführt, die mithilfe des MDaemon Connectors ihre Outlook-Ordner zur gemeinsamen Nutzung freigeben dürfen. Zu diesen Outlook-Ordnern gehören insbesondere auch Kalender, Kontakte und Notizen. Mithilfe der nachfolgend beschriebenen Optionen können Sie dieser Liste Benutzerkonten hinzufügen.

Benutzerkonto hinzufügen
Um der Liste der Benutzerkonten, die den MDaemon Connector nutzen dürfen, ein MDaemon-Benutzerkonto hinzuzufügen, wählen Sie aus diesem Auswahlmenü das gewünschte Benutzerkonto aus, und klicken Sie dann auf *Hinzufügen*. Um ein Benutzerkonto aus der Liste zu entfernen, wählen Sie aus diesem Auswahlmenü das gewünschte Benutzerkonto aus, und klicken Sie dann auf *Entfernen*.

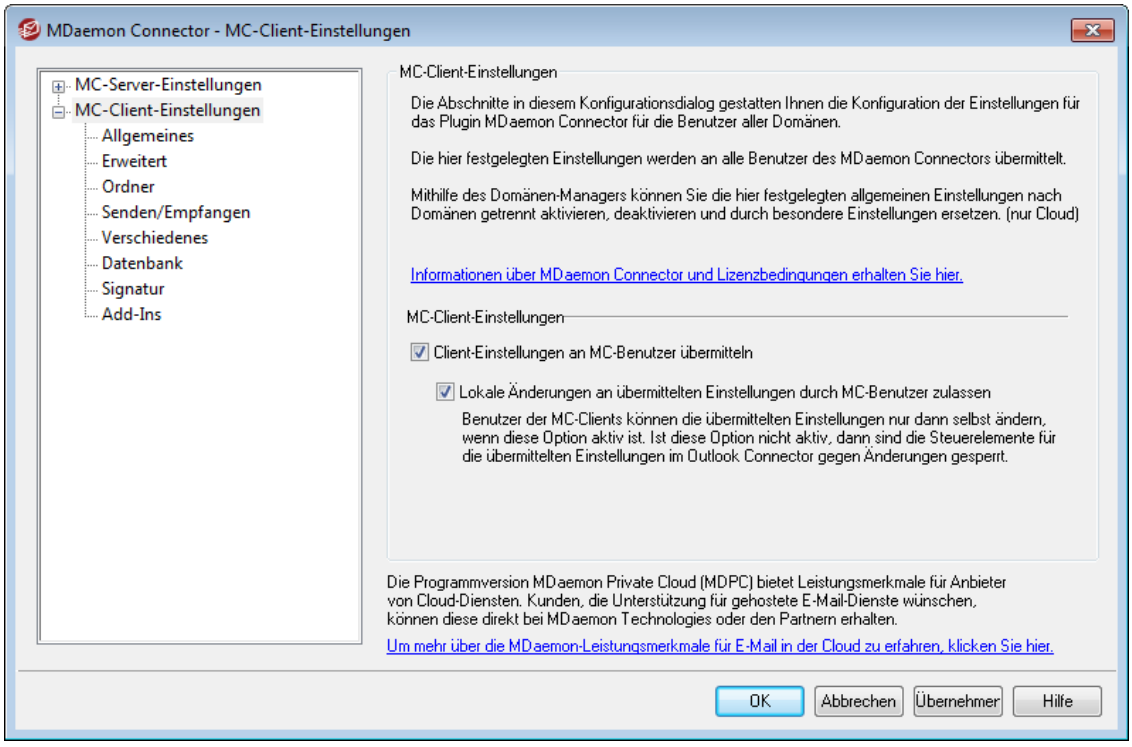
Alle Benutzerkonten für die Nutzung des MDaemon Connectors freischalten
Durch Anklicken dieses Steuerelements schalten Sie alle MDaemon-Benutzerkonten unmittelbar für die Nutzung des MDaemon Connectors frei. Nach dem Anklicken dieses Steuerelements erscheinen alle MDaemon-Benutzerkonten in der Liste der *Benutzerkonten, die den MDaemon Connector nutzen dürfen*.

Benutzerkonten beim ersten Gebrauch des MDaemon Connectors für seine Nutzung freischalten
Diese Option bewirkt, dass ein Benutzerkonto automatisch in die Liste der *Benutzerkonten, die den MDaemon Connector nutzen dürfen*, aufgenommen und für die Nutzung des MDaemon Connectors automatisch freigeschaltet wird, sobald das Benutzerkonto zum ersten Mal eine Verbindung mithilfe des MDaemon Connectors herstellt. **Beachte:** Damit bewirkt diese Option im Ergebnis zugleich, dass alle MDaemon-Benutzerkonten für die Nutzung des MDaemon Connectors freigeschaltet sind. Die Benutzerkonten erscheinen nur nicht in der Liste der Benutzerkonten, solange sie den MDaemon Connector nicht wenigstens einmal genutzt haben.

Siehe auch:

MC-Server-Einstellungen » Einstellungen 386
MC-Client-Einstellungen 388

3.8.2 MC-Client-Einstellungen



Mithilfe des Konfigurationsdialog MC-Client-Einstellungen können Sie die Client-Einstellungen für die Benutzer des MDaemon Connectors verwalten. Die Client-Einstellungen, die Sie in den zugehörigen Konfigurationsdialogen festlegen, übermittelt MDaemon jedes Mal dann an die betroffenen Clients, wenn diese eine Verbindung mit dem Server herstellen. Die Einstellungen werden dann in die zugehörigen Konfigurationsdialoge des MDaemon Connectors übernommen. Die MC-

Client-Einstellungen werden dabei nur dann an die Clients übermittelt, wenn sie sich seit der letzten Übermittlung der Einstellungen an die Clients geändert haben. Mithilfe der Option "*Lokale Änderungen an übermittelten Einstellungen durch MC-Benutzer zulassen*" bestimmen Sie, ob die Benutzer die zentral verwalteten und übermittelten Einstellungen auf ihren Clients ändern dürfen. Ist die Option aktiv, so können die Benutzer die Einstellungen in den Konfigurationsdialogen lokal ändern. Ist die Option nicht aktiv, so sind die Konfigurationsdialoge im MDaemon Connector gegen Änderungen durch die Benutzer gesperrt, und die Benutzer können die zentral verwalteten und übermittelten Einstellungen nicht ändern.

Bestimmte Einstellungen müssen zwangsläufig für die Benutzer oder für Domänen einzeln unterschiedlich getroffen werden. In den MC-Client-Einstellungen sind daher Makros, wie etwa `$USERNAME$`, `$EMAIL$` und `$DOMAIN$` zugelassen. Diese Makros werden bei der Übermittlung der Einstellungen an die Clients durch Daten ersetzt, die sich auf Benutzer oder Domänen einzeln beziehen. Die Festlegung statischer Einstellungen in solchen Feldern, die dynamisch belegt sein müssen, ist zu vermeiden. Wird beispielsweise der Name "Frank Thomas" in der Einstellung "Ihr Name" festgelegt, so wird der Name jedes Benutzers des MDaemon Connectors in "Frank Thomas" geändert, sobald er eine Verbindung mit MDaemon herstellt. Der Abschnitt Allgemeines 391 enthält zur Vereinfachung eine Schaltfläche "*Makro-Übersicht*", mit deren Hilfe Sie eine einfache Liste der unterstützten Makros aufrufen können.

Bei Nutzung von MDaemon Private Cloud steht im Domänen-Manager 181 ein weiterer Konfigurationsdialog MC-Client-Einstellungen zur Verfügung, in dem die Client-Einstellungen für den MDaemon Connector nach Domänen getrennt verwaltet werden können.

Dieses Leistungsmerkmal ist per Voreinstellung abgeschaltet. Es erfordert den MDaemon Connector ab der Client-Version 4.0.0.

MC-Client-Einstellungen

Client-Einstellungen an MC-Benutzer übermitteln
Diese Option bewirkt, dass die Client-Einstellungen, die Sie in den folgenden Konfigurationsdialogen festlegen, bei jedem Verbindungsaufbau durch den MDaemon Connector an die Clients übermittelt werden. Die Einstellungen werden dabei nur übermittelt, falls sich seit der letzten Übermittlung der Einstellungen an die Clients die Einstellungen geändert haben. Diese Option ist per Voreinstellung abgeschaltet.

Lokale Änderungen an übermittelten Einstellungen durch MC-Benutzer zulassen
Diese Option bewirkt, dass die Benutzer die ihnen übermittelten Einstellungen in ihren Clients ändern können. Ist diese Option abgeschaltet, so sind die Konfigurationsdialoge der Outlook-Connector-Clients gegen Änderungen gesperrt, und die Benutzer können keine Änderungen an den Einstellungen vornehmen.

Nehmen Benutzer lokale Änderungen an den zentral verwalteten und übermittelten Einstellungen vor, so verhindert dies nicht die spätere erneute Übermittlung zentral verwalteter Einstellungen und deren Wirksamkeit. Ändert ein Benutzer bestimmte Einstellungen seines MDaemon Connectors, und ändert danach der Administrator die zentral verwalteten Einstellungen, dann werden beim

nächstfolgenden Verbindungsaufbau alle zentral verwalteten Einstellungen erneut an den Client übermittelt. Hierbei werden auch die durch den Benutzer selbst vorgenommenen lokalen Änderungen überschrieben, sodass die übermittelten Einstellungen wieder ohne lokale Änderungen wirksam sind.

Automatische Erkennung der MC-Einstellungen

Benutzer des MDaemon Connectors können während der ersten Konfiguration des Plugins auf ihren Clients im Abschnitt "*Allgemeine Einstellungen*" die Schaltfläche "*Kontoeinstellungen ermitteln und prüfen*" anklicken, sobald sie *Benutzernamen* und *Kennwort* eingegeben haben. Der MDaemon Connector versucht dann, die Server-Daten für das Benutzerkonto automatisch zu ermitteln und die Anmeldedaten auf Gültigkeit zu prüfen.

Um die Verbindung mit dem Server herzustellen, versucht der MDaemon Connector zunächst, allgemein bekannte FQDN- und Servernamen zu nutzen.

Für die IMAP-Verbindung versucht der MDaemon Connector zunächst der Aufbau einer verschlüsselten Verbindung mit `mail.<Domäne>` (z.B. `mail.example.com`) über den besonderen SSL-Port und dann über den normalen Port mit TLS. Gelingt der Verbindungsaufbau mit diesen Daten nicht, so wiederholt der MDaemon Connector den Vorgang mit `imap.<Domäne>`, dann mit `<Domäne>` und schließlich mit `imap.mail.<Domäne>`. Schlagen alle diese Versuche fehl, so wiederholt der MDaemon Connector den gesamten Vorgang mit den genannten Daten in der genannten Reihenfolge, aber ohne Verschlüsselung.

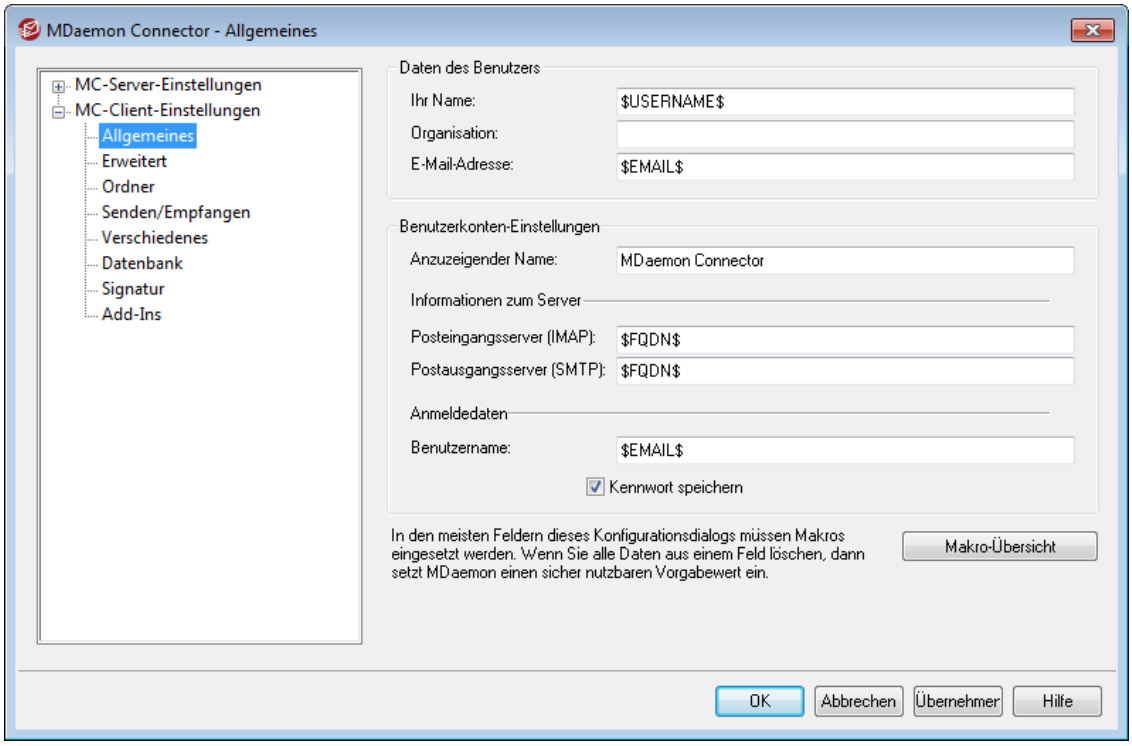
Für die SMTP-Verbindung versucht der MDaemon Connector zunächst den Aufbau einer Verschlüsselten Verbindung mit `mail.<Domäne>` über die Ports 587, 25 und schließlich 465, jeweils zunächst per SSL und dann per TLS. Gelingt der Verbindungsaufbau mit diesen Daten nicht, so wiederholt der MDaemon Connector den Vorgang mit `smtp.<Domäne>`, `<Domäne>` und schließlich mit `smtp.mail.<Domäne>`. Schlagen alle diese Versuche fehl, so wiederholt der MDaemon Connector den gesamten Vorgang mit den genannten Daten in der genannten Reihenfolge, aber ohne Verschlüsselung.

Kann der MDaemon Connector die Verbindung herstellen, und sind dabei auch die Anmeldedaten gültig, so speichert der MDaemon Connector die ermittelten Daten und das Verschlüsselungsverfahren und konfiguriert den Zugang zum Server damit automatisch.

Siehe auch:

MC-Server-Einstellungen » Einstellungen 386
MC-Server-Einstellungen » Benutzerkonten 387
MC-Client-Einstellungen 388

3.8.2.1 Allgemeines



Ist die Option "*Client-Einstellungen an MC-Benutzer übermitteln*" im Abschnitt MC-Client-Einstellungen 388 aktiv, so werden die nachfolgend getroffenen Einstellungen an die MDaemon-Connector-Clients übermittelt, sobald diese eine Verbindung mit dem Server herstellen. Die nachfolgend getroffenen Einstellungen steuern dabei im MDaemon-Connector-Client die Einstellungen im Abschnitt "*Allgemeine Einstellungen*". Die Einstellungen werden nur dann übermittelt, wenn sie sich seit dem letzten Verbindungsaufbau durch den Client geändert haben. Die meisten nachfolgend aufgeführten Felder sollen nicht statische Daten sondern Makros enthalten. Nähere Informationen finden Sie in der Übersicht über die Makros 392 weiter unten.

Daten des Benutzers

Ihr Name
Per Voreinstellung nutzt diese Option das Makro $USERNAME$. Es wird in den Vor- und Nachnamen des Benutzers umgesetzt. Vor- und Nachname erscheinen in der Absenderkopfzeile From der Nachrichten, die der Benutzer versendet.

Organisation
Hier kann der Name des Unternehmens oder der Organisation eingetragen werden.

E-Mail Adresse
Per Voreinstellung nutzt diese Option das Makro $EMAIL$. Es wird in die E-Mail-Adresse des Benutzers umgesetzt. Die E-Mail-Adresse erscheint in der Absenderkopfzeile From der Nachrichten, die der Benutzer versendet.

Benutzerkonten-Einstellungen

Anzuzeigender Name
Dieser Name wird in Outlook als Name für das Benutzerkonto angezeigt und gestattet dem Benutzer die Unterscheidung mehrerer Benutzerkonten innerhalb desselben Profils. Der Name wird nur dem Benutzer selbst angezeigt. Die Voreinstellung lautet "MDaemon Connector".

Informationen zum Server

Posteingangsserver (IMAP)
Hier wird der Hostname des Servers eingetragen, über den der MDaemon-Connector-Client eingehende Nachrichten erhält und verwaltet. Diese Option nutzt per Voreinstellung das Makro $FQDN$.

Postausgangsserver (SMTP)
Hier wird der Hostname des Servers eingetragen, über den der MDaemon-Connector-Client abgehende Nachrichten versendet. Dieser Hostname entspricht in vielen Fällen dem des Posteingangsservers. Diese Option nutzt per Voreinstellung das Makro $FQDN$.

Anmeldedaten

Benutzername
Hier wird der Benutzername eingetragen, mit dem sich der Benutzer an seinem MDaemon-Benutzerkonto über den MDaemon Connector anmeldet, um Zugriff auf sein Benutzerkonto zu erhalten und es zu verwalten. Üblicherweise entspricht der Benutzername der weiter oben festgelegten *E-Mail-Adresse*. Diese Option nutzt per Voreinstellung das Makro $EMAIL$.

Kennwort speichern
Per Voreinstellung speichern die MDaemon-Connector-Clients das Kennwort für den Zugang zum jeweiligen Benutzerkonto. Wird Microsoft Outlook gestartet, so kann sich der MDaemon Connector mit dem E-Mail-Konto anmelden, ohne die Zugangsdaten vom Benutzer abzufragen. Falls Sie wünschen, dass die Benutzer das Kennwort beim Programmstart von Microsoft Outlook jedes Mal neu eingeben müssen, deaktivieren Sie diese Option.

Übersicht über die Makros

Die MC-Client-Einstellungen unterstützen Makros, sodass Einstellungen für verschiedene Benutzer und Domänen dynamisch angepasst werden können. Zu den unterstützten Makros gehören `$USERNAME$`, `$EMAIL$` und `$DOMAIN$`. Diese Makros werden bei der Übermittlung der Konfigurationsdaten an die Clients automatisch durch Daten des jeweiligen Benutzers oder der jeweiligen Domäne ersetzt. Beim Festlegen der einzelnen Optionen muss darauf geachtet werden, dass keine statischen Daten in solche Felder eingetragen werden, deren Inhalte nach Benutzern unterschiedlich sein müssen. Ein Beispiel hierfür ist der Eintrag "Frank Thomas" im Feld *Ihr Name*. Dieser Eintrag würde dazu führen, dass Vor- und Nachname jedes MDaemon-Connector-Benutzers nach dem folgenden Verbindungsaufbau in "Frank Thomas" geändert wird. Die Liste der verfügbaren Makros können Sie durch Anklicken der Schaltfläche *Makro-Übersicht* einsehen.

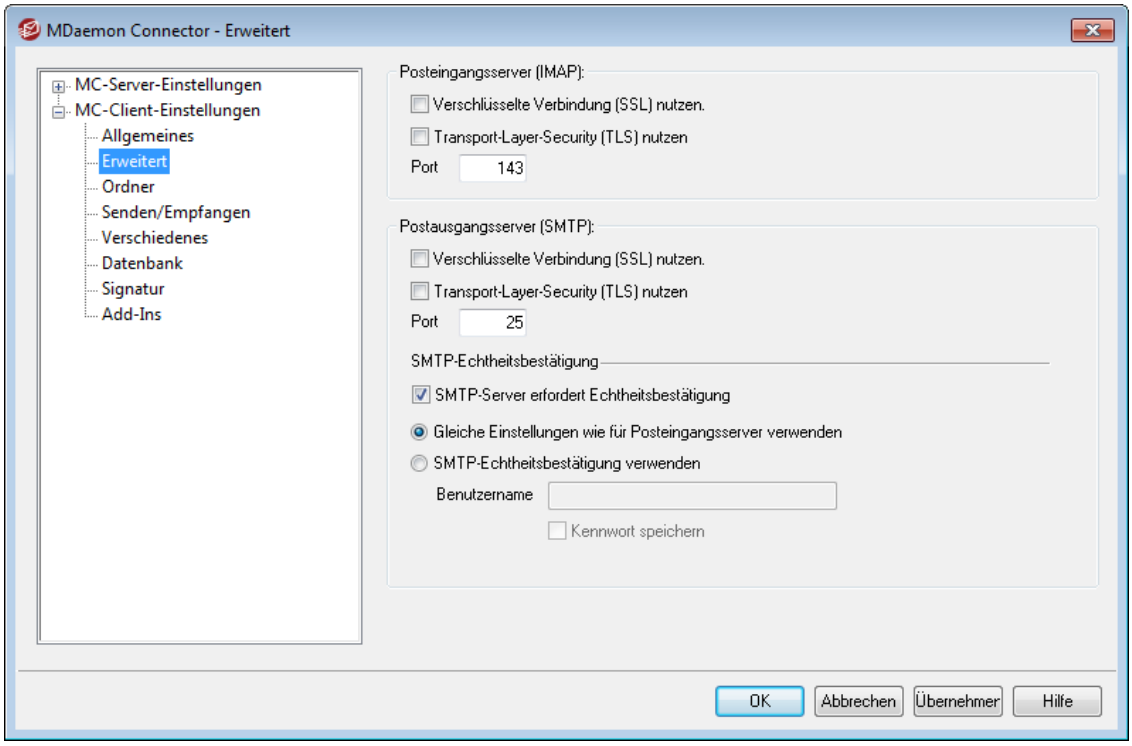
$USERNAME$	Dieses Makro wird in den vollständigen *Vor- und Nachnamen* aus dem Konfigurationsdialog Einzelheiten zum Benutzerkonto[714] des jeweiligen Benutzerkontos umgesetzt.
$EMAIL$	Dieses Makro wird in die E-Mail-Adresse des jeweiligen Benutzerkontos umgesetzt. Es entspricht der Makrokette $MAILBOX$@$DOMAIN$.
$MAILBOX$	Dieses Benutzerkonto wird in den Postfachnamen[714] des jeweiligen Benutzerkontos umgesetzt.
$USERFIRSTNAME$	Dieses Makro wird in den Vornamen des Inhabers des Benutzerkontos umgesetzt.
$USERFIRSTNAMELC$	Dieses Makro wird in den Vornamen des Inhabers des Benutzerkontos in Kleinbuchstaben umgesetzt.
$USERLASTNAME$	Dieses Makro wird in den Nachnamen des Inhabers des Benutzerkontos umgesetzt.
$USERLASTNAMELC$	Dieses Makro wird in den Nachnamen des Inhabers des Benutzerkontos in Kleinbuchstaben umgesetzt.
$USERFIRSTINITIAL$	Dieses Makro wird in den ersten Buchstaben des Vornamens des Inhabers des Benutzerkontos umgesetzt.
$USERFIRSTINITIALLC$	Dieses Makro wird in den ersten Buchstaben des Vornamens des Inhabers des Benutzerkontos in Kleinbuchstaben umgesetzt.
$USERLASTINITIAL$	Dieses Makro wird in den ersten Buchstaben des Nachnamens des Inhabers des Benutzerkontos umgesetzt.
$USERLASTINITIALLC$	Dieses Makro wird in den ersten Buchstaben des Nachnamens des Inhabers des Benutzerkontos in Kleinbuchstaben umgesetzt.
$MAILBOXFIRSTCHARSn$	"n" ist hierbei eine Zahl zwischen 1 und 10. Dieses Makro wird in die ersten "n" Zeichen des Postfachnamens umgesetzt.
$DOMAIN$	Dieses Makro wird in den Domänennamen[714] umgesetzt, der für das Benutzerkonto ausgewählt wurde.

$DOMAINIP$	Dieses Makro wird in die IPv4-Adresse[184] umgesetzt, die mit der Domäne verknüpft ist, die für das Benutzerkonto ausgewählt wurde.
$DOMAINIP6$	Dieses Makro wird in die IPv6-Adresse[184] umgesetzt, die mit der Domäne verknüpft ist, die für das Benutzerkonto ausgewählt wurde.
$FQDN$	Dieses Makro wird in den vollqualifizierten Domänennamen oder SMTP-Hostnamen[184] der Domäne umgesetzt, die für das Benutzerkonto ausgewählt wurde.
$PRIMARYDOMAIN$	Dieses Makro wird durch den Namen der Standard-Domäne[181] von MDaemon ersetzt.
$PRIMARYIP$	Dieses Makro wird durch die IPv4-Adresse[184] ersetzt, die mit der Standard-Domäne[181] von MDaemon verknüpft ist.
$PRIMARYIP6$	Dieses Makro wird durch die IPv6-Adresse[184] ersetzt, die mit der Standard-Domäne[181] von MDaemon verknüpft ist.

Siehe auch:

MC-Client-Einstellungen[388]
MC-Server-Einstellungen » Einstellungen[386]
MC-Server-Einstellungen » Benutzerkonten[387]

3.8.2.2 Erweitert



Ist die Option "*Client-Einstellungen an MC-Benutzer übermitteln*" im Abschnitt MC-Client-Einstellungen 388 aktiv, so werden die nachfolgend getroffenen Einstellungen an die MDaemon-Connector-Clients übermittelt, sobald diese eine Verbindung mit dem Server herstellen. Die nachfolgend getroffenen Einstellungen steuern dabei im MDaemon-Connector-Client die Einstellungen im Abschnitt "*Erweiterte Einstellungen*". Die Einstellungen werden nur dann übermittelt, wenn sie sich seit dem letzten Verbindungsaufbau durch den Client geändert haben.

Posteingangsserver (IMAP)

Verschlüsselte Verbindung (SSL) nutzen
Diese Option bewirkt, dass für die Verbindungen zum Posteingangsserver (IMAP) die Verschlüsselung über SSL genutzt wird. Wenn diese Option aktiv ist, wird der verwendete Port automatisch auf 993 geändert, da dies der Standard-SSL-Port für IMAP-Verbindungen ist.

Transport-Layer-Security (TLS) nutzen
Diese Option bewirkt, dass für die Verbindungen zum Posteingangsserver (IMAP) die Verschlüsselung über TLS genutzt wird.

Port
Auf dem hier eingestellten Port stellen die MDaemon-Connector-Clients Verbindungen zum Posteingangsserver (IMAP) her. Die Voreinstellung lautet 143 für normale IMAP-Verbindungen und 993 für SSL-verschlüsselte IMAP-Verbindungen.

Postausgangsserver (SMTP)

Verschlüsselte Verbindung (SSL) nutzen
Diese Option bewirkt, dass für die Verbindungen zum Postausgangsserver (SMTP) die Verschlüsselung über SSL genutzt wird. Wenn diese Option aktiv ist, wird der

verwendete Port automatisch auf 465 geändert, da dies der Standard-SSL-Port für SMTP-Verbindungen ist.

Transport-Layer-Security (TLS) nutzen
Diese Option bewirkt, dass für die Verbindungen zum Postausgangsserver (SMTP) die Verschlüsselung über TLS genutzt wird.

Port
Auf dem hier eingestellten Port stellen die MDaemon-Connector-Clients Verbindungen zum Postausgangsserver (SMTP) her. Die Voreinstellung lautet 25 für normale SMTP-Verbindungen und 465 für SSL-verschlüsselte SMTP-Verbindungen.

SMTP-Echtheitsbestätigung

SMTP-Server erfordert Echtheitsbestätigung
Viele Server verlangen auch beim Versand eine Anmeldung des Benutzers mit Benutzername und Kennwort. Diese Option, die per Voreinstellung aktiv ist, bewirkt, dass die Anmeldung auch beim Versand von Nachrichten über den Postausgangsserver (SMTP) erfolgt.

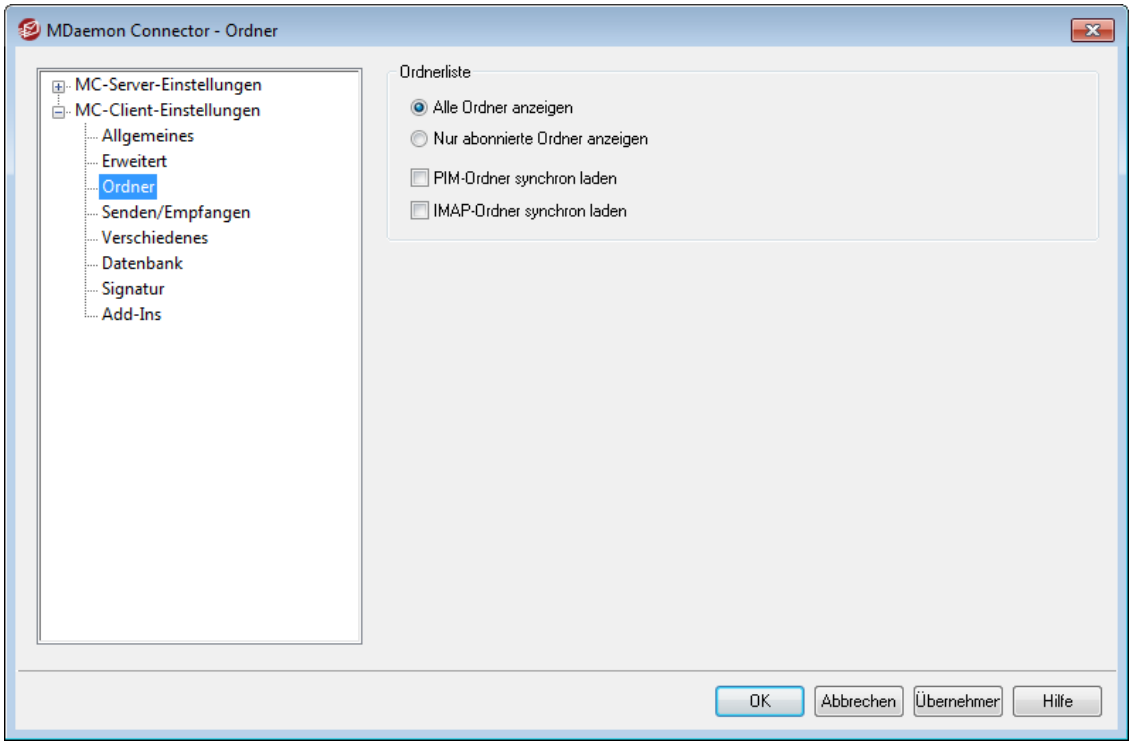
Gleiche Einstellungen wie für Posteingangsserver verwenden
Diese Option bewirkt, dass für die Anmeldung am Postausgangsserver (SMTP) dieselben Anmeldedaten wie für die Anmeldung am Posteingangsserver (IMAP) genutzt werden. Die Option ist per Voreinstellung aktiv.

SMTP-Echtheitsbestätigung verwenden
Mithilfe dieser Option können für die Anmeldung am Postausgangsserver eigene Anmeldedaten angegeben werden, die von den Anmeldedaten für den Posteingangsserver abweichen. Dies kann beispielsweise erforderlich sein, wenn Nachrichten nicht über denselben Server versandt und empfangen werden.

Siehe auch:

MC-Client-Einstellungen 388
MC-Server-Einstellungen » Einstellungen 386
MC-Server-Einstellungen » Benutzerkonten 387

3.8.2.3 Ordner



Ist die Option "*Client-Einstellungen an MC-Benutzer übermitteln*" im Abschnitt MC-Client-Einstellungen 388 aktiv, so werden die nachfolgend getroffenen Einstellungen an die MDaemon-Connector-Clients übermittelt, sobald diese eine Verbindung mit dem Server herstellen. Die nachfolgend getroffenen Einstellungen steuern dabei im MDaemon-Connector-Client die Einstellungen im Abschnitt "*Ordner*". Die Einstellungen werden nur dann übermittelt, wenn sie sich seit dem letzten Verbindungsaufbau durch den Client geändert haben.

Ordnerliste

Alle Ordner anzeigen
Diese Option bewirkt, dass in der Ordnerliste in Outlook alle Ordner auf dem Server erscheinen, auf die der Benutzer des MDaemon Connectors Zugriff hat. Diese Option ist per Voreinstellung aktiv.

Nur abonnierte Ordner anzeigen
Diese Option bewirkt, dass in der Ordnerliste in Outlook nur die Ordner auf dem Server erscheinen, die der Benutzer des MDaemon Connectors abonniert hat.

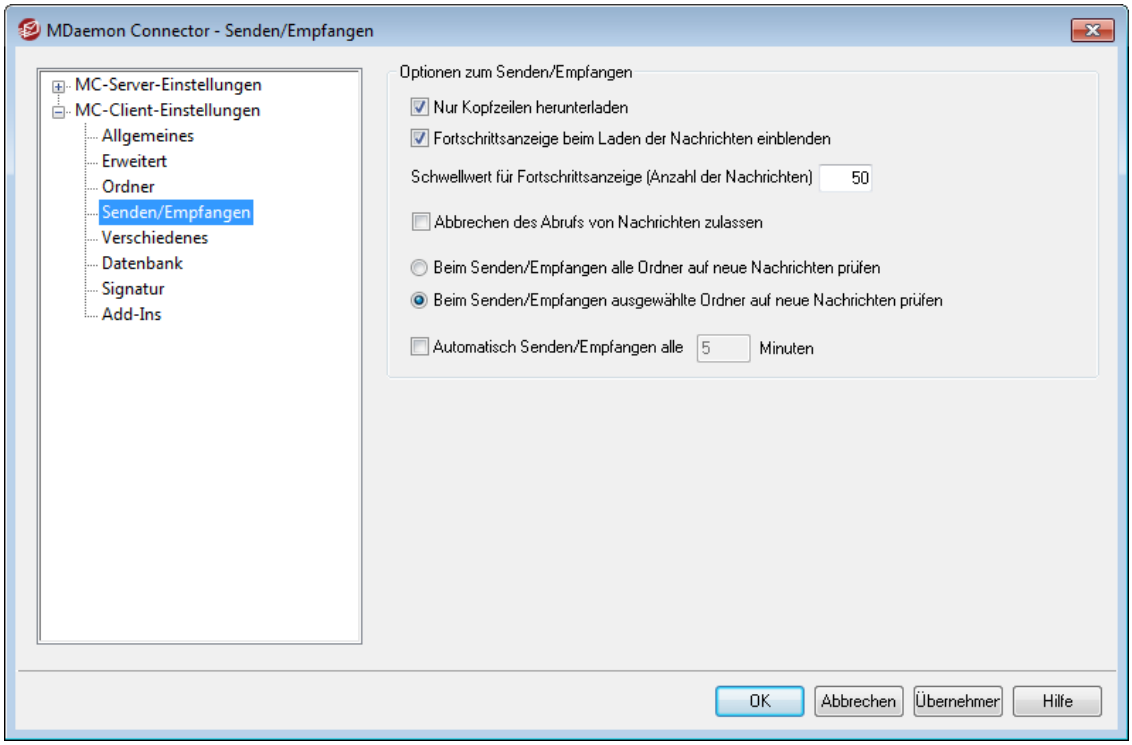
PIM-Ordner synchron laden
Während der MDaemon Connector die Inhalte aus Ordnern mit PIM-Elementen (Ordner, die keine E-Mail-Ordner sind, etwa Kontakte, Kalender und Aufgaben) lädt, können die Benutzer Microsoft Outlook weiterhin nutzen. Wird diese Option aktiviert, so ist Microsoft Outlook während dieser Ladevorgänge für andere Nutzung blockiert, bis alle Daten übermittelt sind. Diese Option sollte daher nur aktiviert werden, wenn sie wirklich gebraucht wird, beispielsweise, weil auf dem Client Software von Drittanbietern installiert ist, die auf die Inhalte der PIM-Ordner zugreift.

IMAP-Ordner synchron laden
Während der MDaemon Connector die Inhalte aus IMAP-Ordnern mit E-Mail-Nachrichten, können die Benutzer Microsoft Outlook weiterhin nutzen. Wird diese Option aktiviert, so ist Microsoft Outlook während dieser Ladevorgänge für andere Nutzung blockiert, bis alle Daten übermittelt sind. Diese Option sollte daher nur aktiviert werden, wenn sie wirklich gebraucht wird, beispielsweise, weil auf dem Client Software von Drittanbietern installiert ist, die auf die Inhalte der E-Mail-Ordner zugreift.

Siehe auch:

MC-Client-Einstellungen 388
MC-Server-Einstellungen » Einstellungen 386
MC-Server-Einstellungen » Benutzerkonten 387

3.8.2.4 Senden/Empfangen



Ist die Option "*Client-Einstellungen an MC-Benutzer übermitteln*" im Abschnitt MC-Client-Einstellungen 388 aktiv, so werden die nachfolgend getroffenen Einstellungen an die MDaemon-Connector-Clients übermittelt, sobald diese eine Verbindung mit dem Server herstellen. Die nachfolgend getroffenen Einstellungen steuern dabei im MDaemon-Connector-Client die Einstellungen im Abschnitt "*Senden/Empfangen*". Die Einstellungen werden nur dann übermittelt, wenn sie sich seit dem letzten Verbindungsaufbau durch den Client geändert haben.

Optionen zum Senden/Empfangen

Nur Kopfzeilen herunterladen
Diese Option bewirkt, dass der MDaemon Connector beim Senden/Empfangen neue Nachrichten nicht sofort vollständig herunterlädt, sondern zunächst nur die

Kopfzeilen (An, Von, Betreff usw.) abruft, sodass sie in der Nachrichtenliste angezeigt werden können. Die vollständigen Nachrichten werden erst abgerufen, wenn der Benutzer sie auch betrachten will. Diese Option ist per Voreinstellung aktiv.

Fortschrittsanzeige beim Laden der Nachrichten einblenden
Diese Option bewirkt, dass der MDaemon Connector bei Übermittlung einer größeren Zahl von Nachrichten eine Fortschrittsanzeige einblendet. Um die Fortschrittsanzeige zu unterdrücken, deaktivieren Sie diese Option.

Schwellwert für Fortschrittsanzeige (Anzahl der Nachrichten)
Ist die Option *Fortschrittsanzeige beim Laden der Nachrichten einblenden* aktiv, so erscheint die Fortschrittsanzeige nur, falls mindestens die hier angegebene Anzahl von Nachrichten abgerufen wird.

Abbrechen des Abrufs von Nachrichten zulassen
Diese Option bewirkt, dass die Benutzer des MDaemon Connectors den Abruf von Nachrichten abbrechen können, beispielsweise während Microsoft Outlook große Nachrichten abruft.

Beim Senden/Empfangen alle Ordner auf neue Nachrichten prüfen
Diese Option bewirkt, dass der MDaemon Connector beim Senden/Empfangen alle E-Mail-Ordner auf neue Nachrichten überprüft.

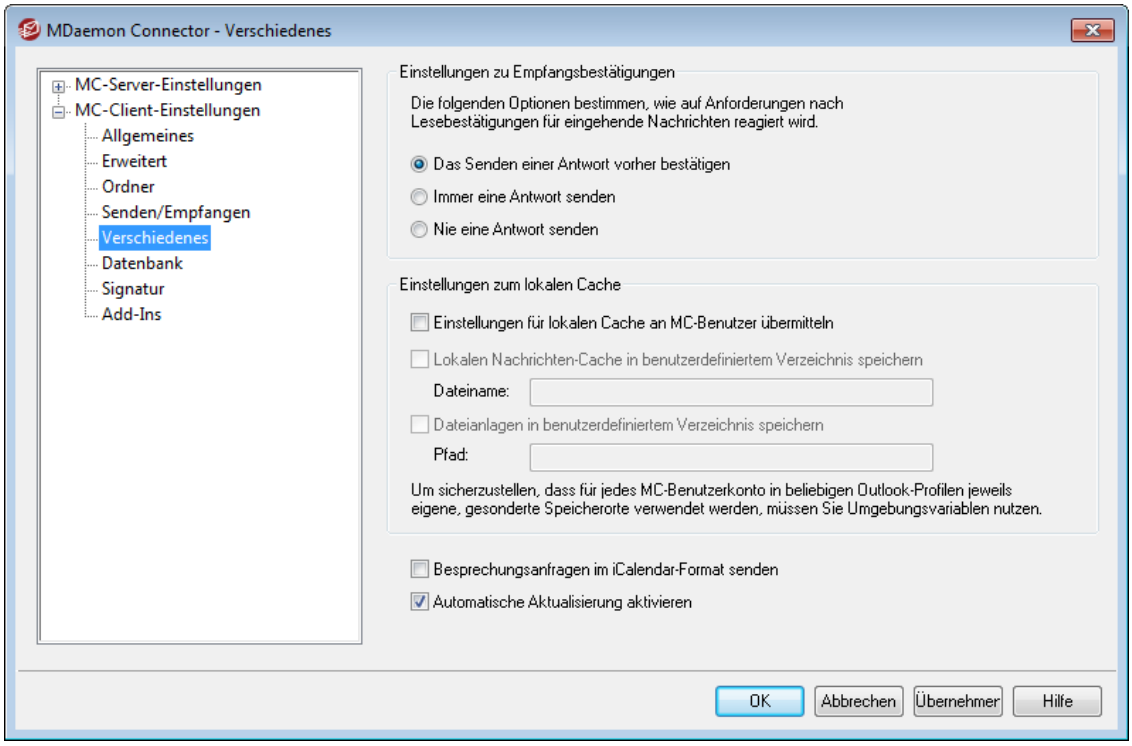
Beim Senden/Empfangen ausgewählte Ordner auf neue Nachrichten prüfen
Diese Option bewirkt, dass der MDaemon Connector beim Senden/Empfangen nur bestimmte, durch den Benutzer ausgewählte Ordner auf neue Nachrichten überprüft.

Automatisch Senden/Empfangen alle [xx] Minuten
Diese Option bewirkt, dass der MDaemon Connector in dem hier in Minuten angegebenen Intervall das Senden und Empfangen von Nachrichten durchführt.

Siehe auch:

MC-Client-Einstellungen 388
MC-Server-Einstellungen » Einstellungen 386
MC-Server-Einstellungen » Benutzerkonten 387

3.8.2.5 Verschiedenes



Ist die Option "*Client-Einstellungen an MC-Benutzer übermitteln*" im Abschnitt MC-Client-Einstellungen 388 aktiv, so werden die nachfolgend getroffenen Einstellungen an die MDaemon-Connector-Clients übermittelt, sobald diese eine Verbindung mit dem Server herstellen. Die nachfolgend getroffenen Einstellungen steuern dabei im MDaemon-Connector-Client die Einstellungen im Abschnitt "*Verschiedenes*". Die Einstellungen werden nur dann übermittelt, wenn sie sich seit dem letzten Verbindungsaufbau durch den Client geändert haben.

Einstellungen zu Empfangsbestätigungen

Eingehende Nachrichten können besondere Kopfzeilen enthalten, durch die eine Lesebestätigung als automatische Antwort an den Absender angefordert wird. Sie teilt dem Absender mit, wann der Empfänger die Nachricht gelesen hat. Die folgenden Optionen steuern, wie der MDaemon Connector solche Anforderungen nach Empfangsbestätigungen behandelt.

Das Senden einer Antwort vorher bestätigen
Diese Option bewirkt, dass der Benutzer in jedem Einzelfall gefragt wird, ob er die Lesebestätigung versenden will. Die Abfrage erscheint, wenn der Benutzer eine Nachricht öffnet, für die der Absender eine Lesebestätigung angefordert hat.

Immer eine Antwort senden
Diese Option bewirkt, dass Lesebestätigungen ohne Rückfrage automatisch versendet werden. Die Lesebestätigung wird dann ohne weiteres versendet, wenn der Benutzer eine Nachricht öffnet, für die der Absender eine Lesebestätigung angefordert hat.

Nie eine Antwort senden
Diese Option bewirkt, dass der MDaemon Connector keine Lesebestätigungen versendet. Es erscheint auch keine Abfrage.

Einstellungen zum lokalen Cache

Die Optionen in diesem Abschnitt bestimmen, in welchen Verzeichnispfaden der lokale Nachrichten-Cache und die Dateianlagen für die Benutzer des MDaemon Connectors gespeichert werden.

Diese Optionen sind nur wirksam, wenn der MDaemon Connector in in einer Version ab 4.5.0 verwendet wird.

Einstellungen für lokalen Cache an MC-Benutzer übermitteln
Per Voreinstellung übermittelt MDaemon diese Einstellungen nicht an die MDaemon-Connector-Clients. Der MDaemon-Connector-Client verschiebt dann die lokal gespeicherten Dateien vom derzeitigen Verzeichnis in das Standard-Verzeichnis oder, falls ein bestimmtes Verzeichnis angegeben ist, in dieses.

Lokalen Nachrichten-Cache in benutzerdefiniertem Verzeichnis speichern (Dateiname)
Mithilfe dieser Option können Sie den lokalen Nachrichten-Cache der MDaemon-Connector-Clients in einem bestimmten Verzeichnis und unter einem bestimmten Dateinamen speichern. Geben Sie hierzu Pfad und Dateinamen an. Sie sollten dabei Umgebungsvariablen und Makros einsetzen, um sicherzugehen, dass für jeden Benutzer ein eigener Verzeichnispfad verwendet wird. Ein Beispiel hierzu:

```
%APPDATA%\Alt-N\Outlook Connector 2.0\Accounts\%OUTLOOKPROFILE%\
  %OUTLOOKEMAIL%\LocalCache.db
```

Dateianlagen in benutzerdefiniertem Verzeichnis speichern (Pfad)
Falls Sie den Verzeichnispfad anpassen wollen, an dem die MDaemon-Connector-Clients die Dateianlagen speichern, geben Sie den gewünschten Pfad hier an. Sie sollten dabei Umgebungsvariablen und Makros einsetzen, um sicherzugehen, dass für jeden Benutzer ein eigener Verzeichnispfad verwendet wird.

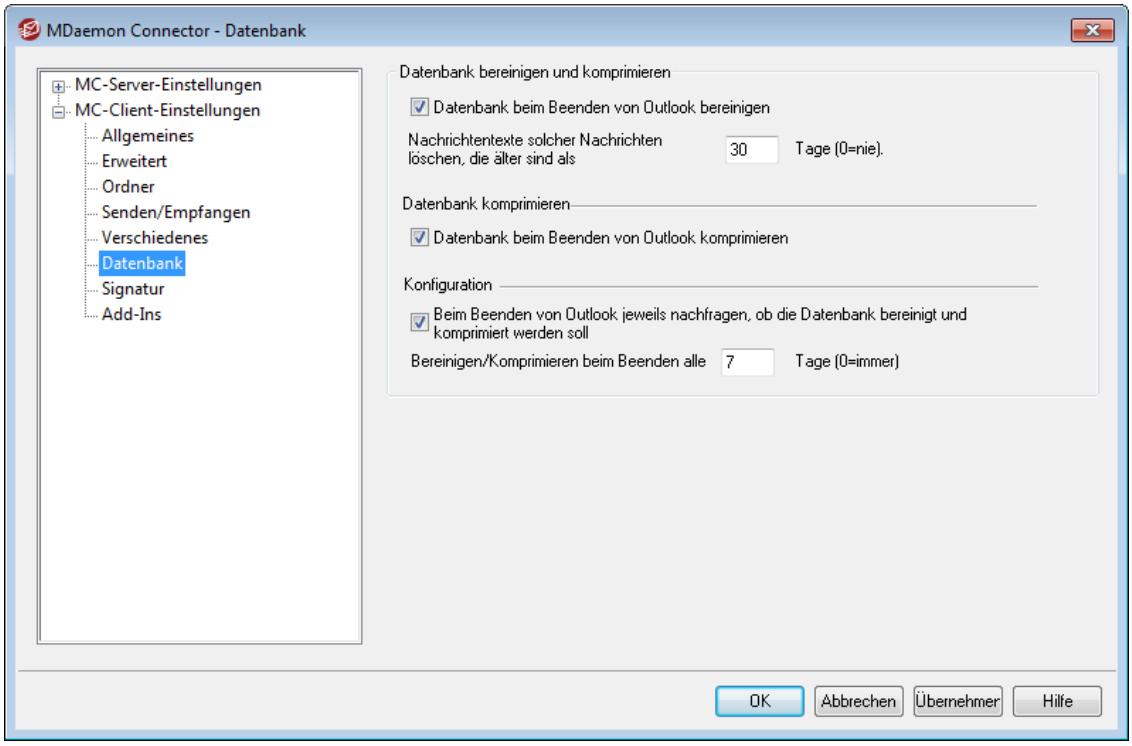
Besprechungsanfragen im iCalendar-Format senden
Diese Option bewirkt, dass der MDaemon Connector Besprechungsanfragen im Format iCalendar (iCal) versendet.

Automatische Aktualisierung aktivieren
Diese Option bewirkt, dass der MDaemon Connector automatisch aktualisiert wird, sobald eine neue Version verfügbar ist. Diese Option ist per Voreinstellung aktiv. Falls Sie die automatische Aktualisierung nicht wünschen, deaktivieren Sie diese Option.

Siehe auch:

MC-Client-Einstellungen 388
MC-Server-Einstellungen » Einstellungen 386
MC-Server-Einstellungen » Benutzerkonten 387

3.8.2.6 Datenbank



Ist die Option "*Client-Einstellungen an MC-Benutzer übermitteln*" im Abschnitt MC-Client-Einstellungen 388 aktiv, so werden die nachfolgend getroffenen Einstellungen an die MDaemon-Connector-Clients übermittelt, sobald diese eine Verbindung mit dem Server herstellen. Die nachfolgend getroffenen Einstellungen steuern dabei im MDaemon-Connector-Client die Einstellungen im Abschnitt "*Verwaltung der Datenbank*". Die Einstellungen werden nur dann übermittelt, wenn sie sich seit dem letzten Verbindungsaufbau durch den Client geändert haben.

Datenbank bereinigen und komprimieren

Datenbank beim Beenden von Outlook bereinigen
Um Speicherplatz zu sparen und die Leistung zu erhöhen, löscht der MDaemon Connector beim Beenden von Microsoft Outlook die Nachrichtentexte alter Nachrichten aus der Datenbank. Die Kopfzeilen der Nachrichten, und die Nachrichten auf dem Server selbst, bleiben dabei erhalten. Es werden nur die lokalen Kopien der Nachrichtentexte gelöscht. Ruft der Benutzer danach eine solche Nachricht erneut auf, dann wird der Nachrichtentext erneut auf den Client übermittelt. Die Bereinigung betrifft nur E-Mail-Nachrichten, nicht jedoch Kontakte, Kalender, Aufgaben, Journale und Notizen. Diese Option ist per Voreinstellung aktiv. Falls Sie die Bereinigung beim Beenden von Microsoft Outlook nicht wünschen, deaktivieren Sie diese Option.

Nachrichtentexte solcher Nachrichten löschen, die älter sind als XX Tage (0=nie)
Diese Option bestimmt das Höchstalter der Nachrichten, ab dem die Nachrichtentexte während der Bereinigung beim Beenden von Microsoft Outlook aus der Datenbank gelöscht werden. Per Voreinstellung werden Nachrichtentexte gelöscht, die älter sind als 30 Tage. Das Alter rechnet von dem Datum, an dem die Nachricht zuletzt geändert wurde. Der Wert 0 bewirkt, dass alte Nachrichtentexte nicht aus der Datenbank gelöscht werden.

Datenbank komprimieren

Datenbank beim Beenden von Outlook komprimieren
Um Speicherplatz zu sparen und die Leistung zu erhöhen, komprimiert und defragmentiert der MDaemon Connector seine Datenbankdatei, die die lokal zwischengespeicherten Kopien der Nachrichten enthält, beim Beenden von Microsoft Outlook. Die Komprimierung wird jedoch nur durchgeführt, wenn Microsoft Outlook ordnungsgemäß beendet wurde. Stürzt Microsoft Outlook ab, oder wird Microsoft Outlook durch den Benutzer über den Taskmanager zwangsweise beendet, so wird die Datenbank nicht komprimiert. Diese Option ist per Voreinstellung aktiv. Die folgernden Optionen im Abschnitt Konfiguration bestimmen, wie oft die Datenbank komprimiert wird, und ob der Benutzer jeweils vorher gefragt wird, ob die Komprimierung durchgeführt werden soll.

Konfiguration

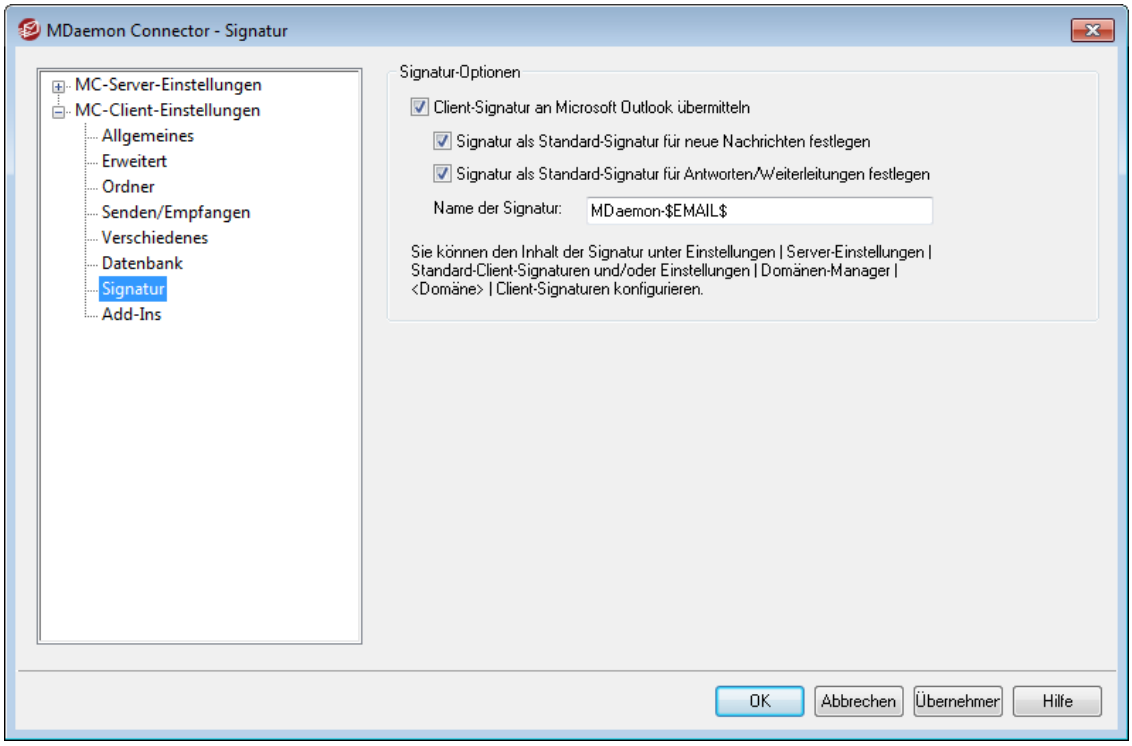
Beim Beenden von Outlook jeweils nachfragen, ob die Datenbank bereinigt und komprimiert werden soll
Diese Option bewirkt, dass der Benutzer beim Beenden von Microsoft Outlook jeweils gefragt wird, ob der MDaemon Connector die Datenbank bereinigen und komprimieren soll. Bestätigt der Benutzer die Abfrage, so werden Bereinigung und Komprimierung durchgeführt, und es erscheint eine Fortschrittsanzeige. Ist diese Option nicht aktiv, so werden Bereinigung und Komprimierung beim Beenden von Microsoft Outlook automatisch durchgeführt, ohne dass der Benutzer gefragt wird; es erscheint dabei eine Fortschrittsanzeige.

Bereinigen/Komprimieren beim Beenden alle XX Tage (0=immer)
Diese Option bestimmt, wie oft der MDaemon Connector die Datenbank beim Beenden bereinigt und komprimiert. Per Voreinstellung werden Bereinigung und Komprimierung alle 7 Tage durchgeführt. Der Wert 0 bewirkt, dass die Datenbank bei jedem Beenden von Microsoft Outlook bereinigt und komprimiert wird.

Siehe auch:

MC-Client-Einstellungen 388
MC-Server-Einstellungen » Einstellungen 386
MC-Server-Einstellungen » Benutzerkonten 387

3.8.2.7 Signatur



Ist die Option "*Client-Einstellungen an MC-Benutzer übermitteln*" im Konfigurationsdialog MC-Client-Einstellungen 388 aktiv, so werden bestimmte Einstellungen aus dem Konfigurationsdialog Signatur in den Konfigurationsdialog Signaturen in Microsoft Outlook übermittelt. Dieser Konfigurationsdialog ist in Microsoft Outlook erreichbar unter **Datei» Optionen » E-Mail » Signaturen**). Die Konfigurationsdaten werden immer dann übermittelt, wenn ein Benutzer mit dem MDaemon Connector eine Verbindung zum Server herstellt. Dieses Leistungsmerkmal erfordert den MDaemon Connector ab Version 6.5.0.

Signatur-Optionen

Client-Signatur an Microsoft Outlook übermitteln
Um die Standard-Client-Signatur 140 oder eine für die Domäne konfigurierte besondere Client-Signatur 206 an Ihre MDaemon-Connector-Benutzer zu übermitteln, aktivieren Sie diese Option. Sie können die Bezeichnung der Signatur im Feld *Name der Signatur* weiter unten konfigurieren.

Signatur als Standard-Signatur für neue Nachrichten festlegen
Diese Option bewirkt, dass die Client-Signatur als Standard-Signatur beim Verfassen neuer Nachrichten verwendet wird.

Signatur als Standard-Signatur für neue Antworten/Weiterleitungen festlegen
Diese Option bewirkt, dass die Client-Signatur als Standard-Signatur in Antworten und weitergeleiteten Nachrichten verwendet wird.

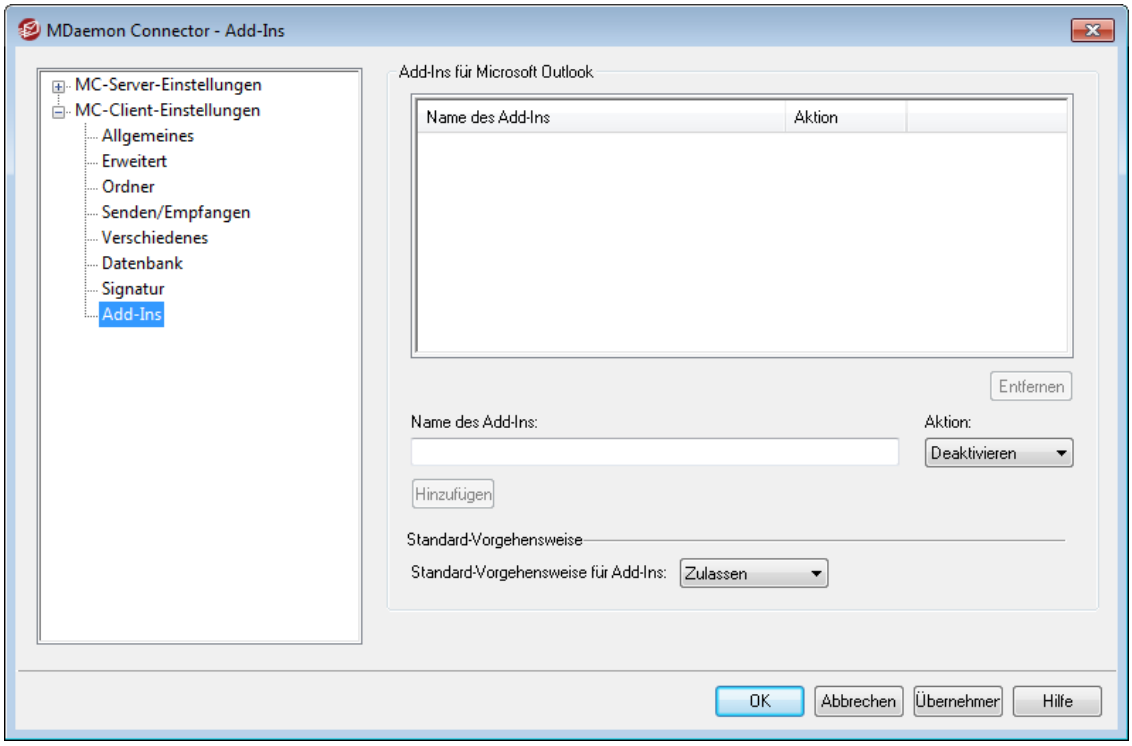
Name der Signatur:
Dieses Feld enthält die Bezeichnung der Signatur. Sie wird bei der Übermittlung an die Benutzer des MDaemon Connectors verwendet, und unter ihr erscheint die Signatur im E-Mail-Konto der Benutzer in Microsoft Outlook. Per Voreinstellung lautet die Bezeichnung "`MDaemon-$EMAIL$`". Das Makro

$EMAIL$ wird dabei in die E-Mail-Adresse des jeweiligen Benutzers umgesetzt. Ein Beispiel hierzu: "`MDaemon-Frank.Thomas@company.test`".

Siehe auch:

MC-Client-Einstellungen 388
MC-Server-Einstellungen » Einstellungen 386
MC-Server-Einstellungen » Benutzerkonten 387
Standard-Client-Signaturen 140
Domänen-Manager » Client-Signaturen 206

3.8.2.8 Add-Ins



Die Einstellungen im Konfigurationsdialog Add-Ins steuern die Nutzung von Add-Ins für Microsoft Outlook durch Ihre MDaemon-Connector-Benutzer. Sie können die Nutzung einzelner oder aller Add-Ins freigeben, und Sie können einzelne Add-Ins wahlweise deaktivieren. Dieses Leistungsmerkmal ist insbesondere dann nützlich, wenn bekannt ist, dass bestimmte Add-Ins einen Konflikt mit dem MDaemon Connector verursachen; Sie können solche Add-Ins deaktivieren, um Problemen vorzubeugen. Das Leistungsmerkmal Add-Ins erfordert den MDaemon Connector ab Version 5.0.

Add-Ins für Microsoft Outlook

In diesem Bereich erscheinen eine Liste der Add-Ins Ihrer Benutzer für Microsoft Outlook und die Aktion, die den Add-Ins zugeordnet ist: *Deaktivieren*, *Zulassen* oder *Standard*. Startet ein MDaemon-Connector-Benutzer Microsoft Outlook, so übermittelt der MDaemon Connector die Liste der Add-Ins, die der Benutzer verwendet, an den MDaemon Connector. Der MC-Client deaktiviert sodann alle Add-Ins, die auf "*Deaktiviert*" gesetzt sind. Add-Ins, die auf "*Zulassen*" gesetzt sind, bleiben unberührt. Add-Ins, die auf "*Standard*" gesetzt sind, werden nach Maßgabe

der *Standard-Vorgehensweise für Add-Ins* behandelt, die weiter unten festgelegt wird.

Der MDaemon Connector kann die Add-Ins in Microsoft Outlook nur für solche Benutzer verwalten, die Ihr MDaemon-Connector-Benutzerkonto in Microsoft Outlook als Standard-Benutzerkonto eingerichtet haben.

Hinzufügen, Entfernen und Bearbeiten von Add-Ins

Hinzufügen eines Add-Ins

Um der Liste ein Add-In hinzuzufügen, geben Sie den *Namen des Add-Ins* so ein, wie er in Microsoft Outlook erscheint, wählen Sie die gewünschte *Aktion*, und klicken Sie danach auf **Hinzufügen**. Diese Option ist insbesondere dann hilfreich, wenn Ihnen Add-Ins bekannt sind, die Sie verwalten wollen, aber noch kein Benutzer eine Verbindung hergestellt hat, auf dessen Rechner diese Add-Ins installiert sind.

Entfernen eines Add-Ins

Um ein Add-In aus der Liste zu löschen, wählen Sie das Add-In in der Liste aus, und klicken Sie danach auf *Entfernen*.

Bearbeiten der Aktion für ein Add-In

Um ein Add-In zu bearbeiten, wählen Sie das Add-In in der Liste aus, wählen Sie anschließend die gewünschte *Aktion* aus dem Dropdown-Menü aus, und klicken Sie zum Abschluss auf **Hinzufügen**.

Standard-Vorgehensweise

Standard-Vorgehensweise für Add-Ins

Sie können diese Option auf *Zulassen* oder *Deaktivieren* setzen. Ist die Standard-Vorgehensweise *Zulassen*, so deaktiviert der MDaemon Connector per Voreinstellung nur solche Add-Ins, die in der Liste auf "*Deaktivieren*" gesetzt sind. Alle anderen Add-Ins bleiben unberührt. Bei Auswahl der Einstellung *Deaktivieren* deaktiviert der MDaemon Connector automatisch alle Add-Ins, die in der Liste nicht auf "*Zulassen*" gesetzt sind. Die Voreinstellung ist *Zulassen*.

Siehe auch:

MC-Client-Einstellungen 388
MC-Server-Einstellungen » Einstellungen 386
MC-Server-Einstellungen » Benutzerkonten 387

3.9 Cluster-Dienst

Die Leistungsmerkmale für den Cluster-Betrieb von MDaemon ermöglichen die gemeinsame Nutzung Ihrer Konfiguration durch mehrere MDaemon-Server in Ihrem Netzwerk. Hiermit können Sie beispielsweise Lastverteilung für die Hardware- oder Software-Auslastung umsetzen und die im E-Mail-Betrieb anfallende Systemlast auf mehrere MDaemon-Server verteilen. Dies kann durch möglichst große Ausnutzung Ihrer E-Mail-Ressourcen Verarbeitungsgeschwindigkeit und Effizienz erhöhen, die Netzwerkauslastung senken und Überlastungen verringern. Es kann außerdem die

Ausfallsicherheit Ihrer E-Mail-Systeme in den Fällen erhöhen, in denen auf einem Server ein Hardware- oder Softwareausfall eintritt.

Die nachfolgende Übersicht soll Ihnen die Kriterien vermitteln, nach denen Sie entscheiden können, ob Sie in Ihrem Netzwerk den Cluster-Betrieb für MDaemon einführen wollen:

Knoten

MDaemon-Cluster bestehen aus einem Primär- und einem oder mehreren Sekundärknoten, die auch als Primär- und Sekundär-Server bezeichnet werden. In jedem Cluster müssen ein MDaemon-Server zum Primär-Knoten und alle anderen MDaemon-Server zu Sekundärknoten bestimmt werden.

- Die Konfiguration des MDaemon-Servers der als Primärknoten arbeitet, wird auf alle anderen Knoten repliziert. Daher können Konfigurationsänderungen nur auf dem Primärknoten durchgeführt werden. Falls Sie auf einen Sekundärknoten zugreifen und dort Konfigurationsänderungen vornehmen, werden diese Änderungen überschrieben. Auf der Benutzeroberfläche der Sekundärknoten stehen daher die meisten Konfigurationsoptionen nicht zur Verfügung.
- Der Cluster-Dienst repliziert nicht die Nachrichten-Verzeichnisse der Benutzerkonten und die öffentlichen Ordner zwischen den Knoten. Alle Knoten nutzen dieselbe Verzeichnisstruktur für die Nachrichten-Verzeichnisse gemeinsam.
- Alle Änderungen an E-Mail-Nachrichten, die auf Sekundärknoten durchgeführt werden, werden an den Primärknoten übermittelt. Von dort aus werden alle anderen Nachrichten über die Änderung informiert.
- Das XML-API der Sekundärknoten gestattet nur Lesezugriffe.
- Alle Knoten eines Clusters sollen sich im selben Netzwerk befinden. Der Cluster-Betrieb ist nicht auf den Betrieb von Knoten ausgelegt, die geografisch voneinander getrennt sind. Eine solche Betriebsart wird nicht empfohlen.
- Alle Knoten eines Clusters müssen denselben Versionsstand von MDaemon aufweisen.
- Für jeden Knoten eines Clusters ist ein eigener Lizenzschlüssel für MDaemon erforderlich. Sie können denselben Lizenzschlüssel nicht auf mehreren Knoten verwenden.

Routing

MDaemon steuert nicht das Routing des Datenverkehrs von und zu einzelnen Knoten. Es empfiehlt sich daher, einen Lastverteiler (Load Balancer) eines Drittanbieters zu verwenden, um das Routing des Datenverkehrs und die Verkehrslenkung zu steuern.

Der Load Balancer muss sog. sticky sessions (das Nachhalten ausgehandelter Verbindungen) unterstützen, damit sichergestellt ist, dass der gesamte Datenverkehr, der von derselben IP-Adresse ausgeht, auch jeweils an denselben Host geroutet wird. Sticky sessions sind besonders für den Datenverkehr der MDaemon-Remoteverwaltung, von Webmail und XMPP wichtig. Diese Dienste sind noch nicht unmittelbar clustergeeignet; Verbindungsinformationen werden daher nicht zwischen den Knoten ausgetauscht. Aufgrund dieser Einschränkung müssen folgende Anforderungen erfüllt werden:

- Alle Verbindungen mit der MDaemon-Remoteverwaltung müssen an den Primärknoten geleitet werden.
- Meldet sich ein Benutzer an einem bestimmten Server an Webmail an, so muss der gesamte Datenverkehr für die hierdurch aufgebaute Verbindung an denselben Server geroutet werden.
- Die in Webmail integrierten Chatfunktionen arbeiten nur dann, wenn der Datenverkehr für Webmail und XMPP an denselben Server geroutet wird.
- Der gesamte Datenverkehr für XMPP muss an denselben Knoten geroutet werden. Benutzer, die Verbindungen mit unterschiedlichen Servern herstellen, können sonst nicht miteinander chatten.
- Angesichts der genannten Anforderungen empfiehlt es sich, dass der gesamte Datenverkehr für HTTP und XMPP an den Primärknoten geroutet wird. Diese Betriebsart ermöglicht die einfachste Konfiguration und verursacht voraussichtlich die geringsten Probleme. Falls Sie nicht alle genannten Leistungsmerkmale nutzen, können Sie möglicherweise auch eine abweichende Konfiguration verwenden. Sticky sessions sind jedoch auch dann erforderlich.

Postfächer und Ordner

Postfächer, öffentliche Ordner und einige weitere Ordner müssen in einem gemeinsam genutzten, freigegebenen Verzeichnis gespeichert sein, auf das alle Knoten im Cluster Zugriff haben. Falls Sie hierfür einen UNC-Pfand nutzen, müssen Sie den Windows-Dienst MDaemon mit Zugriffsrechten auf Netzwerkressourcen versehen, etwa, indem Sie ihn als Benutzer ausführen, der Zugriff auf den UNC-Pfad hat.

- Sie müssen Ihre Verzeichnispfade für Postfächer und Nachrichten-Ordner manuell aktualisieren und die Inhalte der Verzeichnisse in den für den Cluster freigegebenen Speicherort verschieben. MDaemon kann diesen Vorgang für Sie nicht automatisch durchführen, wenn Sie den Cluster-Betrieb einrichten. Der Cluster-Dienst aktualisiert die Datei MDaemon.ini und übernimmt den Netzwerkpfad für Postfächer und öffentliche Ordner, den Sie in der Konfiguration für den Cluster-Dienst angegeben haben.
- Das Verzeichnis Lockfiles für die Sperrdateien muss in einen freigegebenen, gemeinsam genutzten Speicherort verschoben werden. Sie können diesen Vorgang durch den Cluster-Dienst automatisch ausführen lassen. Sie können den Vorgang aber auch manuell ausführen. Bearbeiten Sie hierzu den Eintrag `LockFiles` im Abschnitt `[Directories]` der Datei `MDaemon.ini`. Falls Sie diesen Vorgang durch den Cluster-Dienst ausführen lassen, wird das Verzeichnis LockFiles als Unterverzeichnis des Netzwerkpfads für die Postfächer angelegt.
- Auch das Verzeichnis PEM muss in einen freigegebenen, gemeinsam genutzten Speicherort verschoben werden. Um diesen Vorgang auszuführen, kopieren Sie das Verzeichnis `MDaemon\PEM\` in den neuen gemeinsam genutzten, freigegebenen Speicherort, passen Sie den Eintrag `PEM` im Abschnitt `[Directories]` der Datei `MDaemon.ini` entsprechend an, und starten Sie MDaemon neu.
- Der Netzwerkpfad für die Postfächer, den Sie in der Konfiguration des Cluster-Dienstes angeben, wird in die Vorlage Neue Benutzerkonten übernommen.

Dynamischer Filter

- Der Dynamische Filter[612] sendet alle Anforderungen an den Primärknoten, und die Daten des Primärknotens werden auf alle Sekundärknoten repliziert.
- Ist der Primärknoten außer Betrieb, so nutzen die Sekundärknoten ihre eigene Konfiguration für den Dynamischen Filter. Diese entspricht üblicherweise der Konfiguration auf dem Primärknoten zur der Zeit, als der Primärknoten außer Betrieb ging. Sobald der Primärknoten wieder in Betrieb ist, werden alle Änderungen an der Konfiguration der Sekundärknoten, die zwischenzeitlich möglicherweise vorgenommen wurden, überschrieben.

Zertifikate

- Die SSL-Zertifikate werden automatisch vom Primärknoten auf die Sekundärknoten repliziert.
- MDaemon repliziert auch die eigenen Zertifikats-Einstellungen[579], sodass jeder Knoten im Cluster versucht, dieselben Zertifikate zu nutzen. Ist auf einem Knoten das erforderliche Zertifikat nicht installiert, so ist kein Datenverkehr über SSL, TLS und HTTPS mit diesem Knoten möglich.
- Die Optionen für LetsEncrypt in MDaemon unterstützen derzeit keine Sekundärknoten.

Weiteres

- Die Verlinkung von Dateianlagen[364] kann im Cluster-Betrieb nicht verwendet werden. Sie wird daher bei Aktivierung des Cluster-Betriebs deaktiviert.
- Die automatische Installation neuer Programmversionen[502] muss deaktiviert sein.
- Die Bindung von Domänennamen an IP-Adressen[184] muss deaktiviert sein.
- Alle Knoten eines Clusters sollen auf dieselbe Zeitzone konfiguriert sein, und ihre Systemzeit soll genau übereinstimmen. Stimmen die Zeitzonen nicht überein, oder unterscheiden sich die Systemzeiten um mehr als 1 Sekunde, werden entsprechende Warnungen in das Protokoll des Cluster-Dienstes eingetragen.

Konfiguration des Cluster-Dienstes

Um den Cluster-Dienst zu konfigurieren, gehen Sie folgendermaßen vor:

1. Stellen Sie sicher, dass Sie alle Pfade der Postfächer und der öffentlichen Ordner angepasst haben. Der Primärknoten soll einen Netzwerkpfad für diese Daten nutzen und muss auf die Daten in dem Netzwerkpfad ohne Probleme zugreifen können. Setzen Sie den Vorgang erst fort, wenn dies sichergestellt ist.
2. Alle erforderlichen Zertifikate sollen auf allen Knoten installiert sein.
3. Installieren Sie MDaemon mithilfe eines eigenen Lizenzschlüssels auf einem Sekundärknoten.
4. Rufen Sie auf dem Primärknoten den Konfigurationsdialog **Einstellungen » Cluster-Dienst** auf.
5. Führen Sie einen Rechtsklick in der Liste der registrierten Server aus, und klicken Sie dann auf **Neuen MDaemon-Server dem Cluster hinzufügen**.

Dieser Vorgang kann einige Zeit in Anspruch nehmen, da das Netzwerk nach verfügbaren Servern durchsucht wird.

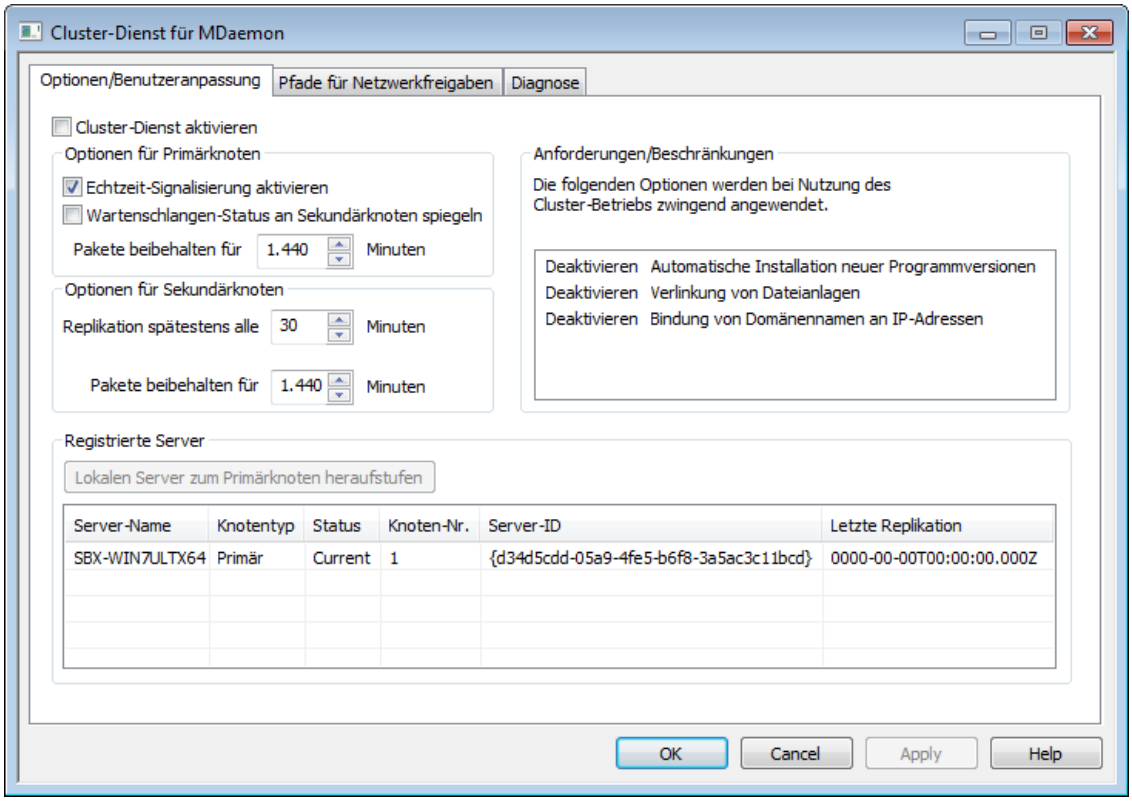
6. Geben Sie im Feld *Servername* den NETBIOS-Namen, die IP-Adresse oder den DNS-Namen des Sekundärknotens an, auf dem MDaemon installiert ist. Sie können auch stattdessen den Server aus dem Auswahlmenü wählen; hierbei kann eine Verzögerung eintreten, da das Netzwerk nach verfügbaren Servern durchsucht wird.
7. Wählen Sie eine *Server-ID* aus.
8. Klicken Sie auf **OK**.
9. Prüfen Sie das Protokoll Plugins/Cluster, um sicherzustellen, dass die beiden Server verbunden sind, und dass die Replikation durchgeführt wird.
10. Rufen Sie auf dem Sekundärknoten den Konfigurationsdialog **Einstellungen » Cluster-Dienst** auf. Prüfen Sie, dass dort im Abschnitt Registrierte Server der Primärknoten und der Sekundärknoten aufgeführt sind.
11. Konfigurieren Sie Ihre Load-Balancing-Hardware oder -Software, um den Datenverkehr im Cluster in Übereinstimmung mit den oben erläuterten Anforderungen zu routen.

Siehe auch:

Cluster-Dienst | Optionen/Benutzeranpassung 410
Cluster-Dienst | Pfade für Netzwerkfreigaben 412
Cluster-Dienst | Diagnose 413

3.9.1 Optionen/Benutzeranpassung

Optionen/Benutzeranpassung



Cluster-Dienst aktivieren

Diese Option aktiviert den Cluster-Dienst.

Optionen für Primärknoten

Echtzeit-Signalisierung aktivieren

Diese Option bewirkt, dass der Primärknoten nach einer Änderung ein Signal zur Replikation an die Sekundärknoten sendet. Dieses Signal teilt den Sekundärknoten mit, dass Sie eine Replikation anfordern müssen, um die Einstellungen zwischen den Knoten abzugleichen. Diese Option ist per Voreinstellung aktiv.

Warteschlangen-Status an Sekundärknoten spiegeln

Diese Option bewirkt, dass Änderungen an den Status der Warteschlangen (etwa angehalten und fortgesetzt), die auf dem Primärknoten durchgeführt werden, auch auf die Sekundärknoten übertragen werden. Die Status ändern sich dort entsprechend.

Optionen für Sekundärknoten

Replikation spätestens alle [xx] Minuten

Diese Option bestimmt, wie lange die Sekundärknoten auf ein Signal des Primärknotens zur Replikation warten, bevor sie selbst unabhängig von diesem Signal die Replikation anfordern. Per Voreinstellung beträgt das Intervall 30 Minuten.

Registrierte Server

In dieser Übersicht erscheinen alle Knoten Ihres MDaemon-Clusters.

Lokalen Server zum Primärknoten heraufstufen
Sie können einen Sekundärknoten zum Primärknoten heraufstufen. Dieser Vorgang muss auf dem Sekundärknoten ausgeführt werden, den Sie heraufstufen wollen. Wählen Sie dort den gewünschten Knoten aus, und klicken Sie danach auf **Heraufstufen**. Der soeben heraufgestufte Primärknoten sollte dann den bisherigen Primärknoten von der Heraufstufung informieren und ihn veranlassen, dem Cluster als Sekundärknoten wieder beizutreten. In Clustern mit mehreren Sekundärknoten müssen die weiteren Sekundärknoten aus dem Cluster entfernt und anschließend dem Cluster wieder hinzugefügt werden.

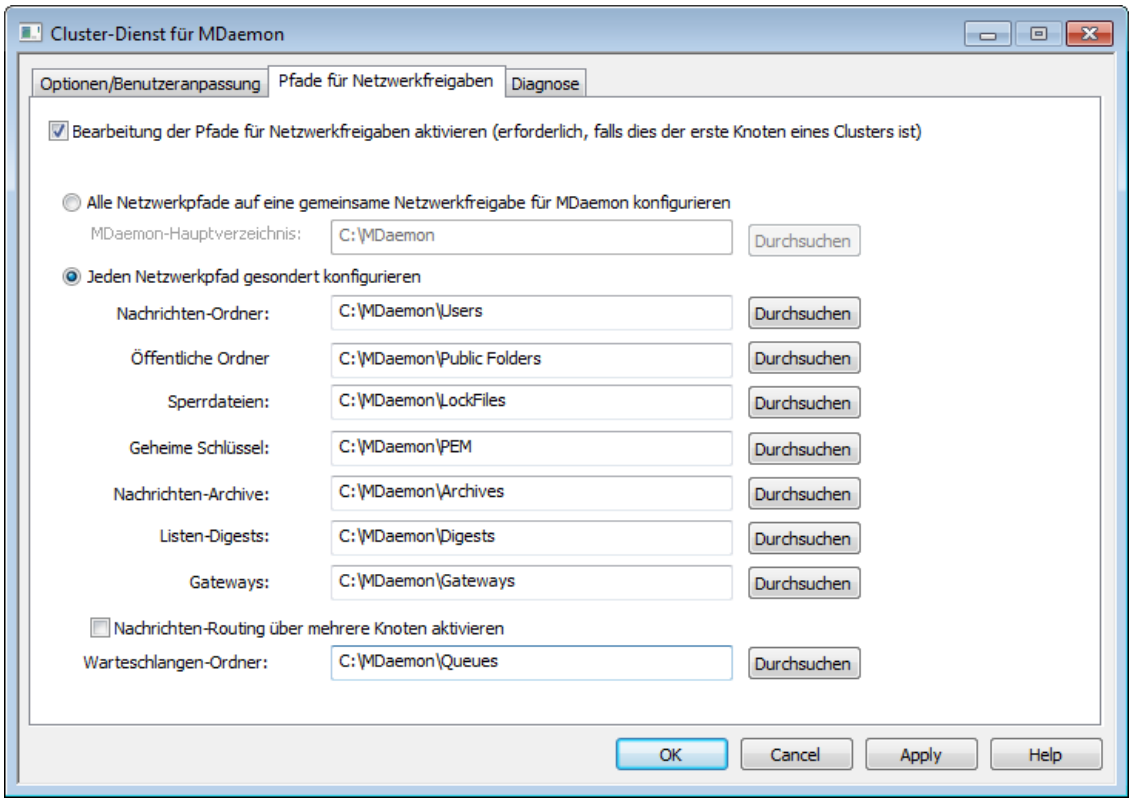
Dem Cluster einen neuen MDaemon-Server hinzufügen
Um dem Cluster einen neuen MDaemon-Server hinzuzufügen, führen Sie einen Rechtsklick auf die Liste der Server aus, und klicken Sie dann auf **Neuen MDaemon-Server dem Cluster hinzufügen**. Es öffnet sich ein Konfigurationsdialog. Geben Sie dort den NETBIOS-Namen, die IP-Adresse oder den DNS-Namen des Sekundärknotens an, auf dem MDaemon installiert ist. Sie können auch stattdessen den Server aus dem Auswahlmenü wählen; hierbei kann eine Verzögerung eintreten, da das Netzwerk nach verfügbaren Servern durchsucht wird.

Siehe auch:

Cluster-Dienst 406
Cluster-Dienst | Pfade für Netzwerkfreigaben 412
Cluster-Dienst | Diagnose 413

3.9.2 Pfade für Netzwerkfreigaben

Pfade für Netzwerkfreigaben



Bearbeitung der Pfade für Netzwerkfreigaben aktivieren (erforderlich, falls dies der erste Knoten eines Clusters ist)

Mithilfe der Optionen in diesem Konfigurationsdialog können Sie die Pfade für die Netzwerkfreigaben konfigurieren, die der MDaemon-Cluster nutzt. Diese Konfiguration ist auf dem ersten Knoten eines Clusters erforderlich, damit die Pfade für die Netzwerkfreigaben an die anderen Knoten repliziert werden können.

Alle Netzwerkfreigaben auf eine gemeinsame Netzwerkfreigabe für MDaemon konfigurieren
Falls Sie alle Pfade für die Netzwerkfreigaben unter einem gemeinsamen übergeordneten Pfad anlegen wollen, aktivieren Sie diese Option. Diese Option bewirkt, dass alle weiteren Pfade auf die Voreinstellungen gesetzt werden. Sie können dann in den folgenden Feldern eingesehen, aber nicht bearbeitet werden.

Jeden Netzwerkpfad gesondert konfigurieren
Mithilfe dieser Option können Sie jeden Pfad für jede Netzwerkfreigabe individuell konfigurieren. Dies ist beispielsweise hilfreich, wenn Sie Nachrichten-Verzeichnisse und Nachrichten-Archive in unterschiedlichen Netzwerkfreigaben speichern wollen.

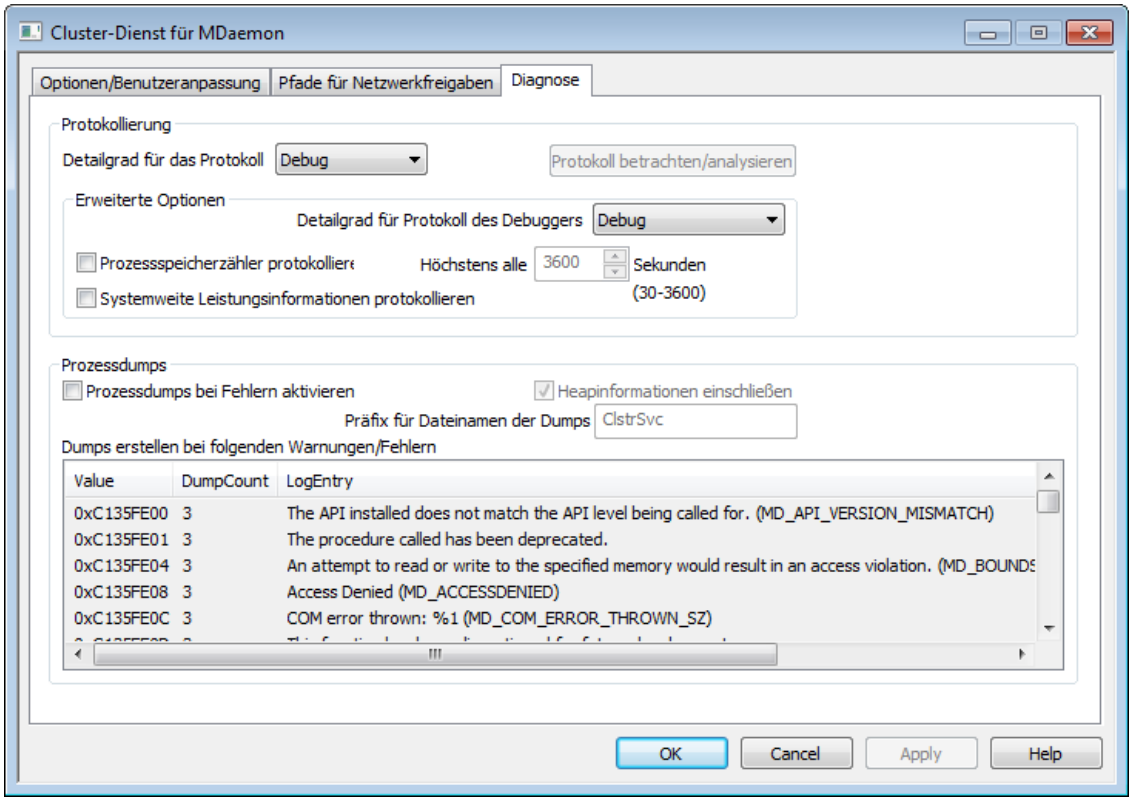
Nachrichten-Routing über mehrere Knoten aktivieren
Das Nachrichten-Routing über mehrere Knoten gestattet die gemeinsame Nutzung von Nachrichten-Warteschlangen durch die Knoten des Clusters. Wenn Sie die Nachrichten durch mehrere Server verarbeiten und zustellen lassen, so wird hierdurch die Auslastung gleichmäßiger verteilt, und es ist weniger wahrscheinlich, dass Nachrichten in den Warteschlangen eines ausgefallenen Servers verbleiben.

Siehe auch:

Cluster-Dienst 406
Cluster-Dienst | Optionen/Benutzeranpassung 410
Cluster-Dienst | Diagnose 413

3.9.3 Diagnose

Diagnose



Protokollierung

Detailgrad für das Protokoll

Der Cluster-Dienst von MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Protokolldatei betrachten/analysieren

Durch Anklicken dieses Steuerelements öffnet sich der erweiterte Protokollbetrachter für MDaemon. Per Voreinstellung werden die Protokolle im

Verzeichnis "..\MDaemon\Logs\" gespeichert.

Erweiterte Optionen

Detailgrad für Protokoll des Debuggers
Diese Option bestimmt den geringsten zulässigen Detailgrad für die Protokolldaten, die an den Debugger übermittelt werden. Die auswählbaren Detailgrade sind dieselben wie in der Tabelle weiter oben.

Prozessspeicherzähler protokollieren
Mithilfe dieser Option können prozessspezifische Informationen über Speicher, Handle und Threads protokolliert werden. Diese Informationen sind hilfreich, um Probleme mit der Zuweisung von Ressourcen und vergleichbare Probleme zu diagnostizieren. Die Protokolleinträge werden nur ausgegeben, wenn die Daten sich seit der letzten Protokollierung geändert haben.

Systemweite Leistungsinformationen protokollieren
Mithilfe dieser Option können systemweite Leistungsdaten protokolliert werden. Diese Informationen sind hilfreich, um Probleme mit der Zuweisung von Ressourcen und vergleichbare Probleme zu diagnostizieren. Die Protokolleinträge werden nur ausgegeben, wenn die Daten sich seit der letzten Protokollierung geändert haben.

Höchstens alle [xx] Sekunden
Diese Option begrenzt die Häufigkeit, mit der die Prozess- und Leistungsinformationen protokolliert werden.

Prozessdumps

Prozessdumps bei Fehlern aktivieren
Diese Option bewirkt die Erstellung von Prozessdumps in den Fällen, in denen die weiter unten angegebenen Warnungen und Fehler auftreten.

Heapinformationen einschließen
Per Voreinstellung werden die Heapinformationen in die Prozessdumps aufgenommen. Falls Sie dies nicht wünschen, deaktivieren Sie dieses Kontrollkästchen.

Präfix für Dateinamen der Dumps
Die Dateinamen der Dump-Dateien beginnen mit dem hier angegeben Text. Der Präfix lautet per Voreinstellung "AirSync".

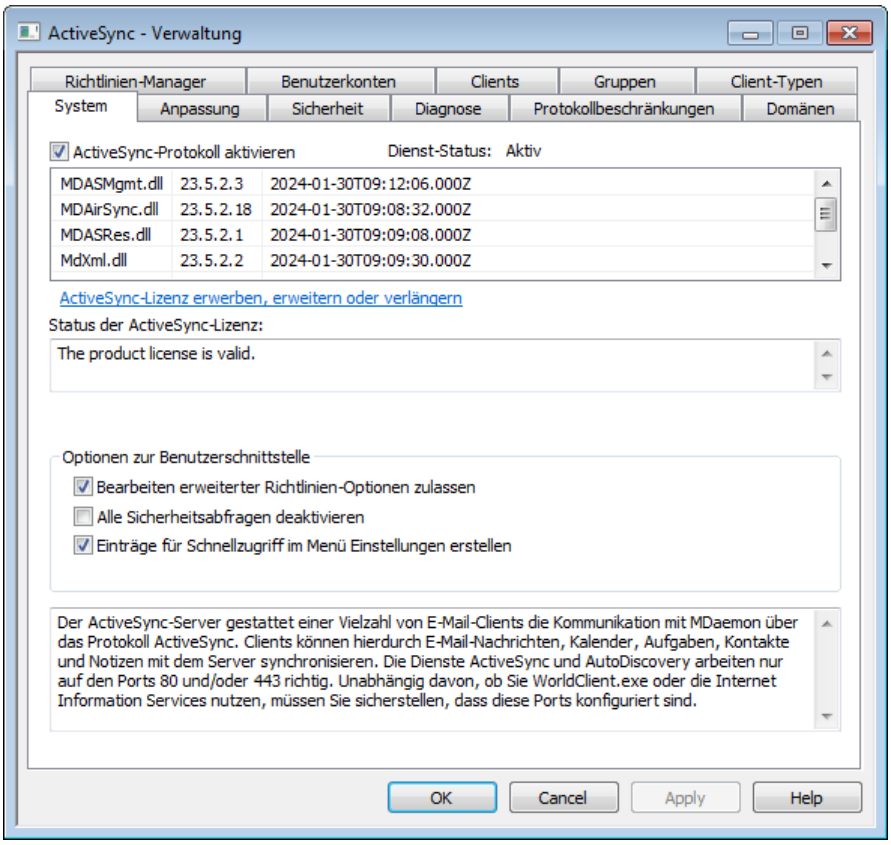
Dumps erstellen bei folgenden Warnungen/Fehlern
Um diese Einträge zu bearbeiten, öffnen Sie durch Rechtsklick in diesem Bereich das Kontextmenü. Mithilfe der dann erscheinenden Menüeinträge *Eintrag hinzufügen, Eintrag bearbeiten* und *Eintrag löschen* können Sie die Liste der Fehler und Warnungen verwalten, die das Erstellen von Prozessdumps auslösen. Für jeden Eintrag können Sie die Anzahl der zulässigen Prozessdumps angeben; wird diese Zahl erreicht, so wird der Eintrag deaktiviert.

Siehe auch:

Cluster-Dienst 406
Cluster-Dienst | Optionen/Benutzeranpassung 410
Cluster-Dienst | Pfade für Netzwerkfreigaben 412

3.10 ActiveSync

3.10.1 System



MDaemon enthält "ActiveSync für MDaemon", einen gesondert zu lizensierenden OTA-ActiveSync-Server (OTA steht hierbei für "Over the Air", drahtlos). Dieser Server kann die E-Mail-Nachrichten, Standard-Kalender und Standard-Kontaktordner der Benutzer zwischen einem MDaemon-Benutzerkonto, auf das auch Zugriff über Webmail möglich ist, und einem Endgerät synchronisieren, das ebenfalls ActiveSync-fähig ist.

ActiveSync für MDaemon läuft, nachdem Sie den Server zum ersten Mal mithilfe eines Testlizenzschlüssels aktiviert haben, für einen Testzeitraum von 30 Tagen. Nach dem Ende dieses Testzeitraums können Sie einen Lizenzschlüssel über www.mdaemon.com oder Ihren lokalen Händler oder Distributor erwerben.

ActiveSync ist eine Webdienst-Erweiterung, die nur auf den Ports **80** (für http-Verbindungen) und **443** (für https-Verbindungen) genutzt werden kann. Die Nutzung dieser Ports ist für die Implementierung von ActiveSync zwingend; ActiveSync kann nicht auf anderen Ports genutzt werden. Wird ActiveSync aktiviert, und nutzen Sie den in WorldClient integrierten Web-Server 322 auf anderen Ports als 80 oder 443, so nutzt der Web-Server von Webmail ab der Aktivierung von ActiveSync zusätzlich auch den Port 80. Falls Sie in den Konfigurationsdialogen Web-Server 322 und SSL &

HTTPS 327 weitere Ports konfiguriert haben, bleiben diese Ports unberührt. Falls Sie einen anderen Web-Server für Webmail nutzen, etwa die IIS, müssen Sie diesen Web-Server so konfigurieren, dass er Port 80 oder 443 nutzt.

Falls Sie ActiveSync in die IIS einbinden wollen, müssen Sie die ActiveSync-DLL von MDaemon (`MDAirSync.dll`) dann aufrufen, wenn eine Anforderung für "`/Microsoft-Server-ActiveSync`" eingeht. Alle ActiveSync-Clients übermitteln diese Anforderung. Manche Versionen der IIS können diese Anforderungen nur dann richtig verarbeiten, wenn Sie hierzu Software von Drittanbietern installieren und konfigurieren.

Die erste Synchronisierung mit einem ActiveSync-Server wird immer als Einwege-Synchronisierung vom Server zum Endgerät hin durchgeführt. Bei dieser ersten Synchronisierung mit ActiveSync gehen alle Daten auf dem mobilen Endgerät verloren. Diese Verhaltensweise ergibt sich aus den Anforderungen für die Implementierung von ActiveSync. Sie müssen daher die Daten auf dem Endgerät sichern, bevor Sie ActiveSync zum ersten Mal nutzen. Die meisten Endgeräte, die ActiveSync unterstützen, warnen die Benutzer davor, **dass alle Daten auf dem Endgerät verloren gehen**, manche Endgeräte geben eine solche Warnung aber nicht aus. Bitte setzen Sie ActiveSync bedachtsam ein.

ActiveSync aktivieren/deaktivieren

Um das *ActiveSync-Protokoll* zu aktivieren, aktivieren Sie die Option *ActiveSync-Protokoll aktivieren*. Sie können dann die Optionen für einzelne Domänen 437 verwenden, um zu bestimmen, ob ActiveSync allen oder nur bestimmten Domänen zur Verfügung stehen soll.

Optionen zur Benutzerschnittstelle

Bearbeiten erweiterter Richtlinien-Optionen zulassen
Diese Option bewirkt, dass die Registerkarte Erweiterte Einstellungen im ActiveSync-Richtlinien-Editor 446 sichtbar wird. Sie enthält verschiedene erweiterte Richtlinien-Optionen, die im Regelfall nicht geändert werden müssen. Diese Option ist per Voreinstellung abgeschaltet.

Alle Sicherheitsabfragen deaktivieren
Per Voreinstellung erscheinen Sicherheitsabfragen, wenn Sie bestimmte ActiveSync-Einstellungen ändern. Falls Sie diese Sicherheitsabfragen nicht wünschen, aktivieren Sie diese Option.

Einträge für Schnellzugriff im Menü Einstellungen erstellen
Diese Option fügt dem Menü Einstellungen » ActiveSync auf der Benutzeroberfläche von MDaemon Einträge für die Überwachung von ActiveSync-Verbindungen und das Programm zum Betrachten und zur Analyse der ActiveSync-Protokolle hinzu. **Beachte:** Auch wenn diese Option deaktiviert ist, sind die entsprechenden Werkzeuge verfügbar. Sie können sie über einen Rechtsklick auf den Eintrag **ActiveSync** im Abschnitt Server der Registerkarte Statistik der Benutzeroberfläche durch Anklicken der Menüeinträge im Kontextmenü aufrufen.

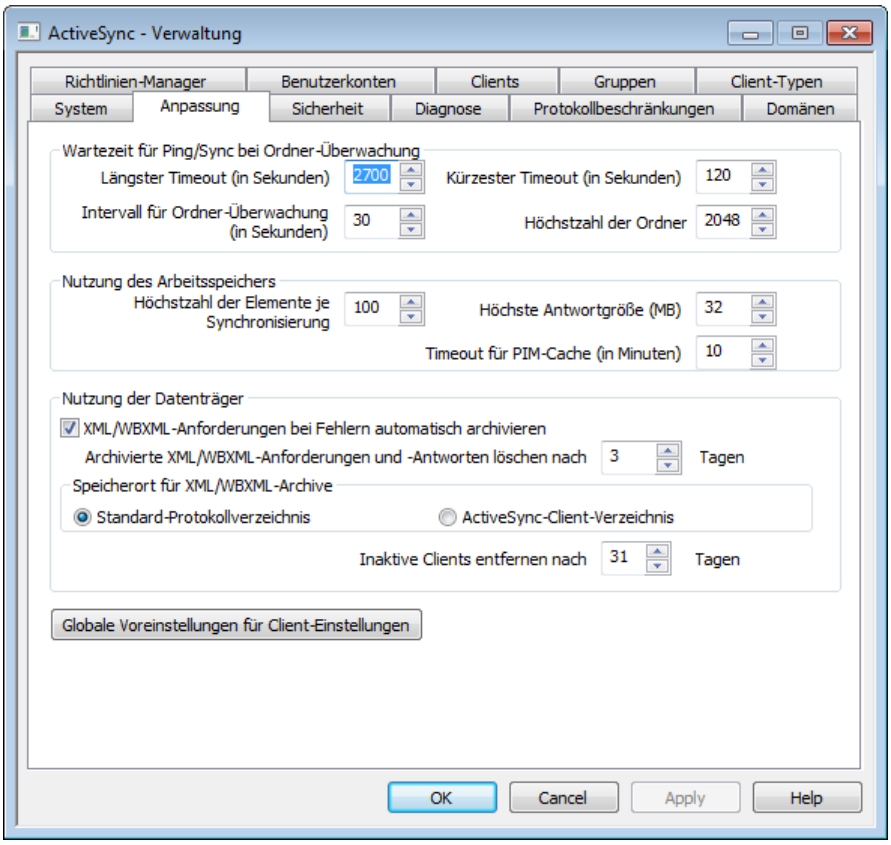
AutoDiscovery-Dienst 80

MDaemon unterstützt den Dienst AutoDiscovery 80, der die automatische Provisionierung von ActiveSync-Einstellungen ermöglicht. Die Benutzer benötigen hierzu nur ihre E-Mail-Adressen und ihre Kennwörter; den Hostnamen des ActiveSync-Servers müssen sie nicht kennen. Die automatische Provisionierung erfordert HTTPS 327.

Siehe auch:

Benutzerkonten-Editor » ActiveSync 763
ActiveSync » Domänen 437
SSL & HTTPS 327
Web-Server 322

3.10.2 Anpassung



Dieser Abschnitt enthält fortgeschrittene Optionen, die im Regelfall nicht angepasst werden müssen. Er enthält auch die Schaltfläche Globale Voreinstellungen für Client-Einstellungen 422, über die die Voreinstellungen für die ActiveSync-Clients konfiguriert werden.

Wartezeit für Ping/Sync bei Ordner-Überwachung

Längster Timeout (in Sekunden, 1200-7200)
Die ist die Höchstdauer in Sekunden, die der MDaemon-ActiveSync-Dienst (MDAS) während der Überwachung eines Ordners wartet, bevor er dem Client eine Antwort übermittelt. Der Wert beträgt per Voreinstellung 2700 Sekunden (45 Minuten).

Kürzester Timeout (in Sekunden, 120-480)
Die ist die Mindestdauer in Sekunden, die der MDaemon-ActiveSync-Dienst (MDAS) während der Überwachung eines Ordners wartet, bevor er dem Client eine Antwort übermittelt. Der Wert beträgt per Voreinstellung 120 Sekunden. Sie können, falls gewünscht, die Anzahl der Verbindungen, die mit dem Server hergestellt werden, verringern, indem Sie diesen Wert erhöhen. Da sich bei höherem Wert die Wartezeit entsprechend verlängert, werden die Clients weniger häufig Verbindungen herstellen.

Intervall für Ordner-Überwachung (in Sekunden, 3-50)
Die ist die Zeitdauer in Sekunden, die der ActiveSync-Dienst zwischen zwei Aktionen zur Ordnerüberwachung wartet. Der Wert beträgt per Voreinstellung 5 Sekunden.

Höchstzahl der Ordner
Die ist die Höchstzahl der Ordner, die jeder ActiveSync-Client auf Änderungen überwachen darf. Der Wert beträgt per Voreinstellung 2048.

Nutzung des Arbeitsspeichers

Höchstzahl der Elemente je Synchronisierung
Die ist die Höchstzahl der Elemente, die der ActiveSync-Dienst als Antwort auf eine Sync-Anforderung an den Client zurückmeldet. Niedrigere Werte bei dieser Option können den Speicherbedarf auf stark ausgelasteten Servern verringern, erfordert aber mehr Verbindungen und Bandbreite. Ein solcher Wert kann auch die Akkulaufzeit herabsetzen, weil die Geräte mehr Anforderungen stellen müssen, um während einer Synchronisierung alle Änderungen übermittelt zu erhalten. Höhere Werte bei dieser Option können den Speicherbedarf erhöhen und sind anfälliger für Kommunikationsfehler. Die Voreinstellung von 100 stellt im Regelfall einen günstigen Kompromiss dar. Es ist aber zu beachten, dass die Clients den Wert vorgeben, den sie nutzen wollen. Dies kann dazu führen, dass die Zahl der Elemente für einzelne Clients unter der Höchstzahl liegt. Die Höchstzahl kann aber nicht überschritten werden; verlangt der Client einen Wert über der Höchstzahl, so wird die Höchstzahl genutzt.

Höchste Antwortgröße (MB)
Dies ist die höchstzulässige Größe einer Antwort auf die Sync-Anforderung eines Clients. Bevor ein bestimmtes Element für die Übermittlung durch den Server an den Client verarbeitet wird, prüft der Server die bis dahin aufgelaufene Größe der Antwort. Erreicht sie diesen Wert, oder überschreitet sie ihn, dann wird dem Client mitgeteilt, dass in der Sammlung weitere Änderungen verfügbar sind, und der Antwort werden keine Elemente mehr hinzugefügt. Dies ist besonders hilfreich auf Servern, deren E-Mail-Nachrichten oft viele und umfangreiche Dateianlagen enthalten.

Timeout für PIM-Cache (in Minuten, 5-60)
PIM-Daten wie Kontakte, Dokumente und Termine sind oft statisch und unterliegen nicht sehr häufigen Änderungen durch die Clients. MDAS speichert solche Daten daher zwischen, um die Übermittlung von Daten auf die Datenträger und von ihnen zu verringern. Ändern sich die Elemente auf dem Datenträger, so werden sie allerdings automatisch neu geladen. Dieser Wert bestimmt, wie lange die Daten der Benutzer im Cache gehalten werden, nachdem zuletzt auf sie zugegriffen wurde.

Nutzung der Datenträger

XML/WBXML-Anforderungen bei Fehlern automatisch archivieren
Falls Sie Optionen *[XML | WBXML]-Anforderungen und -Antworten archivieren* im Konfigurationsdialog Client-Einstellungen[422] deaktiviert haben, können Sie mithilfe dieser Option problematische XML- und WBXML-Anfragen protokollieren. Es werden dabei nur Anfragen archiviert, die Fehler verursachen. Diese Option ist per Voreinstellung aktiv.

Archivierte XML/WBXML-Anforderungen und -Antworten löschen nach [xx] Tagen
Diese Option bestimmt, für welchen Zeitraum die automatisch archivierten Antworten gespeichert werden. Per Voreinstellung beträgt die Speicherdauer 3 Tage.

Speicherort für XML/WBXML-Archive

Standard-Protokollverzeichnis
Diese Option bewirkt, dass die automatisch archivierten XML/WBXML-Anforderungen im Protokollverzeichnis von MDaemon gespeichert werden. Diese Option ist per Voreinstellung aktiv.

ActiveSync-Client-Verzeichnis
Diese Option bewirkt, dass die automatisch archivierten XML/WBXML-Anforderungen nicht im Protokollverzeichnis von MDaemon sondern im Verzeichnis Debug des ActiveSync-Clients gespeichert werden.

Inaktive Clients entfernen nach [xx] Tagen
Diese Option bestimmt, nach wie vielen Tagen ActiveSync-Geräte[464] entfernt werden, wenn sie während dieser Zeit keine Verbindung über ActiveSync hergestellt haben. Wird ein Gerät entfernt, so werden seine Konfiguration und seine Zugriffsrechte gelöscht. Führt das entfernte Gerät später noch einmal eine Synchronisierung über ActiveSync auf dem Server durch, dann behandelt MDaemon den Client so, wie wenn er auf dem Server noch nie verwendet worden wäre. Besteht für die Domäne[437] oder das Benutzerkonto[454] eine Richtlinie, so muss die Provisionierung wiederholt werden. Auch die Erstsynchronisierung der Ordner und die Neusynchronisierung aller abonnierten Ordner müssen erneut durchgeführt werden. Diese Option kann helfen, den Server von Daten alter und nicht mehr genutzter Geräte freizuhalten. Die Voreinstellung für diese Option beträgt 31 Tage. Der Wert 0 bewirkt, dass Geräte nicht automatisch entfernt werden, und zwar unabhängig davon, wie lange sie schon keine Verbindung über ActiveSync mehr hergestellt haben.

Globale Voreinstellungen für Client-Einstellungen

Durch Anklicken dieser Schaltfläche rufen Sie den Konfigurationsdialog für die Globalen Einstellungen für ActiveSync-Clients[422] auf. Sie können dort die Voreinstellungen konfigurieren, die die ActiveSync-Clients nutzen.

ActiveSync-Benachrichtigungen

Rollback-Benachrichtigungen für ActiveSync-Synchronisierungen

Der ActiveSync-Dienst kann die Administratoren benachrichtigen, falls ein Client im Rahmen von Synchronisierungsvorgängen wiederholt oder öfter abgelaufene Sync-Schlüssel übermittelt.

Diese Benachrichtigungen teilen dem Administrator mit, dass der Server für eine bestimmte Sammlung einen Rollback veranlasst hat, weil der Client eine Sync-Anforderung mit dem zuletzt gültigen, zwischenzeitlich aber abgelaufenen Sync-Schlüssel angefordert hat. Die Betreffzeile enthält den Hinweis, dass ein ActiveSync-Client einen abgelaufenen Sync-Schlüssel verwendet. Gründe hierfür können Netzwerkprobleme oder Probleme mit Inhalten sein, die dem Client aus der betroffenen Sammlung früher übermittelt wurden. In manchen Fällen wird eine Element-ID aufgeführt. Ob dies der Fall ist, hängt davon ab, ob dem Client in der vorangegangenen Synchronisierung der Sammlung Elemente übermittelt wurden.

Rollback-Benachrichtigungen bedeuten nicht, dass der betroffene Client nicht mehr synchronisiert ist, sondern dass der Client die Synchronisierung verlieren könnte, und dass das System dies erkannt hat. Rollback-Benachrichtigungen werden je Sammlung nur einmal alle 24 Stunden übermittelt. Sie können mithilfe der folgenden Einträge im Abschnitt `[System]` der Datei `\MDaemon\Data\AirSync.ini` konfiguriert werden:

- [System] SendRollbackNotifications=[0|1|Yes|No|True|False]: Diese Option bestimmt, ob Rollback-Benachrichtigungen gesendet werden. Sie ist per Voreinstellung abgeschaltet.
- [System] RollbackNotificationThreshhold=[1-254]: Dies ist die Anzahl der Rollbacks, die für eine bestimmte Sammlung erreicht sein muss, bevor der Administrator eine Rollback-Benachrichtigung erhält. Da auch vorübergehende kleinere Einschränkungen im Netzbetrieb zu Rollbacks führen können, empfiehlt sich ein Schwellwert von mindestens 5. Die Voreinstellung beträgt 10.
- [System] RollbackNotificationCCUser=[0|1|Yes|No|True|False]: Diese Option bestimmt, dass der betroffene Benutzer, dessen Client einen abgelaufenen Sync-Schlüssel übermittelt hat, eine Kopie der Benachrichtigung an den Administrator erhält. Diese Option ist per Voreinstellung abgeschaltet.

ActiveSync-Benachrichtigungen über beschädigte Nachrichten

Der ActiveSync-Dienst kann die Administratoren benachrichtigen, falls eine bestimmte Nachricht nicht verarbeitet werden kann. Solche Benachrichtigungen werden in Echtzeit versandt und informieren den Administrator darüber, dass ein Nachrichten-Element nicht verarbeitet werden konnte und weitere Vorgänge für dieses Element nicht möglich sind. Die Betreffzeile enthält den Hinweis, dass eine beschädigte Nachricht vorliegt. Solche beschädigten Elemente konnten in früheren Versionen zum Programmabsturz führen. In den meisten solchen Fällen enthält die MSG-Datei keine MIME-Daten. Falls sie MIME-Daten enthält, sind diese Daten wahrscheinlich beschädigt. Mithilfe des Eintrags `CMNCCUser` können Sie dem betroffenen Benutzer eine Kopie der Benachrichtigung senden lassen, damit der Benutzer darauf aufmerksam wird, dass eine Nachricht in seinem Postfach eingegangen ist, die nicht verarbeitet werden konnte. Die richtige Vorgehensweise für solche Nachrichten ist es, sie aus dem Postfach des

Benutzers zu entfernen und zu analysieren. So kann festgestellt werden, warum sie nicht verarbeitet werden konnte, und wie es zu diesem Zustand gekommen ist. Diese Benachrichtigungen können mithilfe der folgenden Einträge im Abschnitt `[System]` der Datei `\MDaemon\Data\AirSync.ini` konfiguriert werden:

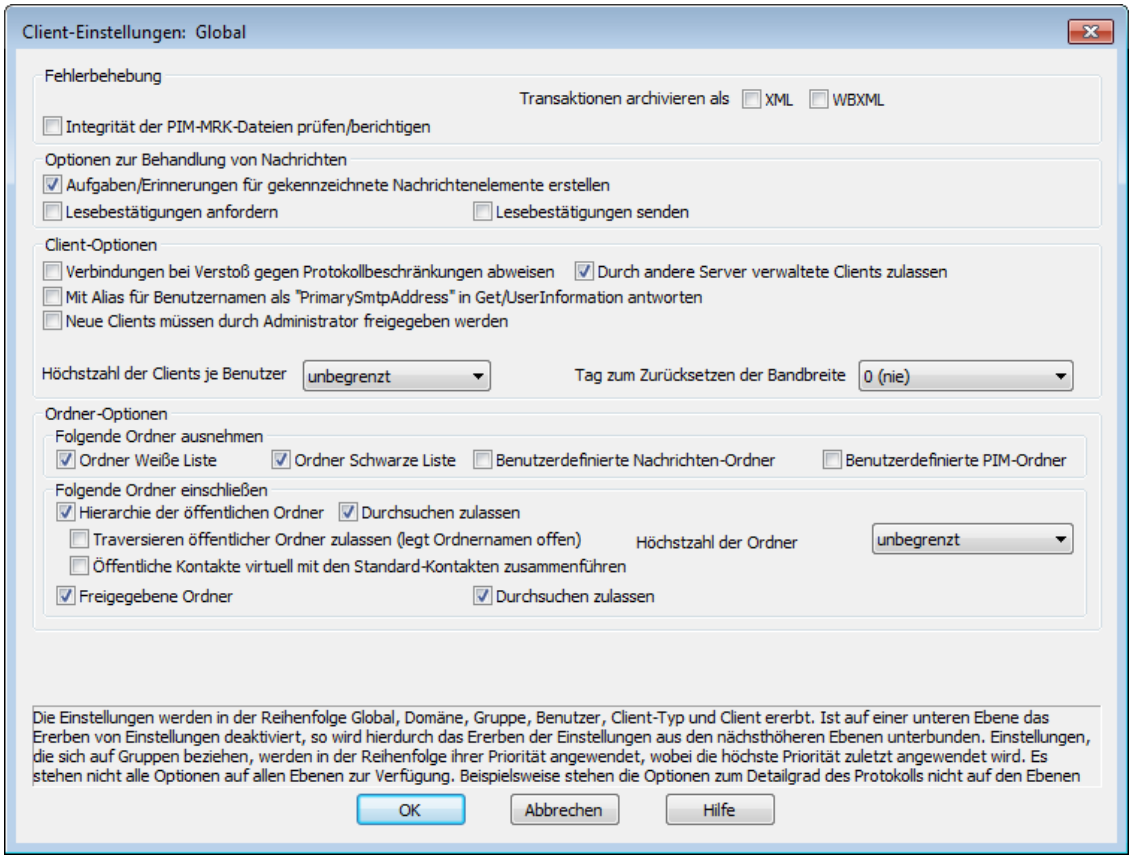
- [System] SendCorruptMessageNotifications=[Yes|No|1|0|True|False]: Versand der Benachrichtigung. Diese Option ist per Voreinstellung aktiv.
- [System] CMNCCUser==[0|1|Yes|No|True|False]: Versand der Benachrichtigung in Kopie an den betroffenen Benutzer. Diese Option ist per Voreinstellung aktiv.

Siehe auch:

ActiveSync » Diagnose 432

3.10.2.1 Client-Einstellungen

Der Konfigurationsdialog Client-Einstellungen enthält die voreingestellten Profile, die für die ActiveSync-Einstellungen angelegt sind. Sie können mithilfe gesonderter Konfigurationsdialoge Profile für die Client-Einstellungen für die folgenden Anwendungsbereiche erstellen und bearbeiten: Global, Domänen 206, Gruppen 474, Benutzerkonten 454, Client-Typen 481 und Clients 464 (dies sind die einzelnen Endgeräte).



Dieser Konfigurationsdialog enthält die systemweit gültigen, globalen Einstellungen für die Verwaltung der ActiveSync-Clients. Entsprechende Konfigurationsdialoge finden Sie auch in den Abschnitten Domänen 437, Benutzerkonten 454 und Clients 464. In diesem weiteren Abschnitten können Sie die Optionen nach Domänen,

Benutzerkonten und Clients getrennt festlegen. Für die globalen Einstellungen müssen Sie hier bestimmte Werte konfigurieren. Die Einstellungen auf den Ebenen der Domänen, Benutzerkonten und Clients sind per Voreinstellung so eingerichtet, dass sie ihre Einstellungen von dem ihnen jeweils übergeordneten Knoten *erben*. Falls Sie in diesem Konfigurationsdialog Änderungen vornehmen, wirken diese Änderungen daher per Voreinstellung auf alle untergeordneten Konfigurationsdialoge, sodass Sie per Voreinstellung alle Clients auf Ihrem Server direkt über diesen Konfigurationsdialog verwalten können. Ändern Sie in einem untergeordneten Konfigurationsdialog eine Einstellung, so übergeht diese Einstellung die hier getroffene Einstellung. Sie können somit nach Domänen, Benutzerkonten und Clients getrennte abweichende Einstellungen festlegen, falls dies erforderlich ist.

Das Prinzip der Einstellungen ist mit dem der Richtlinien 445 vergleichbar. Richtlinien werden Geräten zugewiesen und entscheiden im Allgemeinen über die Leistungsmerkmale, die Geräte nutzen dürfen. Client-Einstellungen entscheiden darüber, wie der Server verschiedene auf die Clients bezogene Optionen handhabt. Hierzu gehören die Entscheidung, wie viele verschiedene ActiveSync-Clients durch ein Benutzerkonto verwendet werden dürfen, ob öffentliche Ordner neben den persönlichen Ordnern der Benutzerkonten mit den Geräten synchronisiert werden dürfen, und ob die Freigabelisten der Benutzer einbezogen werden.

Allgemeines

Fehlerbehebung

Detailgrad für das Protokoll
ActiveSync für MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Einstellung erben Per Voreinstellung wird die Einstellung für den Detailgrad aus der Hierarchie der Client-Einstellungen vom jeweils übergeordneten Knoten ererbt. Clients übernehmen dabei die Einstellung aus dem jeweiligen Client-Typ, Client-Typen übernehmen die Einstellung von den Benutzerkonten, Benutzerkonten übernehmen die Einstellung von den Gruppen,

und so weiter. Die globale Einstellung für alle Clients wird durch die Einstellung für den Detailgrad im Konfigurationsdialog Diagnose 432 bestimmt.

Transaktionen archivieren als [XML | WBXML]
Mithilfe der Optionen *XML...* und *WBXML...* können Sie die zugehörigen Daten speichern; diese Daten können die Fehlersuche erleichtern. Die systemweit wirksamen Optionen sind per Voreinstellung abgeschaltet.

Integrität der PIM-MRK-Dateien prüfen/berichtigen
Diese Option führt für die PIM-Daten der betroffenen Clients Prüf- und Korrekturvorgänge durch. Sie sollen bekannte Probleme erkennen, die eine ordnungsgemäße Synchronisierung verhindern können. Zu diesen Problemen zählen insbesondere doppelte iCal-UIDs und leere Datenfelder, die eigentlich verpflichtend Daten enthalten müssen. Die systemweit wirksame Option ist per Voreinstellung abgeschaltet.

Client-Optionen

Verbindungen bei Verstoß gegen Protokollbeschränkungen abweisen
Diese Option bewirkt, dass Verbindungen von Clients abgewiesen werden, falls sie versuchen eine nicht für die Clients *Zugelassene Protokollversion* zu verwenden. Per Voreinstellung ist diese Option abgeschaltet; dies bedeutet, dass die Protokollbeschränkung keine Verbindungen solcher Clients verhindern, die andere als die zugelassenen Protokollversionen verwenden. Solange die Option abgeschaltet ist, weist MDaemon die Clients zwar an, nur die zugelassenen Protokollversionen zu verwenden, lässt aber bei Nutzung anderer Protokollversionen die Verbindung trotzdem zu. Nähere Informationen finden Sie unter Protokollbeschränkungen 434.

Mit Alias für Benutzernamen als "PrimarySmtpAddress" in Get/UserInformation antworten
Diese Option gestattet es dem Dienst, als Antwort auf eine Anforderung Settings/Get/UserInformation eine etwa vorhandene Alias-Adresse oder eine sekundäre Adresse des betroffenen Benutzerkontos als primäre Adresse zu übermitteln. Hierdurch wird ein Problem umgangen, das mit einer iOS-Aktualisierung nach Version 9.x verursacht wird, und das verhinderte, dass Clients unter einer etwa vorhandenen Alias-Adresse Nachrichten versenden konnten. Die Nutzung dieser Option bewirkt eine nicht standardkonforme Antwort auf die Anforderung Settings/GetUserInformation.

Neue Clients müssen durch Administrator freigegeben werden
Diese Option bewirkt, dass neue Clients sich erst dann mit Benutzerkonten synchronisieren können, wenn sie zunächst durch einen Administrator freigegeben wurden. In der Liste der Clients 464 sind alle Clients aufgeführt, die noch die Freigabe erwarten, und die Administratoren können sie über diese Liste freigeben. Diese Option ist per Voreinstellung abgeschaltet.

Höchstzahl der Clients je Benutzer
Mithilfe dieser Option können Sie die Anzahl der ActiveSync-Clients und -Endgeräte begrenzen, die mit jedem MDaemon-Benutzerkonto verknüpft sein können. Der hier angegebene Wert ist die Höchstzahl zulässiger Clients. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt. Diese Option steht nur in den Client-Einstellungen auf globaler, Domänen- und

Benutzerebene zur Verfügung, nicht jedoch in den Client-Einstellungen für die einzelnen Clients.

Tag zum Zurücksetzen der Bandbreite
Mithilfe dieser Option können Sie Tag bestimmen, an dem in jedem Monat die Bandbreiten-Nutzungsstatistik für die ActiveSync-Endgeräte zurückgesetzt wird. Dieser Vorgang wird während der normalen Bereinigungsvorgänge um Mitternacht aufgeführt und, wie auch andere Bereinigungsvorgänge, in das Protokoll System eingetragen. Der globale Wert lautet per Voreinstellung 0 (nicht zurücksetzen), sodass per Voreinstellung die Nutzungsstatistik nicht zurückgesetzt wird. Für untergeordnete Knoten können Sie abweichende Einstellungen treffen, etwa, um die Einstellung an den Tag anzugleichen, an dem für das betroffene Endgeräte ein neuer Abrechnungszeitraum des Netzbetreibers beginnt.

Sicherheit

Vom Länder-Filter ausnehmen
Wenn Sie diese Option in den Einstellungen eines ActiveSync-Clients aktivieren, kann das Endgerät den Länder-Filter 574 umgehen. Hierdurch kann ein berechtigter Benutzer auf sein Benutzerkonto über ActiveSync beispielsweise auch dann zugreifen, wenn er sich in einem Land befindet, für das Versuche zur Echtheitsbestätigung ansonsten durch den Länder-Filter unterbunden werden. Ein Endgerät kann nur dann vom Länder-Filter ausgenommen sein, wenn es innerhalb des durch die Option Inaktive Clients entfernen nach [x] Tagen 418 im Abschnitt Anpassung bestimmten Zeitraums eine echtheitsbestätigte Verbindung über ActiveSync erfolgreich hergestellt hat.

Adresse der Gegenstelle in Dynamische Freigabeliste aufnehmen
Wenn Sie ein Endgerät vom Länder-Filter ausnehmen, können Sie durch Aktivieren dieser Option die IP-Adresse, von der aus das Endgerät die Verbindung herstellt, in die Freigabeliste eintragen lassen. Hierdurch können beispielsweise andere Clients, die von der selben IP-Adresse aus eine Verbindung herstellen, ebenfalls zugelassen werden.

Durch andere Server provisionierte/verwaltete Clients zulassen
Per Voreinstellung dürfen Clients auch dann Verbindungen zu MDaemon aufbauen, wenn sie auf die Übermittlung der Provisionierungs- und Richtliniendaten durch den ActiveSync-Server hin melden, dass sie auch durch einen oder mehrere andere ActiveSync-Server verwaltet werden. Bei einer solchen Mehrfachverwaltung kann es nicht sichergestellt werden, dass alle auf Ihrem System bestehenden Richtlinien durch den Client auch umgesetzt werden; dies gilt insbesondere dann, wenn sie Richtlinien des anderen ActiveSync-Servers widersprechen. In vielen Fällen setzen die Clients die am stärksten einschränkende Richtlinie um, falls mehrere einander widersprechende Richtlinien vorhanden sind. Um Verbindungen von Clients zu unterbinden, die durch andere ActiveSync-Server verwaltet werden, deaktivieren Sie diese Option.

Löschen der Clients (Zurücksetzen in den Auslieferungszustand) nicht zulassen
Wenn diese Option aktiv ist, dann können ActiveSync-Clients nicht in den **Auslieferungszustand zurückgesetzt** und damit vollständig gelöscht werden. Wenn Sie Clients ferngesteuert in den Auslieferungszustand zurücksetzen wollen, müssen Sie diese Option deaktivieren. Diese Option ist per Voreinstellung deaktiviert. Nähere Informationen finden Sie auf der Seite Clients im Abschnitt **Vollständiges Löschen eines ActiveSync-Clients** 464.

Optionen zur Ordner-Synchronisierung

Optionen zur Ordner-Synchronisierung

Folgende Ordner ausnehmen

Freigegebene Absender/Gesperrte Absender
Per Voreinstellung werden die Kontaktordner mit Freigabelisten und Sperrlisten der Benutzer nicht mit den Geräten synchronisiert. Diese Ordner dienen üblicherweise nur in MDaemon zum Erkennen und Filtern von Spam. Ihre Inhalte brauchen daher nicht auf den Geräten als Kontakte angezeigt zu werden.

Benutzerdefinierte Nachrichten-Ordner
Per Voreinstellung können alle Standard- und benutzerdefinierten Nachrichten-Ordner mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-Nachrichtenordner synchronisiert werden können. Die Standard-Nachrichtenordner sind insbesondere Posteingang, Gesendete Objekte, Gelöschte Objekte und Entwürfe. Ordner, die die Benutzer selbst anlegen, werden dann nicht mehr synchronisiert. Diese Option ist per Voreinstellung abgeschaltet.

Benutzerdefinierte PIM-Ordner
Per Voreinstellung können alle PIM-Ordner (insbesondere Kontakte, Kalender, Notizen und Aufgaben) mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-PIM-Ordner synchronisiert werden können. Ist diese Option aktiv, so wird beispielsweise für jeden Benutzer nur der Standard-Kalender synchronisiert, auch wenn er über mehrere Kalender-Ordner verfügt. Diese Option ist per Voreinstellung abgeschaltet.

Folgende Ordner einschließen

Hierarchie der öffentlichen Ordner
Diese Option bewirkt, dass die öffentlichen Ordner[309], auf die die Benutzer Zugriff haben, in den Ordnerlisten der Benutzer auf ihren ActiveSync-Geräten erscheinen. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der öffentlichen Ordner[309], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Traversieren öffentlicher Ordner zulassen (legt Ordnernamen offen)
Benutzerkonten, die auf Unterordner in öffentlichen Ordnern zugreifen oder diese synchronisieren wollen, müssen per Voreinstellung sowohl für den betroffenen Unterordner als auch für alle ihm übergeordneten öffentlichen Ordner[309] über die Berechtigung Ordner anzeigen[311] verfügen. Fehlt einem Benutzerkonto diese Berechtigung für einen übergeordneten öffentlichen Ordner, so kann er auch den gewünschten Unterordner nicht synchronisieren und nicht auf ihn zugreifen, und zwar auch dann nicht, wenn das Benutzerkonto für diesen Unterordner selbst die erforderliche Berechtigung hat. Mithilfe dieser Option können Sie den Clients Zugriff auf und Synchronisierung von Unterordnern ermöglichen, ohne dass die Clients Berechtigungen für die übergeordneten öffentlichen Ordner haben. **Beachte:** Ist diese Option aktiv, so erlangt der Client zwangsläufig Kenntnis von den Namen der übergeordneten Ordner, auch wenn er für ihre Inhalte keine Zugriffsrechte hat. Hieraus kann sich ein Sicherheitsrisiko ergeben. Die Option

ist per Voreinstellung abgeschaltet.

Höchstzahl zulässiger öffentlicher Ordner
Diese Option begrenzt die Zahl der öffentlichen Ordner, die auf den betroffenen Geräten dargestellt werden können. Ist eine solche Höchstzahl angegeben, dann übermittelt der Server so lange Einträge in der Ordnerliste, bis die Höchstzahl erreicht ist. Danach übermittelt der Server keine Ordner mehr an die Geräte. Die Reihenfolge, in der die Ordner dabei verarbeitet werden, kann weder festgelegt noch vorher bestimmt werden. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt.

Freigegebene Ordner
Diese Option nimmt auch die gemeinsam genutzten Ordner[122], auf die die Benutzer Zugriff haben, in die Ordnerlisten auf ihren ActiveSync-Geräten auf. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der freigegebenen Ordner[742], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Behandlung von Inhalten

Optionen zur Behandlung von Inhalten

Aufgaben/Erinnerungen für durch Clients gekennzeichnete Nachrichtenelemente erstellen
Diese Option ermöglicht es MDaemon, die Benutzer an gekennzeichnete Elemente zu erinnern. Hierzu wird für jede gekennzeichnete E-Mail-Nachricht eine Aufgabe erstellt, wenn der Client dies anfordert. Die globale Option für dieses Leistungsmerkmal ist per Voreinstellung aktiv.

Aktualisierung nach jeder Änderung der Besprechung senden
Manche Clients versenden aktualisierte Besprechungseinladungen nicht richtig, nachdem eine Besprechung geändert wurde. Diese Option bewirkt, dass der ActiveSync-Dienst immer dann aktualisierte Besprechungseinladungen sendet, wenn der Besprechungsorganisator eine Besprechung aktualisiert hat. Diese Option sollte nur für Clients[464] und Client-Typen[481] aktiviert werden, die die aktualisierten Besprechungseinladungen nicht richtig versenden, da sonst aktualisierte Besprechungseinladungen doppelt versandt werden. Aus diesem Grund ist diese Einstellung nur auf den Seiten Clients und Client-Typen verfügbar.

Lesebestätigung für alle versandten Nachrichten anfordern
Diese Option bewirkt, dass der Server für alle durch einen Client versandten E-Mail-Nachrichten Lesebestätigungen anfordert. Diese Option ist per Voreinstellung abgeschaltet.

Vom Absender angeforderte Lesebestätigung senden, sobald Nachricht als gelesen gekennzeichnet ist
Diese Option bewirkt, dass der Server Anforderungen von Lesebestätigungen beachtet und die Lesebestätigungen dann versendet, wenn eine Nachricht durch den Client als gelesen gekennzeichnet wird. Diese Option ist per Voreinstellung abgeschaltet.

Unter dem in der Antwortadresse (ReplyTo) angegebenen Alias senden
Manche Clients gestatten den Absendern nicht den Versand von E-Mail-Nachrichten unter einem Alias. Dieses Leistungsmerkmal wurde im der Version 16.x des Protokolls Exchange ActiveSync (EAS) 434 erstmals unterstützt, aber manche Clients unterstützen die Version 16.x nicht. So nutzt beispielsweise Microsoft Outlook für Windows nur EAS 14.0 und gestattet zwar den Benutzern die Angabe einer anderen Adresse, unter der eine Nachricht versandt werden soll, aber die dann erstellte Nachricht gibt die Auswahl des Benutzers nicht richtig wieder. Diese Option gestattet die Nutzung des Feldes für die Antwortadresse (ReplyTo) zum Versand von Nachrichten dann, wenn als Antwortadresse ein gültiger Alias 827 des Benutzers eingetragen ist. Die globale Option ist per Voreinstellung aktiv.

Öffentliche Kontakte virtuell mit den Standard-Kontakten zusammenführen
Diese Option bewirkt, dass die öffentlichen Kontakte und die Standard-Kontakte der Benutzer auf ihren Geräten als zusammengeführt dargestellt werden. Die Datenbestände der Kontakte bleiben hierbei getrennt; es werden also keine Kontakte zwischen den Kontaktordnern der Benutzer kopiert. Diese Option kann insbesondere für solche Clients hilfreich sein, die das Durchsuchen der Globalen Adressliste (GAL) nicht unterstützen. Diese Option ist per Voreinstellung abgeschaltet.

Absender sperren, wenn Nachricht in Ordner Junk-Email verschoben wird
Ist diese Option aktiv, so wird die Absender-Adresse (Felder Sender und From) einer E-Mail-Adresse in den Kontaktordner für gesperrte Absender eingetragen, sobald ein Client die zugehörige E-Mail-Nachricht in den Ordner für Spam-Nachrichten verschiebt.

Antworten auf Besprechungsanfragen nach Zusage, Ablehnung usw. zwingend senden
Ist diese Option aktiv, so versendet der ActiveSync-Dienst eine Antwort an den Besprechungsorganisator immer dann, wenn ein Client auf eine Besprechungseinladung zusagt, sie ablehnt oder eine sonstige Aktion für die Einladung ausführt. Diese Option ist für solche Clients nützlich, die solche Antworten nicht selbst richtig senden.

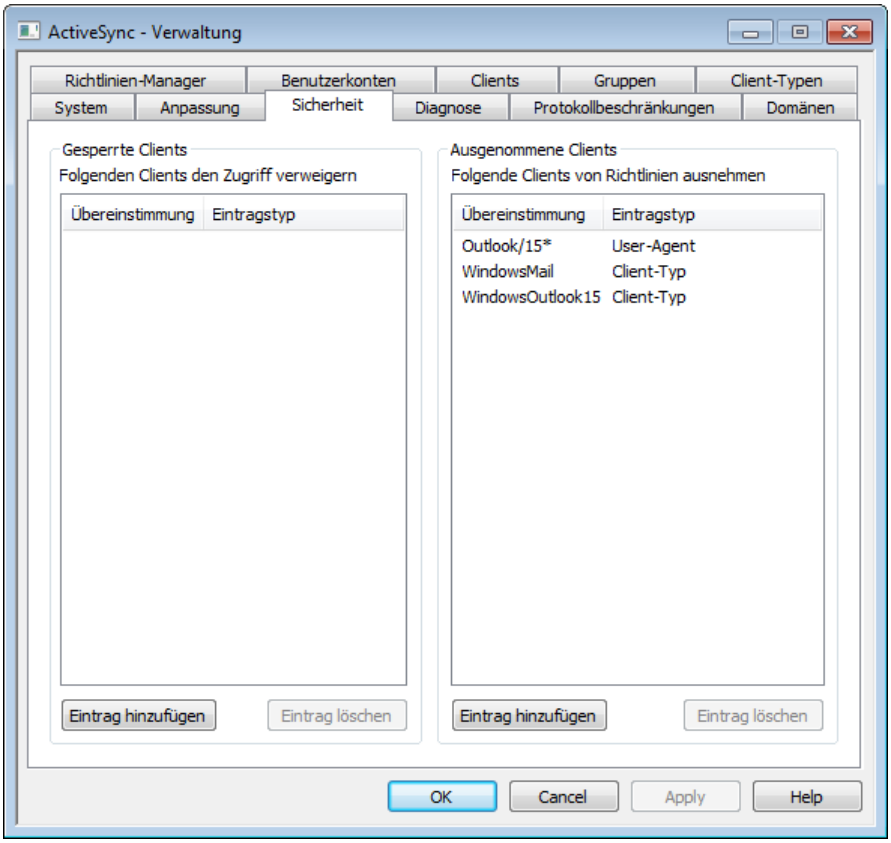
Vorschau auf tatsächlich wirksame Einstellungen

Dieses Steuerelement ist auf allen untergeordneten Konfigurationsdialogen für die Client-Einstellungen (Domänen 437, Benutzerkonten 454 und Clients 464) verfügbar. Per Voreinstellung werden die Optionen auf diesen Konfigurationsdialogen nicht von den übergeordneten Konfigurationsdialogen geerbt. Sie können sich daher mithilfe dieses Steuerelements die Einstellungen anzeigen lassen, die auf den jeweils gerade dargestellten Konfigurationsdialog wirken.

Siehe auch:

ActiveSync » Domänen 437
ActiveSync » Benutzerkonten 454
ActiveSync » Clients 464

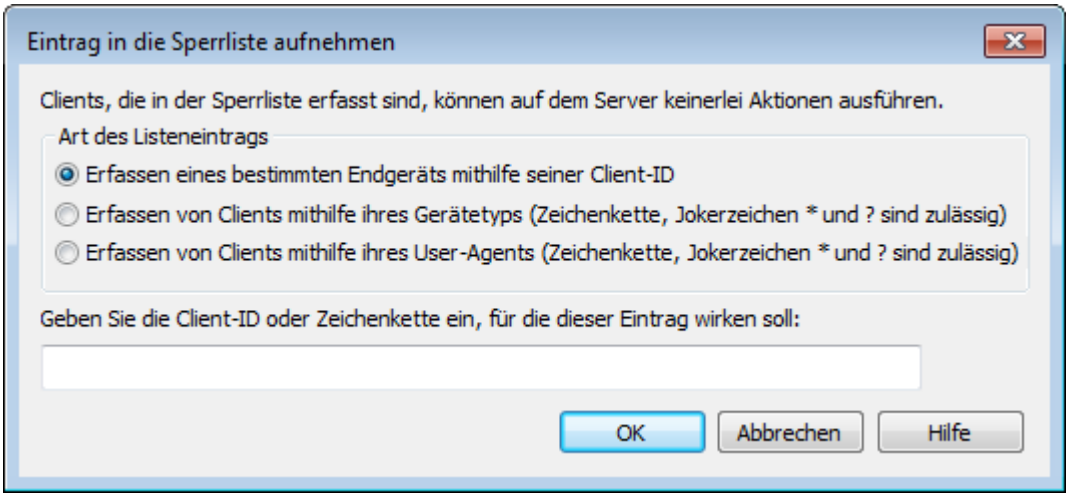
3.10.3 Sicherheit



Gesperrte Clients

Mithilfe dieser Option können Sie für bestimmte Gerätetypen, Geräte-IDs und User-Agents den Zugriff auf den ActiveSync-Server von MDaemon unterbinden.

Hinzufügen eines Eintrags zur Liste der gesperrten Clients
Um der Liste einen Eintrag hinzuzufügen, klicken Sie auf das Steuerelement **Eintrag hinzufügen**, geben Sie die entsprechenden Daten für das Gerät an, und klicken Sie auf **OK**. Sie können die benötigten Daten entweder aus dem Gerät selbst auslesen oder, falls das betroffene Gerät bereits eine Verbindung über ActiveSync mit MDaemon hergestellt hat, aus den ActiveSync-Protokolldateien von MDaemon ersehen.



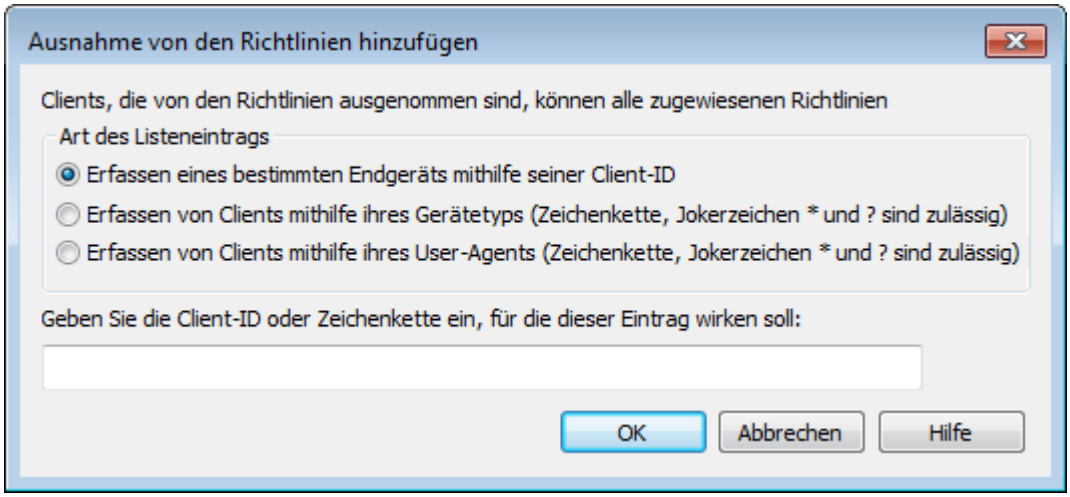
Sie können über den Konfigurationsdialog Geräte-Details[464] einzelne Clients einfach in die Liste der gesperrten Clients aufnehmen. Sie erreichen diesen Konfigurationsdialog über den Abschnitt Clients. Um einen Client in die Sperrliste aufzunehmen, wählen Sie den Client aus,klicken Sie auf **Details**, und klicken Sie dann auf **Diesen Client in die Sperrliste aufnehmen**.

Löschen eines Eintrags aus der Sperrliste
Um Einträge zu löschen, wählen Sie die gewünschten Einträge in der Liste aus, und klicken Sie dann auf das Steuerelement **Eintrag löschen**. Bevor die Einträge tatsächlich gelöscht werden, erscheint eine Sicherheitsabfrage.

Ausgenommene Clients

Mithilfe dieser Option können Sie bestimmte Gerätetypen, Geräte-IDs und User-Agents von der Provisionierung und den Beschränkungen aufgrund von Richtlinien[445] ausnehmen.

Hinzufügen eines Eintrags zur Liste der ausgenommenen Clients
Um der Liste einen Eintrag hinzuzufügen, klicken Sie auf das Steuerelement **Eintrag hinzufügen**, geben Sie die entsprechenden Daten für das Gerät an, und klicken Sie auf **OK**. Sie können die benötigten Daten entweder aus dem Gerät selbst auslesen oder, falls das betroffene Gerät bereits eine Verbindung über ActiveSync mit MDaemon hergestellt hat, aus den ActiveSync-Protokolldateien von MDaemon ersehen.



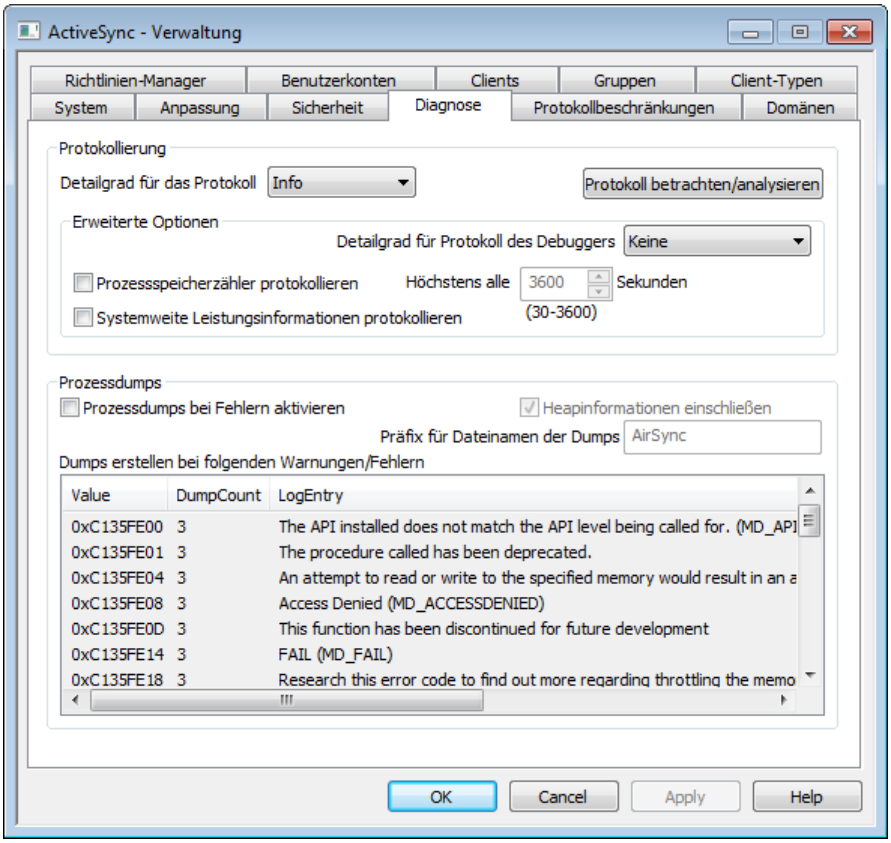
Sie können über den Konfigurationsdialog Geräte-Details 464 einzelne Clients einfach in die Liste der ausgenommenen Clients aufnehmen. Sie erreichen diesen Konfigurationsdialog über den Abschnitt Clients. Um einen Client in die Liste der ausgenommenen Clients aufzunehmen, wählen Sie den Client aus,klicken Sie auf **Details**, und klicken Sie dann auf **Client in Freigabeliste erfasst**.

Löschen eines Eintrags aus der Liste der ausgenommenen Clients
Um Einträge zu löschen, wählen Sie die gewünschten Einträge in der Liste aus, und klicken Sie dann auf das Steuerelement **Eintrag löschen**. Bevor die Einträge tatsächlich gelöscht werden, erscheint eine Sicherheitsabfrage.

Siehe auch:

ActiveSync » Clients 464

3.10.4 Diagnose



Dieser Konfigurationsdialog enthält erweiterte Optionen, die üblicherweise nur zur Fehlersuche oder zur Bereitstellung von Daten für den technischen Support gebraucht werden.

Protokollierung und Archivierung

Dieser Abschnitt enthält die globale Einstellung für den Detailgrad des ActiveSync-Protokolls. Diese Einstellung wird für Domänen übernommen, bei denen der Detailgrad für das Protokoll in den Client-Einstellungen für die Domänen[215] auf "Ererbte oder Voreinstellung nutzen" konfiguriert ist.

Detailgrad für das Protokoll
Der Cluster-Dienst von MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Protokolldatei betrachten/analysieren
Durch Anklicken dieses Steuerelements öffnet sich der erweiterte Protokollbetrachter für MDaemon. Per Voreinstellung werden die Protokolle im Verzeichnis "..\MDaemon\Logs\" gespeichert.

Erweiterte Optionen

Detailgrad für Protokoll des Debuggers
Diese Option bestimmt den geringsten zulässigen Detailgrad für die Protokolldaten, die an den Debugger übermittelt werden. Die auswählbaren Detailgrade sind dieselben wie in der Tabelle weiter oben.

Prozessspeicherzähler protokollieren
Mithilfe dieser Option können prozessspezifische Informationen über Speicher, Handle und Threads protokolliert werden. Diese Informationen sind hilfreich, um Probleme mit der Zuweisung von Ressourcen und vergleichbare Probleme zu diagnostizieren. Die Protokolleinträge werden nur ausgegeben, wenn die Daten sich seit der letzten Protokollierung geändert haben.

Systemweite Leistungsinformationen protokollieren
Mithilfe dieser Option können systemweite Leistungsdaten protokolliert werden. Diese Informationen sind hilfreich, um Probleme mit der Zuweisung von Ressourcen und vergleichbare Probleme zu diagnostizieren. Die Protokolleinträge werden nur ausgegeben, wenn die Daten sich seit der letzten Protokollierung geändert haben.

Höchstens alle [xx] Sekunden
Diese Option begrenzt die Häufigkeit, mit der die Prozess- und Leistungsinformationen protokolliert werden.

Prozessdumps

Prozessdumps bei Fehlern aktivieren
Diese Option bewirkt die Erstellung von Prozessdumps in den Fällen, in denen die weiter unten angegebenen Warnungen und Fehler auftreten.

Heapinformationen einschließen
Per Voreinstellung werden die Heapinformationen in die Prozessdumps aufgenommen. Falls Sie dies nicht wünschen, deaktivieren Sie dieses Kontrollkästchen.

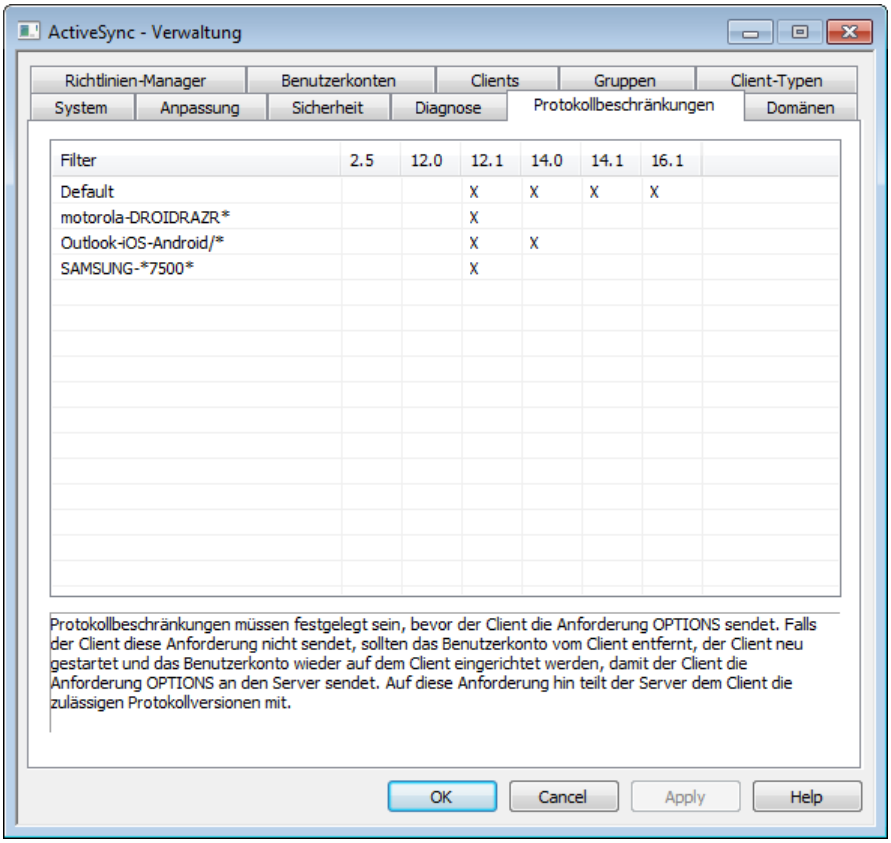
Präfix für Dateinamen der Dumps
Die Dateinamen der Dump-Dateien beginnen mit dem hier angegeben Text. Der Präfix lautet per Voreinstellung "AirSync".

Dumps erstellen bei folgenden Warnungen/Fehlern
Um diese Einträge zu bearbeiten, öffnen Sie durch Rechtsklick in diesem Bereich das Kontextmenü. Mithilfe der dann erscheinenden Menüeinträge *Eintrag hinzufügen, Eintrag bearbeiten* und *Eintrag löschen* können Sie die Liste der Fehler und Warnungen verwalten, die das Erstellen von Prozessdumps auslösen. Für jeden Eintrag können Sie die Anzahl der zulässigen Prozessdumps angeben; wird diese Zahl erreicht, so wird der Eintrag deaktiviert.

Siehe auch:

ActiveSync » Anpassung 418

3.10.5 Protokollbeschränkungen



Beschränkungen der für Geräte zugelassenen Protokolle

Mithilfe der Optionen im Konfigurationsdialog "ActiveSync » Protokollbeschränkungen" können Sie bestimmte Clients und Endgeräte darüber informieren, dass ihre ActiveSync-Protokollversionen von der Nutzung ausgeschlossen sind. Dies ist etwa dann hilfreich, wenn bei bestimmten Gerätetypen festgestellt wurde, dass sie einzelne Protokollversionen zuverlässig unterstützen, andere Protokollversionen hingegen nicht. Mithilfe des Editorfensters Protokollbeschränkung für Geräte hinzufügen/bearbeiten 435 können Sie diese Beschränkung auf der Grundlage der User-Agents oder der Gerätetypen festlegen, und Sie können die Geräte auf die Nutzung der ActiveSync-Protokollversionen 2.5, 12.0, 12.1, 14.0, 14.1 und 16.1 beschränken.

Per Voreinstellung verhindern die Protokollbeschränkungen nicht, dass ein Client ein eigentlich nicht zugelassenes Protokoll nutzt. Dem Client wird vielmehr nur mitgeteilt, welche Protokolle verwendet werden dürfen. Versucht ein Client dann trotzdem, ein eigentlich nicht zugelassenes Protokoll zu verwenden, so lässt MDaemon die Verbindung zu. Falls Sie wünschen, dass alle Verbindungen abgewiesen werden, die gegen eine Protokollbeschränkung verstoßen, aktivieren Sie die Option *Alle Beschränkungen verwendbarer Protokolle umsetzen* in den Konfigurationsdialogen für die Client-Einstellungen 422.

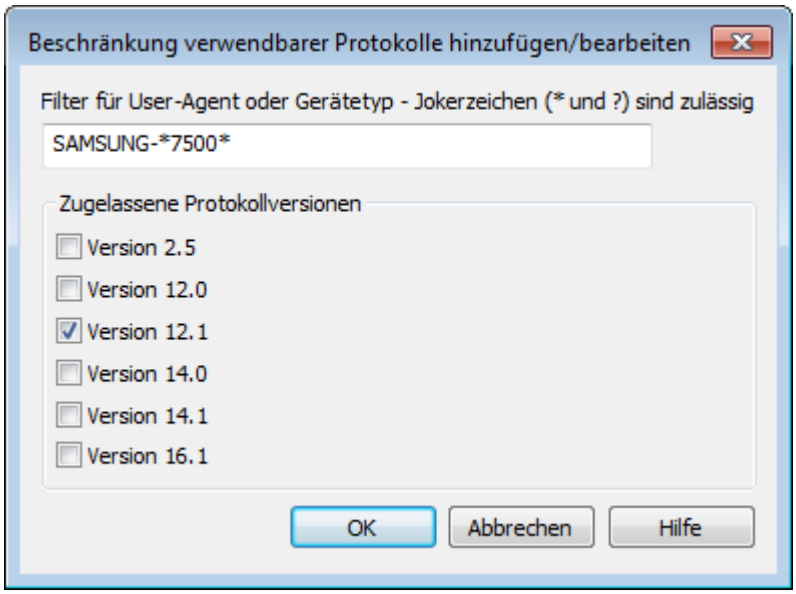
Um Einträge zu bearbeiten, führen Sie einen Rechtsklick auf dem gewünschten Eintrag in der Liste aus. Es erscheint dann ein Kontextmenü mit folgenden Einträgen:

Protokollbeschränkung erstellen
Durch Anklicken dieses Eintrags rufen Sie den Editor Beschränkung verwendbarer Protokolle hinzufügen/bearbeiten 435 auf. Dort können Sie die Protokollbeschränkungen festlegen und bearbeiten.

Protokollbeschränkung bearbeiten
Um eine Beschränkung eines Clients auf eine Protokollversion zu bearbeiten, klicken Sie doppelt auf den gewünschten Eintrag in der Liste (oder führen Sie einen Rechtsklick auf dem Eintrag aus, und klicken Sie dann auf **Beschränkung bearbeiten)**. Nachdem Sie im Editorfenster die gewünschten Änderungen vorgenommen haben, klicken Sie dort auf **OK**

Protokollbeschränkung löschen
Um eine Beschränkung aufzuheben, klicken Sie doppelt auf den gewünschten Eintrag in der Liste (oder führen Sie einen Rechtsklick auf dem Eintrag aus, und klicken Sie dann auf **Beschränkung löschen)**. Beantworten Sie die anschließende Sicherheitsabfrage mit **Ja**, um die Löschung zu bestätigen.

Beschränkung verwendbarer Protokolle hinzufügen/bearbeiten



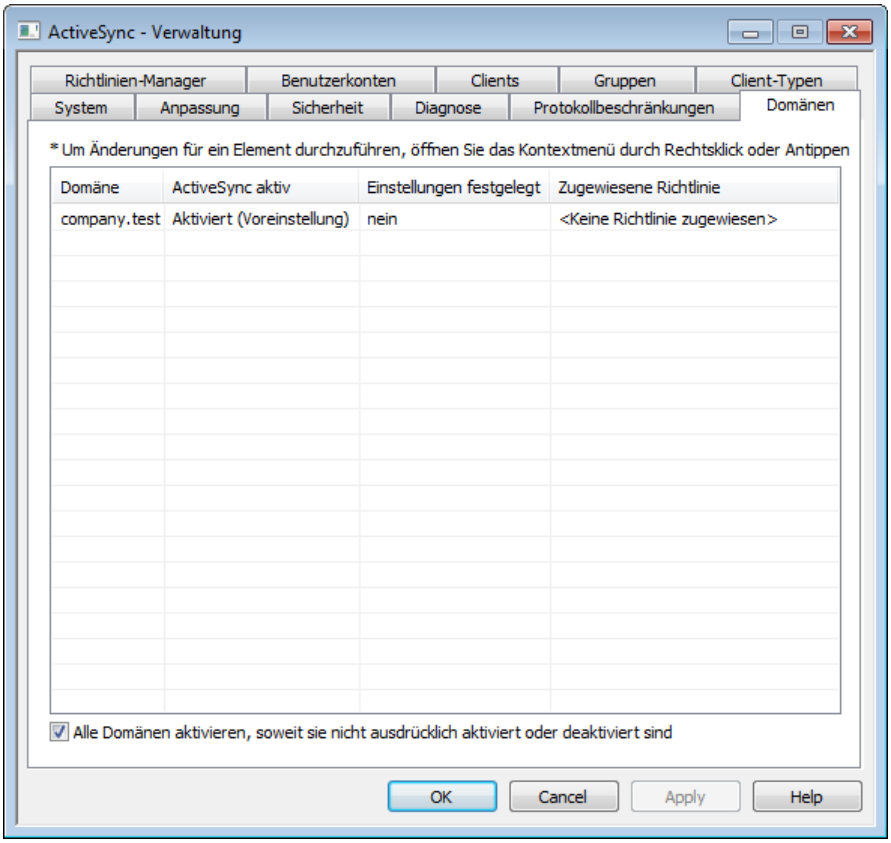
Merkmal für Geräte-Identifikation

Filter für User-Agent oder Gerätetyp
Falls die Protokollbeschränkung auf einen bestimmten User-Agent und/oder Gerätetypen wirken soll, wählen Sie diese Option, und geben Sie den User-Agent und den Gerätetyp an an. Bei der Auswertung der User-Agents berücksichtigt MDaemon die gesamte Zeichenkette bis zum ersten Zeichen "/" einschließlich, falls dieses Zeichen enthalten ist. Ist dieses Zeichen nicht enthalten, so wird die gesamte Zeichenkette ausgewertet. Falls Ihnen der genaue User-Agent oder Gerätetyp nicht bekannt ist, können Sie ihn im ActiveSync-Protokoll von MDaemon finden, sobald das entsprechende Gerät eine Verbindung über ActiveSync mit MDaemon hergestellt hat.

Gerätetyp
Falls die Protokollbeschränkung auf einen bestimmten Gerätetyp wirken soll, wählen Sie diese Option, und geben Sie den Gerätetyp an. Falls Ihnen der genaue Gerätetyp nicht bekannt ist, können Sie ihn in der Systeminformation des Geräts oder, sobald das entsprechende Gerät eine Verbindung über ActiveSync mit MDaemon hergestellt hat, im ActiveSync-Protokoll von MDaemon finden. Sie können diese Informationen auch dem Abschnitt Clients 464 entnehmen, indem Sie dort das betreffende Gerät auswählen und das Steuerelement Details anklicken.

Zugelassene Protokollversionen
Aktivieren Sie hier die Kontrollkästchen aller Protokollversionen, die für den User-Agent und/oder den Gerätetyp unterstützt werden sollen. Stellt der betroffene Client eine Verbindung mit MDaemon her, so wird er dann angewiesen, nur die hier ausgewählten Protokollversionen zu nutzen.

3.10.6 Domänen



Mithilfe dieses Konfigurationsdialogs können Sie die ActiveSync-Einstellungen für Ihre Domänen[181] verwalten. Sie können ActiveSync für jede Domäne aktivieren und deaktivieren, den Domänen ActiveSync-Richtlinien[445] zuweisen, die Standard-Einstellungen für die Clients bearbeiten und die Geräte verwalten, die mit der Domäne verknüpft sind.

ActiveSync für einzelne Domänen aktivieren/deaktivieren

Um ActiveSync für eine einzelne Domäne zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Führen Sie einen Rechtsklick auf dem Eintrag der gewünschten Domäne in der Liste aus.
2. Klicken Sie auf **Aktivieren**, **Deaktivieren** oder **Voreinstellung**. Die Einstellung "*Voreinstellung*" bedeutet, dass die Domäne die Standard-Einstellung übernimmt. Die Standard-Einstellung wird bestimmt durch die Option *Alle Domänen aktivieren, soweit sie nicht ausdrücklich aktiviert oder deaktiviert sind*.

Um ActiveSync zu nutzen, müssen Sie die ActiveSync-Clients auf den Endgeräten der Benutzer richtig konfigurieren. Informationen über die Konfiguration der Clients finden Sie in englischer Sprache, wenn Sie der Verknüpfung *ActiveSync für MDaemon lizensieren, upgraden oder verlängern* im Konfigurationsdialog ActiveSync für MDaemon[416] folgen und bis zu den

> Anweisungen für die Einrichtung der Endgeräte am Ende der Seite scrollen.

Standard-Aktivierungszustand für ActiveSync bearbeiten

Domänen, für die in der Spalte *ActiveSync aktiv* die Werte **Aktiviert (Voreinstellung)** oder **Deaktiviert (Voreinstellung)** eingetragen sind, übernehmen ihre ActiveSync-Einstellung von der Option **Alle Domänen aktivieren, soweit sie nicht ausdrücklich aktiviert oder deaktiviert sind**. Ist diese Option aktiv, so ist ActiveSync für alle Domänen per Voreinstellung aktiv. Ist diese Option nicht aktiv, so ist ActiveSync per Voreinstellung nicht aktiv. Um diese Option für einzelne Domänen zu übergehen, setzen Sie die betroffenen Domänen manuell auf **Aktiviert** oder **Deaktiviert**.

Falls Sie ActiveSync für die gerade bearbeitete Domäne deaktivieren, erscheint eine Sicherheitsabfrage, ob Sie allen Benutzern dieser Domäne die Berechtigung zur Nutzung von ActiveSync entziehen wollen. Um allen Benutzern, die die Berechtigung zur Nutzung von ActiveSync bereits haben, diese Berechtigung zu belassen, klicken Sie auf **Nein**. Um allen Benutzern, die die Berechtigung zur Nutzung von ActiveSync bereits haben, diese Berechtigung zu entziehen, klicken Sie auf **Ja**.

Client-Einstellungen für eine Domäne bearbeiten

Um die Client-Einstellungen für eine Domäne zu verwalten, führen Sie einen Rechtsklick auf dem Eintrag der Domäne in der Liste aus. Per Voreinstellung werden diese Einstellungen von den globalen Client-Einstellungen 422 als dem übergeordneten Knoten geerbt. Nähere Informationen hierzu finden Sie auch im Abschnitt Client-Einstellungen einer Domäne verwalten 438 weiter unten.

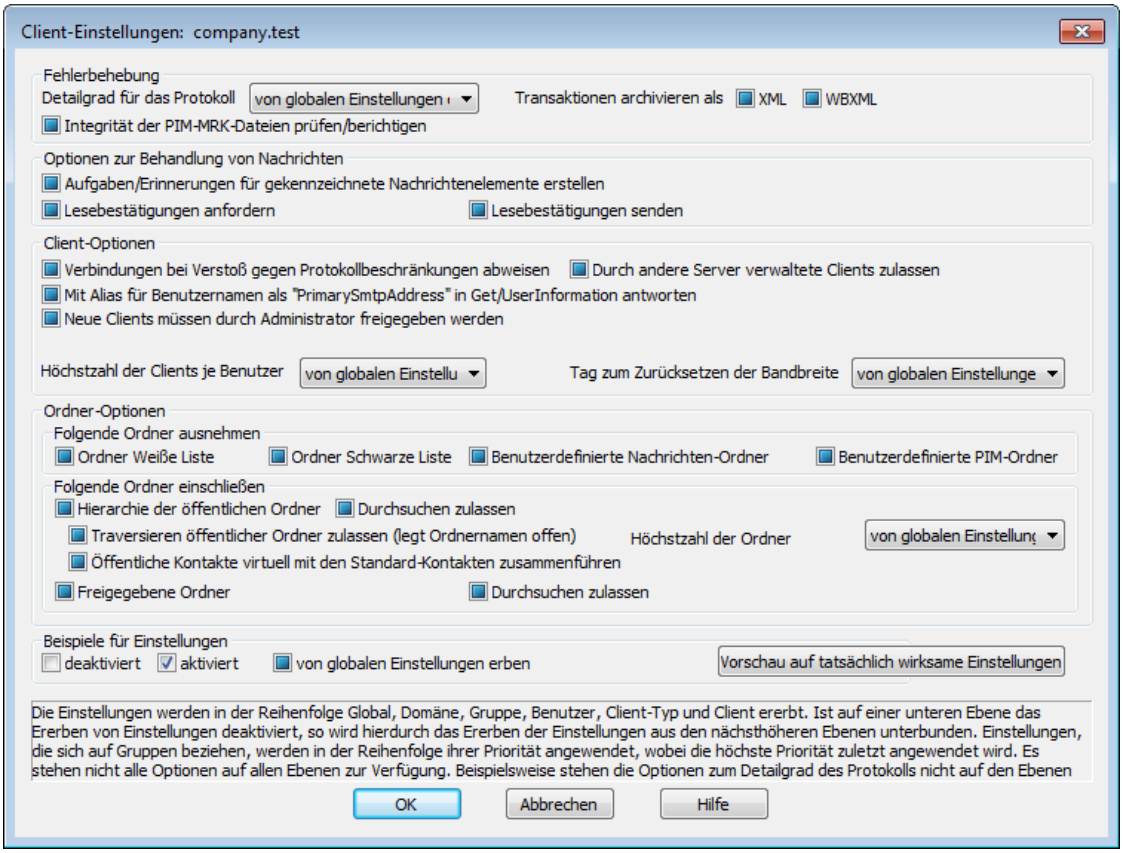
Zuweisen einer Standard-ActiveSync-Richtlinie

Um einer Domäne eine Standard-ActiveSync-Richtlinie zuzuweisen, gehen Sie folgendermaßen vor:

1. Führen Sie einen Rechtsklick auf dem Eintrag der betreffenden Domäne aus der Liste aus.
2. Klicken Sie auf **Richtlinie zuweisen**.
3. Wählen Sie aus der Dropdown-Liste im Bereich *Zuzuweisende Richtlinie* die gewünschte Richtlinie aus (Sie können diese Richtlinien mithilfe des Richtlinien-Managers 445 verwalten).
4. Klicken Sie auf **OK**.

Client-Einstellungen einer Domäne verwalten

Im Konfigurationsdialog Client-Einstellungen können Sie die Standard-Einstellungen für Benutzerkonten und Clients der gerade bearbeiteten Domäne festlegen.



Per Voreinstellung sind alle Optionen in diesem Konfigurationsdialog auf die Option "*Ererbte oder Voreinstellung nutzen*" konfiguriert. Sie erben daher die Einstellungen aus den globalen Client-Einstellungen[422]. In vergleichbarer Weise erben die Client-Einstellungen der Benutzerkonten[454] dieser Domäne die Einstellungen dieses vorliegenden Konfigurationsdialogs, da der Konfigurationsdialog Client-Einstellungen ihr übergeordneter Knoten ist. Falls Sie in diesem Konfigurationsdialog Änderungen vornehmen, wirken diese Änderungen daher per Voreinstellung auf alle untergeordneten Konfigurationsdialoge. Die einzelnen Clients[464] erben per Voreinstellung ihre Einstellungen von den Einstellungen der Benutzerkonten als ihrem übergeordneten Knoten. Sie können daher alle Benutzerkonten und Clients einer Domäne unmittelbar über den vorliegenden Konfigurationsdialog verwalten, und Sie können für einzelne Benutzerkonten und Clients getrennte abweichende Einstellungen festlegen, falls dies erforderlich ist.

Allgemeines

Fehlerbehebung

Detailgrad für das Protokoll

ActiveSync für MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden

allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Einstellung erben Per Voreinstellung wird die Einstellung für den Detailgrad aus der Hierarchie der Client-Einstellungen vom jeweils übergeordneten Knoten ererbt. Clients übernehmen dabei die Einstellung aus dem jeweiligen Client-Typ, Client-Typen übernehmen die Einstellung von den Benutzerkonten, Benutzerkonten übernehmen die Einstellung von den Gruppen, und so weiter. Die globale Einstellung für alle Clients wird durch die Einstellung für den Detailgrad im Konfigurationsdialog Diagnose 432 bestimmt.

Transaktionen archivieren als [XML | WBXML]
Mithilfe der Optionen *XML...* und *WBXML...* können Sie die zugehörigen Daten speichern; diese Daten können die Fehlersuche erleichtern. Die systemweit wirksamen Optionen sind per Voreinstellung abgeschaltet.

Integrität der PIM-MRK-Dateien prüfen/berichtigen
Diese Option führt für die PIM-Daten der betroffenen Clients Prüf- und Korrekturvorgänge durch. Sie sollen bekannte Probleme erkennen, die eine ordnungsgemäße Synchronisierung verhindern können. Zu diesen Problemen zählen insbesondere doppelte iCal-UIDs und leere Datenfelder, die eigentlich verpflichtend Daten enthalten müssen. Die systemweit wirksame Option ist per Voreinstellung abgeschaltet.

Client-Optionen

Verbindungen bei Verstoß gegen Protokollbeschränkungen abweisen
Diese Option bewirkt, dass Verbindungen von Clients abgewiesen werden, falls sie versuchen eine nicht für die Clients *Zugelassene Protokollversion* zu verwenden. Per Voreinstellung ist diese Option abgeschaltet; dies bedeutet, dass die Protokollbeschränkung keine Verbindungen solcher Clients verhindern, die andere als die zugelassenen Protokollversionen verwenden. Solange die Option abgeschaltet ist, weist MDaemon die Clients zwar an, nur die zugelassenen Protokollversionen zu verwenden, lässt aber bei Nutzung anderer Protokollversionen die Verbindung trotzdem zu. Nähere Informationen finden Sie unter Protokollbeschränkungen 434.

Mit Alias für Benutzernamen als "PrimarySmtpAddress" in Get/UserInformation antworten
Diese Option gestattet es dem Dienst, als Antwort auf eine Anforderung Settings/Get/UserInformation eine etwa vorhandene Alias-Adresse oder eine

sekundäre Adresse des betroffenen Benutzerkontos als primäre Adresse zu übermitteln. Hierdurch wird ein Problem umgangen, das mit einer iOS-Aktualisierung nach Version 9.x verursacht wird, und das verhinderte, dass Clients unter einer etwa vorhandenen Alias-Adresse Nachrichten versenden konnten. Die Nutzung dieser Option bewirkt eine nicht standardkonforme Antwort auf die Anforderung Settings/GetUserInformation.

Neue Clients müssen durch Administrator freigegeben werden
Diese Option bewirkt, dass neue Clients sich erst dann mit Benutzerkonten synchronisieren können, wenn sie zunächst durch einen Administrator freigegeben wurden. In der Liste der Clients[464] sind alle Clients aufgeführt, die noch die Freigabe erwarten, und die Administratoren können sie über diese Liste freigeben. Diese Option ist per Voreinstellung abgeschaltet.

Höchstzahl der Clients je Benutzer
Mithilfe dieser Option können Sie die Anzahl der ActiveSync-Clients und -Endgeräte begrenzen, die mit jedem MDaemon-Benutzerkonto verknüpft sein können. Der hier angegebene Wert ist die Höchstzahl zulässiger Clients. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt. Diese Option steht nur in den Client-Einstellungen auf globaler, Domänen- und Benutzerebene zur Verfügung, nicht jedoch in den Client-Einstellungen für die einzelnen Clients.

Tag zum Zurücksetzen der Bandbreite
Mithilfe dieser Option können Sie Tag bestimmen, an dem in jedem Monat die Bandbreiten-Nutzungsstatistik für die ActiveSync-Endgeräte zurückgesetzt wird. Dieser Vorgang wird während der normalen Bereinigungsvorgänge um Mitternacht aufgeführt und, wie auch andere Bereinigungsvorgänge, in das Protokoll System eingetragen. Der globale Wert lautet per Voreinstellung 0 (nicht zurücksetzen), sodass per Voreinstellung die Nutzungsstatistik nicht zurückgesetzt wird. Für untergeordnete Knoten können Sie abweichende Einstellungen treffen, etwa, um die Einstellung an den Tag anzugleichen, an dem für das betroffene Endgeräte ein neuer Abrechnungszeitraum des Netzbetreibers beginnt.

Sicherheit

Vom Länder-Filter ausnehmen
Wenn Sie diese Option in den Einstellungen eines ActiveSync-Clients aktivieren, kann das Endgerät den Länder-Filter[574] umgehen. Hierdurch kann ein berechtigter Benutzer auf sein Benutzerkonto über ActiveSync beispielsweise auch dann zugreifen, wenn er sich in einem Land befindet, für das Versuche zur Echtheitsbestätigung ansonsten durch den Länder-Filter unterbunden werden. Ein Endgerät kann nur dann vom Länder-Filter ausgenommen sein, wenn es innerhalb des durch die Option Inaktive Clients entfernen nach [x] Tagen[418] im Abschnitt Anpassung bestimmten Zeitraums eine echtheitsbestätigte Verbindung über ActiveSync erfolgreich hergestellt hat.

Adresse der Gegenstelle in Dynamische Freigabeliste aufnehmen
Wenn Sie ein Endgerät vom Länder-Filter ausnehmen, können Sie durch Aktivieren dieser Option die IP-Adresse, von der aus das Endgerät die Verbindung herstellt, in die Freigabeliste eintragen lassen. Hierdurch können beispielsweise andere Clients, die von der selben IP-Adresse aus eine Verbindung herstellen, ebenfalls zugelassen werden.

Durch andere Server provisionierte/verwaltete Clients zulassen
Per Voreinstellung dürfen Clients auch dann Verbindungen zu MDaemon aufbauen, wenn sie auf die Übermittlung der Provisionierungs- und Richtliniendaten durch den ActiveSync-Server hin melden, dass sie auch durch einen oder mehrere andere ActiveSync-Server verwaltet werden. Bei einer solchen Mehrfachverwaltung kann es nicht sichergestellt werden, dass alle auf Ihrem System bestehenden Richtlinien durch den Client auch umgesetzt werden; dies gilt insbesondere dann, wenn sie Richtlinien des anderen ActiveSync-Servers widersprechen. In vielen Fällen setzen die Clients die am stärksten einschränkende Richtlinie um, falls mehrere einander widersprechende Richtlinien vorhanden sind. Um Verbindungen von Clients zu unterbinden, die durch andere ActiveSync-Server verwaltet werden, deaktivieren Sie diese Option.

Löschen der Clients (Zurücksetzen in den Auslieferungszustand) nicht zulassen
Wenn diese Option aktiv ist, dann können ActiveSync-Clients nicht in den **Auslieferungszustand zurückgesetzt** und damit vollständig gelöscht werden. Wenn Sie Clients ferngesteuert in den Auslieferungszustand zurücksetzen wollen, müssen Sie diese Option deaktivieren. Diese Option ist per Voreinstellung deaktiviert. Nähere Informationen finden Sie auf der Seite Clients im Abschnitt **Vollständiges Löschen eines ActiveSync-Clients** 464.

Optionen zur Ordner-Synchronisierung

Optionen zur Ordner-Synchronisierung

Folgende Ordner ausnehmen

Freigegebene Absender/Gesperrte Absender
Per Voreinstellung werden die Kontaktordner mit Freigabelisten und Sperrlisten der Benutzer nicht mit den Geräten synchronisiert. Diese Ordner dienen üblicherweise nur in MDaemon zum Erkennen und Filtern von Spam. Ihre Inhalte brauchen daher nicht auf den Geräten als Kontakte angezeigt zu werden.

Benutzerdefinierte Nachrichten-Ordner
Per Voreinstellung können alle Standard- und benutzerdefinierten Nachrichten-Ordner mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-Nachrichtenordner synchronisiert werden können. Die Standard-Nachrichtenordner sind insbesondere Posteingang, Gesendete Objekte, Gelöschte Objekte und Entwürfe. Ordner, die die Benutzer selbst anlegen, werden dann nicht mehr synchronisiert. Diese Option ist per Voreinstellung abgeschaltet.

Benutzerdefinierte PIM-Ordner
Per Voreinstellung können alle PIM-Ordner (insbesondere Kontakte, Kalender, Notizen und Aufgaben) mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-PIM-Ordner synchronisiert werden können. Ist diese Option aktiv, so wird beispielsweise für jeden Benutzer nur der Standard-Kalender synchronisiert, auch wenn er über mehrere Kalender-Ordner verfügt. Diese Option ist per Voreinstellung abgeschaltet.

Folgende Ordner einschließen

Hierarchie der öffentlichen Ordner
Diese Option bewirkt, dass die öffentlichen Ordner[309], auf die die Benutzer Zugriff haben, in den Ordnerlisten der Benutzer auf ihren ActiveSync-Geräten erscheinen. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der öffentlichen Ordner[309], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Traversieren öffentlicher Ordner zulassen (legt Ordnernamen offen)
Benutzerkonten, die auf Unterordner in öffentlichen Ordnern zugreifen oder diese synchronisieren wollen, müssen per Voreinstellung sowohl für den betroffenen Unterordner als auch für alle ihm übergeordneten öffentlichen Ordner[309] über die Berechtigung Ordner anzeigen[311] verfügen. Fehlt einem Benutzerkonto diese Berechtigung für einen übergeordneten öffentlichen Ordner, so kann er auch den gewünschten Unterordner nicht synchronisieren und nicht auf ihn zugreifen, und zwar auch dann nicht, wenn das Benutzerkonto für diesen Unterordner selbst die erforderliche Berechtigung hat. Mithilfe dieser Option können Sie den Clients Zugriff auf und Synchronisierung von Unterordnern ermöglichen, ohne dass die Clients Berechtigungen für die übergeordneten öffentlichen Ordner haben. **Beachte:** Ist diese Option aktiv, so erlangt der Client zwangsläufig Kenntnis von den Namen der übergeordneten Ordner, auch wenn er für ihre Inhalte keine Zugriffsrechte hat. Hieraus kann sich ein Sicherheitsrisiko ergeben. Die Option ist per Voreinstellung abgeschaltet.

Höchstzahl zulässiger öffentlicher Ordner
Diese Option begrenzt die Zahl der öffentlichen Ordner, die auf den betroffenen Geräten dargestellt werden können. Ist eine solche Höchstzahl angegeben, dann übermittelt der Server so lange Einträge in der Ordnerliste, bis die Höchstzahl erreicht ist. Danach übermittelt der Server keine Ordner mehr an die Geräte. Die Reihenfolge, in der die Ordner dabei verarbeitet werden, kann weder festgelegt noch vorher bestimmt werden. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt.

Freigegebene Ordner
Diese Option nimmt auch die gemeinsam genutzten Ordner[122], auf die die Benutzer Zugriff haben, in die Ordnerlisten auf ihren ActiveSync-Geräten auf. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der freigegebenen Ordner[742], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Behandlung von Inhalten

Optionen zur Behandlung von Inhalten

Aufgaben/Erinnerungen für durch Clients gekennzeichnete Nachrichtenelemente erstellen
Diese Option ermöglicht es MDaemon, die Benutzer an gekennzeichnete Elemente

zu erinnern. Hierzu wird für jede gekennzeichnete E-Mail-Nachricht eine Aufgabe erstellt, wenn der Client dies anfordert. Die globale Option für dieses Leistungsmerkmal ist per Voreinstellung aktiv.

Aktualisierung nach jeder Änderung der Besprechung senden
Manche Clients versenden aktualisierte Besprechungseinladungen nicht richtig, nachdem eine Besprechung geändert wurde. Diese Option bewirkt, dass der ActiveSync-Dienst immer dann aktualisierte Besprechungseinladungen sendet, wenn der Besprechungsorganisator eine Besprechung aktualisiert hat. Diese Option sollte nur für Clients 464 und Client-Typen 481 aktiviert werden, die die aktualisierten Besprechungseinladungen nicht richtig versenden, da sonst aktualisierte Besprechungseinladungen doppelt versandt werden. Aus diesem Grund ist diese Einstellung nur auf den Seiten Clients und Client-Typen verfügbar.

Lesebestätigung für alle versandten Nachrichten anfordern
Diese Option bewirkt, dass der Server für alle durch einen Client versandten E-Mail-Nachrichten Lesebestätigungen anfordert. Diese Option ist per Voreinstellung abgeschaltet.

Vom Absender angeforderte Lesebestätigung senden, sobald Nachricht als gelesen gekennzeichnet ist
Diese Option bewirkt, dass der Server Anforderungen von Lesebestätigungen beachtet und die Lesebestätigungen dann versendet, wenn eine Nachricht durch den Client als gelesen gekennzeichnet wird. Diese Option ist per Voreinstellung abgeschaltet.

Unter dem in der Antwortadresse (ReplyTo) angegebenen Alias senden
Manche Clients gestatten den Absendern nicht den Versand von E-Mail-Nachrichten unter einem Alias. Dieses Leistungsmerkmal wurde im der Version 16.x des Protokolls Exchange ActiveSync (EAS) 434 erstmals unterstützt, aber manche Clients unterstützen die Version 16.x nicht. So nutzt beispielsweise Microsoft Outlook für Windows nur EAS 14.0 und gestattet zwar den Benutzern die Angabe einer anderen Adresse, unter der eine Nachricht versandt werden soll, aber die dann erstellte Nachricht gibt die Auswahl des Benutzers nicht richtig wieder. Diese Option gestattet die Nutzung des Feldes für die Antwortadresse (ReplyTo) zum Versand von Nachrichten dann, wenn als Antwortadresse ein gültiger Alias 827 des Benutzers eingetragen ist. Die globale Option ist per Voreinstellung aktiv.

Öffentliche Kontakte virtuell mit den Standard-Kontakten zusammenführen
Diese Option bewirkt, dass die öffentlichen Kontakte und die Standard-Kontakte der Benutzer auf ihren Geräten als zusammengeführt dargestellt werden. Die Datenbestände der Kontakte bleiben hierbei getrennt; es werden also keine Kontakte zwischen den Kontaktordnern der Benutzer kopiert. Diese Option kann insbesondere für solche Clients hilfreich sein, die das Durchsuchen der Globalen Adressliste (GAL) nicht unterstützen. Diese Option ist per Voreinstellung abgeschaltet.

Absender sperren, wenn Nachricht in Ordner Junk-Email verschoben wird
Ist diese Option aktiv, so wird die Absender-Adresse (Felder Sender und From) einer E-Mail-Adresse in den Kontaktordner für gesperrte Absender eingetragen, sobald ein Client die zugehörige E-Mail-Nachricht in den Ordner für Spam-Nachrichten verschiebt.

Antworten auf Besprechungsanfragen nach Zusage, Ablehnung usw. zwingend senden
Ist diese Option aktiv, so versendet der ActiveSync-Dienst eine Antwort an den Besprechungsorganisator immer dann, wenn ein Client auf eine Besprechungseinladung zusagt, sie ablehnt oder eine sonstige Aktion für die Einladung ausführt. Diese Option ist für solche Clients nützlich, die solche Antworten nicht selbst richtig senden.

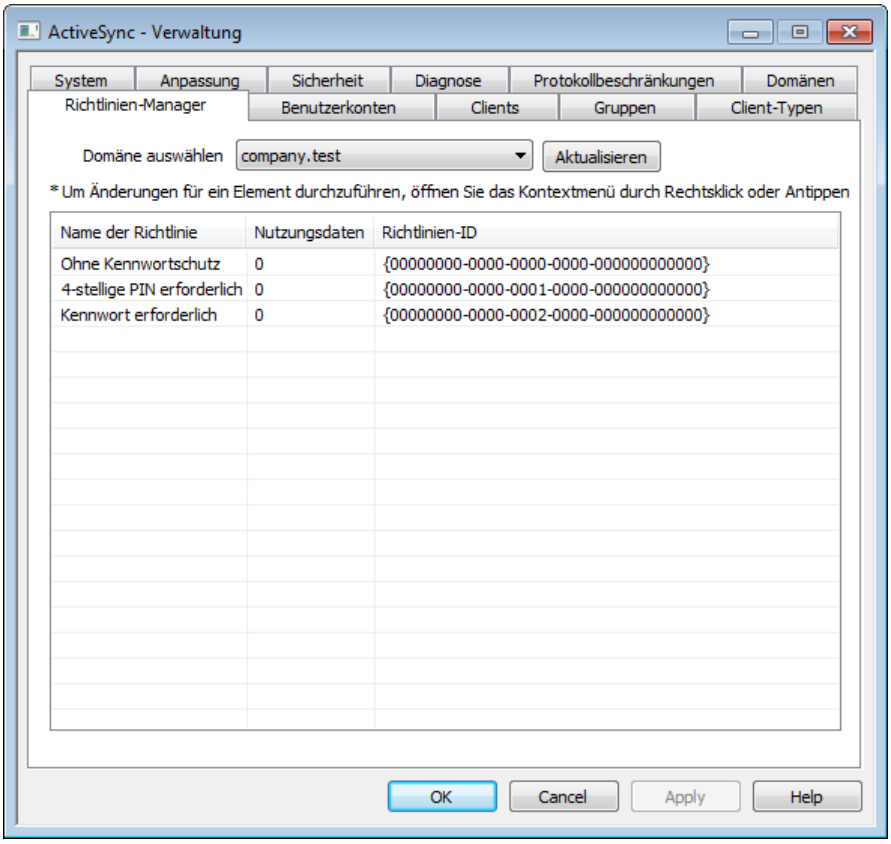
Vorschau auf tatsächlich wirksame Einstellungen

Dieses Steuerelement ist auf allen untergeordneten Konfigurationsdialogen für die Client-Einstellungen (Domänen 437, Benutzerkonten 454 und Clients 464) verfügbar. Per Voreinstellung werden die Optionen auf diesen Konfigurationsdialogen nicht von den übergeordneten Konfigurationsdialogen geerbt. Sie können sich daher mithilfe dieses Steuerelements die Einstellungen anzeigen lassen, die auf den jeweils gerade dargestellten Konfigurationsdialog wirken.

Siehe auch:

Domänen-Manager » ActiveSync - Client-Einstellungen 215
Domain Manager » ActiveSync - Clients 241
ActiveSync » Richtlinien-Manager 445
ActiveSync » Clients 464

3.10.7 Richtlinien-Manager



Mithilfe dieses Konfigurationsdialogs können Sie die ActiveSync-Geräterichtlinien verwalten. Die Richtlinien können ActiveSync-Geräten zugewiesen werden und

steuern auf ihnen verschiedene Optionen. Es stehen Ihnen vordefinierte Richtlinien zur Verfügung, und Sie können selbst Richtlinien erstellen, bearbeiten und löschen. Die Standard-Richtlinien können Domänen 437 und Benutzerkonten 454 zugewiesen werden. Richtlinien können darüber hinaus bestimmten Clients 241 zugewiesen werden.

Bitte beachten Sie, dass nicht alle ActiveSync-Endgeräte alle Richtlinien erkennen. Auch können in der Art der Umsetzung Unterschiede auftreten. Manche Geräte ignorieren bestimmte Elemente und Einstellungen der Richtlinien insgesamt; andere erfordern einen Neustart des Geräts, damit Änderungen wirksam werden. Eine Richtlinie kann jedenfalls frühestens dann wirksam werden, wenn das betroffene Gerät selbst eine Verbindung zum ActiveSync-Server herstellt. Eine "Push-Übermittlung" der Richtlinien an die Geräte, ohne dass diese eine Verbindung zum Server herstellen, ist nicht möglich.

ActiveSync-Richtlinien

Um Änderungen vorzunehmen, öffnen Sie durch Rechtsklick in diesem Bereich das Kontextmenü. Es stehen dann folgende Menüeinträge zur Verfügung:

Richtlinie erstellen
Durch Anklicken dieser Schaltfläche öffnen Sie den Editor für ActiveSync-Richtlinien 446, mit dessen Hilfe Sie die Richtlinien erstellen und bearbeiten können.

Richtlinie löschen
Um eine Richtlinie zu löschen, wählen Sie die gewünschte benutzerdefinierte Richtlinie aus der Übersicht aus, und klicken Sie dann auf *Richtlinie löschen*. Es erscheint eine Sicherheitsabfrage. Um Ihre Entscheidung zum Löschen der Richtlinie zu bestätigen, klicken Sie auf **Ja**. Die vordefinierten Richtlinien können nicht gelöscht werden.

Richtlinie bearbeiten
Um eine Richtlinie zu bearbeiten, wählen Sie die gewünschte benutzerdefinierte Richtlinie aus der Übersicht aus, und klicken Sie dann auf *Richtlinie bearbeiten*. Nehmen Sie die gewünschten Änderungen im Editor für ActiveSync-Richtlinien vor, und klicken Sie dann auf **OK**. Die vordefinierten Richtlinien können nicht bearbeitet werden.

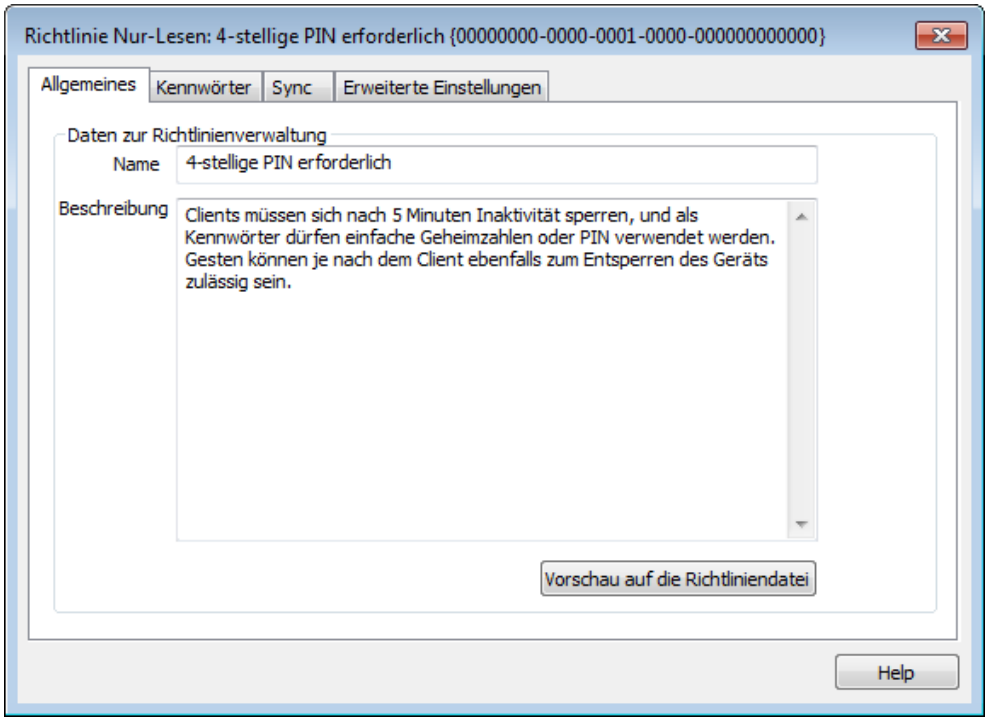
Richtlinien-Nutzungsdaten anzeigen
Durch Anklicken dieser Schaltfläche erhalten Sie eine Übersicht aller Domänen, Benutzerkonten und Clients, denen eine Richtlinie zugewiesen ist. Um diese Übersicht zu erhalten, wählen Sie die gewünschte Richtlinie aus, und klicken Sie dann auf diese Schaltfläche.

Editor für ActiveSync-Richtlinien

Der Editor für ActiveSync-Richtlinien ist in vier Registerkarten unterteilt: Allgemeines, Kennwörter, Sync und Erweiterte Einstellungen. Die Registerkarte Erweiterte Einstellungen ist nur dann sichtbar, wenn Sie die Option *Bearbeiten erweiterter Richtlinienoptionen zulassen* 416 aktivieren. Sie finden diese Option im Konfigurationsdialog ActiveSync-System.

Allgemeines

Auf dieser Registerkarte legen Sie einen Namen und eine Beschreibung für die Richtlinie fest. Sie können auch eine Vorschau auf die Richtliniendatei mit dem aus der Richtlinie erstellten XML-Kode erhalten.



Daten zur Richtlinienverwaltung

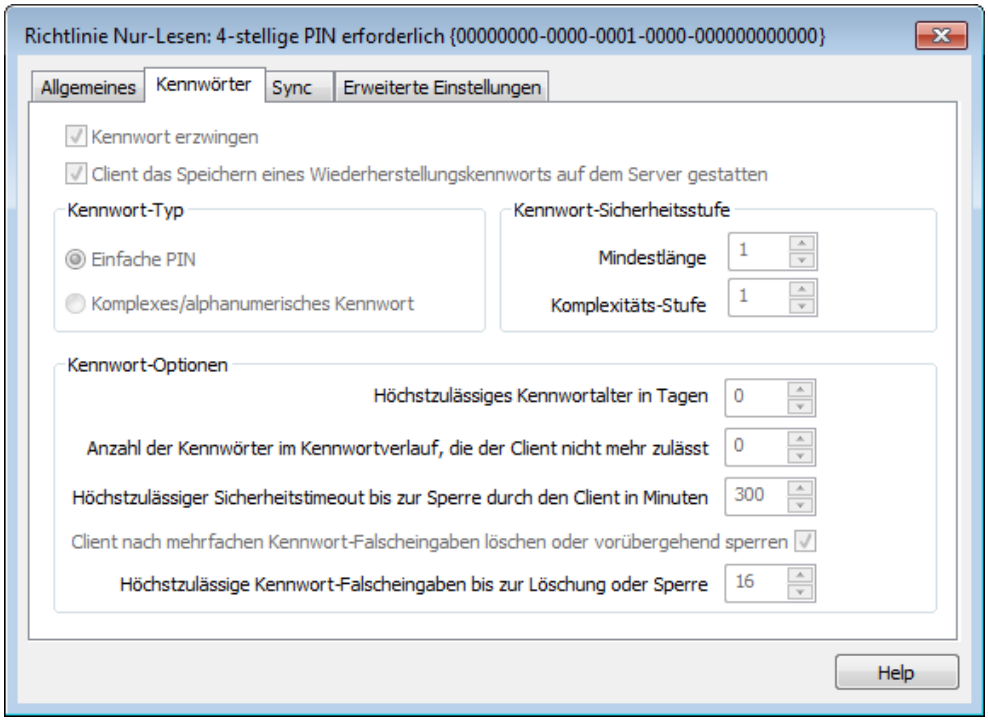
Name
Geben Sie hier den Namen für die benutzerdefinierte Richtlinie ein.

Beschreibung
Geben Sie hier eine Beschreibung für die benutzerdefinierte Richtlinie ein. Diese Beschreibung erscheint unterhalb der Liste der Richtlinien, wenn Sie diese Richtlinie.

Vorschau auf die Richtliniendatei
Um eine Vorschau auf die Richtliniendatei mit dem XML-Kode für die gerade bearbeitete Richtlinie zu erhalten, klicken Sie auf dieses Steuerelement.

Kennwörter

Auf dieser Registerkarte legen Sie die Optionen und Anforderungen an die Kennwörter fest.



Kennwort erzwingen
Diese Option bewirkt, dass auf dem Gerät ein Kennwort gesetzt werden muss. Sie ist per Voreinstellung abgeschaltet.

Gerät das Speichern eines Wiederherstellungskennworts auf dem Server gestatten
Diese Option ermöglicht es den Clients, die ActiveSync-Option zum Wiederherstellen von Kennwörtern zu nutzen. Diese Option speichert auf dem Server ein vorübergehend nutzbares Wiederherstellungskennwort; mit seiner Hilfe kann das Gerät entsperrt werden, falls das Kennwort vergessen wurde. Der Systemverwalter kann dieses Wiederherstellungskennwort im Abschnitt Details 464 für das jeweilige Gerät finden. Die meisten Geräte unterstützen diese Funktion nicht.

Kennwort-Typ

Einfache PIN
Die Wirkung dieser Option hängt wesentlich von der Implementation auf dem jeweiligen Gerät ab. Im Allgemeinen bewirkt diese Option, dass für das Kennwort nur die *Mindestlänge* eingehalten werden muss, ansonsten aber keine Anforderungen an die Komplexität gestellt werden. Diese Option lässt daher auch einfache Kennwörter zu, wie etwa "111", "aaa", "1234", "ABCD" und ähnliches.

Komplexes/alphanumerisches Kennwort
Diese Option erzwingt komplexere und sicherere Gerätekennwörter als die Option *Einfache PIN*. Die Option *Komplexitäts-Stufe* bestimmt im Zusammenhang mit dieser Option die genauen Anforderungen an die Komplexität des Kennworts. Diese Option ist per Voreinstellung aktiv, falls die Richtlinie die Nutzung eines Kennworts erzwingt.

Kennwort-Sicherheitsstufe

Mindestlänge
Diese Option bewirkt, dass das Gerätekennwort mindestens die hier festgelegte Länge haben muss. Die Mindestlänge kann 1 bis 16 Zeichen betragen. Der Wert beträgt per Voreinstellung 1.

Komplexitäts-Stufe
Diese Option bestimmt die Anforderungen an *komplexe/alphanumerische Kennwörter.* Der Wert der Komplexitäts-Stufe legt fest, wie viele verschiedene Zeichenarten das Kennwort enthalten muss. Zeichenarten sind dabei Großbuchstaben, Kleinbuchstaben, Ziffern und nicht-alphanumerische Zeichen (etwa Satzzeichen und Sonderzeichen). Sie können 1 bis 4 verschiedene Zeichentypen verlangen. Wird hier beispielsweise der Wert 2 eingetragen, so muss das Kennwort mindestens zwei verschiedene Zeichenarten aus der Auswahl Großbuchstaben, Kleinbuchstaben, Ziffern und nicht-alphanumerische Zeichen enthalten. Der Wert beträgt per Voreinstellung 1.

Kennwort-Optionen

Höchstzulässiges Kennwortalter in Tagen
Diese Option bewirkt, dass das Gerätekennwort geändert werden muss, sobald es das hier in Tagen angegebene Alter überschritten hat. Sie ist per Voreinstellung abgeschaltet (Wert "0").

Anzahl der Kennwörter im Kennwortverlauf, die das Gerät nicht mehr zulässt
Diese Option bewirkt, dass auf dem Geräte eine Kennwortchronik geführt wird, die verhindert, dass die Benutzer einmal verwendete Gerätekennwörter zu bald wieder verwenden. Der Wert der Option legt fest, wie viele Kennwörter in der Kennwortchronik gespeichert werden. Wird hier etwa der wert "2" eingetragen, und ändert der Benutzer das Gerätekennwort, so darf er als neues Kennwort die letzten beiden Kennwörter, die er verwendet hat, nicht erneut verwenden. Die Option ist per Voreinstellung abgeschaltet (Wert "0").

Höchstzulässiger Sicherheitstimeout bis zur Sperre durch das Gerät in Minuten
Diese Option bestimmt, wie lange ein Gerät ohne Benutzereingaben in Bereitschaft bleiben darf, bevor es sich selbst sperrt. Nach dieser Sperre muss der Benutzer das Gerätekennwort eingeben, wenn er das Gerät wieder nutzen will. Diese Option ist per Voreinstellung abgeschaltet (Wert "0").

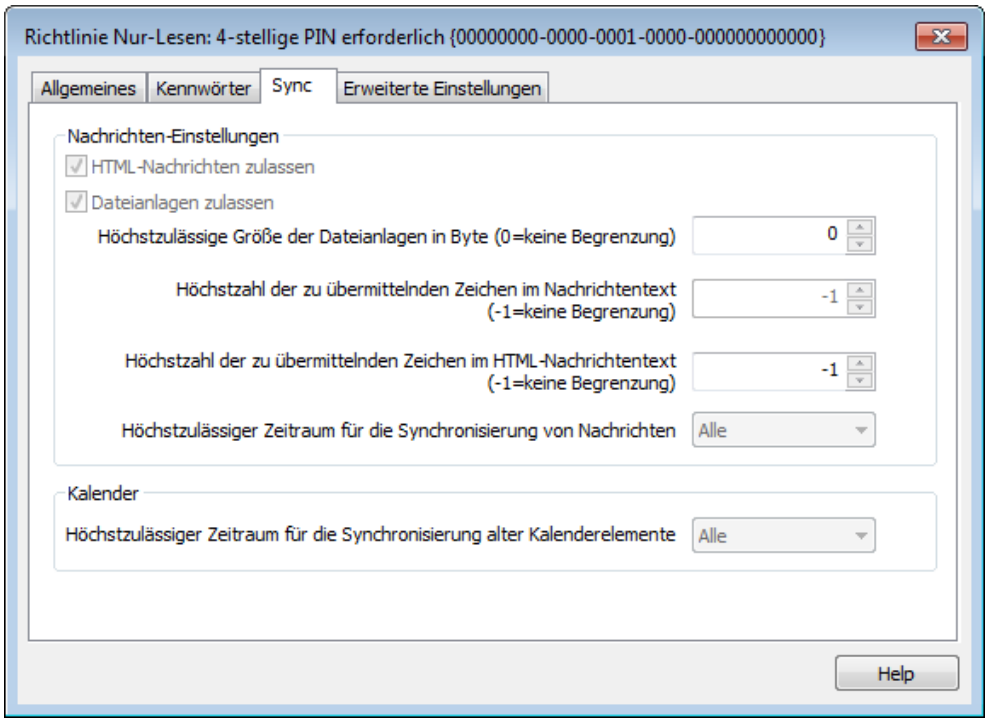
Gerät nach mehrfachen Kennwort-Falscheingaben löschen oder vorübergehend sperren
Diese Option bewirkt, dass sich das Gerät für eine bestimmte Zeit gegen weitere Eingabeversuche sperrt oder sämtliche Daten automatisch löscht, falls der Benutzer das Kennwort mehrfach hintereinander falsch eingibt und dabei die hier festgelegte Höchstzahl an Versuchen überschreitet. Diese Option ist per Voreinstellung abgeschaltet.

Höchstzulässige Kennwort-Falscheingaben bis zur Löschung oder Sperre
Diese Option legt fest, wie viele Versuche für den Benutzer zulässig sind, das Gerätekennwort richtig einzugeben, bevor sich das Gerät sperrt oder löscht. Welche Aktion das Gerät danach durchführt, hängt von dem Gerät

selbst ab. Die Option ist per Voreinstellung abgeschaltet. Diese Option wirkt nur, wenn die Option *Gerät nach mehrfachen Kennwort-Falscheingaben löschen oder vorübergehend sperren* weiter oben aktiv ist.

Sync

Auf dieser Registerkarte konfigurieren Sie verschiedene Optionen für HTML-Nachrichten, die Nutzung von Dateianlagen, die Begrenzung des Datenvolumens für die Übertragung und die Zeiträume, für die E-Mail- und Kalenderdaten synchronisiert werden dürfen.



Nachrichten-Einstellungen

HTML-Nachrichten zulassen
Per Voreinstellung können E-Mail-Nachrichten im HTML-Format an ActiveSync-Clients übermittelt und mit ihnen synchronisiert werden. Falls Sie die Übermittlung und Synchronisierung auf Nur-Text-Nachrichten beschränken wollen, deaktivieren Sie diese Option.

Dateianlagen zulassen
Diese Option gestattet den Geräten das Herunterladen von Dateianlagen. Die Option ist per Voreinstellung aktiv.

Höchstzulässige Größe der Dateianlagen in Byte (0=keine Begrenzung)
Diese Option bestimmt, wie groß Dateianlagen höchstens sein dürfen, damit sie noch automatisch auf das Gerät übermittelt werden. Per Voreinstellung besteht keine Größenbegrenzung (Wert "0").

Höchstzahl der zu übermittelnden Zeichen im Nachrichtentext (-1=keine Begrenzung)
Dieser Wert legt die Höchstzahl der Zeichen im Nachrichtentext von Nur-

Text-Nachrichten fest, die an den Client übermittelt werden. Enthält der Nachrichtentext mehr Zeichen, so wird der Nachrichtentext nach Erreichen des hier festgelegten Grenzwerts abgeschnitten. Per Voreinstellung ist keine Begrenzung aktiv (Wert -1). Falls Sie diesen Wert auf 0 setzen, werden nur die Kopfzeilen der Nachrichten übermittelt.

Höchstzahl der zu übermittelnden Zeichen im HTML-Nachrichtentext (-1=keine Begrenzung)
Dieser Wert legt die Höchstzahl der Zeichen im Nachrichtentext von HTML-Nachrichten fest, die an den Client übermittelt werden. Enthält der Nachrichtentext mehr Zeichen, so wird der Nachrichtentext nach Erreichen des hier festgelegten Grenzwerts abgeschnitten. Per Voreinstellung ist keine Begrenzung aktiv (Wert -1). Falls Sie diesen Wert auf 0 setzen, werden nur die Kopfzeilen der Nachrichten übermittelt.

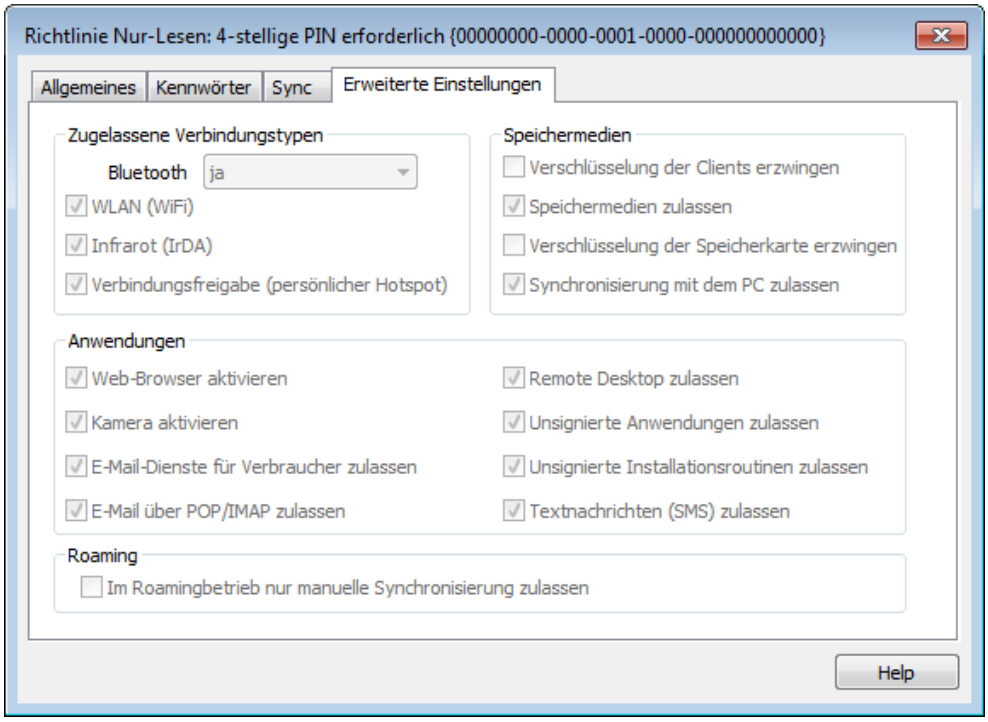
Höchstzulässiger Zeitraum für die Synchronisierung von Nachrichten
Dieses Intervall bestimmt den Zeitraum, jeweils gerechnet von dem aktuellen Tag, für den E-Mail-Nachrichten mit dem Gerät synchronisiert werden können. Per Voreinstellung ist der Wert "Alle" aktiv, sodass alle E-Mail-Nachrichten unabhängig von ihrem Alter mit dem Gerät synchronisiert werden können.

Kalender

Höchstzulässiger Zeitraum für die Synchronisierung alter Kalenderelemente
Dieses Intervall bestimmt den Zeitraum, jeweils gerechnet von dem aktuellen Tag, für den Kalendereinträge mit dem Gerät synchronisiert werden können. Per Voreinstellung ist der Wert "Alle" aktiv, sodass alle Kalendereinträge unabhängig von ihrem Alter mit dem Gerät synchronisiert werden können.

Erweiterte Einstellungen

Auf dieser Registerkarte legen Sie die zugelassenen Verbindungstypen und Anwendungen sowie Einstellungen zu Speichermedien, Verschlüsselung und Roaming fest.



Diese Registerkarte ist nur dann sichtbar, wenn Sie die Option *Bearbeiten erweiterter Richtlinienoptionen zulassen* 416 aktivieren. Sie finden diese Option im Konfigurationsdialog ActiveSync für MDaemon.

Zugelassene Verbindungstypen

Bluetooth

Diese Option bestimmt, ob das Gerät Bluetooth-Verbindungen zulässt. Um Bluetooth-Verbindungen zuzulassen, wählen Sie **ja**, um Bluetooth-Verbindungen zu unterbinden, wählen Sie **nein**, und um Bluetooth-Verbindungen zuzulassen, aber auf Verbindungen mit Freisprechanlagen zu beschränken, wählen Sie **Freisprechen**. Die Voreinstellung für diese Option ist **ja**.

WLAN (WiFi)

Diese Option bestimmt, ob das Gerät WLAN-Verbindungen (WiFi) zulässt. Die Option ist per Voreinstellung aktiv.

Infrarot (IrDA)

Diese Option bestimmt, ob das Gerät Infrarot-Verbindungen (IrDA) zulässt. Die Option ist per Voreinstellung aktiv.

Verbindungsfreigabe (persönlicher Hotspot)

Diese Option bestimmt, ob das Gerät als persönlicher Hotspot arbeiten und die Internet-Verbindungsfreigabe anbieten darf. Die Option ist per Voreinstellung aktiv.

Speichermedien

Geräteverschlüsselung erzwingen

Diese Option bewirkt, dass die Verschlüsselung der Inhalte auf dem Gerät erforderlich ist. Sie wird jedoch nicht durch alle Geräte umgesetzt. Sie ist

per Voreinstellung abgeschaltet.

Speichermedien zulassen
Diese Option bewirkt, dass das Gerät die Nutzung von Speicherkarten zulässt. Die Option ist per Voreinstellung aktiv.

Verschlüsselung der Speicherkarte erzwingen
Diese Option bewirkt, dass das Gerät die Speicherkarten zwingend verschlüsselt. Die Option ist per Voreinstellung abgeschaltet.

Synchronisierung mit dem PC zulassen
Diese Option lässt die Synchronisierung mit PCs über ActiveSync zu. Die Option ist per Voreinstellung aktiv.

Anwendungen

Web-Browser aktivieren
Diese Option bewirkt, dass der Browser auf dem Gerät genutzt werden darf. Sie wird auf einigen Geräten nicht unterstützt, und sie wirkt unter Umständen nicht auf Browser von Drittanbietern. Diese Option ist per Voreinstellung aktiv.

Kamera aktivieren
Diese Option bewirkt, dass die Kamera auf dem Gerät genutzt werden darf. Sie ist per Voreinstellung aktiv.

E-Mail-Dienste für Verbraucher zulassen
Diese Option bewirkt, dass der Benutzer auf dem Gerät persönliche E-Mail-Konten einrichten kann. Ist diese Option deaktiviert, dann hängt es von dem jeweils eingesetzte ActiveSync-Client ab, welche Arten von E-Mail-Benutzerkonten und E-Mail-Diensten noch nutzbar sind. Die Option ist per Voreinstellung aktiv.

E-Mail über POP/IMAP zulassen
Diese Option gestattet die Nutzung der Protokolle POP und IMAP für E-Mail-Benutzerkonten. Die Option ist per Voreinstellung aktiv.

Remote Desktop zulassen
Diese Option gestattet dem Client die Nutzung des Remote Desktops. Die Option ist per Voreinstellung aktiv.

Unsignierte Anwendungen zulassen
Diese Option gestattet die Nutzung unsignierte Anwendungen auf dem Gerät. Die Option ist per Voreinstellung aktiv.

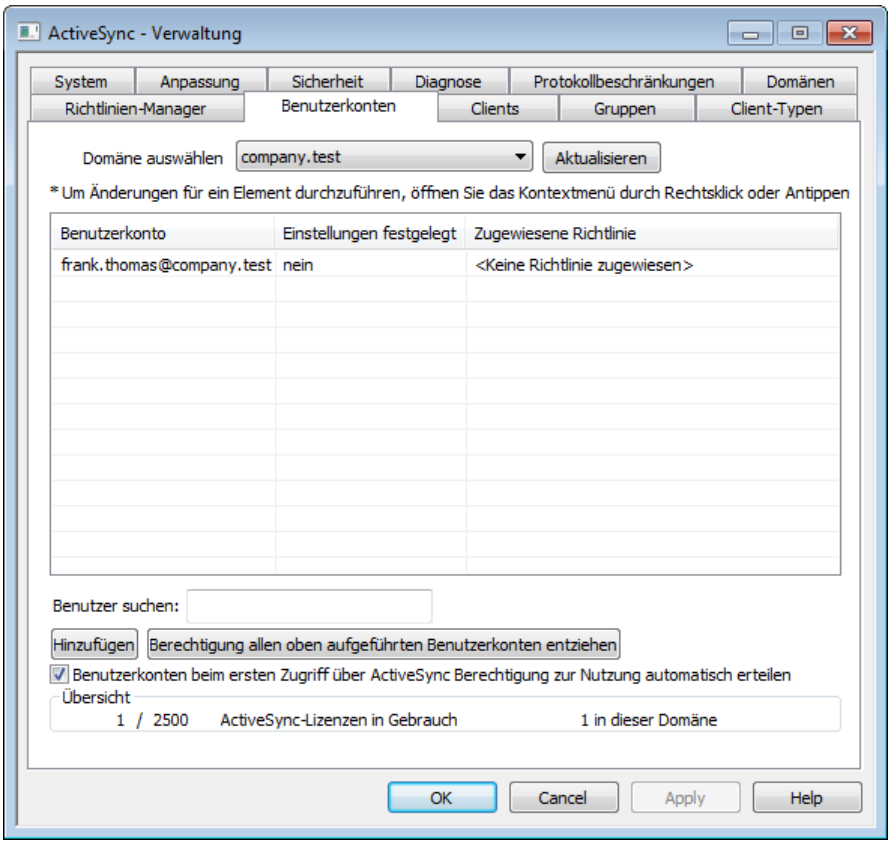
Unsignierte Installationsroutinen zulassen
Diese Option gestattet das Ausführen unsignierter Installationsroutinen auf dem Gerät. Die Option ist per Voreinstellung aktiv.

Textnachrichten (SMS) zulassen
Diese Option gestattet den Versand und Empfang von Textnachrichten auf dem Gerät. Die Option ist per Voreinstellung aktiv.

Roaming

Im Roamingbetrieb nur manuelle Synchronisierung zulassen
Diese Option bewirkt, dass die Synchronisierung mit einem Gerät nur manuell vorgenommen werden kann, und eine automatische Synchronisierung unterbleibt, sobald sich das Gerät im Daten-Roamingbetrieb befindet. Die automatische Synchronisierung kann während des Daten-Roamings erhöhte Entgelte verursachen. Welche Entgelte tatsächlich anfallen, hängt von dem Netzbetreiber und der Vertragsart ab. Diese Option ist per Voreinstellung abgeschaltet.

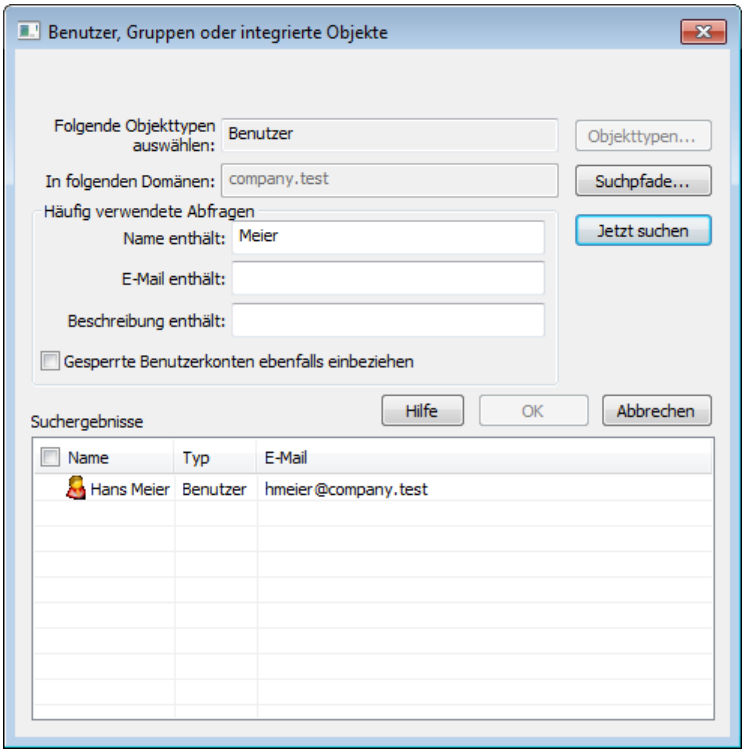
3.10.8 Benutzerkonten



Mithilfe dieses Konfigurationsdialogs können Sie bestimmen, welche Benutzerkonten ActiveSync nutzen dürfen. Sie können Benutzerkonten von Hand hinzufügen und entfernen, alle Benutzerkonten gleichzeitig für die Nutzung von ActiveSync freischalten, die Berechtigung widerrufen, oder MDaemon so konfigurieren, dass die Benutzerkonten bei der ersten Nutzung von ActiveSync automatisch die Berechtigung für die Nutzung erhalten.

Benutzerkonten manuell die Berechtigung erteilen

Um einem Benutzerkonto die Berechtigung für die Nutzung von ActiveSync manuell zu erteilen, wählen Sie die gewünschte Domäne aus der Dropdown-Liste der Domänen aus, und klicken Sie auf **Hinzufügen**. Hierdurch rufen Sie den Auswahldialog für Benutzerkonten auf, von wo aus Sie die gewünschten Benutzerkonten suchen können.



In folgenden Domänen
Hier erscheint die Domäne, die Sie im Abschnitt *Domäne auswählen* bestimmt haben. Sie können in dieser Domäne nach Benutzern suchen.

Häufig verwendete Abfragen
Mithilfe der Optionen in diesem Abschnitt können Sie die Suche eingrenzen. Sie können den Benutzernamen, E-Mail-Adresse und die Beschreibungen[714] der Benutzerkonten durchsuchen und hierbei vollständige oder Teile der Texte suchen. Um alle Benutzer zu erfassen, die Mitglieder der ausgewählten Domänen sind, lassen Sie diese Felder leer.

Gesperrte Benutzerkonten ebenfalls einbeziehen
Diese Option bewirkt, dass die Suche auch gesperrte Benutzerkonten[714] erfasst.

Jetzt suchen
Nachdem Sie die Suchkriterien festgelegt haben, beginnen Sie die Suche durch Anklicken dieses Steuerelements.

Suchergebnisse
Nachdem die Suche ausgeführt wurde, erscheinen die Suchergebnisse in diesem Abschnitt. Wählen Sie alle gewünschten Benutzerkonten aus, und klicken Sie dann auf **OK**, um sie in die Liste der berechtigten Benutzerkonten aufzunehmen.

Berechtigung für Benutzerkonten widerrufen

Um einem Benutzerkonto die Berechtigung zur Nutzung von ActiveSync zu entziehen, führen Sie einen Rechtsklick auf dem Eintrag des Benutzerkontos in der

Liste aus, und klicken Sie danach auf **Berechtigung zur Nutzung von ActiveSync widerrufen**. Um allen Benutzerkonten die Berechtigung zur Nutzung von ActiveSync zu entziehen, klicken Sie auf **Berechtigung allen oben aufgeführten Benutzerkonten entziehen**.

Falls auf Ihrem Server die Option *Benutzerkonten beim ersten Zugriff über ActiveSync Berechtigung zur Nutzung erteilen* aktiv ist, können Sie durch das Widerrufen der Freischaltung für ein Benutzerkonto zwar das Benutzerkonto aus der Liste entfernen; das Benutzerkonto wird jedoch wieder für die Nutzung von ActiveSync freigeschaltet werden, sobald sich ein ActiveSync-Gerät bei dem Benutzerkonto anmeldet.

Benutzerkonten beim ersten Zugriff über ActiveSync Berechtigung zur Nutzung erteilen

Diese Option bewirkt, dass alle Benutzerkonten automatisch für die Nutzung von ActiveSync freigeschaltet werden, sobald sie zum ersten Mal eine Verbindung mit MDaemon über ActiveSync herstellen.

Zuweisen einer ActiveSync-Richtlinie

Um einem Benutzerkonto eine Richtlinie 445 zuzuweisen, gehen Sie folgendermaßen vor:

1. Führen Sie einen Rechtsklick auf dem Eintrag des betreffenden Benutzerkonto in der Dropdown-Liste aus.
2. Klicken Sie auf **Richtlinie anwenden**. Hierdurch wird der Konfigurationsdialog *Richtlinie zuweisen* aufgerufen.
3. Wählen Sie aus der Dropdown-Liste im Bereich *Zuzuweisende Richtlinie* die gewünschte Richtlinie aus (Sie können diese Richtlinien mithilfe des Richtlinien-Managers 445 verwalten).
4. Klicken Sie auf **OK**.

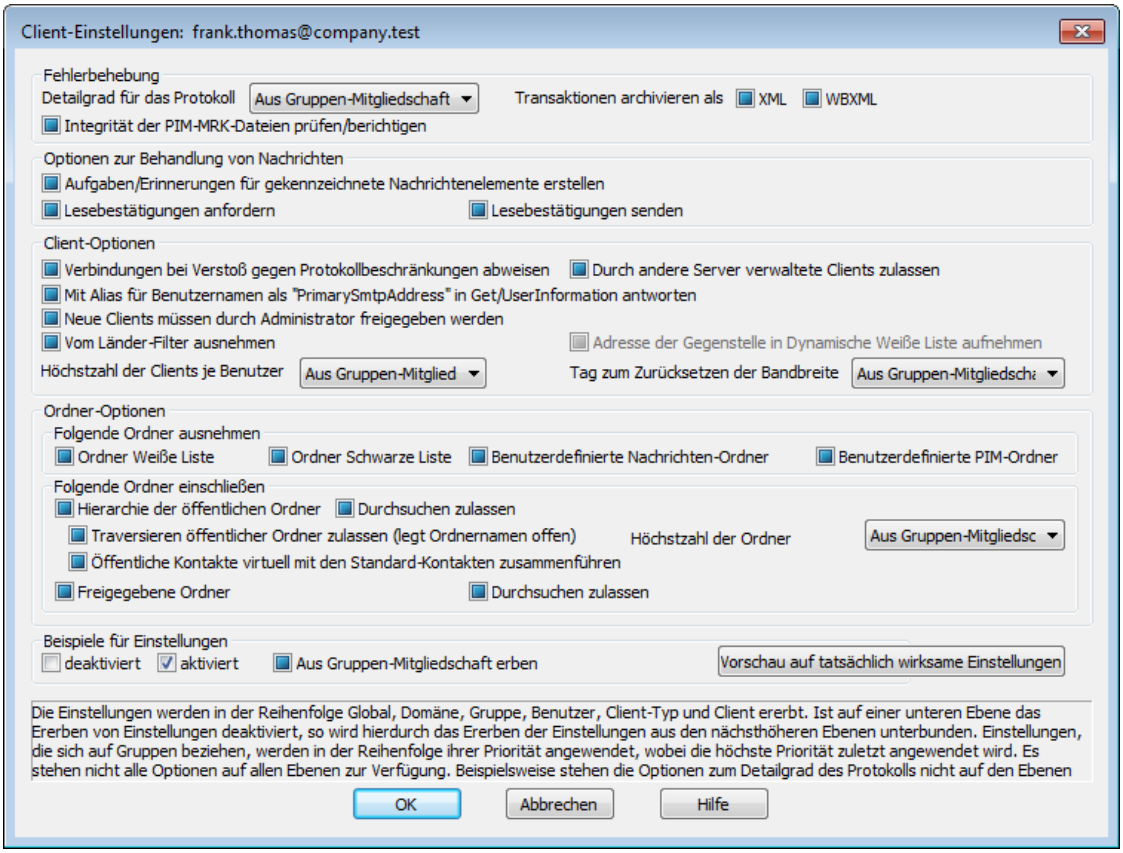
Die ausgewählte Richtlinie wird allen Geräten zugewiesen, die eine Verbindung mit diesem Benutzerkonto herstellen.

Durchsuchen der Liste berechtigter Benutzerkonten

Falls auf Ihrem System zahlreichen Benutzerkonten die Berechtigung zur Nutzung von ActiveSync erteilt ist, können Sie mithilfe des Textfeldes **Benutzer suchen** die Liste nach bestimmten Kriterien filtern. Geben Sie hierzu die ersten Buchstaben der gewünschten E-Mail-Adresse ein.

Client-Einstellungen für Benutzerkonten

Um die Client-Einstellungen für das Benutzerkonto zu verwalten, führen Sie einen Rechtsklick auf dem Eintrag des gewünschten Benutzerkontos aus, und klicken Sie dann auf **Client-Einstellungen anpassen**. Die hier getroffenen Einstellungen werden auf alle ActiveSync-Clients angewendet, die eine Verbindung mit diesem Benutzerkonto herstellen.



Per Voreinstellung sind alle Optionen in diesem Konfigurationsdialog auf die Option "*Ererbte oder Voreinstellung nutzen*" konfiguriert. Sie erben daher, falls sie Mitglied von Gruppen sind, die Client-Einstellungen der Gruppen[474], zu denen sie gehören. Gehört ein Benutzerkonto keiner Gruppe an, so werden die Einstellungen aus den Client-Einstellungen der Domäne[215] ererbt, zu der das Benutzerkonto gehört. Alle Änderungen in den Client-Einstellungen der Domäne wirken sich auch auf den vorliegenden Konfigurationsdialog aus. Nehmen Sie an dem hier vorliegenden Konfigurationsdialog Änderungen vor, so übergehen diese Änderungen für das gerade bearbeitete Benutzerkonto die Client-Einstellungen der Gruppen und der Domäne.

Allgemeines

Fehlerbehebung

Detailgrad für das Protokoll
ActiveSync für MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Einstellung erben Per Voreinstellung wird die Einstellung für den Detailgrad aus der Hierarchie der Client-Einstellungen vom jeweils übergeordneten Knoten ererbt. Clients übernehmen dabei die Einstellung aus dem jeweiligen Client-Typ, Client-Typen übernehmen die Einstellung von den Benutzerkonten, Benutzerkonten übernehmen die Einstellung von den Gruppen, und so weiter. Die globale Einstellung für alle Clients wird durch die Einstellung für den Detailgrad im Konfigurationsdialog Diagnose 432 bestimmt.

Transaktionen archivieren als [XML | WBXML]
Mithilfe der Optionen *XML...* und *WBXML...* können Sie die zugehörigen Daten speichern; diese Daten können die Fehlersuche erleichtern. Die systemweit wirksamen Optionen sind per Voreinstellung abgeschaltet.

Integrität der PIM-MRK-Dateien prüfen/berichtigen
Diese Option führt für die PIM-Daten der betroffenen Clients Prüf- und Korrekturvorgänge durch. Sie sollen bekannte Probleme erkennen, die eine ordnungsgemäße Synchronisierung verhindern können. Zu diesen Problemen zählen insbesondere doppelte iCal-UIDs und leere Datenfelder, die eigentlich verpflichtend Daten enthalten müssen. Die systemweit wirksame Option ist per Voreinstellung abgeschaltet.

Client-Optionen

Verbindungen bei Verstoß gegen Protokollbeschränkungen abweisen
Diese Option bewirkt, dass Verbindungen von Clients abgewiesen werden, falls sie versuchen eine nicht für die Clients *Zugelassene Protokollversion* zu verwenden. Per Voreinstellung ist diese Option abgeschaltet; dies bedeutet, dass die Protokollbeschränkung keine Verbindungen solcher Clients verhindern, die andere als die zugelassenen Protokollversionen verwenden. Solange die Option abgeschaltet ist, weist MDaemon die Clients zwar an, nur die zugelassenen Protokollversionen zu verwenden, lässt aber bei Nutzung anderer Protokollversionen die Verbindung trotzdem zu. Nähere Informationen finden Sie unter Protokollbeschränkungen 434.

Mit Alias für Benutzernamen als "PrimarySmtpAddress" in Get/UserInformation antworten
Diese Option gestattet es dem Dienst, als Antwort auf eine Anforderung Settings/Get/UserInformation eine etwa vorhandene Alias-Adresse oder eine sekundäre Adresse des betroffenen Benutzerkontos als primäre Adresse zu übermitteln. Hierdurch wird ein Problem umgangen, das mit einer iOS-Aktualisierung nach Version 9.x verursacht wird, und das verhinderte, dass

Clients unter einer etwa vorhandenen Alias-Adresse Nachrichten versenden konnten. Die Nutzung dieser Option bewirkt eine nicht standardkonforme Antwort auf die Anforderung Settings/GetUserInformation.

Neue Clients müssen durch Administrator freigegeben werden
Diese Option bewirkt, dass neue Clients sich erst dann mit Benutzerkonten synchronisieren können, wenn sie zunächst durch einen Administrator freigegeben wurden. In der Liste der Clients[464] sind alle Clients aufgeführt, die noch die Freigabe erwarten, und die Administratoren können sie über diese Liste freigeben. Diese Option ist per Voreinstellung abgeschaltet.

Höchstzahl der Clients je Benutzer
Mithilfe dieser Option können Sie die Anzahl der ActiveSync-Clients und -Endgeräte begrenzen, die mit jedem MDaemon-Benutzerkonto verknüpft sein können. Der hier angegebene Wert ist die Höchstzahl zulässiger Clients. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt. Diese Option steht nur in den Client-Einstellungen auf globaler, Domänen- und Benutzerebene zur Verfügung, nicht jedoch in den Client-Einstellungen für die einzelnen Clients.

Tag zum Zurücksetzen der Bandbreite
Mithilfe dieser Option können Sie Tag bestimmen, an dem in jedem Monat die Bandbreiten-Nutzungsstatistik für die ActiveSync-Endgeräte zurückgesetzt wird. Dieser Vorgang wird während der normalen Bereinigungsvorgänge um Mitternacht aufgeführt und, wie auch andere Bereinigungsvorgänge, in das Protokoll System eingetragen. Der globale Wert lautet per Voreinstellung 0 (nicht zurücksetzen), sodass per Voreinstellung die Nutzungsstatistik nicht zurückgesetzt wird. Für untergeordnete Knoten können Sie abweichende Einstellungen treffen, etwa, um die Einstellung an den Tag anzugleichen, an dem für das betroffene Endgeräte ein neuer Abrechnungszeitraum des Netzbetreibers beginnt.

Sicherheit

Vom Länder-Filter ausnehmen
Wenn Sie diese Option in den Einstellungen eines ActiveSync-Clients aktivieren, kann das Endgerät den Länder-Filter[574] umgehen. Hierdurch kann ein berechtigter Benutzer auf sein Benutzerkonto über ActiveSync beispielsweise auch dann zugreifen, wenn er sich in einem Land befindet, für das Versuche zur Echtheitsbestätigung ansonsten durch den Länder-Filter unterbunden werden. Ein Endgerät kann nur dann vom Länder-Filter ausgenommen sein, wenn es innerhalb des durch die Option Inaktive Clients entfernen nach [x] Tagen[418] im Abschnitt Anpassung bestimmten Zeitraums eine echtheitsbestätigte Verbindung über ActiveSync erfolgreich hergestellt hat.

Adresse der Gegenstelle in Dynamische Freigabeliste aufnehmen
Wenn Sie ein Endgerät vom Länder-Filter ausnehmen, können Sie durch Aktivieren dieser Option die IP-Adresse, von der aus das Endgerät die Verbindung herstellt, in die Freigabeliste eintragen lassen. Hierdurch können beispielsweise andere Clients, die von der selben IP-Adresse aus eine Verbindung herstellen, ebenfalls zugelassen werden.

Durch andere Server provisionierte/verwaltete Clients zulassen
Per Voreinstellung dürfen Clients auch dann Verbindungen zu MDaemon aufbauen, wenn sie auf die Übermittlung der Provisionierungs- und Richtliniendaten durch den ActiveSync-Server hin melden, dass sie auch durch

einen oder mehrere andere ActiveSync-Server verwaltet werden. Bei einer solchen Mehrfachverwaltung kann es nicht sichergestellt werden, dass alle auf Ihrem System bestehenden Richtlinien durch den Client auch umgesetzt werden; dies gilt insbesondere dann, wenn sie Richtlinien des anderen ActiveSync-Servers widersprechen. In vielen Fällen setzen die Clients die am stärksten einschränkende Richtlinie um, falls mehrere einander widersprechende Richtlinien vorhanden sind. Um Verbindungen von Clients zu unterbinden, die durch andere ActiveSync-Server verwaltet werden, deaktivieren Sie diese Option.

Löschen der Clients (Zurücksetzen in den Auslieferungszustand) nicht zulassen
Wenn diese Option aktiv ist, dann können ActiveSync-Clients nicht in den **Auslieferungszustand zurückgesetzt** und damit vollständig gelöscht werden. Wenn Sie Clients ferngesteuert in den Auslieferungszustand zurücksetzen wollen, müssen Sie diese Option deaktivieren. Diese Option ist per Voreinstellung deaktiviert. Nähere Informationen finden Sie auf der Seite Clients im Abschnitt **Vollständiges Löschen eines ActiveSync-Clients** 464.

Optionen zur Ordner-Synchronisierung

Optionen zur Ordner-Synchronisierung

Folgende Ordner ausnehmen

Freigegebene Absender/Gesperrte Absender
Per Voreinstellung werden die Kontaktordner mit Freigabelisten und Sperrlisten der Benutzer nicht mit den Geräten synchronisiert. Diese Ordner dienen üblicherweise nur in MDaemon zum Erkennen und Filtern von Spam. Ihre Inhalte brauchen daher nicht auf den Geräten als Kontakte angezeigt zu werden.

Benutzerdefinierte Nachrichten-Ordner
Per Voreinstellung können alle Standard- und benutzerdefinierten Nachrichten-Ordner mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-Nachrichtenordner synchronisiert werden können. Die Standard-Nachrichtenordner sind insbesondere Posteingang, Gesendete Objekte, Gelöschte Objekte und Entwürfe. Ordner, die die Benutzer selbst anlegen, werden dann nicht mehr synchronisiert. Diese Option ist per Voreinstellung abgeschaltet.

Benutzerdefinierte PIM-Ordner
Per Voreinstellung können alle PIM-Ordner (insbesondere Kontakte, Kalender, Notizen und Aufgaben) mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-PIM-Ordner synchronisiert werden können. Ist diese Option aktiv, so wird beispielsweise für jeden Benutzer nur der Standard-Kalender synchronisiert, auch wenn er über mehrere Kalender-Ordner verfügt. Diese Option ist per Voreinstellung abgeschaltet.

Folgende Ordner einschließen

Hierarchie der öffentlichen Ordner
Diese Option bewirkt, dass die öffentlichen Ordner 309, auf die die Benutzer Zugriff haben, in den Ordnerlisten der Benutzer auf ihren ActiveSync-Geräten erscheinen. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der öffentlichen Ordner[309], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Traversieren öffentlicher Ordner zulassen (legt Ordnernamen offen)
Benutzerkonten, die auf Unterordner in öffentlichen Ordnern zugreifen oder diese synchronisieren wollen, müssen per Voreinstellung sowohl für den betroffenen Unterordner als auch für alle ihm übergeordneten öffentlichen Ordner[309] über die Berechtigung Ordner anzeigen[311] verfügen. Fehlt einem Benutzerkonto diese Berechtigung für einen übergeordneten öffentlichen Ordner, so kann er auch den gewünschten Unterordner nicht synchronisieren und nicht auf ihn zugreifen, und zwar auch dann nicht, wenn das Benutzerkonto für diesen Unterordner selbst die erforderliche Berechtigung hat. Mithilfe dieser Option können Sie den Clients Zugriff auf und Synchronisierung von Unterordnern ermöglichen, ohne dass die Clients Berechtigungen für die übergeordneten öffentlichen Ordner haben. **Beachte:** Ist diese Option aktiv, so erlangt der Client zwangsläufig Kenntnis von den Namen der übergeordneten Ordner, auch wenn er für ihre Inhalte keine Zugriffsrechte hat. Hieraus kann sich ein Sicherheitsrisiko ergeben. Die Option ist per Voreinstellung abgeschaltet.

Höchstzahl zulässiger öffentlicher Ordner
Diese Option begrenzt die Zahl der öffentlichen Ordner, die auf den betroffenen Geräten dargestellt werden können. Ist eine solche Höchstzahl angegeben, dann übermittelt der Server so lange Einträge in der Ordnerliste, bis die Höchstzahl erreicht ist. Danach übermittelt der Server keine Ordner mehr an die Geräte. Die Reihenfolge, in der die Ordner dabei verarbeitet werden, kann weder festgelegt noch vorher bestimmt werden. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt.

Freigegebene Ordner
Diese Option nimmt auch die gemeinsam genutzten Ordner[122], auf die die Benutzer Zugriff haben, in die Ordnerlisten auf ihren ActiveSync-Geräten auf. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der freigegebenen Ordner[742], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Behandlung von Inhalten

Optionen zur Behandlung von Inhalten

Aufgaben/Erinnerungen für durch Clients gekennzeichnete Nachrichtenelemente erstellen
Diese Option ermöglicht es MDaemon, die Benutzer an gekennzeichnete Elemente zu erinnern. Hierzu wird für jede gekennzeichnete E-Mail-Nachricht eine Aufgabe erstellt, wenn der Client dies anfordert. Die globale Option für dieses Leistungsmerkmal ist per Voreinstellung aktiv.

Aktualisierung nach jeder Änderung der Besprechung senden
Manche Clients versenden aktualisierte Besprechungseinladungen nicht richtig, nachdem eine Besprechung geändert wurde. Diese Option bewirkt, dass der

ActiveSync-Dienst immer dann aktualisierte Besprechungseinladungen sendet, wenn der Besprechungsorganisator eine Besprechung aktualisiert hat. Diese Option sollte nur für Clients[464] und Client-Typen[481] aktiviert werden, die die aktualisierten Besprechungseinladungen nicht richtig versenden, da sonst aktualisierte Besprechungseinladungen doppelt versandt werden. Aus diesem Grund ist diese Einstellung nur auf den Seiten Clients und Client-Typen verfügbar.

Lesebestätigung für alle versandten Nachrichten anfordern
Diese Option bewirkt, dass der Server für alle durch einen Client versandten E-Mail-Nachrichten Lesebestätigungen anfordert. Diese Option ist per Voreinstellung abgeschaltet.

Vom Absender angeforderte Lesebestätigung senden, sobald Nachricht als gelesen gekennzeichnet ist
Diese Option bewirkt, dass der Server Anforderungen von Lesebestätigungen beachtet und die Lesebestätigungen dann versendet, wenn eine Nachricht durch den Client als gelesen gekennzeichnet wird. Diese Option ist per Voreinstellung abgeschaltet.

Unter dem in der Antwortadresse (ReplyTo) angegebenen Alias senden
Manche Clients gestatten den Absendern nicht den Versand von E-Mail-Nachrichten unter einem Alias. Dieses Leistungsmerkmal wurde im der Version 16.x des Protokolls Exchange ActiveSync (EAS)[434] erstmals unterstützt, aber manche Clients unterstützen die Version 16.x nicht. So nutzt beispielsweise Microsoft Outlook für Windows nur EAS 14.0 und gestattet zwar den Benutzern die Angabe einer anderen Adresse, unter der eine Nachricht versandt werden soll, aber die dann erstellte Nachricht gibt die Auswahl des Benutzers nicht richtig wieder. Diese Option gestattet die Nutzung des Feldes für die Antwortadresse (ReplyTo) zum Versand von Nachrichten dann, wenn als Antwortadresse ein gültiger Alias[827] des Benutzers eingetragen ist. Die globale Option ist per Voreinstellung aktiv.

Öffentliche Kontakte virtuell mit den Standard-Kontakten zusammenführen
Diese Option bewirkt, dass die öffentlichen Kontakte und die Standard-Kontakte der Benutzer auf ihren Geräten als zusammengeführt dargestellt werden. Die Datenbestände der Kontakte bleiben hierbei getrennt; es werden also keine Kontakte zwischen den Kontaktordnern der Benutzer kopiert. Diese Option kann insbesondere für solche Clients hilfreich sein, die das Durchsuchen der Globalen Adressliste (GAL) nicht unterstützen. Diese Option ist per Voreinstellung abgeschaltet.

Absender sperren, wenn Nachricht in Ordner Junk-Email verschoben wird
Ist diese Option aktiv, so wird die Absender-Adresse (Felder Sender und From) einer E-Mail-Adresse in den Kontaktordner für gesperrte Absender eingetragen, sobald ein Client die zugehörige E-Mail-Nachricht in den Ordner für Spam-Nachrichten verschiebt.

Antworten auf Besprechungsanfragen nach Zusage, Ablehnung usw. zwingend senden
Ist diese Option aktiv, so versendet der ActiveSync-Dienst eine Antwort an den Besprechungsorganisator immer dann, wenn ein Client auf eine Besprechungseinladung zusagt, sie ablehnt oder eine sonstige Aktion für die Einladung ausführt. Diese Option ist für solche Clients nützlich, die solche Antworten nicht selbst richtig senden.

Vorschau auf tatsächlich wirksame Einstellungen

Dieses Steuerelement ist auf allen untergeordneten Konfigurationsdialogen für die Client-Einstellungen (Domänen 437, Benutzerkonten 454 und Clients 464) verfügbar. Per Voreinstellung werden die Optionen auf diesen Konfigurationsdialogen nicht von den übergeordneten Konfigurationsdialogen geerbt. Sie können sich daher mithilfe dieses Steuerelements die Einstellungen anzeigen lassen, die auf den jeweils gerade dargestellten Konfigurationsdialog wirken.

Mithilfe dieses Konfigurationsdialogs können Sie die Benutzerkonten bestimmen, die die Berechtigung zur Nutzung von ActiveSync haben. Sie können Benutzerkonten die Berechtigung manuell erteilen und entziehen, und Sie können MDaemon veranlassen, den Benutzerkonten bei der ersten Nutzung von ActiveSync die Berechtigung automatisch zu erteilen.

Benutzerkonten die Berechtigung zur Nutzung von ActiveSync erteilen

Benutzerkonten manuell hinzufügen
Um einem Benutzerkonto die Berechtigung zur Nutzung von ActiveSync manuell zu erteilen, geben Sie die E-Mail-Adresse des gewünschten Benutzerkontos in das Eingabefeld *ActiveSync-Benutzerkonten* ein, und klicken Sie dann auf *Hinzufügen*. Um einem Benutzerkonto die Berechtigung zu entziehen, wählen Sie das Benutzerkonto in der Liste aus, und klicken Sie dann auf *Entfernen*.

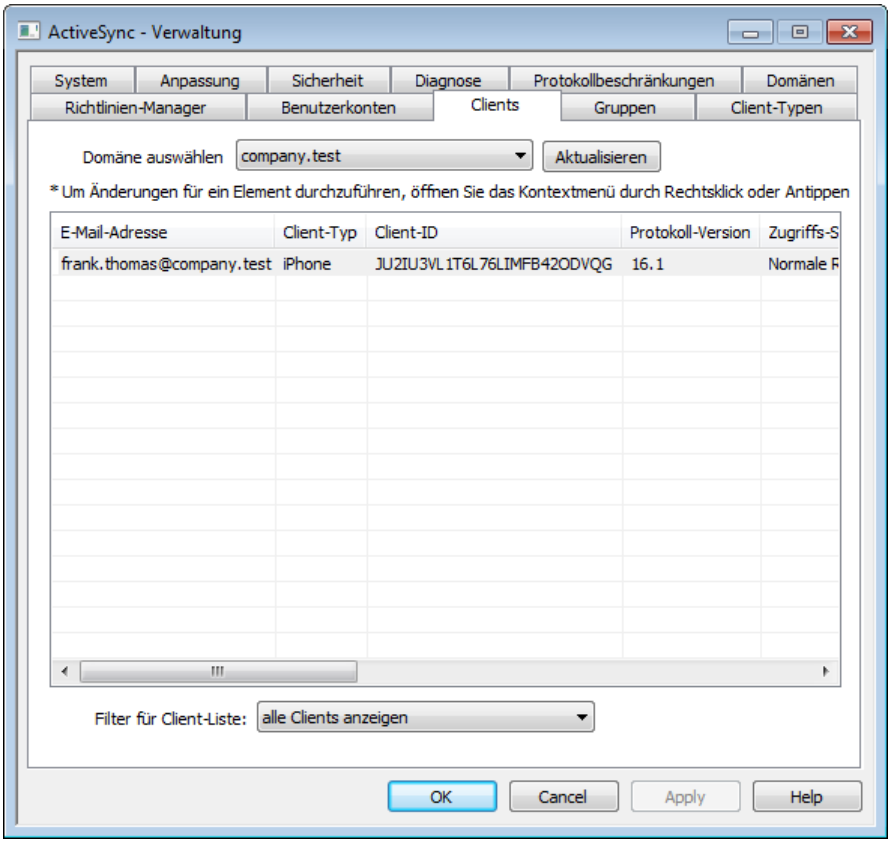
Sie können einem Benutzerkonto auch die Berechtigung erteilen und entziehen, indem Sie auf der Seite Client-Einstellungen 764 für das Benutzerkonto die Einstellung *ActiveSync-Dienste für dieses Benutzerkonto aktivieren* bearbeiten.

Benutzerkonten beim ersten Zugriff über ActiveSync Berechtigung zur Nutzung erteilen
Diese Option bewirkt, dass MDaemon automatisch den Benutzerkonten die Berechtigung zur Nutzung von ActiveSync erteilt, sobald sie das erste Mal eine Verbindung über ActiveSync herstellen.

Siehe auch:

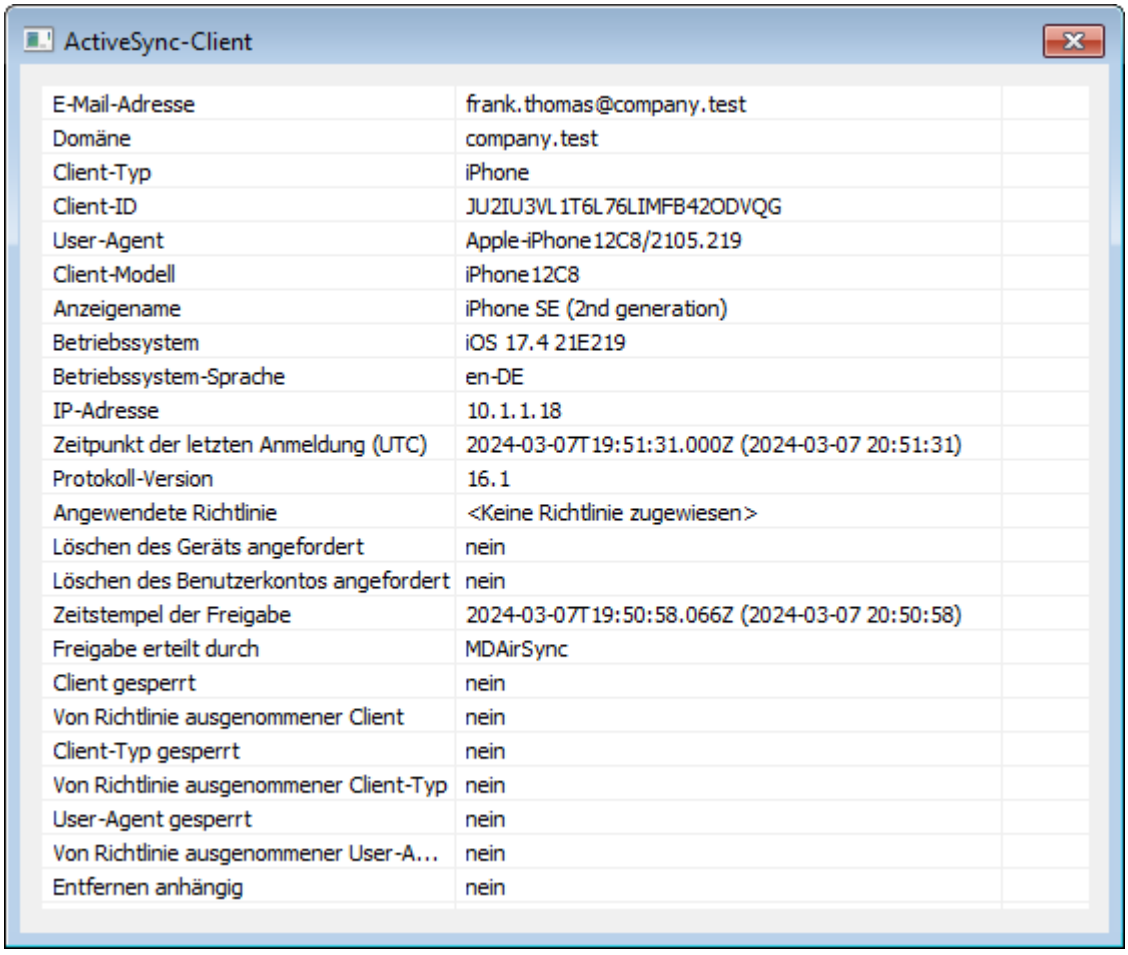
ActiveSync » Client-Einstellungen 422
ActiveSync » Domänen 437
ActiveSync » Clients 464
Benutzerkonten » ActiveSync - Client-Einstellungen 764
Benutzerkonten » ActiveSync-Clients 772

3.10.9 Clients



In diesem Konfigurationsdialog wird für jeden mit der ausgewählten Domäne verknüpften ActiveSync-Client ein Eintrag angezeigt. Um nähere Informationen zu einem Client zu erhalten, klicken Sie doppelt auf seinen Eintrag. Durch Rechtsklick auf einem Eintrag öffnen Sie ein Kontextmenü, über das Sie die Einstellungen für den Client anpassen, Statistiken zum Client einsehen und weitere Vorgänge ausführen können.

Details zu ActiveSync-Clients



Um Detailinformationen über Endgeräte einzusehen, wählen Sie den Eintrag für das Endgerät aus, und klicken Sie dann auf **Details**, oder klicken Sie doppelt auf den Eintrag des Endgeräts. In dem Konfigurationsdialog Details können Sie Informationen über das Gerät einsehen, dem Gerät Richtlinien zuweisen, seine Client-Einstellungen bearbeiten und das Gerät in den Sperrlisten und Freigabelisten[429] erfassen.

Geräte-Einstellungen

Um die Einstellungen für ein Gerät zu bearbeiten, wählen Sie das Gerät aus, und klicken Sie auf **Einstellungen**. Per Voreinstellung werden diese Einstellungen aus den Client-Einstellungen des zugehörigen Benutzerkontos[454] geerbt. Nähere Informationen finden Sie weiter unten unter Verwalten der Client-Einstellungen eines Geräts.

Zuweisen einer ActiveSync-Richtlinie

Um einem Gerät eine Richtlinie[445] zuzuweisen, gehen Sie folgendermaßen vor:

1. Führen Sie auf dem Eintrag des gewünschten Geräts in der Übersicht einen Rechtsklick aus.
2. Klicken Sie auf **Richtlinie anwenden**. Hierdurch wird der Konfigurationsdialog Richtlinie zuweisen aufgerufen.
1. Wählen Sie aus dem Auswahlmenü der **zuzuweisenden Richtlinien** die gewünschte Richtlinie aus.

3. Klicken Sie auf **OK**.

Statistik

Um Statistikdaten für ein Gerät einzusehen, führen Sie einen Rechtsklick auf dem Eintrag des gewünschten Geräts aus, und klicken Sie danach auf **Statistiken anzeigen**. Es öffnet sich die Übersicht Client-Statistik, auf der verschiedene Daten zur Nutzungsstatistik des Geräts einsehbar sind.

Statistik zurücksetzen

Um die Statistikdaten für ein Gerät zurückzusetzen, führen Sie auf dem Eintrag des gewünschten Geräts einen Rechtsklick aus, und klicken Sie danach auf **Statistiken zurücksetzen.** Bestätigen Sie die anschließenden Sicherheitsabfrage durch Anklicken von **OK**.

Entfernen eines ActiveSync-Clients

Um einen ActiveSync-Clients zu entfernen, führen Sie einen Rechtsklick auf dem Eintrag des gewünschten Clients aus, und klicken Sie danach auf **Löschen**. Beantworten Sie die anschließende Sicherheitsabfrage mit **Ja**. Hierdurch werden der Client aus der Liste entfernt und alle Informationen zur Synchronisierung aus MDaemon gelöscht. Führt der entfernte Client später noch einmal eine Synchronisierung über ActiveSync auf dem Server durch, dann behandelt MDaemon den Client so, wie wenn er auf dem Server noch nie verwendet worden wäre. Alle Gerätedaten müssen dann mit MDaemon neu synchronisiert werden.

Vollständiges Löschen eines ActiveSync-Clients

Ist dem ausgewählten ActiveSync-Client eine Richtlinie 445 zugewiesen, und hat der Client die Richtlinie übernommen und entsprechend geantwortet, dann kann dieser Client ferngesteuert vollständig gelöscht werden. Um den Client vollständig zu löschen, führen Sie auf dem Client einen Rechtsklick aus (bei Nutzung der MDaemon-Remoteverwaltung wählen Sie den Client aus), und klicken Sie danach auf **Gerät löschen**. Sobald der Client das nächste Mal eine Verbindung zu MDaemon herstellt, übermittelt MDaemon den Löschbefehl an den Client und fordert ihn auf, sich in den Auslieferungszustand zurückzusetzen. Je nach Client kann dies zur Löschung aller Inhalte, auch etwa installierter Apps, führen. Solange der ActiveSync-Eintrag für den Client besteht, übermittelt MDaemon den Löschbefehl auch bei jedem späteren Verbindungsaufbau erneut. Falls Sie den Client löschen wollen, tragen Sie ihn zunächst in die Sperrliste 429 ein, damit er künftig keine Verbindungen mehr zu MDaemon herstellen kann. Wird ein gelöschtes Endgerät beispielsweise wiedergefunden, und soll er wieder Verbindungen zum Server herstellen können, dann wählen Sie das Gerät aus, und klicken Sie auf **Löschvorgänge abbrechen**. Entfernen Sie das Gerät außerdem aus der Sperrliste.

Daten aus dem Benutzerkonto eines ActiveSync-Clients löschen

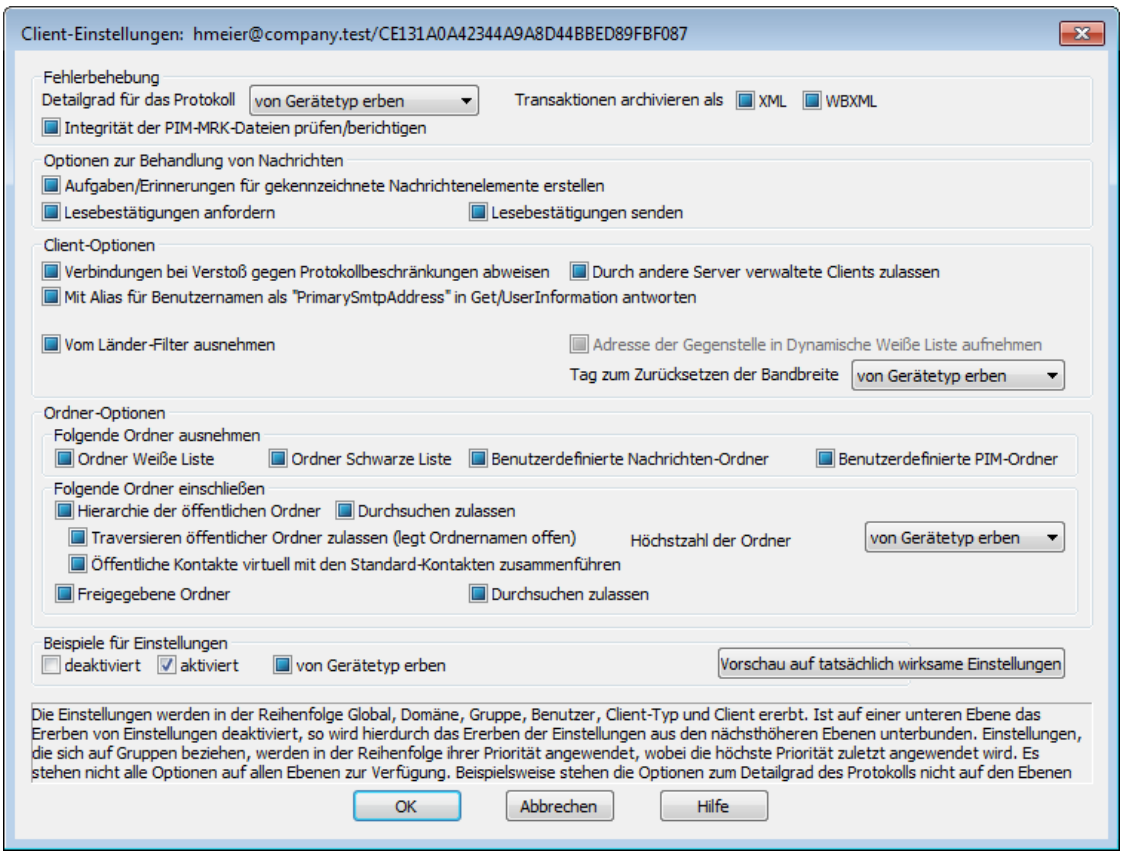
Um die Nachrichten und PIM-Daten von einem Client oder Endgerät zu löschen, führen Sie auf dem Eintrag des gewünschten Geräts einen Rechtsklick aus, und klicken Sie danach auf **Nachrichten des Benutzerkontos und PIM-Elemente vom Client löschen**. Dieser Löschvorgang ist dem vollständigen Löschen eines ActiveSync-Clients ähnlich, das weiter oben beschrieben ist. Es werden aber nicht alle Daten des Clients gelöscht, sondern es werden nur die Daten des Benutzerkontos entfernt, wie etwa E-Mail-Nachrichten, Kalendereinträge, Kontakte und ähnliche Daten. Alle anderen Daten, wie Apps, Fotos und Musik, bleiben unverändert.

Client freigeben

Ist im Konfigurationsdialog ActiveSync - Client-Einstellungen 422 die Option "*Neue Clients müssen durch Administrator freigegeben werden*" aktiv, so können Sie mit diesem Steuerelement Clients freigeben, Wählen Sie dazu den gewünschten Client aus, und klicken Sie danach auf **Client zur Synchronisierung berechtigen**. Nach der Freigabe kann sich der Client mit dem Server synchronisieren.

Verwalten der Client-Einstellungen eines Geräts

Die Client-Einstellungen für einzelne Geräte gestatten Ihnen die Verwaltung der Client-Einstellungen für bestimmte einzelne Endgeräte.



Per Voreinstellung werden alle Optionen in diesem Konfigurationsdialog vom übergeordneten Knoten geerbt, oder es werden die Standardeinstellungen verwendet. Im Falle der Client-Einstellungen ist der übergeordnete Knoten das Benutzerkonto, dem das Gerät zugeordnet ist. Seine Client-Einstellungen werden im Konfigurationsdialog Client-Einstellungen 454 des Benutzerkontos konfiguriert, dem das Gerät zugeordnet ist. Änderungen, die Sie in diesem Konfigurationsdialog vornehmen, übergehen die auf Client-Ebene festgelegten Einstellungen für dieses Gerät.

Allgemeines

Fehlerbehebung

Detailgrad für das Protokoll

ActiveSync für MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten

Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Einstellung erben Per Voreinstellung wird die Einstellung für den Detailgrad aus der Hierarchie der Client-Einstellungen vom jeweils übergeordneten Knoten ererbt. Clients übernehmen dabei die Einstellung aus dem jeweiligen Client-Typ, Client-Typen übernehmen die Einstellung von den Benutzerkonten, Benutzerkonten übernehmen die Einstellung von den Gruppen, und so weiter. Die globale Einstellung für alle Clients wird durch die Einstellung für den Detailgrad im Konfigurationsdialog Diagnose 432 bestimmt.

Transaktionen archivieren als [XML | WBXML]
Mithilfe der Optionen *XML...* und *WBXML...* können Sie die zugehörigen Daten speichern; diese Daten können die Fehlersuche erleichtern. Die systemweit wirksamen Optionen sind per Voreinstellung abgeschaltet.

Integrität der PIM-MRK-Dateien prüfen/berichtigen
Diese Option führt für die PIM-Daten der betroffenen Clients Prüf- und Korrekturvorgänge durch. Sie sollen bekannte Probleme erkennen, die eine ordnungsgemäße Synchronisierung verhindern können. Zu diesen Problemen zählen insbesondere doppelte iCal-UIDs und leere Datenfelder, die eigentlich verpflichtend Daten enthalten müssen. Die systemweit wirksame Option ist per Voreinstellung abgeschaltet.

Client-Optionen

Verbindungen bei Verstoß gegen Protokollbeschränkungen abweisen
Diese Option bewirkt, dass Verbindungen von Clients abgewiesen werden, falls sie versuchen eine nicht für die Clients *Zugelassene Protokollversion* zu verwenden. Per Voreinstellung ist diese Option abgeschaltet; dies bedeutet, dass die Protokollbeschränkung keine Verbindungen solcher Clients verhindern, die andere als die zugelassenen Protokollversionen verwenden. Solange die Option abgeschaltet ist, weist MDaemon die Clients zwar an, nur die zugelassenen Protokollversionen zu verwenden, lässt aber bei Nutzung anderer Protokollversionen die Verbindung trotzdem zu. Nähere Informationen finden Sie

unter Protokollbeschränkungen 434.

Mit Alias für Benutzernamen als "PrimarySmtpAddress" in Get/UserInformation antworten
Diese Option gestattet es dem Dienst, als Antwort auf eine Anforderung Settings/Get/UserInformation eine etwa vorhandene Alias-Adresse oder eine sekundäre Adresse des betroffenen Benutzerkontos als primäre Adresse zu übermitteln. Hierdurch wird ein Problem umgangen, das mit einer iOS-Aktualisierung nach Version 9.x verursacht wird, und das verhinderte, dass Clients unter einer etwa vorhandenen Alias-Adresse Nachrichten versenden konnten. Die Nutzung dieser Option bewirkt eine nicht standardkonforme Antwort auf die Anforderung Settings/GetUserInformation.

Neue Clients müssen durch Administrator freigegeben werden
Diese Option bewirkt, dass neue Clients sich erst dann mit Benutzerkonten synchronisieren können, wenn sie zunächst durch einen Administrator freigegeben wurden. In der Liste der Clients 464 sind alle Clients aufgeführt, die noch die Freigabe erwarten, und die Administratoren können sie über diese Liste freigeben. Diese Option ist per Voreinstellung abgeschaltet.

Höchstzahl der Clients je Benutzer
Mithilfe dieser Option können Sie die Anzahl der ActiveSync-Clients und -Endgeräte begrenzen, die mit jedem MDaemon-Benutzerkonto verknüpft sein können. Der hier angegebene Wert ist die Höchstzahl zulässiger Clients. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt. Diese Option steht nur in den Client-Einstellungen auf globaler, Domänen- und Benutzerebene zur Verfügung, nicht jedoch in den Client-Einstellungen für die einzelnen Clients.

Tag zum Zurücksetzen der Bandbreite
Mithilfe dieser Option können Sie Tag bestimmen, an dem in jedem Monat die Bandbreiten-Nutzungsstatistik für die ActiveSync-Endgeräte zurückgesetzt wird. Dieser Vorgang wird während der normalen Bereinigungsvorgänge um Mitternacht aufgeführt und, wie auch andere Bereinigungsvorgänge, in das Protokoll System eingetragen. Der globale Wert lautet per Voreinstellung 0 (nicht zurücksetzen), sodass per Voreinstellung die Nutzungsstatistik nicht zurückgesetzt wird. Für untergeordnete Knoten können Sie abweichende Einstellungen treffen, etwa, um die Einstellung an den Tag anzugleichen, an dem für das betroffene Endgeräte ein neuer Abrechnungszeitraum des Netzbetreibers beginnt.

Sicherheit

Vom Länder-Filter ausnehmen
Wenn Sie diese Option in den Einstellungen eines ActiveSync-Clients aktivieren, kann das Endgerät den Länder-Filter 574 umgehen. Hierdurch kann ein berechtigter Benutzer auf sein Benutzerkonto über ActiveSync beispielsweise auch dann zugreifen, wenn er sich in einem Land befindet, für das Versuche zur Echtheitsbestätigung ansonsten durch den Länder-Filter unterbunden werden. Ein Endgerät kann nur dann vom Länder-Filter ausgenommen sein, wenn es innerhalb des durch die Option Inaktive Clients entfernen nach [x] Tagen 418 im Abschnitt Anpassung bestimmten Zeitraums eine echtheitsbestätigte Verbindung über ActiveSync erfolgreich hergestellt hat.

Adresse der Gegenstelle in Dynamische Freigabeliste aufnehmen
Wenn Sie ein Endgerät vom Länder-Filter ausnehmen, können Sie durch

Aktivieren dieser Option die IP-Adresse, von der aus das Endgerät die Verbindung herstellt, in die Freigabeliste eintragen lassen. Hierdurch können beispielsweise andere Clients, die von der selben IP-Adresse aus eine Verbindung herstellen, ebenfalls zugelassen werden.

Durch andere Server provisionierte/verwaltete Clients zulassen
Per Voreinstellung dürfen Clients auch dann Verbindungen zu MDaemon aufbauen, wenn sie auf die Übermittlung der Provisionierungs- und Richtliniendaten durch den ActiveSync-Server hin melden, dass sie auch durch einen oder mehrere andere ActiveSync-Server verwaltet werden. Bei einer solchen Mehrfachverwaltung kann es nicht sichergestellt werden, dass alle auf Ihrem System bestehenden Richtlinien durch den Client auch umgesetzt werden; dies gilt insbesondere dann, wenn sie Richtlinien des anderen ActiveSync-Servers widersprechen. In vielen Fällen setzen die Clients die am stärksten einschränkende Richtlinie um, falls mehrere einander widersprechende Richtlinien vorhanden sind. Um Verbindungen von Clients zu unterbinden, die durch andere ActiveSync-Server verwaltet werden, deaktivieren Sie diese Option.

Löschen der Clients (Zurücksetzen in den Auslieferungszustand) nicht zulassen
Wenn diese Option aktiv ist, dann können ActiveSync-Clients nicht in den **Auslieferungszustand zurückgesetzt** und damit vollständig gelöscht werden. Wenn Sie Clients ferngesteuert in den Auslieferungszustand zurücksetzen wollen, müssen Sie diese Option deaktivieren. Diese Option ist per Voreinstellung deaktiviert. Nähere Informationen finden Sie auf der Seite Clients im Abschnitt **Vollständiges Löschen eines ActiveSync-Clients** 464.

Optionen zur Ordner-Synchronisierung

Optionen zur Ordner-Synchronisierung

Folgende Ordner ausnehmen

Freigegebene Absender/Gesperrte Absender
Per Voreinstellung werden die Kontaktordner mit Freigabelisten und Sperrlisten der Benutzer nicht mit den Geräten synchronisiert. Diese Ordner dienen üblicherweise nur in MDaemon zum Erkennen und Filtern von Spam. Ihre Inhalte brauchen daher nicht auf den Geräten als Kontakte angezeigt zu werden.

Benutzerdefinierte Nachrichten-Ordner
Per Voreinstellung können alle Standard- und benutzerdefinierten Nachrichten-Ordner mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-Nachrichtenordner synchronisiert werden können. Die Standard-Nachrichtenordner sind insbesondere Posteingang, Gesendete Objekte, Gelöschte Objekte und Entwürfe. Ordner, die die Benutzer selbst anlegen, werden dann nicht mehr synchronisiert. Diese Option ist per Voreinstellung abgeschaltet.

Benutzerdefinierte PIM-Ordner
Per Voreinstellung können alle PIM-Ordner (insbesondere Kontakte, Kalender, Notizen und Aufgaben) mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-PIM-Ordner synchronisiert werden können. Ist diese Option aktiv, so wird beispielsweise für jeden Benutzer nur der Standard-Kalender synchronisiert, auch wenn er über mehrere Kalender-

Ordner verfügt. Diese Option ist per Voreinstellung abgeschaltet.

Folgende Ordner einschließen

Hierarchie der öffentlichen Ordner
Diese Option bewirkt, dass die öffentlichen Ordner[309], auf die die Benutzer Zugriff haben, in den Ordnerlisten der Benutzer auf ihren ActiveSync-Geräten erscheinen. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der öffentlichen Ordner[309], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Traversieren öffentlicher Ordner zulassen (legt Ordnernamen offen)
Benutzerkonten, die auf Unterordner in öffentlichen Ordnern zugreifen oder diese synchronisieren wollen, müssen per Voreinstellung sowohl für den betroffenen Unterordner als auch für alle ihm übergeordneten öffentlichen Ordner[309] über die Berechtigung Ordner anzeigen[311] verfügen. Fehlt einem Benutzerkonto diese Berechtigung für einen übergeordneten öffentlichen Ordner, so kann er auch den gewünschten Unterordner nicht synchronisieren und nicht auf ihn zugreifen, und zwar auch dann nicht, wenn das Benutzerkonto für diesen Unterordner selbst die erforderliche Berechtigung hat. Mithilfe dieser Option können Sie den Clients Zugriff auf und Synchronisierung von Unterordnern ermöglichen, ohne dass die Clients Berechtigungen für die übergeordneten öffentlichen Ordner haben. **Beachte:** Ist diese Option aktiv, so erlangt der Client zwangsläufig Kenntnis von den Namen der übergeordneten Ordner, auch wenn er für ihre Inhalte keine Zugriffsrechte hat. Hieraus kann sich ein Sicherheitsrisiko ergeben. Die Option ist per Voreinstellung abgeschaltet.

Höchstzahl zulässiger öffentlicher Ordner
Diese Option begrenzt die Zahl der öffentlichen Ordner, die auf den betroffenen Geräten dargestellt werden können. Ist eine solche Höchstzahl angegeben, dann übermittelt der Server so lange Einträge in der Ordnerliste, bis die Höchstzahl erreicht ist. Danach übermittelt der Server keine Ordner mehr an die Geräte. Die Reihenfolge, in der die Ordner dabei verarbeitet werden, kann weder festgelegt noch vorher bestimmt werden. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt.

Freigegebene Ordner
Diese Option nimmt auch die gemeinsam genutzten Ordner[122], auf die die Benutzer Zugriff haben, in die Ordnerlisten auf ihren ActiveSync-Geräten auf. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der freigegebenen Ordner[742], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Behandlung von Inhalten

Optionen zur Behandlung von Inhalten

Aufgaben/Erinnerungen für durch Clients gekennzeichnete Nachrichtenelemente erstellen
Diese Option ermöglicht es MDaemon, die Benutzer an gekennzeichnete Elemente zu erinnern. Hierzu wird für jede gekennzeichnete E-Mail-Nachricht eine Aufgabe erstellt, wenn der Client dies anfordert. Die globale Option für dieses Leistungsmerkmal ist per Voreinstellung aktiv.

Aktualisierung nach jeder Änderung der Besprechung senden
Manche Clients versenden aktualisierte Besprechungseinladungen nicht richtig, nachdem eine Besprechung geändert wurde. Diese Option bewirkt, dass der ActiveSync-Dienst immer dann aktualisierte Besprechungseinladungen sendet, wenn der Besprechungsorganisator eine Besprechung aktualisiert hat. Diese Option sollte nur für Clients 464 und Client-Typen 481 aktiviert werden, die die aktualisierten Besprechungseinladungen nicht richtig versenden, da sonst aktualisierte Besprechungseinladungen doppelt versandt werden. Aus diesem Grund ist diese Einstellung nur auf den Seiten Clients und Client-Typen verfügbar.

Lesebestätigung für alle versandten Nachrichten anfordern
Diese Option bewirkt, dass der Server für alle durch einen Client versandten E-Mail-Nachrichten Lesebestätigungen anfordert. Diese Option ist per Voreinstellung abgeschaltet.

Vom Absender angeforderte Lesebestätigung senden, sobald Nachricht als gelesen gekennzeichnet ist
Diese Option bewirkt, dass der Server Anforderungen von Lesebestätigungen beachtet und die Lesebestätigungen dann versendet, wenn eine Nachricht durch den Client als gelesen gekennzeichnet wird. Diese Option ist per Voreinstellung abgeschaltet.

Unter dem in der Antwortadresse (ReplyTo) angegebenen Alias senden
Manche Clients gestatten den Absendern nicht den Versand von E-Mail-Nachrichten unter einem Alias. Dieses Leistungsmerkmal wurde im der Version 16.x des Protokolls Exchange ActiveSync (EAS) 434 erstmals unterstützt, aber manche Clients unterstützen die Version 16.x nicht. So nutzt beispielsweise Microsoft Outlook für Windows nur EAS 14.0 und gestattet zwar den Benutzern die Angabe einer anderen Adresse, unter der eine Nachricht versandt werden soll, aber die dann erstellte Nachricht gibt die Auswahl des Benutzers nicht richtig wieder. Diese Option gestattet die Nutzung des Feldes für die Antwortadresse (ReplyTo) zum Versand von Nachrichten dann, wenn als Antwortadresse ein gültiger Alias 827 des Benutzers eingetragen ist. Die globale Option ist per Voreinstellung aktiv.

Öffentliche Kontakte virtuell mit den Standard-Kontakten zusammenführen
Diese Option bewirkt, dass die öffentlichen Kontakte und die Standard-Kontakte der Benutzer auf ihren Geräten als zusammengeführt dargestellt werden. Die Datenbestände der Kontakte bleiben hierbei getrennt; es werden also keine Kontakte zwischen den Kontaktordnern der Benutzer kopiert. Diese Option kann insbesondere für solche Clients hilfreich sein, die das Durchsuchen der Globalen Adressliste (GAL) nicht unterstützen. Diese Option ist per Voreinstellung abgeschaltet.

Absender sperren, wenn Nachricht in Ordner Junk-Email verschoben wird
Ist diese Option aktiv, so wird die Absender-Adresse (Felder Sender und From) einer E-Mail-Adresse in den Kontaktordner für gesperrte Absender eingetragen, sobald ein Client die zugehörige E-Mail-Nachricht in den Ordner für Spam-Nachrichten verschiebt.

Antworten auf Besprechungsanfragen nach Zusage, Ablehnung usw. zwingend senden
Ist diese Option aktiv, so versendet der ActiveSync-Dienst eine Antwort an den Besprechungsorganisator immer dann, wenn ein Client auf eine Besprechungseinladung zusagt, sie ablehnt oder eine sonstige Aktion für die Einladung ausführt. Diese Option ist für solche Clients nützlich, die solche Antworten nicht selbst richtig senden.

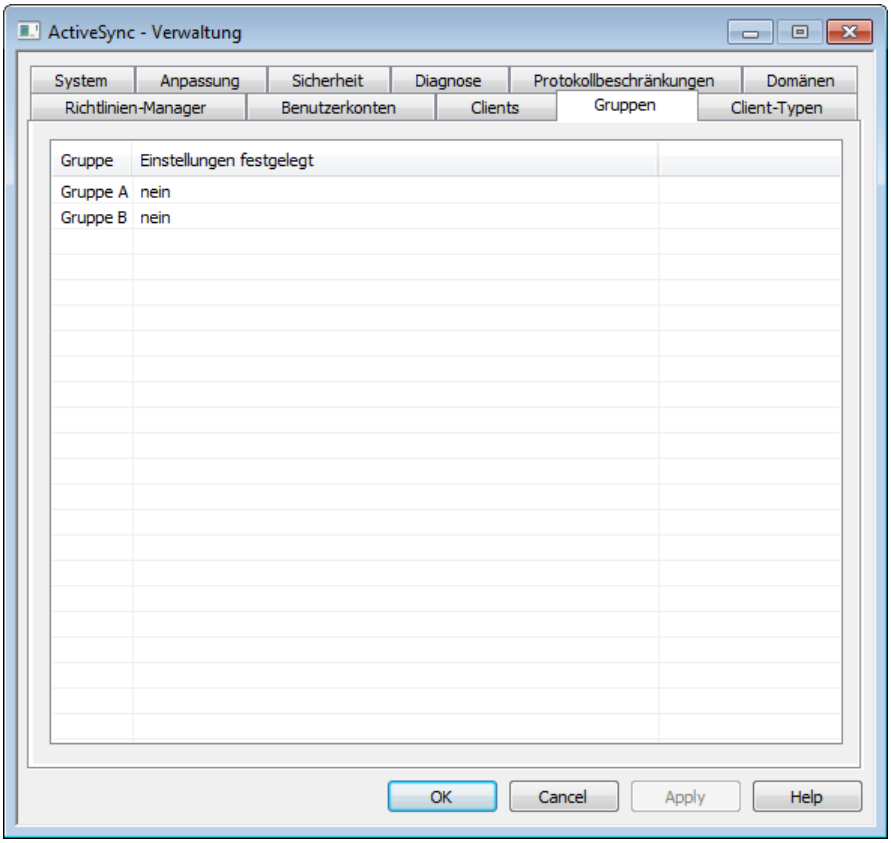
Vorschau auf tatsächlich wirksame Einstellungen

Dieses Steuerelement ist auf allen untergeordneten Konfigurationsdialogen für die Client-Einstellungen (Domänen 437, Benutzerkonten 454 und Clients 464) verfügbar. Per Voreinstellung werden die Optionen auf diesen Konfigurationsdialogen nicht von den übergeordneten Konfigurationsdialogen geerbt. Sie können sich daher mithilfe dieses Steuerelements die Einstellungen anzeigen lassen, die auf den jeweils gerade dargestellten Konfigurationsdialog wirken.

Siehe auch:

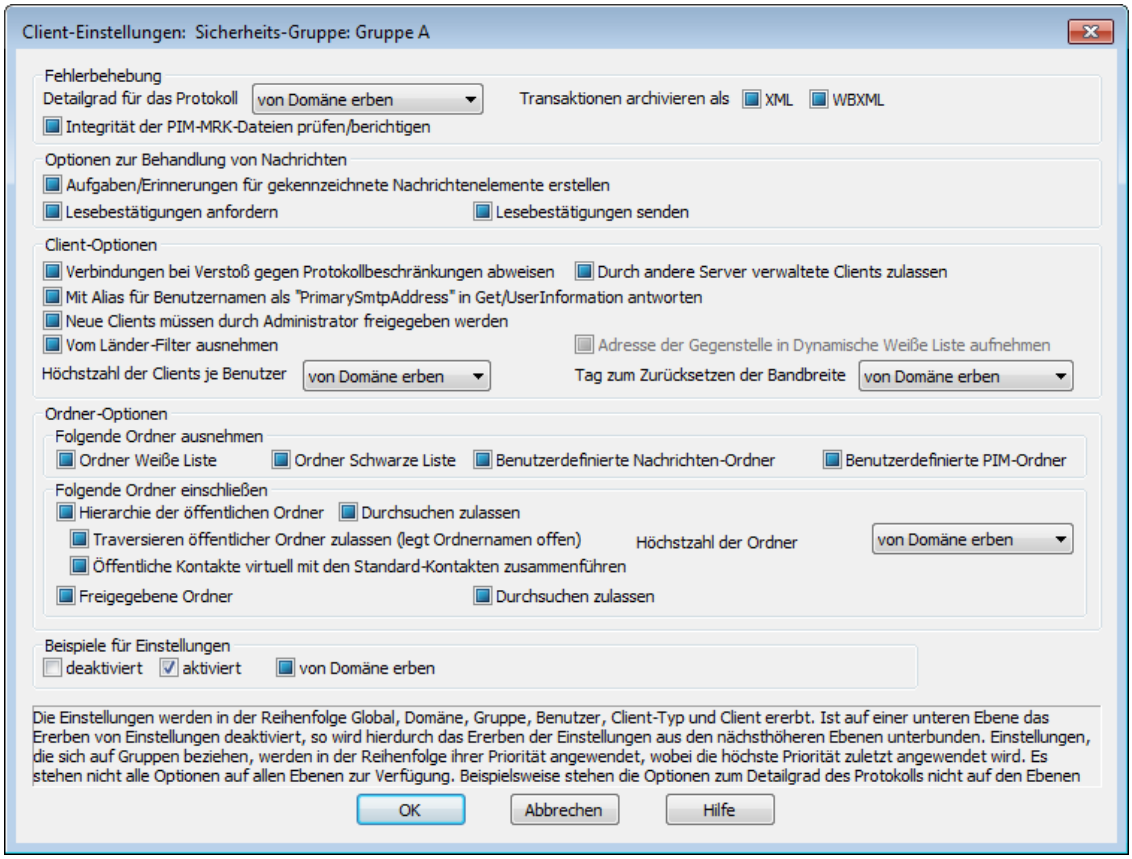
ActiveSync » Client-Einstellungen 422
ActiveSync » Domänen 437
ActiveSync » Benutzerkonten 454

3.10.10 Gruppen



Mithilfe dieses Konfigurationsdialogs können Sie individuelle ActiveSync-Client-Einstellungen für einzelne Gruppen[782] von Benutzerkonten festlegen. In diesem Konfigurationsdialog erscheinen alle bestehenden Gruppen. Für jede Gruppe erscheint die Information, ob besonders angepasste Einstellungen festgelegt sind. Um die Client-Einstellungen für eine Gruppe zu bearbeiten, klicken Sie doppelt auf den Eintrag der Gruppe in der Liste, oder führen Sie auf dem Eintrag der Gruppe einen Rechtsklick aus, und klicken Sie danach auf **Client-Einstellungen anpassen**.

Client-Einstellungen für einzelne Gruppen



Per Voreinstellung ererbt jede Gruppe ihre Einstellungen von den Client-Einstellungen der Domäne[215] der Benutzer. Wenn Sie in diesem Konfigurationsdialog eine Client-Einstellung für eine Gruppe festlegen, so geht diese Einstellung für die Mitglieder dieser Gruppe allen dieser Einstellung widersprechenden Einstellungen der Domänen der Benutzer vor. Falls Sie die Client-Einstellungen für die Gruppe auf eine bestimmtes Gruppenmitglied oder auf einen bestimmten Client nicht anwenden wollen, können Sie die abweichende Einstellungen für Benutzerkonto[454], Client-Typ[481] oder Client[464] bearbeiten. Diese genannten Client-Einstellungen gehen den widersprechenden Client-Einstellungen für die Gruppe.

Allgemeines

Fehlerbehebung

Detailgrad für das Protokoll
ActiveSync für MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Einstellung erben Per Voreinstellung wird die Einstellung für den Detailgrad aus der Hierarchie der Client-Einstellungen vom jeweils übergeordneten Knoten ererbt. Clients übernehmen dabei die Einstellung aus dem jeweiligen Client-Typ, Client-Typen übernehmen die Einstellung von den Benutzerkonten, Benutzerkonten übernehmen die Einstellung von den Gruppen, und so weiter. Die globale Einstellung für alle Clients wird durch die Einstellung für den Detailgrad im Konfigurationsdialog Diagnose[432] bestimmt.

Transaktionen archivieren als [XML | WBXML]
Mithilfe der Optionen *XML...* und *WBXML...* können Sie die zugehörigen Daten speichern; diese Daten können die Fehlersuche erleichtern. Die systemweit wirksamen Optionen sind per Voreinstellung abgeschaltet.

Integrität der PIM-MRK-Dateien prüfen/berichtigen
Diese Option führt für die PIM-Daten der betroffenen Clients Prüf- und Korrekturvorgänge durch. Sie sollen bekannte Probleme erkennen, die eine ordnungsgemäße Synchronisierung verhindern können. Zu diesen Problemen zählen insbesondere doppelte iCal-UIDs und leere Datenfelder, die eigentlich verpflichtend Daten enthalten müssen. Die systemweit wirksame Option ist per Voreinstellung abgeschaltet.

Client-Optionen

Verbindungen bei Verstoß gegen Protokollbeschränkungen abweisen
Diese Option bewirkt, dass Verbindungen von Clients abgewiesen werden, falls sie versuchen eine nicht für die Clients *Zugelassene Protokollversion* zu verwenden. Per Voreinstellung ist diese Option abgeschaltet; dies bedeutet, dass die Protokollbeschränkung keine Verbindungen solcher Clients verhindern, die andere als die zugelassenen Protokollversionen verwenden. Solange die Option abgeschaltet ist, weist MDaemon die Clients zwar an, nur die zugelassenen Protokollversionen zu verwenden, lässt aber bei Nutzung anderer Protokollversionen die Verbindung trotzdem zu. Nähere Informationen finden Sie unter Protokollbeschränkungen[434].

Mit Alias für Benutzernamen als "PrimarySmtpAddress" in Get/UserInformation antworten
Diese Option gestattet es dem Dienst, als Antwort auf eine Anforderung Settings/Get/UserInformation eine etwa vorhandene Alias-Adresse oder eine sekundäre Adresse des betroffenen Benutzerkontos als primäre Adresse zu übermitteln. Hierdurch wird ein Problem umgangen, das mit einer iOS-Aktualisierung nach Version 9.x verursacht wird, und das verhinderte, dass Clients unter einer etwa vorhandenen Alias-Adresse Nachrichten versenden

konnten. Die Nutzung dieser Option bewirkt eine nicht standardkonforme Antwort auf die Anforderung Settings/GetUserInformation.

Neue Clients müssen durch Administrator freigegeben werden
Diese Option bewirkt, dass neue Clients sich erst dann mit Benutzerkonten synchronisieren können, wenn sie zunächst durch einen Administrator freigegeben wurden. In der Liste der Clients[464] sind alle Clients aufgeführt, die noch die Freigabe erwarten, und die Administratoren können sie über diese Liste freigeben. Diese Option ist per Voreinstellung abgeschaltet.

Höchstzahl der Clients je Benutzer
Mithilfe dieser Option können Sie die Anzahl der ActiveSync-Clients und -Endgeräte begrenzen, die mit jedem MDaemon-Benutzerkonto verknüpft sein können. Der hier angegebene Wert ist die Höchstzahl zulässiger Clients. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt. Diese Option steht nur in den Client-Einstellungen auf globaler, Domänen- und Benutzerebene zur Verfügung, nicht jedoch in den Client-Einstellungen für die einzelnen Clients.

Tag zum Zurücksetzen der Bandbreite
Mithilfe dieser Option können Sie Tag bestimmen, an dem in jedem Monat die Bandbreiten-Nutzungsstatistik für die ActiveSync-Endgeräte zurückgesetzt wird. Dieser Vorgang wird während der normalen Bereinigungsvorgänge um Mitternacht aufgeführt und, wie auch andere Bereinigungsvorgänge, in das Protokoll System eingetragen. Der globale Wert lautet per Voreinstellung 0 (nicht zurücksetzen), sodass per Voreinstellung die Nutzungsstatistik nicht zurückgesetzt wird. Für untergeordnete Knoten können Sie abweichende Einstellungen treffen, etwa, um die Einstellung an den Tag anzugleichen, an dem für das betroffene Endgeräte ein neuer Abrechnungszeitraum des Netzbetreibers beginnt.

Sicherheit

Vom Länder-Filter ausnehmen
Wenn Sie diese Option in den Einstellungen eines ActiveSync-Clients aktivieren, kann das Endgerät den Länder-Filter[574] umgehen. Hierdurch kann ein berechtigter Benutzer auf sein Benutzerkonto über ActiveSync beispielsweise auch dann zugreifen, wenn er sich in einem Land befindet, für das Versuche zur Echtheitsbestätigung ansonsten durch den Länder-Filter unterbunden werden. Ein Endgerät kann nur dann vom Länder-Filter ausgenommen sein, wenn es innerhalb des durch die Option Inaktive Clients entfernen nach [x] Tagen[418] im Abschnitt Anpassung bestimmten Zeitraums eine echtheitsbestätigte Verbindung über ActiveSync erfolgreich hergestellt hat.

Adresse der Gegenstelle in Dynamische Freigabeliste aufnehmen
Wenn Sie ein Endgerät vom Länder-Filter ausnehmen, können Sie durch Aktivieren dieser Option die IP-Adresse, von der aus das Endgerät die Verbindung herstellt, in die Freigabeliste eintragen lassen. Hierdurch können beispielsweise andere Clients, die von der selben IP-Adresse aus eine Verbindung herstellen, ebenfalls zugelassen werden.

Durch andere Server provisionierte/verwaltete Clients zulassen
Per Voreinstellung dürfen Clients auch dann Verbindungen zu MDaemon aufbauen, wenn sie auf die Übermittlung der Provisionierungs- und Richtliniendaten durch den ActiveSync-Server hin melden, dass sie auch durch einen oder mehrere andere ActiveSync-Server verwaltet werden. Bei einer solchen

Mehrfachverwaltung kann es nicht sichergestellt werden, dass alle auf Ihrem System bestehenden Richtlinien durch den Client auch umgesetzt werden; dies gilt insbesondere dann, wenn sie Richtlinien des anderen ActiveSync-Servers widersprechen. In vielen Fällen setzen die Clients die am stärksten einschränkende Richtlinie um, falls mehrere einander widersprechende Richtlinien vorhanden sind. Um Verbindungen von Clients zu unterbinden, die durch andere ActiveSync-Server verwaltet werden, deaktivieren Sie diese Option.

Löschen der Clients (Zurücksetzen in den Auslieferungszustand) nicht zulassen
Wenn diese Option aktiv ist, dann können ActiveSync-Clients nicht in den **Auslieferungszustand zurückgesetzt** und damit vollständig gelöscht werden. Wenn Sie Clients ferngesteuert in den Auslieferungszustand zurücksetzen wollen, müssen Sie diese Option deaktivieren. Diese Option ist per Voreinstellung deaktiviert. Nähere Informationen finden Sie auf der Seite Clients im Abschnitt **Vollständiges Löschen eines ActiveSync-Clients** 464.

Optionen zur Ordner-Synchronisierung

Optionen zur Ordner-Synchronisierung

Folgende Ordner ausnehmen

Freigegebene Absender/Gesperrte Absender
Per Voreinstellung werden die Kontaktordner mit Freigabelisten und Sperrlisten der Benutzer nicht mit den Geräten synchronisiert. Diese Ordner dienen üblicherweise nur in MDaemon zum Erkennen und Filtern von Spam. Ihre Inhalte brauchen daher nicht auf den Geräten als Kontakte angezeigt zu werden.

Benutzerdefinierte Nachrichten-Ordner
Per Voreinstellung können alle Standard- und benutzerdefinierten Nachrichten-Ordner mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-Nachrichtenordner synchronisiert werden können. Die Standard-Nachrichtenordner sind insbesondere Posteingang, Gesendete Objekte, Gelöschte Objekte und Entwürfe. Ordner, die die Benutzer selbst anlegen, werden dann nicht mehr synchronisiert. Diese Option ist per Voreinstellung abgeschaltet.

Benutzerdefinierte PIM-Ordner
Per Voreinstellung können alle PIM-Ordner (insbesondere Kontakte, Kalender, Notizen und Aufgaben) mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-PIM-Ordner synchronisiert werden können. Ist diese Option aktiv, so wird beispielsweise für jeden Benutzer nur der Standard-Kalender synchronisiert, auch wenn er über mehrere Kalender-Ordner verfügt. Diese Option ist per Voreinstellung abgeschaltet.

Folgende Ordner einschließen

Hierarchie der öffentlichen Ordner
Diese Option bewirkt, dass die öffentlichen Ordner 309, auf die die Benutzer Zugriff haben, in den Ordnerlisten der Benutzer auf ihren ActiveSync-Geräten erscheinen. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der öffentlichen

Ordner[309], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Traversieren öffentlicher Ordner zulassen (legt Ordnernamen offen)
Benutzerkonten, die auf Unterordner in öffentlichen Ordnern zugreifen oder diese synchronisieren wollen, müssen per Voreinstellung sowohl für den betroffenen Unterordner als auch für alle ihm übergeordneten öffentlichen Ordner[309] über die Berechtigung Ordner anzeigen[311] verfügen. Fehlt einem Benutzerkonto diese Berechtigung für einen übergeordneten öffentlichen Ordner, so kann er auch den gewünschten Unterordner nicht synchronisieren und nicht auf ihn zugreifen, und zwar auch dann nicht, wenn das Benutzerkonto für diesen Unterordner selbst die erforderliche Berechtigung hat. Mithilfe dieser Option können Sie den Clients Zugriff auf und Synchronisierung von Unterordnern ermöglichen, ohne dass die Clients Berechtigungen für die übergeordneten öffentlichen Ordner haben. **Beachte:** Ist diese Option aktiv, so erlangt der Client zwangsläufig Kenntnis von den Namen der übergeordneten Ordner, auch wenn er für ihre Inhalte keine Zugriffsrechte hat. Hieraus kann sich ein Sicherheitsrisiko ergeben. Die Option ist per Voreinstellung abgeschaltet.

Höchstzahl zulässiger öffentlicher Ordner
Diese Option begrenzt die Zahl der öffentlichen Ordner, die auf den betroffenen Geräten dargestellt werden können. Ist eine solche Höchstzahl angegeben, dann übermittelt der Server so lange Einträge in der Ordnerliste, bis die Höchstzahl erreicht ist. Danach übermittelt der Server keine Ordner mehr an die Geräte. Die Reihenfolge, in der die Ordner dabei verarbeitet werden, kann weder festgelegt noch vorher bestimmt werden. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt.

Freigegebene Ordner
Diese Option nimmt auch die gemeinsam genutzten Ordner[122], auf die die Benutzer Zugriff haben, in die Ordnerlisten auf ihren ActiveSync-Geräten auf. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der freigegebenen Ordner[742], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Behandlung von Inhalten

Optionen zur Behandlung von Inhalten

Aufgaben/Erinnerungen für durch Clients gekennzeichnete Nachrichtenelemente erstellen
Diese Option ermöglicht es MDaemon, die Benutzer an gekennzeichnete Elemente zu erinnern. Hierzu wird für jede gekennzeichnete E-Mail-Nachricht eine Aufgabe erstellt, wenn der Client dies anfordert. Die globale Option für dieses Leistungsmerkmal ist per Voreinstellung aktiv.

Aktualisierung nach jeder Änderung der Besprechung senden
Manche Clients versenden aktualisierte Besprechungseinladungen nicht richtig, nachdem eine Besprechung geändert wurde. Diese Option bewirkt, dass der ActiveSync-Dienst immer dann aktualisierte Besprechungseinladungen sendet, wenn der Besprechungsorganisator eine Besprechung aktualisiert hat. Diese

Option sollte nur für Clients[464] und Client-Typen[481] aktiviert werden, die die aktualisierten Besprechungseinladungen nicht richtig versenden, da sonst aktualisierte Besprechungseinladungen doppelt versandt werden. Aus diesem Grund ist diese Einstellung nur auf den Seiten Clients und Client-Typen verfügbar.

Lesebestätigung für alle versandten Nachrichten anfordern
Diese Option bewirkt, dass der Server für alle durch einen Client versandten E-Mail-Nachrichten Lesebestätigungen anfordert. Diese Option ist per Voreinstellung abgeschaltet.

Vom Absender angeforderte Lesebestätigung senden, sobald Nachricht als gelesen gekennzeichnet ist
Diese Option bewirkt, dass der Server Anforderungen von Lesebestätigungen beachtet und die Lesebestätigungen dann versendet, wenn eine Nachricht durch den Client als gelesen gekennzeichnet wird. Diese Option ist per Voreinstellung abgeschaltet.

Unter dem in der Antwortadresse (ReplyTo) angegebenen Alias senden
Manche Clients gestatten den Absendern nicht den Versand von E-Mail-Nachrichten unter einem Alias. Dieses Leistungsmerkmal wurde im der Version 16.x des Protokolls Exchange ActiveSync (EAS)[434] erstmals unterstützt, aber manche Clients unterstützen die Version 16.x nicht. So nutzt beispielsweise Microsoft Outlook für Windows nur EAS 14.0 und gestattet zwar den Benutzern die Angabe einer anderen Adresse, unter der eine Nachricht versandt werden soll, aber die dann erstellte Nachricht gibt die Auswahl des Benutzers nicht richtig wieder. Diese Option gestattet die Nutzung des Feldes für die Antwortadresse (ReplyTo) zum Versand von Nachrichten dann, wenn als Antwortadresse ein gültiger Alias[827] des Benutzers eingetragen ist. Die globale Option ist per Voreinstellung aktiv.

Öffentliche Kontakte virtuell mit den Standard-Kontakten zusammenführen
Diese Option bewirkt, dass die öffentlichen Kontakte und die Standard-Kontakte der Benutzer auf ihren Geräten als zusammengeführt dargestellt werden. Die Datenbestände der Kontakte bleiben hierbei getrennt; es werden also keine Kontakte zwischen den Kontaktordnern der Benutzer kopiert. Diese Option kann insbesondere für solche Clients hilfreich sein, die das Durchsuchen der Globalen Adressliste (GAL) nicht unterstützen. Diese Option ist per Voreinstellung abgeschaltet.

Absender sperren, wenn Nachricht in Ordner Junk-Email verschoben wird
Ist diese Option aktiv, so wird die Absender-Adresse (Felder Sender und From) einer E-Mail-Adresse in den Kontaktordner für gesperrte Absender eingetragen, sobald ein Client die zugehörige E-Mail-Nachricht in den Ordner für Spam-Nachrichten verschiebt.

Antworten auf Besprechungsanfragen nach Zusage, Ablehnung usw. zwingend senden
Ist diese Option aktiv, so versendet der ActiveSync-Dienst eine Antwort an den Besprechungsorganisator immer dann, wenn ein Client auf eine Besprechungseinladung zusagt, sie ablehnt oder eine sonstige Aktion für die Einladung ausführt. Diese Option ist für solche Clients nützlich, die solche Antworten nicht selbst richtig senden.

Vorschau auf tatsächlich wirksame Einstellungen

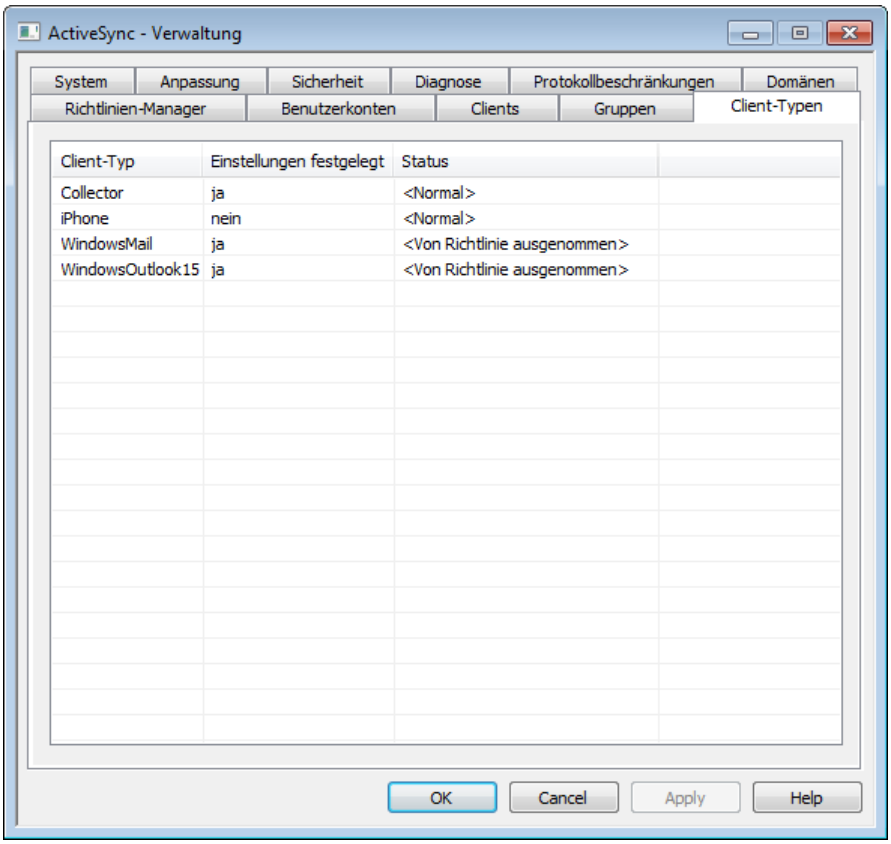
Dieses Steuerelement ist auf allen untergeordneten Konfigurationsdialogen für die

Client-Einstellungen (Domänen[437], Benutzerkonten[454] und Clients[464]) verfügbar. Per Voreinstellung werden die Optionen auf diesen Konfigurationsdialogen nicht von den übergeordneten Konfigurationsdialogen geerbt. Sie können sich daher mithilfe dieses Steuerelements die Einstellungen anzeigen lassen, die auf den jeweils gerade dargestellten Konfigurationsdialog wirken.

Siehe auch:

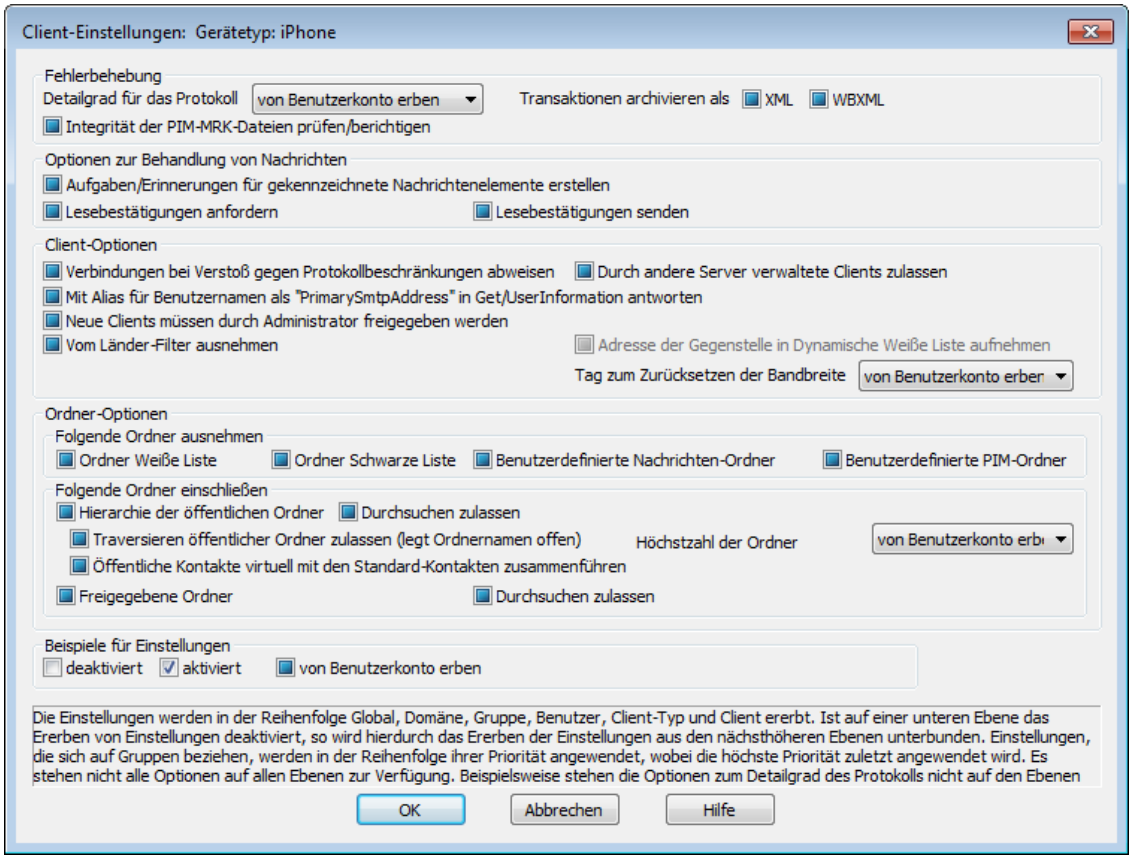
ActiveSync » Domänen[437]
ActiveSync » Benutzerkonten[454]
ActiveSync » Clients[464]

3.10.11 Client-Typen



Mithilfe dieses Konfigurationsdialogs können Sie individuelle ActiveSync-Client-Einstellungen für einzelne Typen von ActiveSync-Clients festlegen. In diesem Konfigurationsdialog erscheinen die Client-Typen aller jeweils zur Nutzung von ActiveSync berechtigten Clients[464]. Für jeden Client-Typen erscheint die Information, ob besonders angepasste Einstellungen festgelegt sind. Um die Client-Einstellungen für einen Client-Typen zu bearbeiten, klicken Sie doppelt auf den Eintrag des Client-Typen in der Liste, oder führen Sie auf dem Eintrag des Client-Typen einen Rechtsklick aus, und klicken Sie danach auf **Client-Einstellungen anpassen**. Mithilfe des Kontextmenüs, das nach einem Rechtsklick erscheint, können Sie außerdem die angepassten Einstellungen wieder entfernen, den Client-Typen in die Freigabelisten und Ausnahmelisten[429] für ActiveSync eintragen und aus ihnen wieder entfernen.

Client-Einstellungen für einzelne Client-Typen



Per Voreinstellung ererbt jeder Client-Typ seine Einstellungen von den Client-Einstellungen des Benutzerkontos 764. Wenn Sie in diesem Konfigurationsdialog eine Client-Einstellung für einen Client-Typen festlegen, so geht diese Einstellung für diesen Client-Typen allen dieser Einstellung widersprechenden Einstellungen aller Benutzerkonten vor. Falls Sie die Client-Einstellungen für den Client-Typen auf einen bestimmten einzelnen Client nicht anwenden wollen, können Sie die Einstellungen für den Client-Typen in den Client-Einstellungen für die einzelnen Clients 464 bearbeiten. Die Client-Einstellungen für die einzelnen Clients gehen den widersprechenden Client-Einstellungen für die Client-Typen vor.

Allgemeines

Fehlerbehebung

Detailgrad für das Protokoll
ActiveSync für MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden

allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Einstellung erben Per Voreinstellung wird die Einstellung für den Detailgrad aus der Hierarchie der Client-Einstellungen vom jeweils übergeordneten Knoten ererbt. Clients übernehmen dabei die Einstellung aus dem jeweiligen Client-Typ, Client-Typen übernehmen die Einstellung von den Benutzerkonten, Benutzerkonten übernehmen die Einstellung von den Gruppen, und so weiter. Die globale Einstellung für alle Clients wird durch die Einstellung für den Detailgrad im Konfigurationsdialog Diagnose 432 bestimmt.

Transaktionen archivieren als [XML | WBXML]
Mithilfe der Optionen *XML...* und *WBXML...* können Sie die zugehörigen Daten speichern; diese Daten können die Fehlersuche erleichtern. Die systemweit wirksamen Optionen sind per Voreinstellung abgeschaltet.

Integrität der PIM-MRK-Dateien prüfen/berichtigen
Diese Option führt für die PIM-Daten der betroffenen Clients Prüf- und Korrekturvorgänge durch. Sie sollen bekannte Probleme erkennen, die eine ordnungsgemäße Synchronisierung verhindern können. Zu diesen Problemen zählen insbesondere doppelte iCal-UIDs und leere Datenfelder, die eigentlich verpflichtend Daten enthalten müssen. Die systemweit wirksame Option ist per Voreinstellung abgeschaltet.

Client-Optionen

Verbindungen bei Verstoß gegen Protokollbeschränkungen abweisen
Diese Option bewirkt, dass Verbindungen von Clients abgewiesen werden, falls sie versuchen eine nicht für die Clients *Zugelassene Protokollversion* zu verwenden. Per Voreinstellung ist diese Option abgeschaltet; dies bedeutet, dass die Protokollbeschränkung keine Verbindungen solcher Clients verhindern, die andere als die zugelassenen Protokollversionen verwenden. Solange die Option abgeschaltet ist, weist MDaemon die Clients zwar an, nur die zugelassenen Protokollversionen zu verwenden, lässt aber bei Nutzung anderer Protokollversionen die Verbindung trotzdem zu. Nähere Informationen finden Sie unter Protokollbeschränkungen 434.

Mit Alias für Benutzernamen als "PrimarySmtpAddress" in Get/UserInformation antworten
Diese Option gestattet es dem Dienst, als Antwort auf eine Anforderung Settings/Get/UserInformation eine etwa vorhandene Alias-Adresse oder eine sekundäre Adresse des betroffenen Benutzerkontos als primäre Adresse zu

übermitteln. Hierdurch wird ein Problem umgangen, das mit einer iOS-Aktualisierung nach Version 9.x verursacht wird, und das verhinderte, dass Clients unter einer etwa vorhandenen Alias-Adresse Nachrichten versenden konnten. Die Nutzung dieser Option bewirkt eine nicht standardkonforme Antwort auf die Anforderung Settings/GetUserInformation.

Neue Clients müssen durch Administrator freigegeben werden
Diese Option bewirkt, dass neue Clients sich erst dann mit Benutzerkonten synchronisieren können, wenn sie zunächst durch einen Administrator freigegeben wurden. In der Liste der Clients[464] sind alle Clients aufgeführt, die noch die Freigabe erwarten, und die Administratoren können sie über diese Liste freigeben. Diese Option ist per Voreinstellung abgeschaltet.

Höchstzahl der Clients je Benutzer
Mithilfe dieser Option können Sie die Anzahl der ActiveSync-Clients und -Endgeräte begrenzen, die mit jedem MDaemon-Benutzerkonto verknüpft sein können. Der hier angegebene Wert ist die Höchstzahl zulässiger Clients. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt. Diese Option steht nur in den Client-Einstellungen auf globaler, Domänen- und Benutzerebene zur Verfügung, nicht jedoch in den Client-Einstellungen für die einzelnen Clients.

Tag zum Zurücksetzen der Bandbreite
Mithilfe dieser Option können Sie Tag bestimmen, an dem in jedem Monat die Bandbreiten-Nutzungsstatistik für die ActiveSync-Endgeräte zurückgesetzt wird. Dieser Vorgang wird während der normalen Bereinigungsvorgänge um Mitternacht aufgeführt und, wie auch andere Bereinigungsvorgänge, in das Protokoll System eingetragen. Der globale Wert lautet per Voreinstellung 0 (nicht zurücksetzen), sodass per Voreinstellung die Nutzungsstatistik nicht zurückgesetzt wird. Für untergeordnete Knoten können Sie abweichende Einstellungen treffen, etwa, um die Einstellung an den Tag anzugleichen, an dem für das betroffene Endgeräte ein neuer Abrechnungszeitraum des Netzbetreibers beginnt.

Sicherheit

Vom Länder-Filter ausnehmen
Wenn Sie diese Option in den Einstellungen eines ActiveSync-Clients aktivieren, kann das Endgerät den Länder-Filter[574] umgehen. Hierdurch kann ein berechtigter Benutzer auf sein Benutzerkonto über ActiveSync beispielsweise auch dann zugreifen, wenn er sich in einem Land befindet, für das Versuche zur Echtheitsbestätigung ansonsten durch den Länder-Filter unterbunden werden. Ein Endgerät kann nur dann vom Länder-Filter ausgenommen sein, wenn es innerhalb des durch die Option Inaktive Clients entfernen nach [x] Tagen[418] im Abschnitt Anpassung bestimmten Zeitraums eine echtheitsbestätigte Verbindung über ActiveSync erfolgreich hergestellt hat.

Adresse der Gegenstelle in Dynamische Freigabeliste aufnehmen
Wenn Sie ein Endgerät vom Länder-Filter ausnehmen, können Sie durch Aktivieren dieser Option die IP-Adresse, von der aus das Endgerät die Verbindung herstellt, in die Freigabeliste eintragen lassen. Hierdurch können beispielsweise andere Clients, die von der selben IP-Adresse aus eine Verbindung herstellen, ebenfalls zugelassen werden.

Durch andere Server provisionierte/verwaltete Clients zulassen
Per Voreinstellung dürfen Clients auch dann Verbindungen zu MDaemon aufbauen,

wenn sie auf die Übermittlung der Provisionierungs- und Richtliniendaten durch den ActiveSync-Server hin melden, dass sie auch durch einen oder mehrere andere ActiveSync-Server verwaltet werden. Bei einer solchen Mehrfachverwaltung kann es nicht sichergestellt werden, dass alle auf Ihrem System bestehenden Richtlinien durch den Client auch umgesetzt werden; dies gilt insbesondere dann, wenn sie Richtlinien des anderen ActiveSync-Servers widersprechen. In vielen Fällen setzen die Clients die am stärksten einschränkende Richtlinie um, falls mehrere einander widersprechende Richtlinien vorhanden sind. Um Verbindungen von Clients zu unterbinden, die durch andere ActiveSync-Server verwaltet werden, deaktivieren Sie diese Option.

Löschen der Clients (Zurücksetzen in den Auslieferungszustand) nicht zulassen
Wenn diese Option aktiv ist, dann können ActiveSync-Clients nicht in den **Auslieferungszustand zurückgesetzt** und damit vollständig gelöscht werden. Wenn Sie Clients ferngesteuert in den Auslieferungszustand zurücksetzen wollen, müssen Sie diese Option deaktivieren. Diese Option ist per Voreinstellung deaktiviert. Nähere Informationen finden Sie auf der Seite Clients im Abschnitt **Vollständiges Löschen eines ActiveSync-Clients** 464.

Optionen zur Ordner-Synchronisierung

Optionen zur Ordner-Synchronisierung

Folgende Ordner ausnehmen

Freigegebene Absender/Gesperrte Absender
Per Voreinstellung werden die Kontaktordner mit Freigabelisten und Sperrlisten der Benutzer nicht mit den Geräten synchronisiert. Diese Ordner dienen üblicherweise nur in MDaemon zum Erkennen und Filtern von Spam. Ihre Inhalte brauchen daher nicht auf den Geräten als Kontakte angezeigt zu werden.

Benutzerdefinierte Nachrichten-Ordner
Per Voreinstellung können alle Standard- und benutzerdefinierten Nachrichten-Ordner mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-Nachrichtenordner synchronisiert werden können. Die Standard-Nachrichtenordner sind insbesondere Posteingang, Gesendete Objekte, Gelöschte Objekte und Entwürfe. Ordner, die die Benutzer selbst anlegen, werden dann nicht mehr synchronisiert. Diese Option ist per Voreinstellung abgeschaltet.

Benutzerdefinierte PIM-Ordner
Per Voreinstellung können alle PIM-Ordner (insbesondere Kontakte, Kalender, Notizen und Aufgaben) mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-PIM-Ordner synchronisiert werden können. Ist diese Option aktiv, so wird beispielsweise für jeden Benutzer nur der Standard-Kalender synchronisiert, auch wenn er über mehrere Kalender-Ordner verfügt. Diese Option ist per Voreinstellung abgeschaltet.

Folgende Ordner einschließen

Hierarchie der öffentlichen Ordner
Diese Option bewirkt, dass die öffentlichen Ordner 309, auf die die Benutzer Zugriff haben, in den Ordnerlisten der Benutzer auf ihren ActiveSync-Geräten erscheinen. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der öffentlichen Ordner[309], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Traversieren öffentlicher Ordner zulassen (legt Ordnernamen offen)
Benutzerkonten, die auf Unterordner in öffentlichen Ordnern zugreifen oder diese synchronisieren wollen, müssen per Voreinstellung sowohl für den betroffenen Unterordner als auch für alle ihm übergeordneten öffentlichen Ordner[309] über die Berechtigung Ordner anzeigen[311] verfügen. Fehlt einem Benutzerkonto diese Berechtigung für einen übergeordneten öffentlichen Ordner, so kann er auch den gewünschten Unterordner nicht synchronisieren und nicht auf ihn zugreifen, und zwar auch dann nicht, wenn das Benutzerkonto für diesen Unterordner selbst die erforderliche Berechtigung hat. Mithilfe dieser Option können Sie den Clients Zugriff auf und Synchronisierung von Unterordnern ermöglichen, ohne dass die Clients Berechtigungen für die übergeordneten öffentlichen Ordner haben. **Beachte:** Ist diese Option aktiv, so erlangt der Client zwangsläufig Kenntnis von den Namen der übergeordneten Ordner, auch wenn er für ihre Inhalte keine Zugriffsrechte hat. Hieraus kann sich ein Sicherheitsrisiko ergeben. Die Option ist per Voreinstellung abgeschaltet.

Höchstzahl zulässiger öffentlicher Ordner
Diese Option begrenzt die Zahl der öffentlichen Ordner, die auf den betroffenen Geräten dargestellt werden können. Ist eine solche Höchstzahl angegeben, dann übermittelt der Server so lange Einträge in der Ordnerliste, bis die Höchstzahl erreicht ist. Danach übermittelt der Server keine Ordner mehr an die Geräte. Die Reihenfolge, in der die Ordner dabei verarbeitet werden, kann weder festgelegt noch vorher bestimmt werden. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt.

Freigegebene Ordner
Diese Option nimmt auch die gemeinsam genutzten Ordner[122], auf die die Benutzer Zugriff haben, in die Ordnerlisten auf ihren ActiveSync-Geräten auf. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der freigegebenen Ordner[742], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Behandlung von Inhalten

Optionen zur Behandlung von Inhalten

Aufgaben/Erinnerungen für durch Clients gekennzeichnete Nachrichtenelemente erstellen
Diese Option ermöglicht es MDaemon, die Benutzer an gekennzeichnete Elemente zu erinnern. Hierzu wird für jede gekennzeichnete E-Mail-Nachricht eine Aufgabe erstellt, wenn der Client dies anfordert. Die globale Option für dieses Leistungsmerkmal ist per Voreinstellung aktiv.

Aktualisierung nach jeder Änderung der Besprechung senden
Manche Clients versenden aktualisierte Besprechungseinladungen nicht richtig, nachdem eine Besprechung geändert wurde. Diese Option bewirkt, dass der

ActiveSync-Dienst immer dann aktualisierte Besprechungseinladungen sendet, wenn der Besprechungsorganisator eine Besprechung aktualisiert hat. Diese Option sollte nur für Clients[464] und Client-Typen[481] aktiviert werden, die die aktualisierten Besprechungseinladungen nicht richtig versenden, da sonst aktualisierte Besprechungseinladungen doppelt versandt werden. Aus diesem Grund ist diese Einstellung nur auf den Seiten Clients und Client-Typen verfügbar.

Lesebestätigung für alle versandten Nachrichten anfordern
Diese Option bewirkt, dass der Server für alle durch einen Client versandten E-Mail-Nachrichten Lesebestätigungen anfordert. Diese Option ist per Voreinstellung abgeschaltet.

Vom Absender angeforderte Lesebestätigung senden, sobald Nachricht als gelesen gekennzeichnet ist
Diese Option bewirkt, dass der Server Anforderungen von Lesebestätigungen beachtet und die Lesebestätigungen dann versendet, wenn eine Nachricht durch den Client als gelesen gekennzeichnet wird. Diese Option ist per Voreinstellung abgeschaltet.

Unter dem in der Antwortadresse (ReplyTo) angegebenen Alias senden
Manche Clients gestatten den Absendern nicht den Versand von E-Mail-Nachrichten unter einem Alias. Dieses Leistungsmerkmal wurde im der Version 16.x des Protokolls Exchange ActiveSync (EAS)[434] erstmals unterstützt, aber manche Clients unterstützen die Version 16.x nicht. So nutzt beispielsweise Microsoft Outlook für Windows nur EAS 14.0 und gestattet zwar den Benutzern die Angabe einer anderen Adresse, unter der eine Nachricht versandt werden soll, aber die dann erstellte Nachricht gibt die Auswahl des Benutzers nicht richtig wieder. Diese Option gestattet die Nutzung des Feldes für die Antwortadresse (ReplyTo) zum Versand von Nachrichten dann, wenn als Antwortadresse ein gültiger Alias[827] des Benutzers eingetragen ist. Die globale Option ist per Voreinstellung aktiv.

Öffentliche Kontakte virtuell mit den Standard-Kontakten zusammenführen
Diese Option bewirkt, dass die öffentlichen Kontakte und die Standard-Kontakte der Benutzer auf ihren Geräten als zusammengeführt dargestellt werden. Die Datenbestände der Kontakte bleiben hierbei getrennt; es werden also keine Kontakte zwischen den Kontaktordnern der Benutzer kopiert. Diese Option kann insbesondere für solche Clients hilfreich sein, die das Durchsuchen der Globalen Adressliste (GAL) nicht unterstützen. Diese Option ist per Voreinstellung abgeschaltet.

Absender sperren, wenn Nachricht in Ordner Junk-Email verschoben wird
Ist diese Option aktiv, so wird die Absender-Adresse (Felder Sender und From) einer E-Mail-Adresse in den Kontaktordner für gesperrte Absender eingetragen, sobald ein Client die zugehörige E-Mail-Nachricht in den Ordner für Spam-Nachrichten verschiebt.

Antworten auf Besprechungsanfragen nach Zusage, Ablehnung usw. zwingend senden
Ist diese Option aktiv, so versendet der ActiveSync-Dienst eine Antwort an den Besprechungsorganisator immer dann, wenn ein Client auf eine Besprechungseinladung zusagt, sie ablehnt oder eine sonstige Aktion für die Einladung ausführt. Diese Option ist für solche Clients nützlich, die solche Antworten nicht selbst richtig senden.

Vorschau auf tatsächlich wirksame Einstellungen

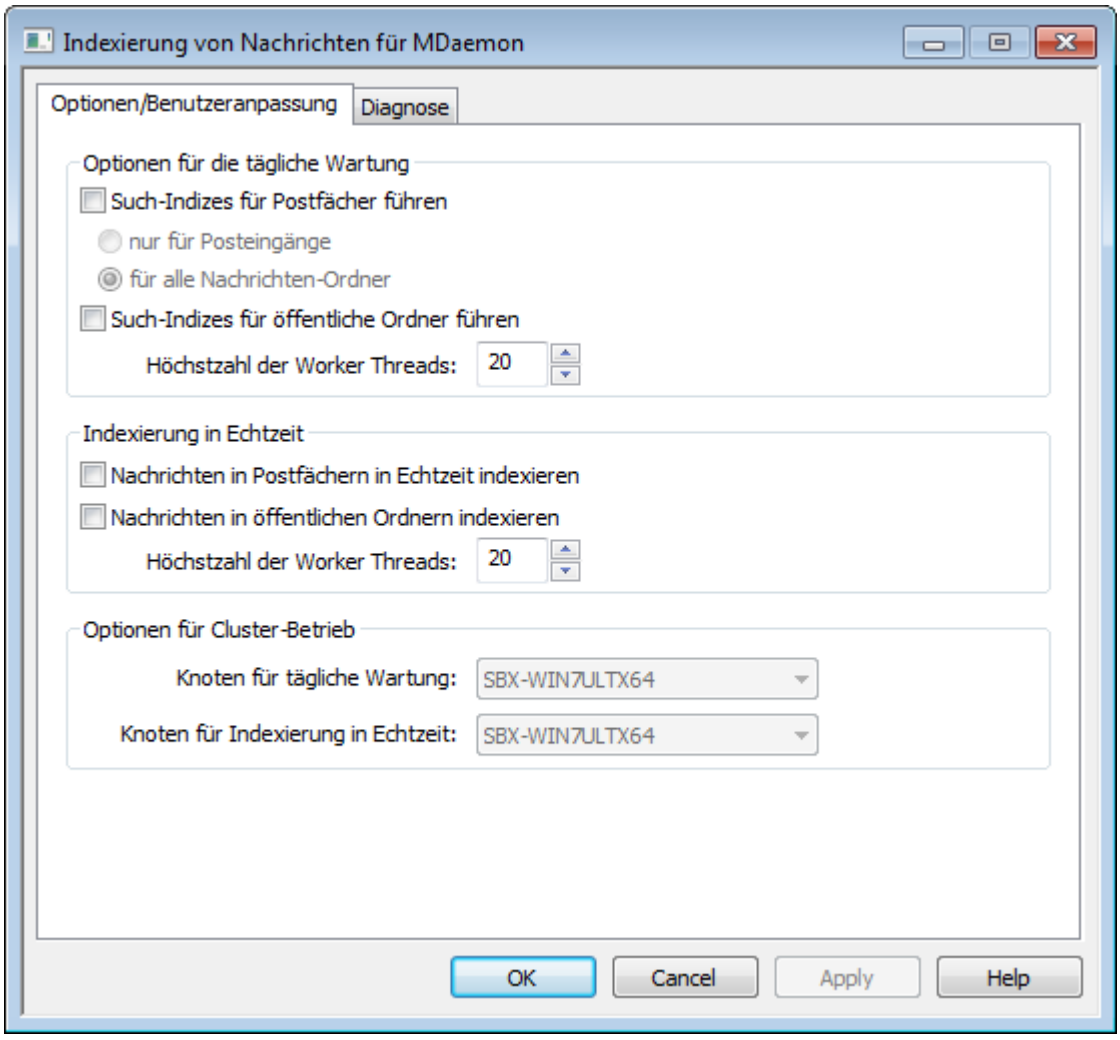
Dieses Steuerelement ist auf allen untergeordneten Konfigurationsdialogen für die Client-Einstellungen (Domänen 437, Benutzerkonten 454 und Clients 464) verfügbar. Per Voreinstellung werden die Optionen auf diesen Konfigurationsdialogen nicht von den übergeordneten Konfigurationsdialogen geerbt. Sie können sich daher mithilfe dieses Steuerelements die Einstellungen anzeigen lassen, die auf den jeweils gerade dargestellten Konfigurationsdialog wirken.

Siehe auch:

ActiveSync » Benutzerkonten 454
ActiveSync » Clients 464
ActiveSync » Sicherheit 429

3.11 Indexierung von Nachrichten

3.11.1 Optionen/Benutzeranpassung



Im Konfigurationsdialog für die Indexierung von Nachrichten können Sie die Echtzeit-Verarbeitung und die Verarbeitung während der täglichen Wartung für die Such-Indizes konfigurieren, die durch Webmail, ActiveSync und die Remoteverwaltung genutzt werden.

Optionen für die tägliche Wartung

Die Optionen in diesem Abschnitt steuern die täglich um Mitternacht durchgeführte Such-Indexierung.

Such-Indizes für Postfächer führen
Diese Option bewirkt, dass für die Nachrichten-Ordner in Ihren Postfächern Such-Indizes geführt werden. Sie können dabei wählen, ob die Indizes nur für die Posteingänge oder für alle Nachrichten-Ordner geführt werden.

Such-Indizes für öffentliche Ordner führen
Diese Option bewirkt, dass für Ihre öffentlichen Ordner[309] Such-Indizes geführt werden. Sie können dabei festlegen, wie viele Threads an dieser Indexierung höchstens gleichzeitig arbeiten dürfen.

Indexierung in Echtzeit

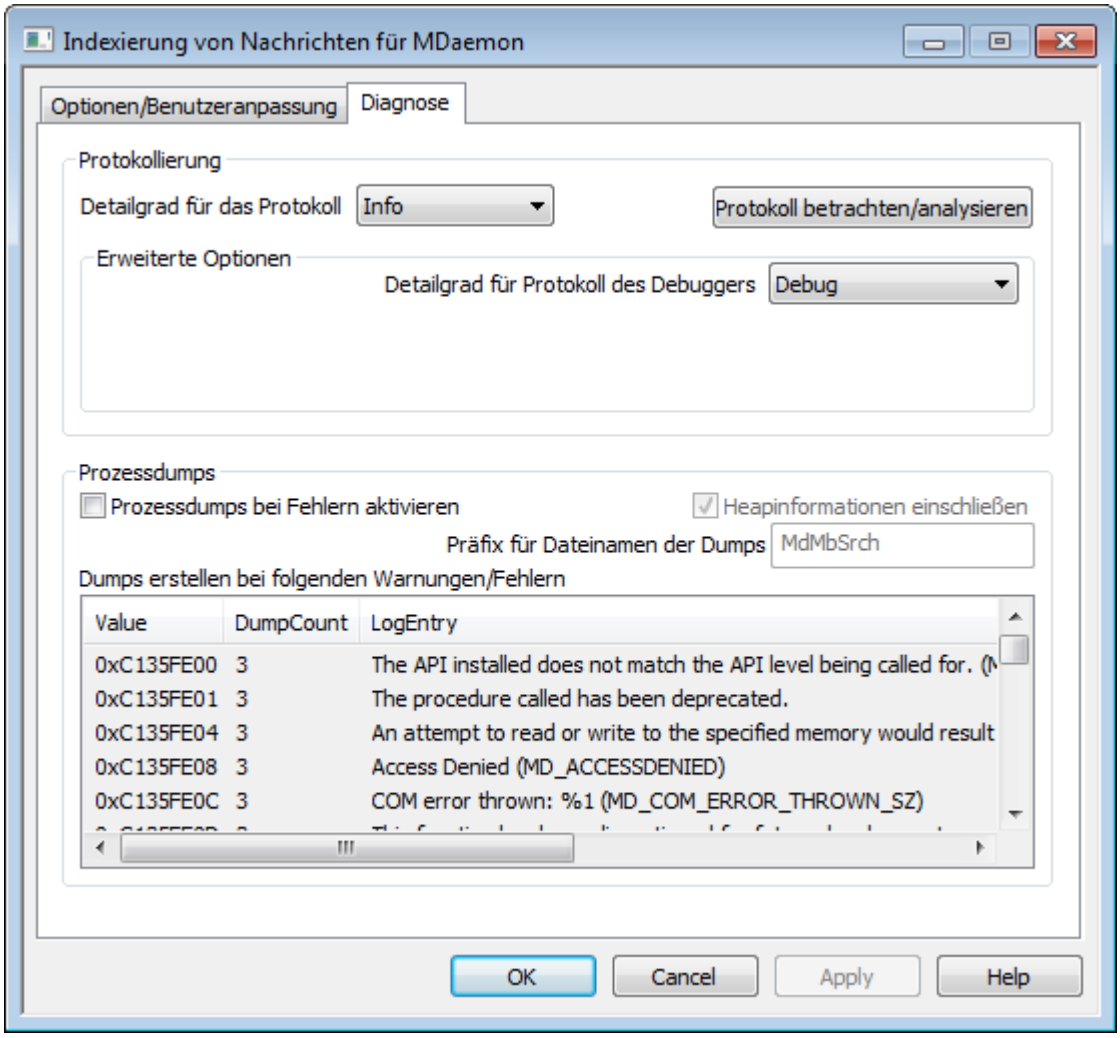
Nachrichten in Postfächern in Echtzeit indexieren
Diese Option bewirkt, dass die Indexierung in den Postfächern in Echtzeit durchgeführt wird. Die Such-Indizes werden hierdurch stets auf dem aktuellen Stand gehalten date.

Nachrichten in öffentlichen Ordnern indexieren
Diese Option bewirkt, dass die Indexierung in den öffentlichen Ordnern[309] in Echtzeit durchgeführt wird.

Optionen für Cluster-Betrieb

Falls Sie MDaemon im Cluster-Betrieb einsetzen, können Sie mithilfe der Optionen in diesem Abschnitt die Knoten im Cluster bestimmen, auf denen die tägliche Wartung der Indizes und die Indexierung in Echtzeit durchgeführt werden.

3.11.2 Diagnose



Dieser Konfigurationsdialog enthält erweiterte Optionen, die üblicherweise nur zur Fehlersuche bei der Indexierung von Nachrichten oder zur Bereitstellung von Daten für den technischen Support gebraucht werden.

Protokollierung

Detailgrad für das Protokoll
Der Cluster-Dienst von MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Protokolldatei betrachten/analysieren
Durch Anklicken dieses Steuerelements öffnet sich der erweiterte Protokollbetrachter für MDaemon. Per Voreinstellung werden die Protokolle im Verzeichnis "..\MDaemon\Logs\" gespeichert.

Erweiterte Optionen

Detailgrad für Protokoll des Debuggers
Diese Option bestimmt den geringsten zulässigen Detailgrad für die Protokolldaten, die an den Debugger übermittelt werden. Die auswählbaren Detailgrade sind dieselben wie in der Tabelle weiter oben.

Prozessdumps

Prozessdumps bei Fehlern aktivieren
Diese Option bewirkt die Erstellung von Prozessdumps in den Fällen, in denen die weiter unten angegebenen Warnungen und Fehler auftreten.

Heapinformationen einschließen
Per Voreinstellung werden die Heapinformationen in die Prozessdumps aufgenommen. Falls Sie dies nicht wünschen, deaktivieren Sie dieses Kontrollkästchen.

Präfix für Dateinamen der Dumps
Die Dateinamen der Dump-Dateien beginnen mit dem hier angegeben Text. Der Präfix lautet per Voreinstellung "AirSync".

Dumps erstellen bei folgenden Warnungen/Fehlern
Um diese Einträge zu bearbeiten, öffnen Sie durch Rechtsklick in diesem Bereich das Kontextmenü. Mithilfe der dann erscheinenden Menüeinträge *Eintrag hinzufügen, Eintrag bearbeiten* und *Eintrag löschen* können Sie die Liste der Fehler und Warnungen verwalten, die das Erstellen von Prozessdumps auslösen. Für jeden Eintrag können Sie die Anzahl der zulässigen Prozessdumps angeben; wird diese Zahl erreicht, so wird der Eintrag deaktiviert.

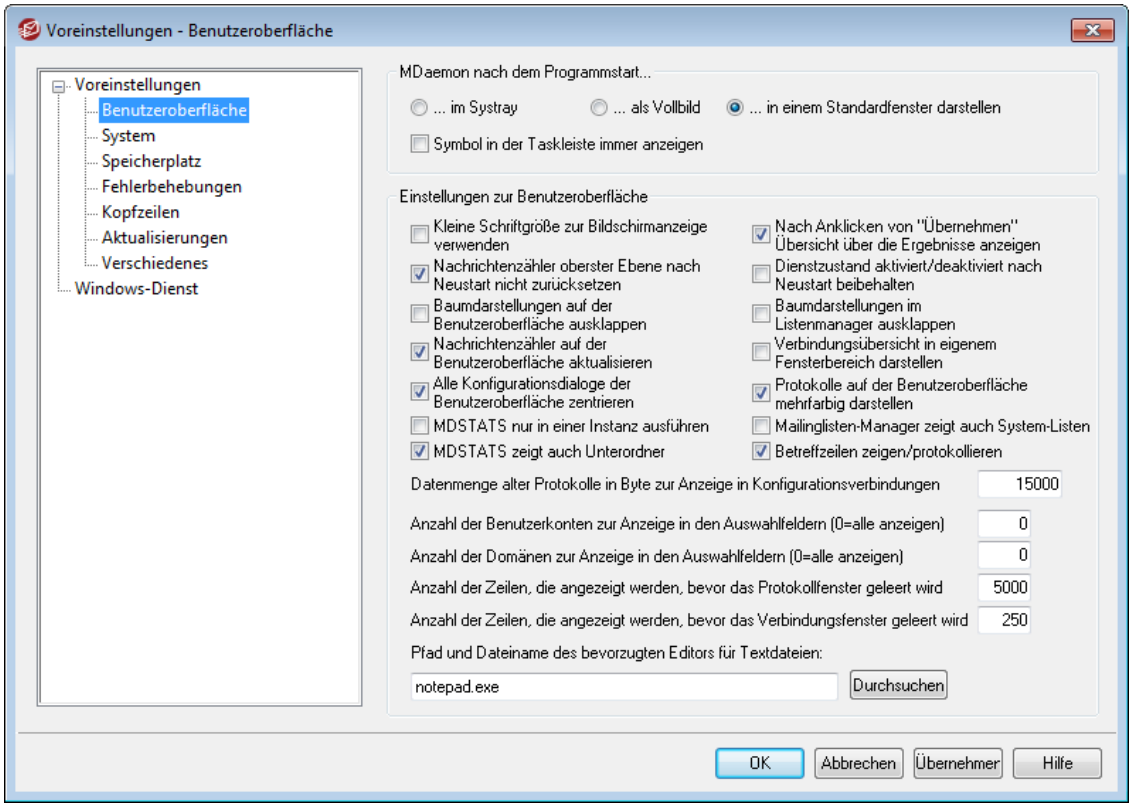
Siehe auch:

Dynamischer Filter » Optionen/Benutzeranpassung 612

3.12 Voreinstellungen

3.12.1 Voreinstellungen

3.12.1.1 Benutzeroberfläche



MDaemon nach dem Programmstart...

...im Systray darstellen
Um MDaemon beim Start nur als Symbol im Systray anzuzeigen, wird diese Option gewählt.

...als Vollbild darstellen
Mit dieser Option wird MDaemon in einem maximierten Fenster gestartet.

...in einem Standardfenster darstellen
Soll MDaemon in einem Standard-Fenster gestartet werden, ist diese Option zu wählen.

Symbol in der Taskleiste immer anzeigen
Diese Option bewirkt, dass MDaemon beim Start in die Taskleiste ausgeblendet wird und im ausgeblendeten Zustand sowohl in der Taskleiste als auch im Systray erscheint. Falls MDaemon in ausgeblendetem Zustand nicht in der Taskleiste angezeigt werden soll, deaktivieren Sie diese Option. Es erscheint dann nur das Symbol im Systray.

Optionen zur Benutzeroberfläche

Kleine Schriftgröße zur Bildschirmanzeige verwenden
Mit dieser Option werden für den rechten Abschnitt der Benutzeroberfläche besonders kleine Schriftarten ausgewählt.

Nach Anklicken von "Übernehmen" Übersicht über die Ergebnisse anzeigen
Per Voreinstellung erscheint nach dem Anklicken des Steuerelements "Übernehmen" ein Meldungsfenster, das bestätigt, dass die in dem gerade geöffneten Konfigurationsdialog vorgenommenen Änderungen gespeichert wurden. Falls Sie diese Bestätigung nicht wünschen, deaktivieren Sie diese Option. Die Änderungen werden dann übernommen, ohne dass ein Hinweistext dies bestätigt.

Nachrichtenzähler oberster Ebene nach Neustart nicht zurücksetzen
Diese Option bewirkt, dass die Zählerstände der Zähler auf der obersten Ebene im Abschnitt Statistik der Benutzeroberfläche von MDaemon auch nach einem Neustart des Servers erhalten bleiben.

Dienstzustand aktiviert/deaktiviert nach Neustart beibehalten
Ist diese Option gesetzt, behält MDaemon den Zustand seiner Serverdienste (aktiviert/deaktiviert) auch nach einem Neustart bei.

Baumdarstellungen auf der Benutzeroberfläche ausklappen
Diese Option bewirkt, dass die baumartig angeordneten Knoten in den links angeordneten Navigationsbereichen verschiedener Konfigurationsdialoge automatisch ausgeklappt werden. Diese Option wirkt nicht auf den Mailinglisten-Manager 269. Falls Sie auch das automatische Ausklappen der Baumdarstellung für Mailinglisten wünschen, aktivieren Sie die Option *Baumdarstellungen im Listenmanager ausklappen*.

Baumdarstellungen im Listenmanager ausklappen
Diese Option bewirkt, dass die baumartig angeordneten Knoten im links angeordneten Navigationsbereich des Mailinglisten-Manager 269 automatisch ausgeklappt werden.

Nachrichtenzähler auf der Benutzeroberfläche aktualisieren
Diese Option bestimmt, ob MDaemon die Zahl der Nachrichten in den Warteschlangen durch direkten Datenträgerzugriff ermittelt.

Verbindungsübersicht in eigenem Fensterbereich darstellen
Diese Option bewirkt, dass die Registerkarte Verbindungen auf der Benutzeroberfläche von MDaemon von den übrigen Registerkarten getrennt und in einem eigenen Fensterbereich dargestellt wird. Änderungen an dieser Option werden erst nach einem Neustart der Benutzeroberfläche von MDaemon wirksam. Die Option zum Umschalten der Ansicht im Menü Fenster ist dann nicht mehr verfügbar.

Alle Konfigurationsdialoge der Benutzeroberfläche zentrieren
Diese Option bewirkt, dass alle Dialogfenster nach dem Öffnen auf dem Bildschirm zentriert werden und nicht überlappend dargestellt werden. Wenn Sie zulassen wollen, dass die Dialogfenster einander überlappen, deaktivieren Sie diese Option. Beachten Sie aber, dass dann die Dialogfenster teilweise außerhalb des Bildschirmbereichs oder des jeweiligen Fensters erscheinen können. Diese Option ist per Voreinstellung abgeschaltet.

Protokolle auf der Benutzeroberfläche mehrfarbig darstellen
Diese Option bewirkt, dass der Text, der in einigen Registerkarten der Benutzeroberfläche von MDaemon zur Überwachung und Protokollierung von Ereignissen 76 dargestellt wird, in verschiedenen Farben erscheint. Diese Option ist per Voreinstellung abgeschaltet. Änderungen an dieser Option werden erst nach einem Neustart von MDaemon wirksam. Nähere Informationen hierzu finden Sie im Abschnitt Farblich getrennte Darstellung der Elemente aus Verbindungsprotokollen 180.

MDSTATS nur in einer Instanz ausführen
Diese Option bewirkt, dass nur eine Instanz des Warteschlangen- und Statistikmanagers 875 von MDaemon gleichzeitig ausgeführt werden kann. Wird bei laufendem Manager versucht, den Manager erneut zu starten, so wird hierdurch lediglich das Fenster der bereits laufenden Instanz in den Vordergrund gebracht.

MDSTATS zeigt auch Unterordner
Diese Option bewirkt, dass der Warteschlangen- und Statistikmanager 875 Unterordner anzeigt, die in den verschiedenen Warteschlangen und Nachrichtenverzeichnissen der Benutzer enthalten sind.

Mailinglisten-Manager zeigt auch System-Listen
Diese Option bewirkt, dass im Mailinglisten-Manager 269 auch die durch MDaemon automatisch erzeugen System-Mailinglisten (z.B. Everyone@ und MasterEveryone@) erscheinen. Für automatisch erzeugte System-Mailinglisten stehen nur beschränkt konfigurierbare Einstellungen zur Verfügung. Ist diese Option abgeschaltet, so sind die System-Mailinglisten zwar im Mailinglisten-Manager nicht sichtbar, sie stehen aber weiterhin zur Nutzung zur Verfügung. Diese Option ist per Voreinstellung abgeschaltet.

Betreffzeilen zeigen/protokollieren
Per Voreinstellung werden die Betreffzeilen ("Subject:") auf den Registerkarten der Benutzeroberfläche von MDaemon angezeigt und in den Protokolldateien vermerkt. Da die Betreffzeilen Informationen enthalten können, von denen die Absender der Nachrichten nicht wünschen, dass diese direkt angezeigt und protokolliert werden, und da in Mailinglisten die Benutzer auch ihre Kennwörter in die Betreffzeilen eintragen können, wird empfohlen, Anzeige und Protokollierung der Betreffzeilen zu deaktivieren. Hierzu deaktivieren Sie diese Option.

Datenmenge alter Protokolle in Byte zur Anzeige in Konfigurationsverbindungen
Diese Option bestimmt, wie viele Protokolldaten auf den Registerkarten zur Überwachung und Protokollierung von Ereignissen 76 von Konfigurationsverbindungen angezeigt werden. Die Voreinstellung beträgt 15.000 Byte.

Anzahl der Benutzerkonten zur Anzeige in den Auswahlfeldern (0=alle anzeigen)
Diese Option begrenzt die Anzahl der Benutzerkonten, die in verschiedenen Auswahllisten und anderen Konfigurationsdialogen auf der Benutzeroberfläche angezeigt werden. So lange hier ein von 0 (alle anzeigen) abweichender Wert eingetragen ist, erscheinen die Menüpunkte "Benutzerkonto bearbeiten" und "Benutzerkonto löschen im Menü Benutzerkonten nicht mehr. Die entsprechenden Funktionen stehen dann nur im Benutzerkonten-Manager 712 zur Verfügung. Änderungen in diesem Feld werden erst nach einem Neustart von MDaemon wirksam. Die Voreinstellung für diesen Wert beträgt "0", sodass alle Benutzerkonten angezeigt werden.

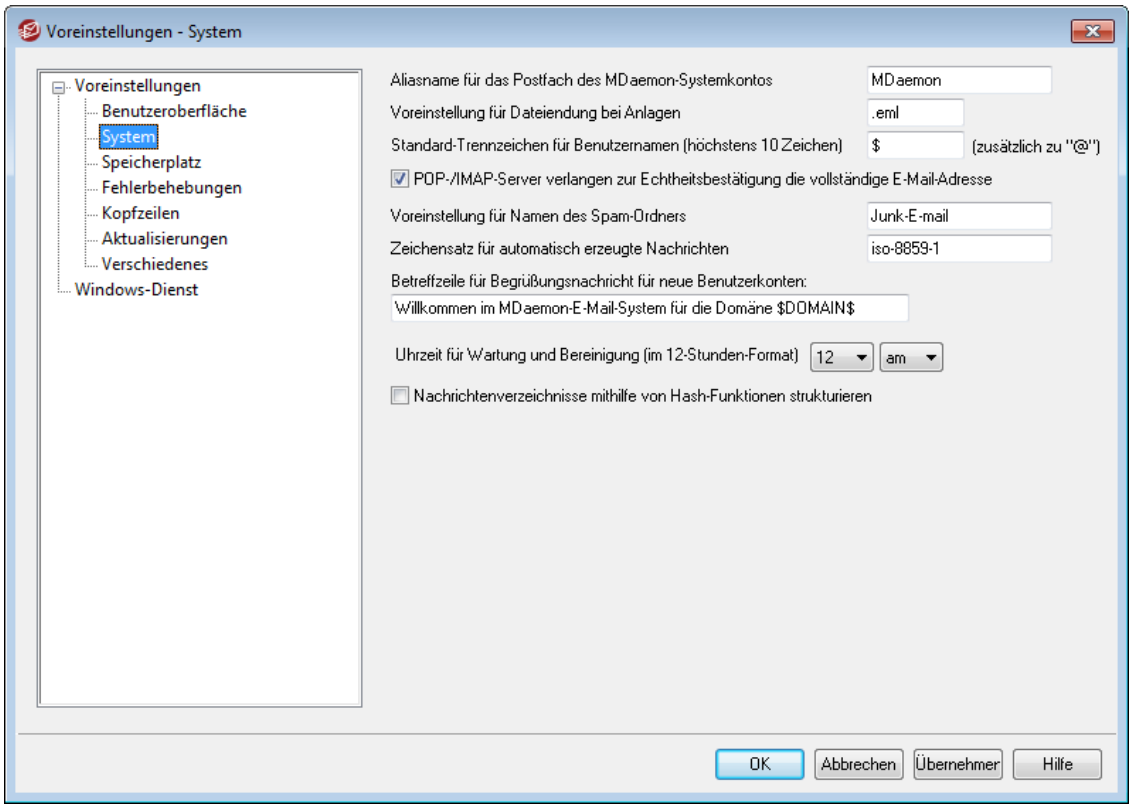
Anzahl der Domänen zur Anzeige in den Auswahlfeldern (0=alle anzeigen)
Diese Einstellung legt fest, wie viele Domänen auf der Benutzeroberfläche angezeigt werden dürfen. Änderungen an diesem Wert wirken sich erst nach einem Neustart von MDaemon aus. Die Voreinstellung für diesen Wert beträgt "0", sodass alle Domänen angezeigt werden.

Zahl der Zeilen, die angezeigt werden, bevor das Protokollfenster geleert wird
Diese Option legt fest, wie viele Protokollzeilen auf der Benutzeroberfläche angezeigt werden dürfen, bevor das Fenster geleert wird. Die Einstellungen zum Systemprotokoll werden von dieser Option nicht berührt; sie bezieht sich nur auf die Bildschirmanzeige.

Zahl der Zeilen, die angezeigt werden, bevor das Verbindungsfenster geleert wird
Mit dieser Einstellung wird die Zahl der Protokollzeilen begrenzt, die in einem Verbindungsfenster 91 angezeigt werden, bevor es geleert wird. Die Einstellung wirkt sich nicht auf das Systemprotokoll aus.

Pfad und Dateiname des bevorzugten Editors für Textdateien
Per Voreinstellung ruft die Benutzeroberfläche von MDaemon das Programm Notepad.exe alls Texteditor zur Bearbeitung von Dateien auf. Sie können stattdessen auch einen anderen Texteditor auswählen; tragen Sie hierzu den Pfad und den Namen der ausführbaren Datei in diese Feld ein.

3.12.1.2 System



Aliasname für das Postfach des MDaemon-Systemkontos [Adresse]
Nachrichten, die das System automatisch erzeugt, tragen diese Adresse als Absender. Solche Nachrichten sind insbesondere Anmeldebestätigungen,

Meldungen über Fehler bei der Zustellung und verschiedene andere Bestätigungen.

Voreinstellung für Dateiendung bei Anlagen
Automatisch erzeugte Nachrichten und Dateianlagen für solche Nachrichten tragen diese Dateiendung. Erzeugt MDaemon z.B. eine Warnmeldung an den Postmaster wegen einer bestimmten Nachricht, so wird jene Nachricht mit der hier angegebenen Endung als Anlage mit versandt.

Standard-Trennzeichen für Benutzernamen (höchstens 10 Zeichen)
Das hier angegebene Zeichen (auch eine Zeichenkette ist möglich) kann als Alternative zu dem Zeichen "@" verwendet werden, wenn die vollständige E-Mail-Adresse als Anmeldename dient. Diese Funktion ist dann sinnvoll, wenn Mailclients eingesetzt werden, die das Zeichen "@" nicht als Teil des Anmelde- oder Benutzernamens zulassen. Wird hier z.B. "$" eingetragen, so können sich die Benutzer wahlweise mit "user1@example.com" oder "user1$example.com" anmelden.

POP-/IMAP-Server verlangen zur Echtheitsbestätigung die vollständige E-Mail-Adresse
Die POP- und IMAP-Server von MDaemon verlangen per Voreinstellung, dass sich Benutzer mit ihrer vollständigen E-Mail-Adresse als Benutzernamen bei MDaemon anmelden. Falls Sie auch Anmeldungen zulassen wollen, bei denen als Benutzername nur der Postfachname angegeben wird (z.B. "user1" statt "user1@example.com"), so können Sie diese Option deaktivieren. Diese Vorgehensweise empfiehlt sich aber nicht, da Anmeldungen nur mit dem Postfachnamen mehrdeutig sind, falls MDaemon mehrere Domänen verwaltet.

Voreinstellung für Namen des Spam-Ordners
In diesem Feld wird der Name jener Spam-Ordner angegeben, die MDaemon für die Benutzer automatisch anlegen kann. Die Voreinstellung lautet "Junk E-mail" und stimmt damit mit dem entsprechenden Ordnernamen in Microsoft Office 2003 überein.

Zeichensatz für automatisch erzeugte Nachrichten
Hier wird der Zeichensatz angegeben, in dem automatisch erzeugte Nachrichten abgefasst werden sollen. Der Zeichensatz iso-8859-1 ist für alle Sprachversionen von MDaemon voreingestellt.

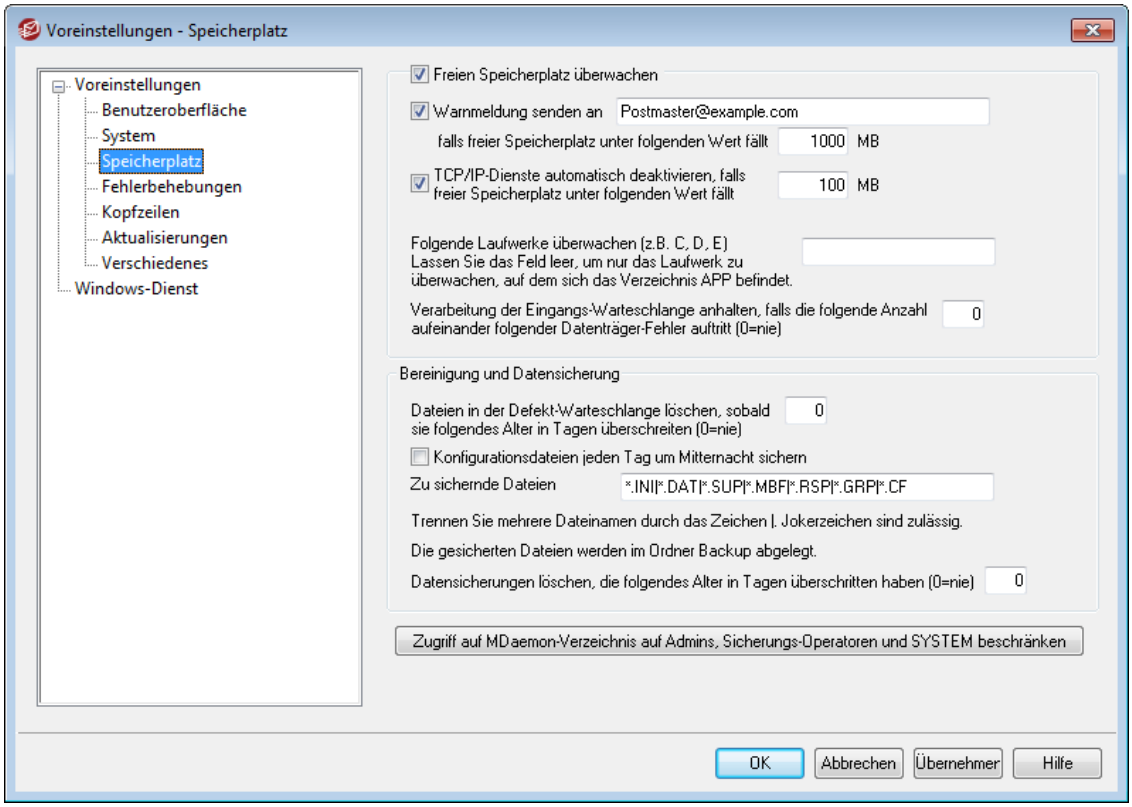
Betreffzeile für Begrüßungsnachricht für neue Benutzerkonten:
Dieser Text erscheint als Betreff in den Begrüßungsnachrichten für neue Benutzer, die MDaemon üblicherweise versendet eingefügt. Im Übrigen wird der Nachrichtentext anhand der Datei `NEWUSERHELP.DAT` im Verzeichnis … `\MDaemon\app\` erstellt. Die Betreffzeile darf alle Makros enthalten, die auch in Skripten für Autobeantworter 836 zulässig sind.

Uhrzeit für Wartung und Bereinigung (im 12-Stunden-Format) [1-12] [am/pm]
Diese Option bestimmt, zu welcher Uhrzeit täglich die Bereinigungs- und Wartungsvorgänge ausgeführt werden. Die Voreinstellung ist Mitternacht (12 am); es wird empfohlen, diese Voreinstellung beizubehalten. Die Uhrzeit muss im 12-Stunden-Format angegeben werden, wobei 12 am für Mitternacht, 12 pm hingegen für 12.00 Uhr mittags steht.

Unabhängig von der Einstellung, die in dieser Option getroffen wird, laufen bestimmte Vorgänge immer an jedem Tag um Mitternacht ab. Hierzu gehören etwa die Pflege der Protokolle und das Ausführen der Datei `midnight.bat`.

Nachrichtenverzeichnisse mithilfe von Hash-Funktionen strukturieren
Diese Option bewirkt, dass MDaemon die Nachrichten-Verzeichnisse automatisch untergliedert. MDaemon erstellt dazu bis zu 65 Unterverzeichnisse. Diese Untergliederung kann die Systemleistung bei Systemen mit hoher Auslastung steigern, sie kann sie jedoch bei Systemen mit durchschnittlicher Auslastung leicht verringern. Diese Option ist per Voreinstellung abgeschaltet.

3.12.1.3 Speicherplatz



Freien Speicherplatz überwachen
MDaemon überwacht den freien Speicherplatz auf dem Laufwerk, auf dem sich die Datei `MDaemon.exe` befindet, wenn diese Option aktiv ist.

Warnmeldung senden an [Benutzer oder Adresse], falls freier Speicherplatz unter folgenden Wert fällt [xx] MB
Mit dieser Option kann MDaemon bei Unterschreiten der angegebenen Grenze an den ausgewählten eigenen Benutzer oder die angegebene E-Mail-Adresse eine Warnnachricht senden. Per Voreinstellung beträgt dieser Wert 1000 MB.

TCP/IP-Dienste automatisch deaktivieren, falls freier Speicherplatz unter folgenden Wert fällt [xx] MB
Diese Option veranlasst MDaemon, bei Unterschreiten des angegebenen Schwellwerts seine sämtliche TCP/IP-Dienste abzuschalten. Per Voreinstellung beträgt dieser Wert 100 MB.

Folgende Laufwerke überwachen (z.B. C, D, E)
Diese Option bewirkt, dass der freie Speicherplatz auf mehreren Laufwerken überwacht wird. Geben Sie hierzu die Laufwerksbuchstaben aller zu überwachenden Laufwerke ein. Falls dieses Feld leer ist, wird nur das Laufwerk überwacht, das das MDaemon-Verzeichnis `\app\` enthält.

Verarbeitung der Eingangs-Warteschlange anhalten, falls die folgende Anzahl aufeinander folgender Datenträger-Fehler auftritt (0=nie)
Tritt die hier angegebene Zahl von Datenträger-Fehlern während der Verarbeitung der Eingangs-Warteschlange auf, so unterbricht MDaemon die Verarbeitung dieser Warteschlange, bis der zugrunde liegende Fehler behoben ist. Der Postmaster wird durch eine E-Mail-Nachricht auf diesen Zustand aufmerksam gemacht.

Bereinigung und Datensicherung

Dateien in der Defekt-Warteschlange löschen, sobald sie folgendes Alter in Tagen überschreiten(0=nie)
Diese Option veranlasst MDaemon, alte Dateien aus der Defekt-Warteschlange zu löschen, sobald sie das hier in Tagen angegebene Alter überschritten haben. Falls Sie die Nachrichten nicht automatisch aus der Defekt-Warteschlange löschen lassen wollen, tragen Sie hier den Wert 0 ein.

Konfigurationsdateien jeden Tag um Mitternacht sichern
Diese Option bewirkt, dass MDaemon alle Konfigurationsdateien jeden Tag um Mitternacht in das Sicherungsverzeichnis (Backup) sichert.

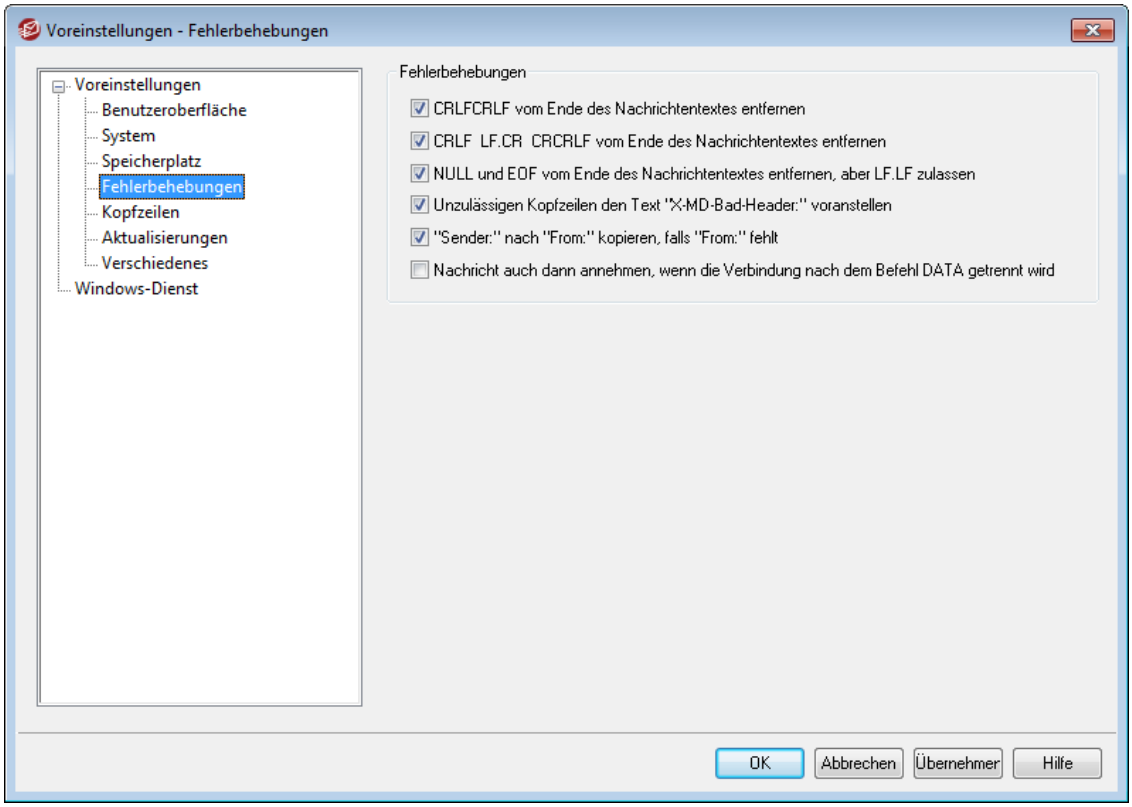
Zu sichernde Dateien
In dieser Liste wird genau angegeben, welche Dateien und Dateitypen gesichert werden müssen. Jokerzeichen sind zulässig, die einzelnen Einträge, die Dateinamen und Namenserweiterungen sein können, müssen durch das Zeichen "|" getrennt werden.

Datensicherungen löschen, die folgendes Alter in Tagen überschritten haben (0=nie)
Diese Option bewirkt, dass alte Datensicherungen automatisch gelöscht werden. Dateien, die das hier in Tagen angegebene Alter überschritten haben, werden während der Bereinigung um Mitternacht gelöscht. Die Voreinstellung beträgt 0; dieser Wert bewirkt, dass alte Datensicherungen nicht automatisch gelöscht werden.

Zugriff auf MDaemon-Verzeichnis auf Admins, Sicherungs-Operatoren und SYSTEM beschränken

Durch Anklicken dieses Steuerelements können Sie den Zugriff auf das Hauptverzeichnis `\MDaemon\` und seine Unterverzeichnisse auf die folgenden Windows-Benutzerkonten und -Benutzergruppen beschränken: Administratoren, Sicherungs-Operatoren und SYSTEM.

3.12.1.4 Fehlerbehebungen



CRLFCRLF vom Ende des Nachrichtentextes entfernen
Bestimmte Mailclients können Nachrichten, die mit mehreren aufeinander folgenden Zeilensprüngen und Zeilenvorschüben enden (CRLFCRLF), nicht richtig anzeigen. Ist diese Option aktiv, so entfernt MDaemon aufeinander folgende Zeichenfolgen `CRLFCRLF` vom Ende des Nachrichtentextes. Diese Option ist per Voreinstellung aktiv.

CRLF LF.CR CRCRLF vom Ende des Nachrichtentextes entfernen
Per Voreinstellung entfernt MDaemon diese Zeichenfolge vom Ende von Nachrichten, da sie bei manchen Mailclients zu Problemen führt. Deaktivieren Sie diese Option, falls Sie diese Zeichenfolge nicht aus den Nachrichten entfernen wollen.

NULL & EOF vom Ende des Nachrichtentextes entfernen, aber LF.LF zulassen
Diese Option entfernt `Null`-Zeichen und Dateiendezeichen (EOF) aus dem Nachrichtentext, lässt aber zu, dass Nachrichten mit `LF.LF` und der normalen Sequenz `CRLF.CRLF`, die das Ende einer Nachricht anzeigt, enden. Diese Option ist per Voreinstellung aktiv.

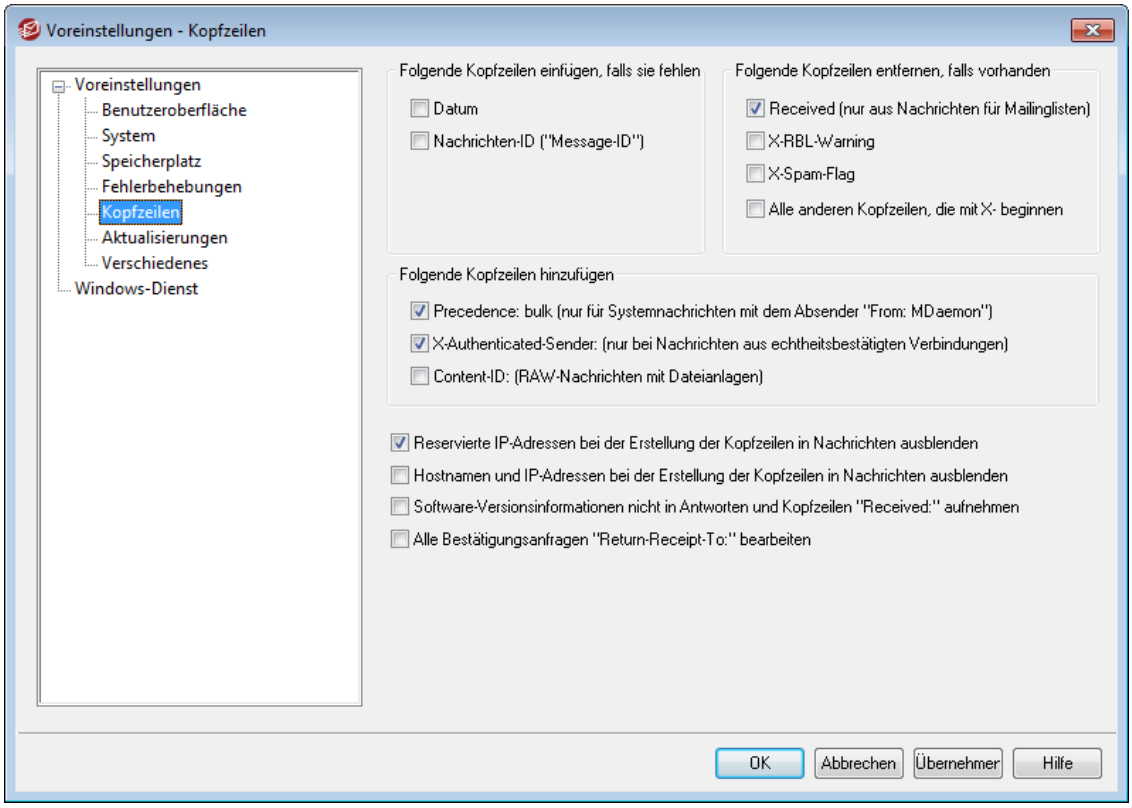
Unzulässigen Kopfzeilen den Text "X-MD-Bad-Header:" voranstellen
Ist diese Option aktiv, so stellt MDaemon ungültigen Kopfzeilen, die während der Verarbeitung von Nachrichten gefunden werden, den Text "`X-MD-Bad-Header:`" voran. Diese Option ist per Voreinstellung aktiv.

"Sender:" nach "From:" kopieren, falls "From:" fehlt
Manche Mailclients erstellen beim Verfassen einer Nachricht die Kopfzeile `FROM:` nicht. Sie tragen stattdessen die Daten, die in die Kopfzeile `FROM:` gehören, in die

Kopfzeile `Sender:` ein. Hieraus entstehen Probleme für einige Mailserver und den Empfänger der Nachricht. Um diese Probleme zu verhindern, erstellt MDaemon die fehlende Kopfzeile `FROM:` und bestückt sie mit dem Inhalt der Kopfzeile `Sender:`, falls diese Option aktiv ist. Die Option ist per Voreinstellung aktiv.

Nachricht auch dann annehmen, wenn eine Verbindung nach dem Befehl DATA getrennt wird
Diese Option bewirkt, dass MDaemon Nachrichten auch dann annimmt und zustellt, wenn die Verbindung, über die die Nachrichten übermittelt werden, während oder unmittelbar nach der Übermittlung des Befehls `DATA` in der SMTP-Verarbeitung abbricht. Diese Option soll nur in Ausnahmefällen verwendet werden, da sie zu doppelten Nachrichten führen kann.

3.12.1.5 Kopfzeilen



Folgende Kopfzeilen einfügen, falls sie fehlen

Datum
Mit dieser Option fügt MDaemon jeder Nachricht ohne Datumsfeld ("`Date:`") ein solches hinzu und setzt als Wert das Datum ein, an dem MDaemon die Nachricht erstmals empfangen hat. Manche Mail-Programme lassen die Datumskopfzeile weg; dies kann zu Problemen mit einigen Mail-Servern führen, die Nachrichten ohne Datumskopfzeile nicht befördern. Mithilfe dieser Option lassen sich solche Probleme beim Versand von Nachrichten umgehen.

Nachrichten-ID ("Message-ID")
Wird eine Nachricht ohne die Kopfzeile "Nachrichten-ID" ("`Message-ID`") verarbeitet, so fügt MDaemon eine der Nachricht eine zufällig erzeugte Nachrichten-ID hinzu.

Folgende Kopfzeilen entfernen, falls vorhanden

Received (nur aus Nachrichten für Mailinglisten)
Hiermit werden aus Listennachrichten alle vorhandenen "Received:"-Kopfzeilen aus Nachrichten für Mailinglisten entfernt.

X-RBL-Warning
Soll MDaemon alle Kopfzeilen "X-RBL-Warning:" aus den Nachrichten löschen, so muss diese Option aktiviert werden. Per Voreinstellung ist sie nicht aktiv.

X-Spam-Flag
Ist das Entfernen alter Kopfzeilen "X-Spam-Flag:" aus den Nachrichten gewünscht, so muss diese Option aktiviert werden.

Alle Kopfzeilen, die mit X- beginnen
MDaemon und andere Mailserver nutzen viele severspezifische Kopfzeilen, die unter dem Oberbegriff Typ X- zusammengefasst werden, um die Nachrichten zuzustellen, den Versandweg und das Routing zu bestimmen, und viele weitere Funktionen auszuführen. Ist diese Option aktiv, so entfernt MDaemon diese Kopfzeilen aus den Nachrichten. **Beachte:** Diese Funktion entfernt nicht die Kopfzeilen X-RBL-Warning.n Falls Sie solche Kopfzeilen entfernen lassen wollen, nutzen Sie hierfür die Option *"X-RBL-Warning"* weiter oben.

Folgende Kopfzeilen hinzufügen

Precedence: bulk (nur für Systemnachrichten mit dem Absender "From: MDaemon")
Diese Option bewirkt, dass alle Systemnachrichten, die durch MDaemon versandt werden (Begrüßungsnachrichten, Warnmeldungen, Meldungen über Zustellfehler usw.), eine Kopfzeile "Precedence: bulk" erhalten.

X-Authenticated-Sender: (nur bei Nachrichten aus echtheitsbestätigten Verbindungen)
MDaemon kann auf Wunsch eine Kopfzeile "X-Authenticated-Sender:" in Nachrichten einfügen, die während einer Verbindung mit Echtheitsbestätigung durch den Befehl AUTH übermittelt wurden. Falls Sie diese Kopfzeile nicht einfügen wollen, deaktivieren Sie diese Option.

Content-ID: (RAW-Nachrichten mit Dateianlagen)
Hiermit fügt MDaemon eine eindeutige Kopfzeile MIME Content-ID in solche Nachrichten ein, die MDaemon aus einer RAW-Datei erstellt hat, die ihrerseits Dateianlagen enthält.

Abschnitt "For" in "Received:"-Kopfzeilen
Hiermit fügt MDaemon Kopfzeilen mit dem Inhalt "For [SMTP-Empfänger]" in diejenigen "Received:"-Kopfzeilen der Nachrichten ein, die durch MDaemon hinzugefügt wurden.

Reservierte IP-Adressen bei der Erstellung der Kopfzeilen in Nachrichten ausblenden
Diese Option ist per Voreinstellung aktiv. Sie bewirkt, dass IP-Adressen aus reservierten Adressbereichen in bestimmten, durch MDaemon erstellten Kopfzeilen nicht erscheinen. Reservierte IP-Adressen umfassen folgende Bereiche : 127.0.0.*, 192.168.*.*, 10.*.*.* und 172.16.0.0/12. Falls Sie auch die IP-Adressen Ihrer Domänen (einschließlich der LAN-Domänen) nicht in die Kopfzeilen aufnehmen lassen wollen, können Sie dies durch Bearbeiten des folgenden

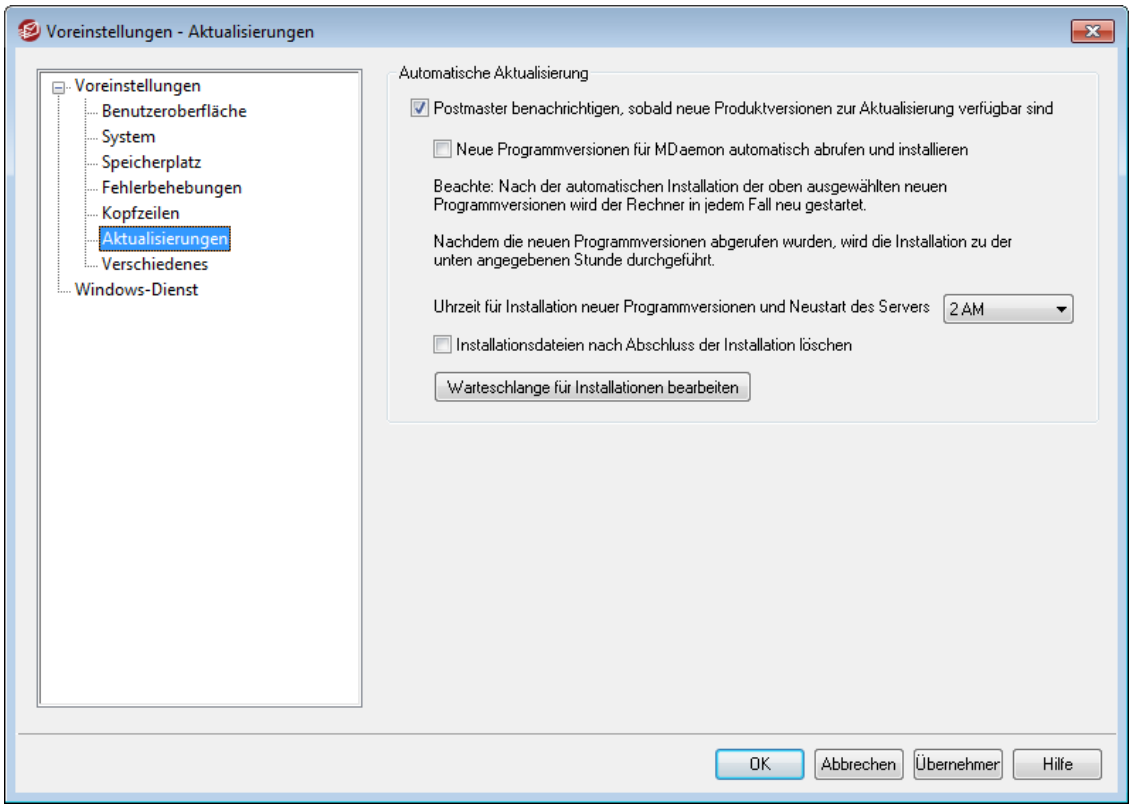
Eintrags in der Datei `MDaemon.ini` im MDaemon-Verzeichnis `app` erreichen: `[Special] HideMyIPs=Yes` ("Ja", Voreinstellung ist No, "Nein").

Hostnamen und IP-Adressen bei der Erstellung der Kopfzeilen in Nachrichten ausblenden
Diese Option bewirkt, dass Hostnamen und IP-Adressen bei der Erstellung der Kopfzeilen "Received:" nicht in die Kopfzeilen aufgenommen werden. Diese Option ist per Voreinstellung abgeschaltet.

Software-Versionsinformationen aus Protokollmeldungen und Kopfzeilen "Received" ausblenden
Diese Option bewirkt, dass MDaemon bei der Erstellung der Kopfzeilen "`Received`" die eigene Softwareversion und andere vergleichbar kennzeichnende Daten nicht in die Inhalte der Kopfzeilen aufnimmt. Diese Option ist per Voreinstellung abgeschaltet.

Alle Bestätigungsanfragen "Return-Receipt-To:" bearbeiten
Ist diese Option aktiv, so versendet MDaemon auf Anforderung Empfangsbestätigungen für eingehende Nachrichten. Ist die Option abgeschaltet, so werden Anforderungen von Zustellbestätigungen ignoriert. Diese Option ist per Voreinstellung aktiv.

3.12.1.6 Aktualisierungen



Automatische Aktualisierung

Mithilfe der Leistungsmerkmale zur automatischen Aktualisierung kann MDaemon den Postmaster benachrichtigen, sobald eine neue Programmversion von MDaemon verfügbar ist. MDaemon kann wahlweise auch die neuen Versionen automatisch abrufen und installieren. Nach jeder automatischen Installation einer

neuen Version wird das System neu gestartet. Die Installationsdateien werden abgerufen, sobald eine neue Version gefunden wird, und die Installation und der Neustart des Systems können zeitgesteuert zu einem vorbestimmten Zeitpunkt erfolgen. Alle Installationen werden im Systemprotokoll von MDaemon protokolliert, und der Postmaster wird informiert, sobald eine Aktualisierung durchgeführt wurde.

Postmaster benachrichtigen, sobald neue Produktversionen zur Aktualisierung verfügbar sind
Diese Option veranlasst MDaemon, den Postmaster zu informieren, falls eine neue Produktversion verfügbar ist. Diese Option ist per Voreinstellung aktiv.

Ist MDaemon zur automatischen Installation neuer Versionen konfiguriert, so wird diese Benachrichtigung nicht versandt. Stattdessen wird der Postmaster nach der Installation der neuen Version informiert, und es werden ihm dabei die Informationen aus dem Abschnitt *Zur besonderen Beachtung* der Versionsinformationen übermittelt.

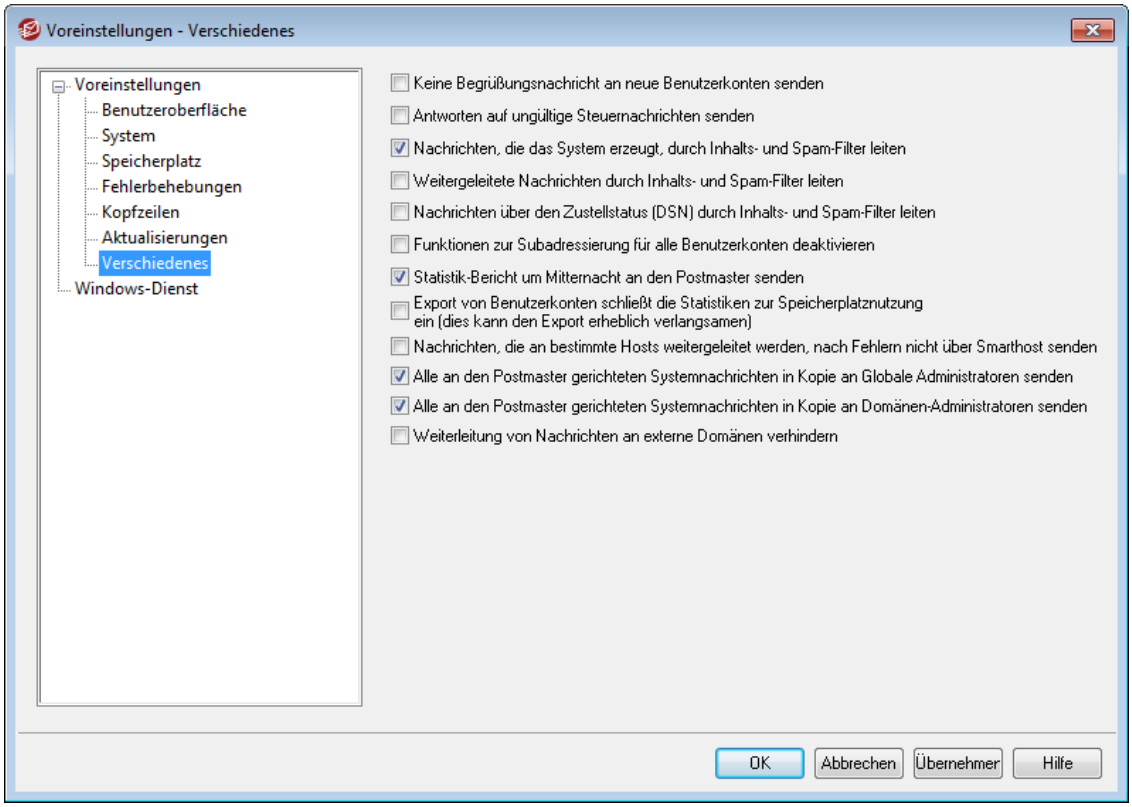
Neue Programmversionen für MDaemon automatisch abrufen und installieren
Diese Option bewirkt, dass neue Versionen von MDaemon automatisch abgerufen und installiert werden. Neue Versionen werden dabei abgerufen, sobald sie gefunden werden, und sie werden zu der weiter unten festgelegten Stunde installiert. Diese Option ist per Voreinstellung aktiv.

Uhrzeit für Installation neuer Programmversionen und Neustart des Servers
Neue Programmversionen werden automatisch abgerufen und im Verzeichnis `\MDaemon\Updates` abgelegt, sobald sie gefunden werden. Sie werden jedoch erst zu der hier angegebenen Stunde installiert. Nach jeder Installation einer neuen Programmversion wird das System automatisch neu gestartet. Die Uhrzeit muss in diesem Feld aus technischen Gründen im 12-Stunden-Format mit AM/PM angegeben werden. Die Voreinstellung lautet 2 AM, also 02:00 Uhr.

Installationsdateien nach Abschluss der Installation löschen
Diese Option bewirkt, dass die abgerufenen Installationsdateien nach dem erfolgreichen Abschluss der Installation gelöscht werden.

Warteschlange für Installationen bearbeiten
Wird eine neue Programmversion erkannt und abgerufen, so wird sie in die Warteschlange für die Installationen eingereiht, um später installiert zu werden. Diese Warteschlange, in der alle Programmversionen stehen, die auf ihre Installation warten, ist in der Datei `QueuedUpdates.dat` gespeichert. Sie können durch Anklicken dieser Schaltfläche die Warteschlange einsehen und anstehende Installationen aus ihr löschen.

3.12.1.7 Verschiedenes



Keine Begrüßungsnachricht an neue Benutzerkonten senden
MDaemon erstellt grundsätzlich eine Begrüßungsnachricht aus der Datei `NEWUSERHELP.DAT` und sendet sie an neue Benutzer, wenn deren Benutzerkonto angelegt wird. Diese Option unterbindet den Versand der Begrüßungsnachricht.

Antworten auf ungültige Steuernachrichten senden
Versendet ein Absender eine E-Mail-Nachricht als Steuernachricht an das System, und enthält diese Nachricht keine gültigen Befehle, dann beantwortet MDaemon per Voreinstellung diese Steuernachricht nicht. Diese Option bewirkt, dass MDaemon eine ungültige Steuernachricht mit einem Hinweis beantwortet, dass kein gültiger Befehl in der Steuernachricht festgestellt werden konnte.

Nachrichten, die das System erzeugt, durch Inhalts-und Spam-Filter leiten
Diese Option bewirkt per Voreinstellung, dass durch das System erstellte Nachrichten durch den Inhaltsfilter und den Spam-Filter verarbeitet werden. Falls Sie solche Nachrichten von der Verarbeitung durch den Inhaltsfilter und den Spam-Filter ausnehmen wollen, deaktivieren Sie diese Option.

Weitergeleitete Nachrichten durch Inhalts- und Spam-Filter leiten
Diese Option bewirkt, dass weitergeleitete Nachrichten durch den Inhaltsfilter und den Spam-Filter verarbeitet werden. Diese Option ist per Voreinstellung abgeschaltet.

Nachrichten über den Zustellstatus (DSN) durch Inhalts- und Spam-Filter leiten
Diese Option bewirkt, dass Nachrichten über den Zustellstatus (DSN) durch den Inhaltsfilter und den Spam-Filter verarbeitet werden. Falls Sie solche Nachrichten von der Verarbeitung durch den Inhaltsfilter und den Spam-Filter ausnehmen wollen, deaktivieren Sie diese Option.

Funktionen zur Subadressierung für alle Benutzerkonten deaktivieren
Diese Option bewirkt, dass die Funktionen zur Subadressierung systemweit abgeschaltet werden. Die Einstellungen der einzelnen Benutzerkonten werden dabei übergangen, sodass die Subadressierung in jedem Falle gesperrt wird. Nähere Informationen über die Subadressierung erhalten Sie im Abschnitt IMAP-Filter 736 des Benutzerkonten-Editors.

Statistik-Bericht um Mitternacht an den Postmaster senden
Per Voreinstellung wird jeden Tag um Mitternacht ein Statistik-Bericht an den Postmaster gesandt. Falls Sie diese Berichte nicht versenden lassen wollen, deaktivieren Sie diese Option. Die Option bezieht sich auf die Registerkarte Statistik 76 auf der Benutzeroberfläche von MDaemon.

Export von Benutzerkonten schließt die Statistiken zur Speicherplatznutzung ein (dies kann den Export erheblich verlangsamen)
Per Voreinstellung umfasst der Export von Benutzerkonten keine Informationen über die Zahl der in den Benutzerverzeichnissen abgelegten Dateien und den hierdurch belegten Speicherplatz. Falls Sie diese Informationen ebenfalls in die Exporte einfügen wollen, aktivieren Sie diese Option. Die Nutzung dieser Option kann den Export jedoch deutlich verlangsamen.

Nachrichten, die an bestimmte Hosts weitergeleitet werden, nach Fehlern nicht über Smarthosts senden
Benutzerkonten können mithilfe der "Erweiterten Einstellungen zur Weiterleitung" im Abschnitt Weiterleitung 727 des Benutzerkonten-Editors so konfiguriert werden, dass ihre Nachrichten direkt an einen bestimmten Host oder Server weitergeleitet werden und nicht die üblichen Zustellroutinen von MDaemon durchlaufen. Tritt während einer solchen direkten Weiterleitung ein Zustellfehler auf, dann verschiebt MDaemon die fragliche Nachricht per Voreinstellung in die Defekt-Warteschlange. Wenn Sie diese Option aktivieren, dann verschiebt MDaemon die Nachrichten stattdessen in die Wiederholungs-Warteschlange 864 und führt nach den Einstellungen zur erneuten Zustellung weitere Zustellversuche aus.

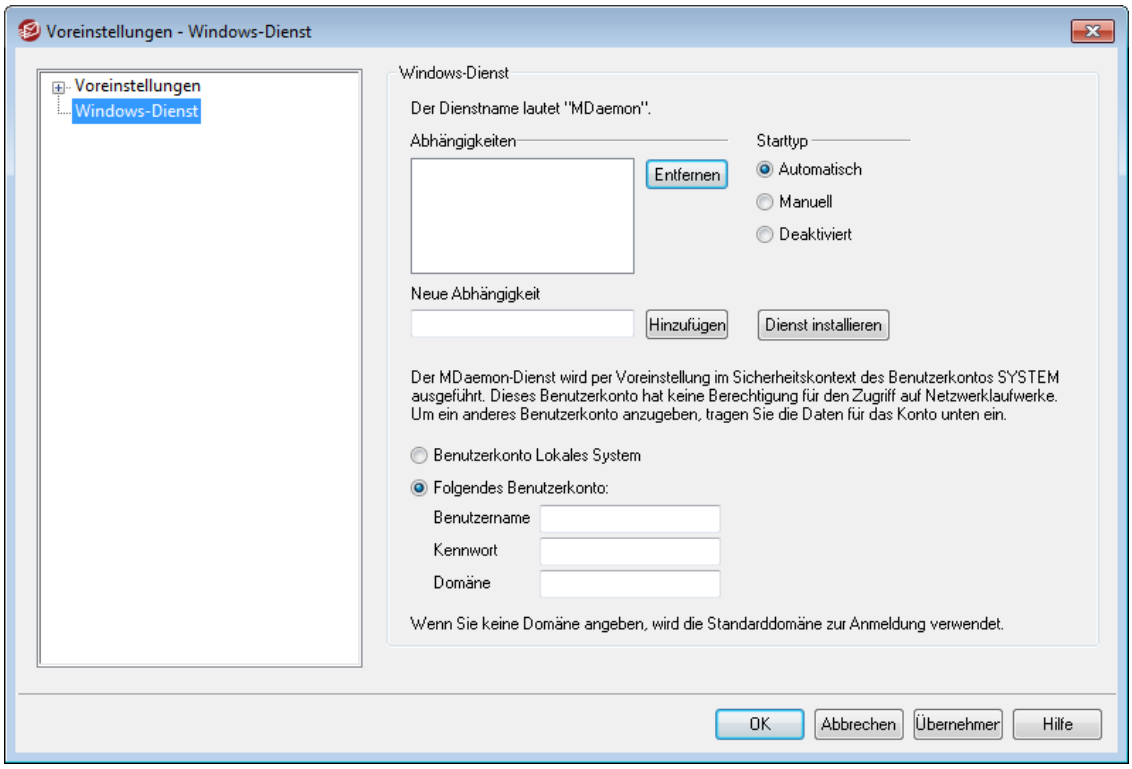
Alle an den Postmaster gerichteten Systemnachrichten in Kopie an Globale Administratoren senden
Per Voreinstellung werden die durch das System für den Postmaster erstellten Nachrichten auch an die Globalen Administratoren 757 gesendet. Globale Administratoren erhalten dabei alle Nachrichten, einschließlich der Berichte über die Warteschlangen, Statistikberichte, Versionsinformationen, Fehlermeldungen "Benutzer unbekannt" für alle Domänen, Benachrichtigungen über Datenträgerfehler, Benachrichtigungen über Einfrieren und Sperren von Benutzerkonten für alle Domänen (sie können die Benutzerkonten wieder freigeben und entsperren, wie es auch für Domänen-Administratoren möglich ist), Warnnachrichten über die Lizenzen und die Laufzeit der Betaversionen, Spam-Berichte und anderes. Falls Sie nicht wünschen, dass die Globalen Administratoren diese Benachrichtigungen empfangen, deaktivieren Sie diese Option.

Alle an den Postmaster gerichteten Systemnachrichten in Kopie an Domänen-Administratoren senden
Per Voreinstellung werden die durch das System für den Postmaster erstellten Nachrichten auch an die Domänen-Administratoren 757 gesandt. Die Domänen-Administratoren erhalten dabei aber nur solche Nachrichten, die sich auf die von ihnen verwalteten Domänen beziehen. Falls Sie nicht wünschen, dass die

Domänen-Administratoren diese Benachrichtigungen empfangen, deaktivieren Sie diese Option.

Weiterleitung von Nachrichten an externe Domänen verhindern
Diese Option bewirkt, dass Benutzerkonten Nachrichten nicht an Empfänger außerhalb ihrer eigenen Domäne weiterleiten können. Richtet ein Benutzer dann eine Weiterleitung an einen Empfänger in einer anderen Domäne ein, so werden diese externen Zieladressen für die Weiterleitung ignoriert. Diese Einstellung wirkt nur auf Nachrichten, die mithilfe der Einstellungen zur Weiterleitung von Nachrichten 727 für das jeweilige Benutzerkonto weitergeleitet werden.

3.12.2 Windows-Dienst



Windows-Dienst

Wird MDaemon als Windows-Systemdienst ausgeführt, so lautet der Dienstname "MDaemon".

Abhängigkeiten
Hier sind die Namen der Windows-Systemdienste angegeben, die **vor dem Start** des MDaemon-Dienstes gestartet sein müssen.

Starttyp
Hier wird festgelegt, ob und wie der MDaemon-Dienst gestartet wird. Zur Auswahl stehen automatisch, manuell und deaktiviert.

Dienst installieren/entfernen
Durch Anklicken dieses Steuerelements können Sie den MDaemon-Dienst installieren und entfernen.

Zugriff auf Netzwerk-Ressourcen

MDaemon wird als Dienst normalerweise unter dem Benutzerkonto SYSTEM ausgeführt; dieses Konto darf jedoch nicht auf Netzwerkressourcen zugreifen. Das führt dazu, dass MDaemon keine Nachrichten auf anderen Rechnern im Netzwerk ablegen kann. Sollen Netzwerkverbindungen und Netzwerkfreigaben benutzt werden, so müssen hier die Anmeldedaten eines Benutzerkontos eingetragen werden, das über entsprechende Berechtigungen auf den Netzwerkfreigaben verfügt. Falls dies nötig ist, kann ein eigenes Windows-Benutzerkonto für MDaemon angelegt werden, wobei vor allem darauf zu achten ist, dass es ausreichende Zugriffsrechte für die zu benutzenden Netzwerkfreigaben erhält. MDaemon als Dienst kann dann auf Netzwerkpfade in UNC-Schreibweise oder auf gemappte Laufwerke zugreifen, und auch alle durch MDaemon gestarteten Programme erhalten die Rechte des Benutzerkontos von MDaemon.

Benutzername
Hier wird der Anmeldename des Windows-Benutzerkontos für MDaemon eingetragen.

Kennwort
Hier wird das Kennwort des Windows-Benutzerkontos angegeben.

Domäne
Die Windows-Domäne, in der das Benutzerkonto eingerichtet wurde, muss hier eingetragen werden. Falls die Standarddomäne benutzt werden soll, bleibt das Feld leer.

Kapitel IV

4 Das Menü Sicherheit

MDaemon enthält umfassende Sicherheitsfunktionen. Sie erhalten über das Menü Sicherheit in der Menüleiste von MDaemon Zugriff auf die folgenden Sicherheitsfunktionen:

- **AntiVirus** 648 — MDaemon kann Computer-Viren filtern und stoppen, die über E-Mail verbreitet werden. Dazu bietet diese Software den Benutzern eine vollständige und nahtlose Einbindung in MDaemon, wie sie keine andere Software erreicht. MDaemon AntiVirus erkennt, sperrt, repariert oder löscht alle E-Mail-Nachrichten, in denen ein Virus festgestellt wurde. AntiVirus stellt unter anderem auch Leistungsmerkmale der Outbreak Protection 643 zur Verfügung, mit deren Hilfe das System gegen bestimmte Spam-, Phishing- und Virenangriffe geschützt werden kann, die durch herkömmliche Schutzmechanismen auf Basis von Inhaltsauswertung und Signaturen vielleicht nicht entdeckt werden.
- **Inhaltsfilter** 649 — Ein höchst vielseitiges Inhaltsfilter-System mit uneingeschränkter Multithread-Unterstützung erlaubt es, das Verhalten des Servers vom Inhalt eingehender und abgehender Nachrichten abhängig zu machen. Kopfzeilen können in Nachrichten eingefügt und aus ihnen gelöscht werden, die Nachrichten können einen Fußtext erhalten, Dateianlagen können entfernt, Kopien können automatisch an andere Benutzer geleitet werden, Instant-Messages können ausgelöst, externe Programme ausgeführt werden, und vieles mehr.
- **Spam-Filter** 678 — Die Technik des neuen Spam-Filters prüft E-Mail-Nachrichten durch heuristische Verfahren, um eine Bewertung zu errechnen. Anhand dieser Bewertung stellt das System fest, wie wahrscheinlich es ist, dass es sich bei der Nachricht um Spam handelt. Aufgrund dieser Feststellung kann der Server dann bestimmte Aktionen auslösen, etwa die Nachricht abweisen oder kennzeichnen.Siehe auch: Spam-Fallen 709.
- **Sperrlisten für DNS** 704 — Mithilfe mehrerer Dienste, die Sperrlisten für DNS unterhalten, und die der Benutzer auch selbst auswählen kann, wird bei jeder Übertragung einer Nachricht an den Server geprüft, ob sie von einer IP-Adresse ausgeht, die von einem solchen Dienst in einer Sperrliste geführt wird. Trifft dies zu, so wird die Nachricht abgewiesen oder entsprechend markiert.
- **Relaiskontrolle** 513 — Hiermit wird festgelegt, wie MDaemon mit Nachrichten verfahren soll, die weder von einer lokalen Adresse kommen noch an eine lokale Adresse gerichtet sind.
- **IP-Abschirmung** 522 — Wenn eine Verbindung von einem hier eingetragenen Domänennamen aus zum Server hergestellt wird, muss die IP-Adresse der Gegenstelle der hier erfassten entsprechen.
- **SMTP-Echtheitsbestätigung** 524 — Diese Einstellungen steuern das Verhalten von MDaemon, falls ein Benutzer eine Nachricht an MDaemon sendet, der nicht zuerst durch Anmeldename und Kennwort identifiziert wurde.
- **Rückwärtssuche** 515 — MDaemon kann DNS-Server abfragen, um die Echtheit von Domänennamen und Adressen zu prüfen, die während der Anlieferung von Nachrichten übermittelt wurden. Diese Funktion kann dazu verdächtige Nachrichten abweisen oder ihnen eine besondere Kopfzeile hinzufügen. Ergebnisse der Rückwärtssuche werden auch in den Systemprotokollen vermerkt.

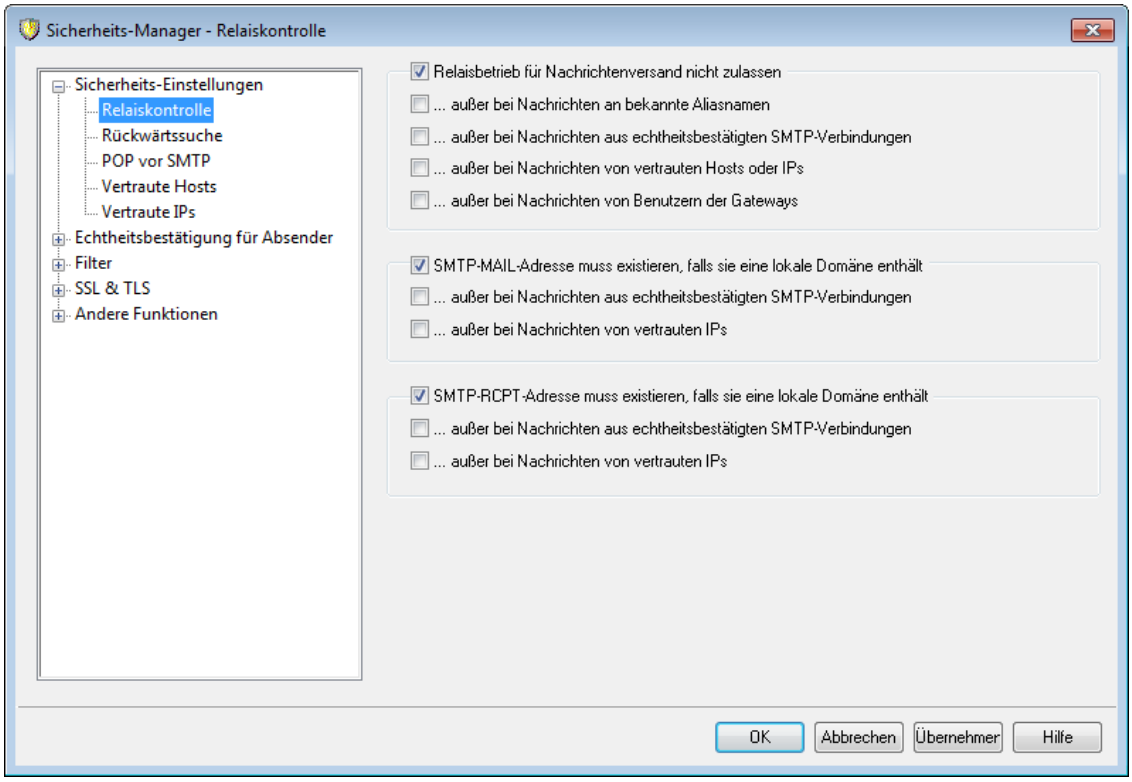
- **POP vor SMTP** 519 — Diese Einstellungen verlangen von den Benutzern, erst über POP ihre Postfächer abzufragen, bevor sie eine Nachricht über MDaemon versenden dürfen. Hierdurch wird sichergestellt, dass der Absender ein gültiges MDaemon-Benutzerkonto hat und daher den Mailserver verwenden darf.
- **Vertraute Hosts** 520 — Diese Domänennamen und IP-Adressen mit Vertrauensstellungen sind von den Relais-Einstellungen ausgenommen
- **SPF** 527 — Für alle Domänen sind MX-Einträge veröffentlicht, in denen die Rechner erfasst sind, die Nachrichten für die Domänen empfangen dürfen. Aus diesen Einträgen ergibt sich aber nicht, welche Rechner für diese Domänen Nachrichten versenden dürfen. Das Sender-Policy-Framework (SPF) ermöglicht es, für Domänen "umgekehrte MX-Einträge" zu veröffentlichen, aus denen dann die Rechner ersichtlich sind, die für die Domäne Nachrichten versenden dürfen.
- **DomainKeys Identified Mail** 529 — Das Verfahren DomainKeys Identified Mail (DKIM) prüft E-Mail-Nachrichten und kann die Nutzung gefälschter Absenderdaten (das "Spoofing") verhindern. Es können auch benutzt werden, um die Intaktheit eingehender Nachrichten zu prüfen und sicherzustellen, dass der Inhalt einer Nachricht nicht verändert wurde, nachdem sie den Mailserver des Absenders verlassen hat. Um die entsprechenden Leistungsmerkmale bereitzustellen, kommen Schlüsselpaare aus je einem öffentlichen und einem geheimen Schlüssel zum Einsatz. Abgehende Nachrichten werden mithilfe eines geheimen Schlüssels signiert, eingehende signierte Nachrichten werden anhand des öffentlichen Schlüssels des Absenders geprüft, der über den DNS-Server des Absenders abrufbar sein muss.
- **Zertifizierung** 554 — Die Zertifizierung von Nachrichten ist Schutzmechanismus, in dessen Rahmen eine Stelle bestätigt oder dafür einsteht, dass eine andere Stelle gewissen ordnungsgemäße E-Mail-Praktiken anwendet. Die Zertifizierung ist vorteilhaft, da sie helfen kann, zu verhindern, dass Nachrichten eine unnötige Analyse durch den Spam-Filter durchlaufen. Sie kann auch helfen, die Ressourcen für die Verarbeitung einzelner Nachrichten zu verringern.
- **Sperrliste für Absender** 560 — Liste der Adressen, die keine Nachrichten über das System versenden dürfen.
- **IP-Filter** 563 — Verbindungen von hier eingetragenen Adressen lässt der Server, je nach Einstellung, zu oder weist sie ab.
- **Host-Filter** 565 — Verbindungen von hier eingetragenen Hostnamen (Domänennamen) lässt der Server, je nach Einstellung, zu oder weist sie ab.
- **Dynamischer Filter** 612 — Mithilfe des Dynamischen Filters kann MDaemon bestimmte Muster in eingehenden Verbindungen nachverfolgen, hieraus verdächtige Aktivität erkennen und entsprechend reagieren. Sie können IP-Adressen (oder Adressbereiche) gegen weitere Verbindungen sperren 616, falls in Verbindungen von diesen IP-Adressen aus mehrfach innerhalb eines bestimmten Zeitraums fehlgeschlagene Versuche zur Echtheitsbestätigung ausgehen. Sie können auch Benutzerkonten einfrieren 616, falls von Gegenstellen für diese zu oft in zu kurzer Zeit fehlgeschlagene Versuche zur Echtheitsbestätigung durchgeführt werden.
- **SSL & TLS** 577 — MDaemon unterstützt das Secure-Sockets-Layer-Protokoll (SSL) für SMTP, POP und IMAP sowie für die Web-Server von Webmail und der Remoteverwaltung. SSL ist das Standardprotokoll für gesicherte Kommunikation zwischen Server und Client im Internet.

- **Schutz gegen Rückstreuung** [598] — Als "Rückstreuung" bezeichnet man Antworten auf E-Mail-Nachrichten, die bei Benutzern des lokalen Systems eingehen, obwohl diese Benutzer die Ursprungsnachrichten gar nicht versendet hatten. Rückstreuung tritt auf, wenn Spam oder durch Viren versandte Nachrichten einen Antwort-Pfad mit gefälschter Absenderadresse enthalten. Um die Rückstreuung zu bekämpfen, enthält MDaemon in Version 9.6 eine Funktion zum Schutz gegen Rückstreuung. Sie bewirkt, dass Statusnachrichten und Nachrichten von Autobeantwortern nur dann an die Benutzer weitergeleitet werden, wenn die Benutzer die Ursprungsnachrichten selbst versandt haben. Dazu dient ein Hashverfahren mit geheimem Schlüssel, das einen bestimmten uhrzeitabhängigen Kode in den "Antwort-Pfad" der abgehenden Nachrichten einfügt.
- **Bandbreitenbegrenzung** [601] — Die Bandbreitenbegrenzung gestattet die Überwachung und Steuerung der von MDaemon genutzten Übertragungsbandbreite durch Drosselung der Übertragungsgeschwindigkeit. Die gewünschte Geschwindigkeit für Verbindungen und die einzelnen Serverdienste lässt sich so beeinflussen; für alle wichtigen Serverdienste von MDaemon sind nach Domänen sowie Domänen-Gateways getrennte Einstellungen möglich.
- **Teergrube** [604] — Eine Technik, die eine Verbindung mit Absicht verlangsamen und verzögern kann, sobald eine bestimmte Anzahl RCPT-Befehle vom Absender einer Nachricht übermittelt wurden. Die Funktion soll Spammer von dem Versuch abhalten, über den Server unverlangte Massensendungen ("Spam") zu versenden. Die Methode fußt auf der Annahme, dass der Versuch, Massensendungen über den Server zu versenden, für Spammer unattraktiv wird, wenn der Versand jeder einzelnen Nachricht unverhältnismäßig lange Zeit in Anspruch nimmt, und dass Spammer solche Versuche alsbald aufgeben.
- **Graue Liste** [606] — Die Graue Liste ist eine Technik zur Bekämpfung von Spam. Sie nutzt die Tatsache, dass SMTP-Server die Zustellung von Nachrichten wiederholt, bei deren erstem Zustellversuch der Server des Empfängers den Fehlerkode für einen vorübergehenden Fehler gemeldet hat (etwa "Bitte versuchen Sie es später erneut." oder "Please try again later."). Wird diese Technik genutzt, und trifft eine Nachricht von einer Gegenstelle ein, die nicht bereits in einer Freigabeliste erfasst oder dem System bislang nicht bekannt war, so werden Absender und Empfänger der Nachricht und die IP-Adresse des zustellenden Servers protokolliert; danach wird die Nachricht während der SMTP-Übertragung unter Hinweis auf einen vorübergehenden Fehler abgewiesen. Versucht ein legitimer Absender etwas später die Zustellung erneut, so wird die Nachricht angenommen. Da Spamversender üblicherweise keine weiteren Zustellversuche unternehmen, kann die Graue Liste die Zahl der Spam-Nachrichten, die Ihre Benutzer erhalten, deutlich verringern.
- **LAN-IP-Adressen** [610] — In diesem Konfigurationsdialog tragen Sie die IP-Adressen ein, die über Ihr lokales Netzwerk (LAN) erreichbar sind. Datenverkehr mit den IP-Adressen wird wie lokaler Datenverkehr behandelt und von verschiedenen Sicherheits-Maßnahmen und Maßnahmen zur Spam-Abwehr ausgenommen.
- **Nutzungsrichtlinien** [611] — Mit dieser Funktion werden Nutzungsbedingungen für das eigene System erstellt, die zu Beginn jeder SMTP-Verbindung an eine Gegenstelle übertragen werden, bevor diese mit der Postzustellung beginnt. Ein gängiges Beispiel für solche Nutzungsbedingungen ist der Hinweis "Relaisbetrieb ist auf diesem System gesperrt".

4.1 Sicherheits-Manager

4.1.1 Sicherheitseinstellungen

4.1.1.1 Relaiskontrolle



Im Konfigurationsdialog Relaiskontrolle (erreichbar unter Sicherheit » Sicherheits-Einstellungen » Relaiskontrolle) legen Sie fest, ob und wie der Server fremde Nachrichten bearbeiten soll, die weder aus einer lokalen Domäne stammen noch an eine solche gerichtet sind. Die Weiterleitung fremder Post wird auch als Relaisbetrieb oder "Mail Relaying" bezeichnet. Falls der Server solche Post nicht weiterleiten soll, kann der Relaisbetrieb hier beschränkt werden.

Der Mailserver soll unter keinen Umständen freien ("offenen") Relaisbetrieb zulassen, da dann die Gefahr besteht, dass der Server selbst in den Datenbanken der Sperrlisten für DNS (DNS-BL) 704 erfasst wird. Von freiem Relaisbetrieb ist besonders abzuraten, da Spam-Versender offene Relais gerne ausnutzen, um ihre Spuren zu verwischen.

Relaisbetrieb für Nachrichten

Relaisbetrieb für Nachrichtenversand nicht zulassen
Ist diese Option aktiv, weit MDaemon alle Nachrichten zurück, bei denen weder Absender noch Empfänger (`FROM` und `TO`)lokale Benutzer sind.

...außer bei Nachrichten an bekannte Aliasnamen
Diese Option setzt die Relaiskontrolle bei Nachrichten für Adress-Aliasnamen 827 außer Kraft.

...außer bei Nachrichten aus echtheitsbestätigten SMTP-Verbindungen
Hiermit leitet MDaemon Nachrichten immer dann weiter, wenn sie in SMTP-Verbindungen nach erfolgreicher Echtheitsbestätigung übertragen wurden.

...außer bei Nachrichten von vertrauten Hosts oder IPs
Soll der Relaisbetrieb für Nachrichten zugelassen werden, die durch vertraute Hosts oder IP-Adressen übermittelt wurden, so muss diese Option aktiv sein.

...außer bei Nachrichten von Benutzern der Gateways
Diese Option bewirkt, dass MDaemon den Relaisbetrieb für Nachrichten zulässt, die über Domänen-Gateways zugestellt werden. Die Relais-Kontrolle wird dabei übergangen; diese Option ist per Voreinstellung deaktiviert, und es empfiehlt sich nicht, sie zu nutzen.

Prüfung von Benutzerkonten

SMTP-MAIL-Adresse muss existieren, falls sie eine lokale Domäne enthält
Diese Option bewirkt, dass der Wert für den Befehl MAIL, der während der SMTP-Verbindung übermittelt wird, daraufhin überprüft wird, ob er auf ein tatsächlich bestehendes Benutzerkonto verweist. Diese Prüfung findet statt, wenn die im Befehl MAIL übermittelte Adresse angeblich aus einer lokalen Domäne oder einem Gateway stammt.

...außer bei Nachrichten aus echtheitsbestätigten SMTP-Verbindungen
Diese Option bewirkt, dass eine Nachricht von der Option *SMTP-MAIL-Adresse muss existieren...* ausgenommen ist, falls sie über eine echtheitsbestätigte SMTP-Verbindung übermittelt wurde.

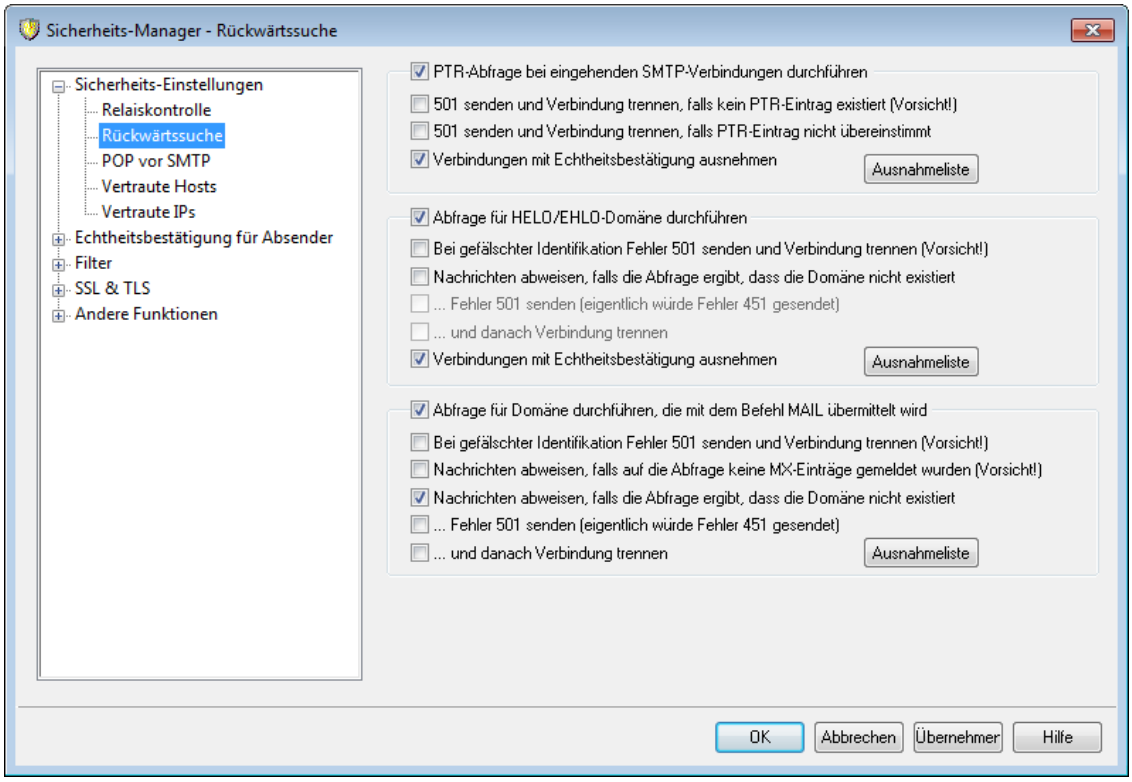
...außer bei Nachrichten von vertrauten IPs
Diese Option bewirkt, dass eine Nachricht von der Option *SMTP-MAIL-Adresse muss existieren...* ausgenommen ist, falls sie von einer vertrauten IP-Adresse übermittelt wurde.

SMTP-RCPT-Adresse muss existieren, falls sie eine lokale Domäne enthält
Diese Option bewirkt, dass der Wert für den Befehl RCPT, der während der SMTP-Verbindung übermittelt wird, daraufhin überprüft wird, ob er auf ein tatsächlich bestehendes Benutzerkonto verweist. Diese Prüfung findet statt, wenn die im Befehl RCPT übermittelte Adresse angeblich aus einer lokalen Domäne oder einem Gateway stammt.

...außer bei Nachrichten aus echtheitsbestätigten SMTP-Verbindungen
Diese Option bewirkt, dass eine Nachricht von der Option *SMTP-RCPT-Adresse muss existieren...* ausgenommen ist, falls sie über eine echtheitsbestätigte SMTP-Verbindung übermittelt wurde.

...außer bei Nachrichten von vertrauten IPs
Diese Option bewirkt, dass eine Nachricht von der Option *SMTP-RCPT-Adresse muss existieren...* ausgenommen ist, falls sie von einer vertrauten IP-Adresse übermittelt wurde.

4.1.1.2 Rückwärtssuche



Mithilfe der Einstellungen in diesem Konfigurationsdialog kann MDaemon veranlasst werden, Domänennamen, die zusammen mit den Befehlen `HELO/EHLO` und `MAIL` übermittelt wurden, einer Rückwärtssuche zu unterziehen. Dabei versucht MDaemon, alle MX-und A-Einträge für die zu prüfende Domäne in Erfahrung zu bringen. Sodann wird die IP-Adresse der Gegenstelle, die den Verbindungsaufbau versucht, mit diesen Adressen verglichen, um festzustellen, ob sich der Absender vielleicht einer falschen Identität bedient.

Es lässt sich auch eine Rückwärtssuche nach PTR-Einträgen von IP-Adressen durchführen, die eine Verbindung aufbauen wollen. Diese Option erlaubt entweder den Verbindungsabbruch oder das Einfügen einer Kopfzeile zur Warnung in die Nachricht, falls für die IP-Adresse kein entsprechender PTR-Eintrag besteht.

Schließlich entspricht es der allgemeinen Auffassung, dass Nachrichten von Gegenstellen, die sich mit einem nicht bestehenden Domänennamens identifizieren, nicht zwingend angenommen werden müssen. Daher besteht auch die Möglichkeit, Nachrichten abzuweisen, bei denen die Rückwärtssuche einen Fehler "Domäne nicht gefunden" vom DNS-Server ergibt. MDaemon meldet in solchen Fällen einen Fehler `451` an die Gegenstelle, weist die Nachricht ab und lässt die SMTP-Verbindung bestehen. Wahlweise kann aber auch ein Fehler `501` gemeldet oder die Socket-Verbindung geschlossen werden; auch beides zusammen ist möglich. Hierfür stehen entsprechende Optionen zur Verfügung.

Vertraute IP-Adressen und der localhost (127.0.0.1) sind immer von der Prüfung durch Rückwärtssuche ausgenommen.

PTR-Abfrage bei eingehenden SMTP-Verbindungen durchführen
Falls MDaemon eine Suche nach PTR-Einträgen (Pointer-Record-Einträgen) bei allen eingehenden SMTP-Verbindungen durchführen soll, ist diese Option zu aktivieren.

501 senden und Verbindung trennen, falls kein PTR-Eintrag existiert (Vorsicht!)
Ist diese Option aktiv, so sendet MDaemon den Fehlerkode `501` (Syntaxfehler in den Parametern oder Befehlen) und trennt anschließend die Verbindung, falls kein PTR-Eintrag für die betreffende Domäne existiert.

501 senden und Verbindung trennen, falls PTR-Eintrag nicht übereinstimmt
Ist diese Option aktiv, so sendet MDaemon den Fehlerkode `501` (Syntaxfehler in den Parametern oder Befehlen) und trennt anschließend die Verbindung, falls das Ergebnis der PTR-Abfrage nicht mit der betreffenden Domäne übereinstimmt.

Verbindungen mit Echtheitsbestätigung ausnehmen
Diese Option bewirkt, dass die PTR-Abfrage bei eingehenden SMTP-Verbindungen erst nach Übermittlung des SMTP-Befehls MAIL durchgeführt wird. So kann vor der Abfrage festgestellt werden, ob die Verbindung echtheitsbestätigt ist.

Ausnahmeliste
Ein Klick auf dieses Steuerelement öffnet den Konfigurationsdialog für die Ausnahmeliste für die PTR-Abfrage. Hier können die IP-Adressen, Domänen und Hosts erfasst werden, die von der Rückwärtssuche durch die PTR-Abfrage ausgenommen sein sollen.

Abfrage für HELO/EHLO-Domäne durchführen
Hiermit wird der Domänenname aus dem Befehl `HELO/EHLO` überprüft. Der Befehl `HELO/EHLO` wird durch den Absender benutzt, um sich gegenüber dem Server zu identifizieren. Der hierbei durch den Absender übergebene Domänenname wird vom Server benutzt, um den Abschnitt "`from`" der "`Received`"-Kopfzeile auszufüllen.

Bei gefälschter Identifikation Fehler 501 senden und Verbindung trennen (Vorsicht!)
Diese Option bewirkt, dass ein Fehler `501` gemeldet und die Verbindung getrennt wird, falls eine Abfrage ergeben hat, dass die übermittelte Identifikation offenbar gefälscht ist.

Die Feststellung, dass die von einer Gegenstelle gesendete Identifikation gefälscht ist, kann häufig unzutreffend sein, wenn sie nur aufgrund einer Rückwärtssuche getroffen wird. Es ist immer noch üblich, dass Mailserver sich mit Daten identifizieren, die sich über eine Rückwärtssuche nicht ihrer IP-Adresse zuordnen lassen. Dies kann durch Beschränkungen des ISP veranlasst sein oder andere nachvollziehbare Gründe haben. Aus diesem Grund sollte die oben beschriebene Funktion sehr vorsichtig eingesetzt werden; sie könnte zur Abweisung einiger ansonsten nicht zu beanstandender Nachrichten führen.

Nachrichten abweisen, die falls Abfrage ergibt, dass die Domäne nicht existiert
Ergibt die Rückwärtssuche den Fehler "`Domäne nicht gefunden`", so wird die Nachricht unter Meldung des Fehlers `451` abgewiesen, falls diese Option

gesetzt ist ("Angeforderte Aktion abgebrochen: lokaler Fehler bei der Verarbeitung") Die Verbindung bleibt dann bestehen und nimmt bis zu einer ordentlichen Beendigung ihren Fortgang.

...Fehler 501 senden (eigentlich würde Fehler 451 gesendet)
Hiermit kann nach einem Fehler "`Domäne nicht gefunden`" des Fehlers `451` der Fehler `501` ("Syntaxfehler bei Parametern oder Argumenten") als Antwort ausgegeben werden.

...und danach Verbindung trennen
Diese Option trennt die Verbindung sofort, wenn der Fehler "`Domäne nicht gefunden`" auf eine Rückwärtssuche hin aufgetreten ist.

Verbindungen mit Echtheitsbestätigung ausnehmen
Diese Option bewirkt, dass die Abfrage bei eingehenden SMTP-Verbindungen erst nach Übermittlung des SMTP-Befehls MAIL durchgeführt wird. So kann vor der Abfrage festgestellt werden, ob die Verbindung echtheitsbestätigt ist.

Ausnahmeliste
Ein Klick auf dieses Steuerelement öffnet den Konfigurationsdialog für die Ausnahmeliste für die HELO/EHLO-Abfrage. Hier können die IP-Adressen, Domänen und Hosts erfasst werden, die von der Rückwärtssuche durch die HELO/EHLO-Abfrage ausgenommen sein sollen.

Abfrage für Domäne durchführen, die mit dem Befehl MAIL übermittelt wird
Diese Option bewirkt, dass eine Rückwärtssuche für jenen Domänennamen durchgeführt wird, der innerhalb als Parameter des `MAIL`-Befehls während der Verbindung übergeben wird. Die Adresse, die zusammen mit dem Befehl `MAIL` übermittelt wird, soll der Antwortpfad für die Nachricht sein und entspricht üblicherweise dem Postfach, von dem sie ausgeht. Es kann stattdessen aber auch die Adresse angegeben sein, an die Fehlermeldungen gerichtet werden sollen.

Bei gefälschter Identifikation Fehler 501 senden und Verbindung trennen (Vorsicht!)
Diese Option bewirkt, dass ein Fehler `501` gemeldet und die Verbindung getrennt wird, falls eine Abfrage ergeben hat, dass die übermittelte Identifikation offenbar gefälscht ist.

Die Feststellung, dass die von einer Gegenstelle gesendete Identifikation gefälscht ist, kann häufig unzutreffend sein, wenn sie nur aufgrund einer Rückwärtssuche getroffen wird. Es ist immer noch üblich, dass Mailserver sich mit Daten identifizieren, die sich über eine Rückwärtssuche nicht ihrer IP-Adresse zuordnen lassen. Dies kann durch Beschränkungen des ISP veranlasst sein oder andere nachvollziehbare Gründe haben. Aus diesem Grund sollte die oben beschriebene Funktion sehr vorsichtig eingesetzt werden; sie könnte zur Abweisung einiger ansonsten nicht zu beanstandender Nachrichten führen.

Nachrichten abweisen, falls auf die Abfrage keine MX-Einträge gemeldet wurden (Vorsicht!)'
Diese Option bewirkt, dass die Übermittlung von Nachrichten über den Befehl MAIL von solchen Domänen abgewiesen wird, für die keine MX-Einträge bestehen. Diese Option ist per Voreinstellung abgeschaltet und soll mit Bedacht eingesetzt werden. Gültige Domänen können auch bestehen, ohne MX-Einträge zu haben, und sie können ohne diese auch Nachrichten senden und empfangen.

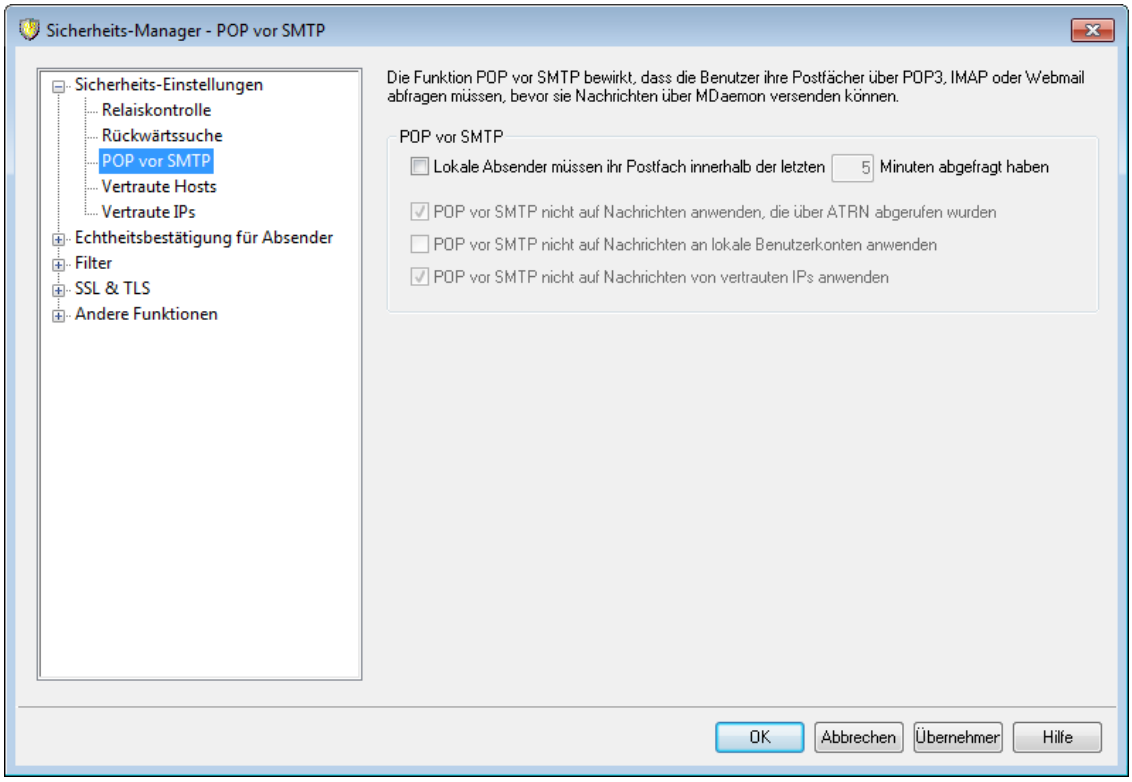
Nachrichten abweisen, die falls Abfrage ergibt, dass die Domäne nicht existiert
Ergibt die Rückwärtssuche den Fehler "`Domäne nicht gefunden`", so wird die Nachricht unter Meldung des Fehlers `451` abgewiesen, falls diese Option gesetzt ist ("Angeforderte Aktion abgebrochen: lokaler Fehler bei der Verarbeitung") Die Verbindung bleibt dann bestehen und nimmt bis zu einer ordentlichen Beendigung ihren Fortgang.

...Fehler 501 senden (eigentlich würde Fehler 451 gesendet)
Hiermit kann bei nicht gefundener Domäne statt des Fehlers `451` der Fehler `501` ("Syntaxfehler bei Parametern oder Argumenten") als Antwort ausgegeben werden.

...und danach Verbindung trennen
Diese Option trennt die Verbindung sofort, wenn der Fehler "`Domäne nicht gefunden`" auf eine Rückwärtssuche hin aufgetreten ist.

Ausnahmeliste
Ein Klick auf dieses Steuerelement öffnet den Konfigurationsdialog für die Ausnahmeliste für die MAIL-Abfrage. Hier können die IP-Adressen, Domänen und Hosts erfasst werden, die von der Rückwärtssuche durch die MAIL-Abfrage ausgenommen sein sollen.

4.1.1.3 POP vor SMTP



POP vor SMTP

Lokale Absender müssen ihr Postfach innerhalb der letzten [xx] Minuten abgefragt haben
Diese Funktion bewirkt, dass lokale Benutzer nur dann Nachrichten über MDaemon versenden dürfen, wenn sie innerhalb der hier angegebenen Zeit vor dem Versand ihr lokales Postfach abgefragt haben.

POP vor SMTP nicht auf Nachrichten anwenden, die über ATRN abgerufen wurden
Mit dieser Option lassen sich Nachrichten, die über ATRN 264 empfangen wurden, von den Beschränkungen der Funktion POP vor SMTP ausnehmen.

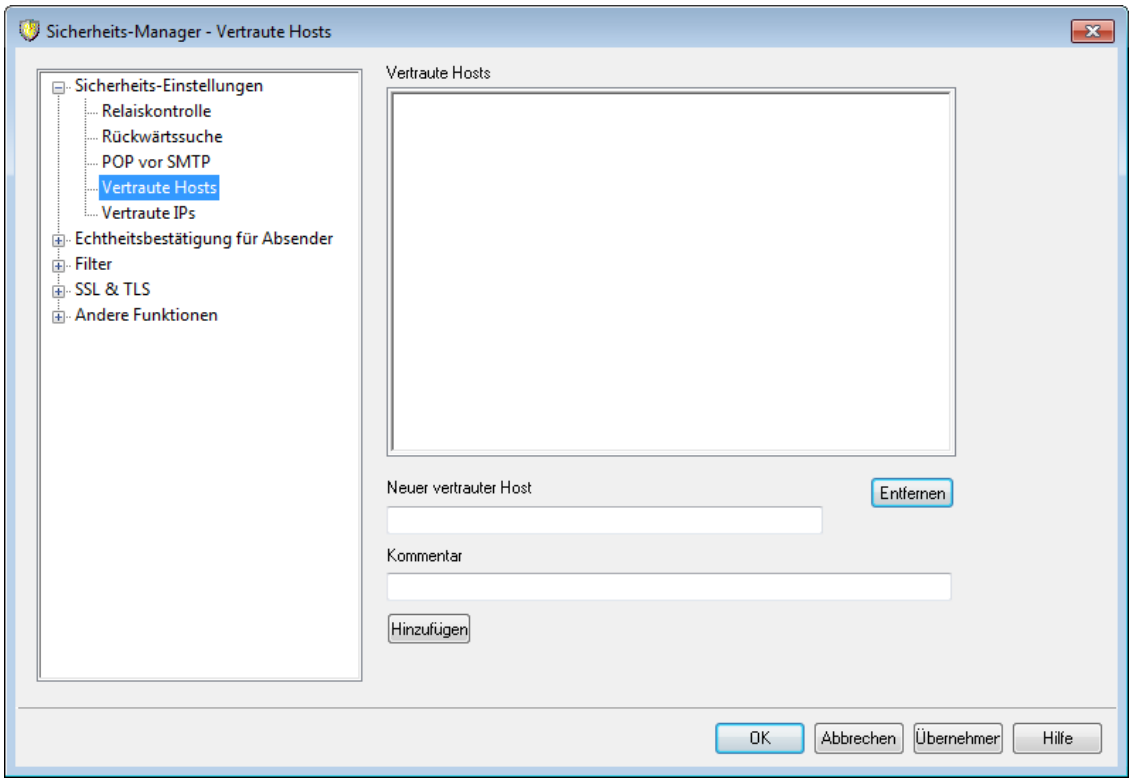
POP vor SMTP nicht auf Nachrichten an lokale Benutzerkonten anwenden
Diese Option bewirkt, dass bei Nachrichten zwischen zwei lokalen Benutzern die Funktion POP vor SMTP außer Kraft tritt. MDaemon prüft normalerweise die Einhaltung der Funktion POP vor SMTP, sobald der Absender einer Nachricht bekannt ist. Diese Option bewirkt, dass MDaemon auch die Bekanntgabe des Empfängers noch abwartet, bevor über die Annahme der Nachricht entschieden wird.

POP vor SMTP nicht auf Nachrichten von vertrauten IPs anwenden
Ist diese Option aktiv, so sind Domänen, die im Konfigurationsdialog vertraute Hosts 520 erfasst sind, von der Funktion POP vor SMTP ausgenommen.

Sie können auch echtheitsbestätigte Verbindungen von der Funktion POP vor SMTP ausnehmen. Hierfür steht im

Konfigurationsdialog SMTP-Echtheitsbestätigung[524] eine entsprechende Option zur Verfügung.

4.1.1.4 Vertraute Hosts



Verschiedene Konfigurationsdialoge und Leistungsmerkmale für die Systemsicherheit in MDaemon enthalten Optionen, mit deren Hilfe Sie "Vertraute Hosts" und "Vertraute Domänen" von der Bearbeitung durch die betroffenen Leistungsmerkmale ausnehmen können. In diesem Konfigurationsdialog bestimmen Sie die Vertrauten Hosts und Vertrauten Domänen, auf die sich die genannten Optionen beziehen.

Vertraute Hosts
Hier sind die Hosts eingetragen, die von bestimmten Sicherheitsoptionen ausgenommen sein sollen.

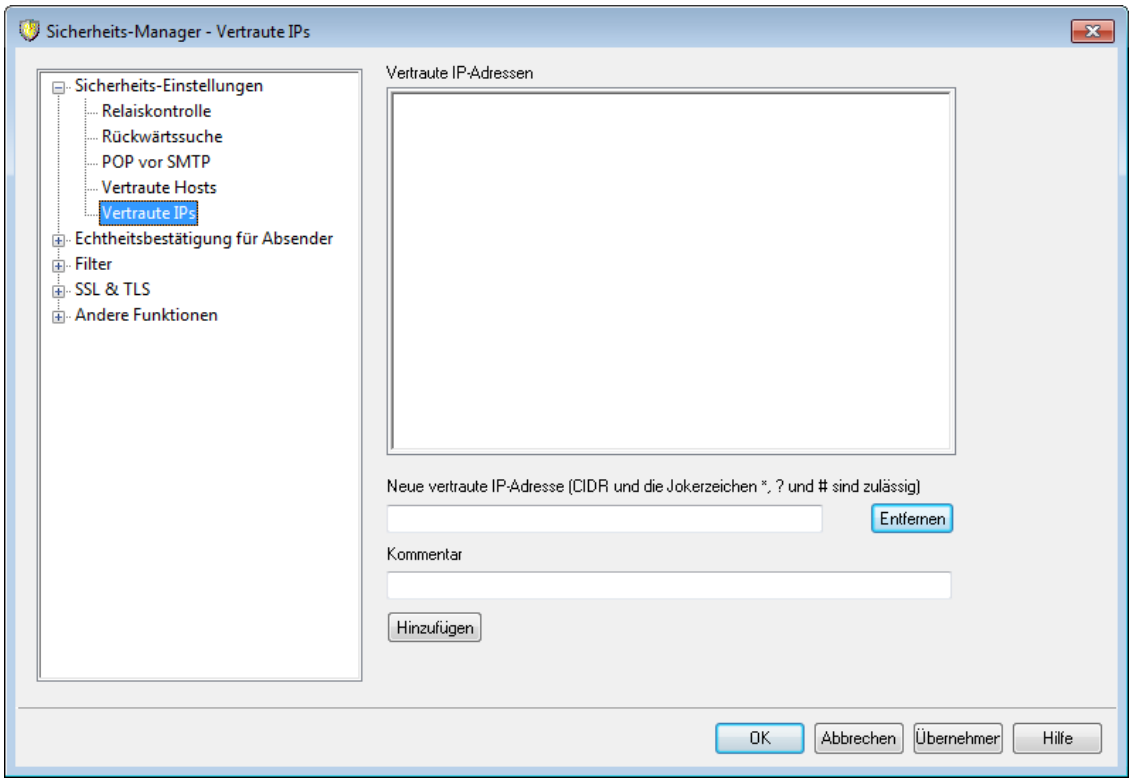
Neuer vertrauter Host
Geben Sie hier den Domänennamen ein, den Sie in die Liste *Vertraute Hosts* eintragen wollen.

Kommentar
In dieses Feld können Sie einen Kommentar zu dem gerade bearbeiteten Eintrag eingeben.

Hinzufügen
Durch Anklicken dieses Steuerelements fügen Sie den neuen Domänennamen der Liste *Vertraute Hosts* hinzu.

Entfernen
Durch Anklicken dieses Steuerelements entfernen Sie die ausgewählten Einträge aus der Liste *Vertraute Hosts*.

4.1.1.5 Vertraute IPs



On various dialogs and security features throughout MDaemon you will see options that allow you to choose whether or not "Trusted IPs" will be exceptions to or exempt from those options. The IP addresses you list on this screen are the ones to which those options refer.

Verschiedene Konfigurationsdialoge und Leistungsmerkmale für die Systemsicherheit in MDaemon enthalten Optionen, mit deren Hilfe Sie "Vertraute IPs" von der Bearbeitung durch die betroffenen Leistungsmerkmale ausnehmen können. In diesem Konfigurationsdialog bestimmen Sie die Vertrauten IPs, auf die sich die genannten Optionen beziehen.

Vertraute IP-Adressen
Hier sind die IP-Adressen eingetragen, die von bestimmten Sicherheitsoptionen ausgenommen sein sollen.

Neue vertraute IP-Adresse
Geben Sie hier die IP-Adresse ein, den Sie in die Liste *Vertraute IP-Adressen* eintragen wollen.

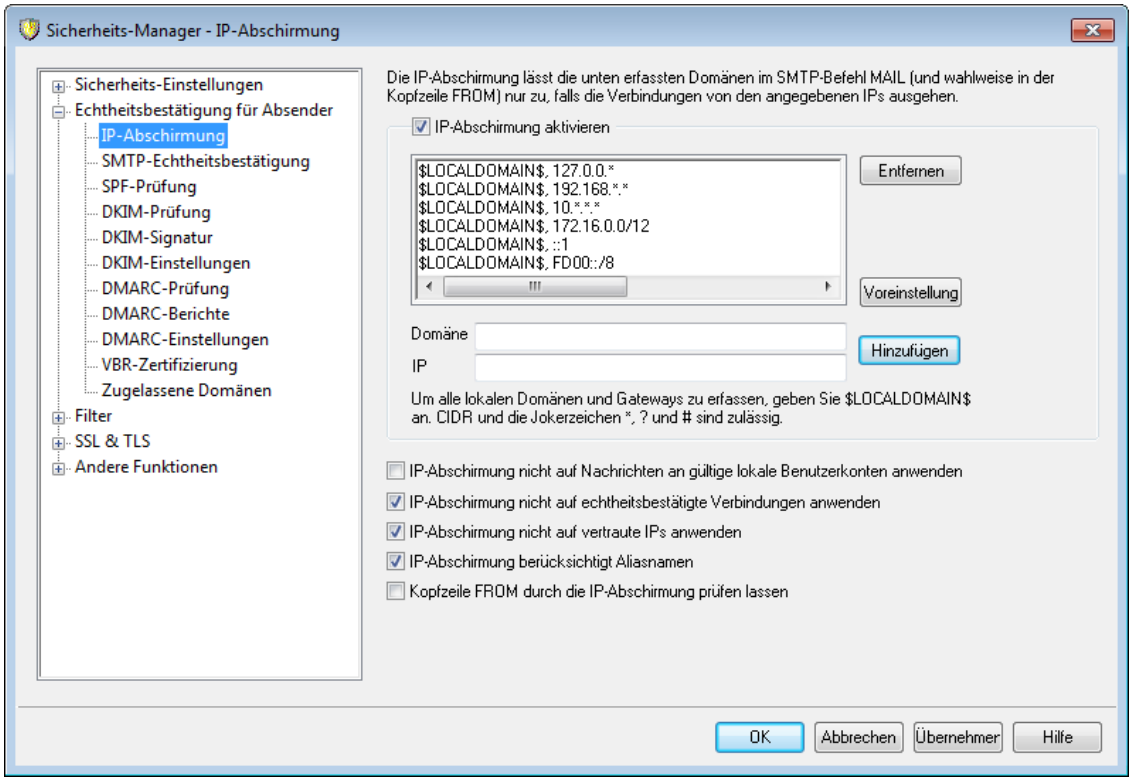
Kommentar
In dieses Feld können Sie einen Kommentar zu dem gerade bearbeiteten Eintrag eingeben.

Hinzufügen
Durch Anklicken dieses Steuerelements fügen Sie die neue IP-Adresse der Liste *Vertraute IP-Adressen* hinzu.

Entfernen
Durch Anklicken dieses Steuerelements entfernen Sie die ausgewählten Einträge aus der Liste *Vertraute IP-Adressen.*

4.1.2 Echtheitsbestätigung für Absender

4.1.2.1 IP-Abschirmung



Die IP-Abschirmung (erreichbar über Sicherheit » Sicherheits-Einstellungen » Echtheitsbestätigung für Absender) besteht aus einer Liste von Domänennamen und den zugehörigen IP-Adressen, der während des Protokolldialogs im Rahmen der Übermittlung des SMTP-Befehls `MAIL From` geprüft wird. Eine SMTP-Verbindung von einem Benutzer einer der hier erfassten Domänen wird nur dann zugelassen, wenn die IP-Adresse der Gegenstelle mit der erfassten Adresse übereinstimmt. Ist also z.B. der lokale Domänenname example.com, und benutzen die Rechner im lokalen LAN IP-Adressen von 192.168.0.0 bis 192.168.0.255, so kann durch diese Funktion ein IP-Schirm angelegt werden, welcher den Domänennamen example.com mit dem IP-Adressbereich 192.168.0.* verknüpft (Jokerzeichen sind zulässig). Wird dann eine SMTP-Verbindung zu MDaemon aufgebaut und sendet die Gegenstelle "`MAIL FROM <benutzer@example.com>`", wird die Verbindung nur zugelassen, falls die Adresse der Gegenstelle im Bereich 192.168.0.0 bis 192.168.0.255 liegt.

IP-Abschirmung aktivieren

Um die IP-Abschirmung abzuschalten, deaktivieren Sie diese Option. Die IP-Abschirmung ist die Liste der überwachten Domänennamen und der zugehörigen IP-Adressen, die bei Verbindungsversuchen auf Übereinstimmung geprüft werden.

Domänenname
Hier wird zunächst der Domänenname für die Verknüpfung mit einer bestimmten IP-Adresse eingetragen. Sie können auch das Makro `$LOCALDOMAIN$` nutzen, um alle lokalen Domänen einschließlich der Gateways zu erfassen. Falls Sie dieses Makro nutzen, muss die IP-Abschirmung nach Änderungen an den lokalen Domänen oder Gateways nicht von Hand aktualisiert werden. Per Voreinstellung werden der IP-Abschirmung Einträge hinzugefügt, die alle reservierten IP-Adressbereiche mit `$LOCALDOMAIN$` verknüpfen.

IP-Adresse
Hierher wird die IP-Adresse zu dem oben angegebenen Domänennamen eingetragen. Sie muss im Dezimalformat, getrennt durch Punkte, angegeben werden.

Hinzufügen
Klicken Sie auf *Hinzufügen*, um die Domäne und den IP-Adressbereich der Liste hinzuzufügen

Entfernen
Durch anklicken dieses Steuerelements werden die jeweils ausgewählten Einträge aus der Liste gelöscht.

IP-Abschirmung nicht auf Nachrichten an gültige lokale Benutzerkonten anwenden
Soll der Abgleich von Domäne und IP-Adresse nur bei Nachrichten an nicht-lokale oder ungültige lokale Benutzer durchgeführt werden, so ist diese Option auszuwählen. Sie verhindert, dass sich fremde Benutzer als Benutzer des eigenen Systems ausgeben, um etwa die Relais-Sperre zu umgehen, verringert aber gleichzeitig die Systemlast, weil Gegenstellen, die Nachrichten von außen an Benutzer des eigenen Systems senden, nicht geprüft werden. Falls Sie neben dieser Option auch die Option *IP-Abschirmung berücksichtigt Aliasnamen* aktivieren, werden Nachrichten an gültige Aliasnamen ebenfalls angenommen.

IP-Abschirmung nicht auf echtheitsbestätigte Verbindungen anwenden
Wenn diese Option aktiv ist, wirken die Beschränkungen der IP-Abschirmung nicht auf echtheitsbestätigte Benutzer. Nachrichten von echtheitsbestätigten Nutzern werden ohne Rücksicht auf die IP-Adressen angenommen, von denen aus die Benutzer eine Verbindung herstellen. Führt ein Benutzer keine Echtheitsbestätigung durch, und wird sein Verbindungsversuch oder Zugriff daher abgewiesen, so wird an den SMTP-Client die Meldung "Echtheitsbestätigung erforderlich" ("Authentication required") übermittelt. Der Benutzer erhält damit einen Hinweis darauf, dass er das Problem beseitigen kann, indem er seinen Mailclient so einrichtet, dass vor dem Versand von Nachrichten eine Echtheitsbestätigung durchgeführt wird. Diese Option ist per Voreinstellung eingeschaltet.

IP-Abschirmung nicht auf vertraute IPs anwenden
Diese Option bewirkt, dass die IP-Abschirmung für solche Verbindungen nicht wirksam wird, die von Vertrauten IP-Adressen 520 ausgehen. Diese Option ist per Voreinstellung aktiv.

IP-Abschirmung berücksichtigt Aliasnamen
Durch diese Option, die per Voreinstellung aktiv ist, wird die IP-Abschirmung veranlasst, im Rahmen der Prüfung von Domänen/IP-Zuordnungen auf Konflikte mit der IP-Abschirmung auch Adress-Aliasnamen auszuwerten. Die IP-Abschirmung löst dann die Aliasnamen in die Benutzerkonten auf, auf das sie

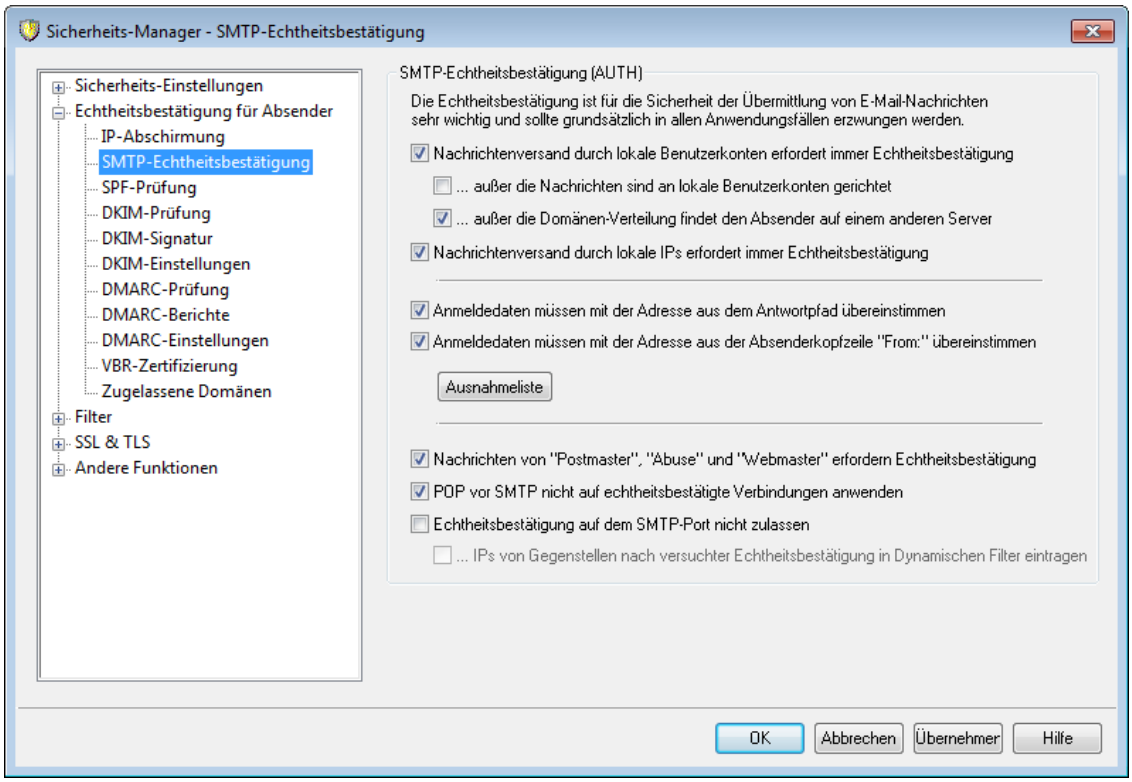
verweisen. Ist die Option nicht aktiv, so behandelt die IP-Abschirmung jeden Aliasnamen wie eine Adresse, die von dem Benutzerkonto unabhängig ist, auf das er verweist. Ist also die IP-Adresse eines Aliasnamens in der IP-Abschirmung gesperrt, wird die Nachricht abgewiesen. Diese Option ist im Abschnitt Optionen 829 des Konfigurationsdialogs für die Aliasnamen gespiegelt. Änderungen an der Einstellung wirken sich auf beide Konfigurationsdialoge aus.

Falls eingehende Nachrichten, die an gültige Adress-Aliasnamen gerichtet sind, von den Beschränkungen der IP-Abschirmung ausgenommen sein sollen, aktivieren Sie sowohl diese Option, als auch die Option *IP-Abschirmung nicht auf Nachrichten an gültige lokale Benutzerkonten anwenden* weiter oben.

Kopfzeile FROM durch die IP-Abschirmung prüfen lassen
Diese Option veranlasst die IP-Abschirmung, neben der Adresse, die bei Nachrichten aus dem Parameter zum SMTP-Befehl MAIL entnommen wird, auch die Adresse zu prüfen, die aus der Kopfzeile FROM der Nachricht entnommen wird. Diese Option ist per Voreinstellung abgeschaltet.

Die Nutzung dieser Option kann bei bestimmten Arten von Nachrichten, wie etwa bei Nachrichten aus Mailinglisten, Probleme verursachen. Sie sollten diese Option daher nur dann aktivieren, wenn Sie sich sicher sind, dass Sie sie auch wirklich benötigen.

4.1.2.2 SMTP-Echtheitsbestätigung



SMTP-Echtheitsbestätigung (AUTH)

Nachrichtenversand durch lokale Benutzerkonten erfordert immer Echtheitsbestätigung
Ist diese Option aktiv, und versendet ein Absender eine Nachricht, die nach ihrer Absenderadresse aus einer durch MDaemon verwalteten Domäne stammt, so muss sich der Absender mit Benutzername und Kennwort angemeldet haben, damit die Nachricht entgegengenommen und weitergeleitet wird. Diese Option ist per Voreinstellung aktiv.

...außer die Nachrichten sind an lokale Benutzerkonten gerichtet
Falls der Versand von Nachrichten durch lokale Benutzerkonten grundsätzlich nur nach Echtheitsbestätigung zulässig ist, kann es gewünscht sein, Nachrichten von lokalen Benutzern an lokale Benutzer von diesem Erfordernis auszunehmen. Dies wird durch Aktivieren dieser Option erreicht. Beachte: Dies kann etwa dann erforderlich sein, wenn einige Benutzer für eingehende und abgehende Nachrichten unterschiedliche Mailserver nutzen müssen.

...außer die Domänen-Verteilung findet den Absender auf einem anderen Server
Absender, die durch die Domänen-Verteilung 117 auf einem anderen Server gefunden werden, sind durch diese Option von der Option *Nachrichtenversand durch lokale Benutzerkonten erfordert immer Echtheitsbestätigung* oben ausgenommen. Diese Option ist per Voreinstellung aktiv. Falls Sie auch für solche Absender die Echtheitsbestätigung verlangen wollen, deaktivieren Sie diese Option.

Nachrichtenversand durch lokale IPs erfordert immer Echtheitsbestätigung
Diese Option bewirkt, dass für eingehende Nachrichten, die von lokalen IP-Adressen aus versandt werden, eine Echtheitsbestätigung immer verlangt wird. Wird keine Echtheitsbestätigung durchgeführt, oder schlägt sie fehl, so wird die betroffene Nachricht abgewiesen. Vertraute IPs 521 sind von diesem Erfordernis ausgenommen. Bei Neuinstallationen ist diese Option per Voreinstellung aktiv.

Anmeldedaten müssen mit der Adresse aus dem Antwortpfad übereinstimmen
Diese Option bewirkt, dass die Anmeldedaten für die SMTP-Echtheitsbestätigung mit den Daten übereinstimmen müssen, die im Antwortpfad der Nachricht enthalten sind. Diese Option ist per Voreinstellung aktiv. Falls Sie den Abgleich zwischen Anmeldedaten und Antwortpfad nicht wünschen, deaktivieren Sie diese Option. Damit Speicherung und Übermittlung von Gateway-Nachrichten nicht beeinträchtigt werden, ist im Konfigurationsdialog Globale Gateway-Einstellungen 254 eine Option enthalten, mit der per Voreinstellung die Gateway-Nachrichten vom Abgleich der Anmeldedaten ausgenommen werden.

Anmeldedaten müssen mit der Adresse aus der Asenderkopfzeile "From:" übereinstimmen
Diese Option bewirkt, dass die Anmeldedaten für die SMTP-Echtheitsbestätigung mit den Daten übereinstimmen müssen, die in der Absenderkopfzeile "From:" der Nachricht enthalten sind. Diese Option ist per Voreinstellung aktiv. Falls Sie den Abgleich zwischen Anmeldedaten und Absenderkopfzeile "From:" nicht wünschen, deaktivieren Sie diese Option. Damit Speicherung und Übermittlung von Gateway-Nachrichten nicht beeinträchtigt werden, ist im Konfigurationsdialog Globale Gateway-Einstellungen 254 eine Option enthalten, mit der per Voreinstellung die Gateway-Nachrichten vom Abgleich der Anmeldedaten ausgenommen werden.

Ausnahmeliste
In dieser Ausnahmeliste für Abgleich der Anmeldedaten mit Adressdaten können Sie E-Mail-Adressen erfassen, die von den beiden Optionen *"Anmeldedaten müssen mit ... übereinstimmen"* oben ausgenommen sind. Damit die Ausnahme von der Prüfung auf Übereinstimmung mit dem Antwortpfad wirksam wird, muss die Adresse aus dem **Antwortpfad** in der Ausnahmeliste erfasst sein. Damit die Ausnahme von der Prüfung auf Übereinstimmung mit der Absenderkopfzeile From wirksam wird, muss die Adresse aus der Absenderkopfzeile **From:** in der Ausnahmeliste erfasst sein.

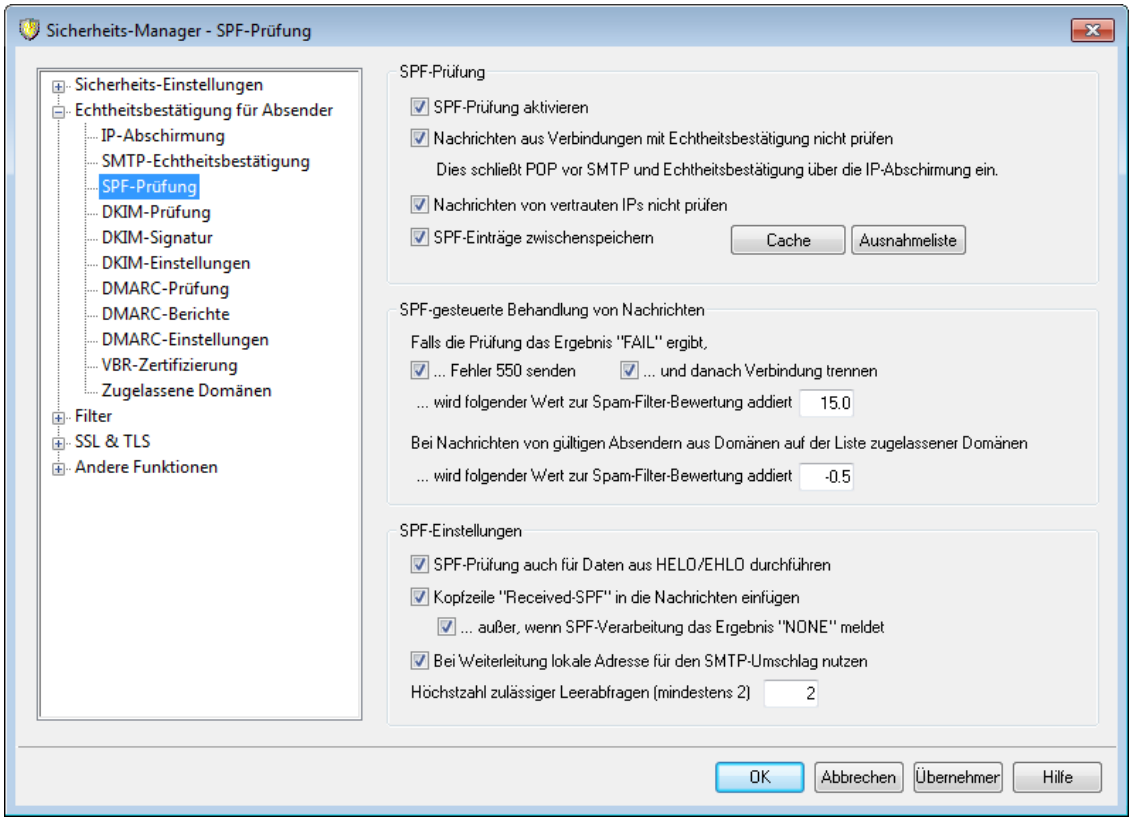
Nachrichten von "Postmaster", "Abuse" und "Webmaster" erfordern Echtheitsbestätigung
Ist diese Option aktiv, so nimmt MDaemon Nachrichten mit den Absenderadressen "postmaster@...", "abuse@..." und "webmaster@..." aus den eigenen Domänen nur dann zur Zustellung an, wenn diese Nachrichten über Verbindungen mit Echtheitsbestätigung übertragen wurden. Spam-Versender und Hacker wissen, dass diese Adressen auf vielen Systemen bestehen, und sie könnten daher versuchen, die Adressen als gefälschte Absenderadressen zu nutzen, um so Nachrichten über den Mailserver zu versenden. Diese Option verhindert solche missbräuchliche Nutzung, und zwar auch durch nicht berechtigte Benutzer der eigenen Domäne. Diese Option ist im Abschnitt Optionen 829 des Konfigurationsdialogs für die Aliasnamen gespiegelt. Änderungen an der Einstellung wirken sich auf beide Konfigurationsdialoge aus.

POP vor SMTP nicht auf echtheitsbestätigte Verbindungen anwenden
Bei Nutzung der Sicherheitsfunktion POP vor SMTP 519 können mithilfe dieser Option die Benutzer, die sich mit Benutzernamen und Kennwort echtheitsbestätigen, die Funktion POP vor SMTP umgehen. Sie müssen dann vor dem Versand von Nachrichten ihr Postfach nicht abgerufen haben.

Echtheitsbestätigung auf dem SMTP-Port nicht zulassen
Diese Option deaktiviert die Unterstützung für AUTH auf dem SMTP-Port. Wenn diese Option aktiv ist, wird AUTH nicht in der Antwort auf den Befehl EHLO angeboten, und es wird als unbekannter Befehl behandelt, falls ein SMTP-Client AUTH übermittelt. Die Einstellung "*...IPs von Gegenstellen nach versuchter Echtheitsbestätigung in Dynamischen Filter eintragen*" unten ist in den Konfigurationen besonders nützlich, in denen alle ordnungsgemäßen Benutzerkonten den MSA-Port oder einen anderen Post nutzen, um Nachrichten mit Echtheitsbestätigung zu übermitteln. In solchen Konfigurationen besteht die Annahme, dass Versuche zur Echtheitsbestätigung auf dem SMTP-Port von Angreifern ausgehen..

> **... IPs von Gegenstellen nach versuchter Echtheitsbestätigung in Dynamischen Filter eintragen**
> Ist die Option *Echtheitsbestätigung auf dem SMTP-Port nicht zulassen* oben aktiv, so bewirkt diese Option, dass alle IP-Adressen der Clients in den Dynamischen Filter eingetragen werden, die trotzdem auf dem SMTP-Port die Echtheitsbestätigung versuchen. Die Verbindungen werden dann jeweils sofort getrennt.

4.1.2.3 SPF-Prüfung



MDaemon unterstützt das Sender-Policy-Framework (SPF), um die Server von Absendern zu prüfen und gegen Fälschung von Absenderdaten (englisch "Spoofing") und Ausspähen von Daten und Informationen (englisch "Phishing") zu schützen. In beiden genannten Fällen versucht der Absender einer Nachricht, den Anschein zu erwecken, die Nachricht stamme von einem anderen Absender.

Für viele Domänen sind im Domain-Name-System (DNS) MX-Einträge veröffentlicht, in denen die Standorte erfasst sind, die Nachrichten für die Domänen empfangen dürfen. Diese Einträge geben aber keine Auskunft darüber, welche Rechner für die betreffende Domäne Nachrichten *versenden* dürfen. Das Sender-Policy-Framework (SPF) gestattet die Veröffentlichung von Absender-Einträgen für Domänen; diese geben Auskunft über die Rechner, die für eine Domäne Nachrichten versenden dürfen. MDaemon kann durch Prüfung eingehender Nachrichten über eine SPF-Abfrage festzustellen versuchen, ob der Server des Absenders für die Domäne, zu der er angeblich gehört, auch tatsächlich Nachrichten versenden darf. Daraus lässt sich dann feststellen, ob die Absender-Adresse gefälscht oder vorgetäuscht (englisch "spoofed") ist.

Die Einstellungen in diesem Konfigurationsdialog steuern die Nutzung des SPF durch Ihren Server.

Nähere Informationen über SPF erhalten Sie unter:

http://www.open-spf.org

SPF-Prüfung

SPF-Prüfung aktivieren
Ist diese Option aktiv, so prüft MDaemon für jede eingehende Nachricht, ob der sie übermittelnde Server berechtigt ist, für den in der Nachricht angegebenen

Absender Nachrichten zuzustellen. Hierzu fragt MDaemon die SPF-Daten aus dem DNS ab. Der Hostname, den MDaemon prüft, wird dem Parameter des Befehls `MAIL` entnommen, wie er während des SMTP-Protokolldialogs übermittelt wird. Die SPF-Prüfung ist per Voreinstellung abgeschaltet.

Nachrichten aus Verbindungen mit Echtheitsbestätigung nicht prüfen
Diese Einstellung bewirkt, dass für Verbindungen mit Echtheitsbestätigung keine SPF-Prüfung durchgeführt wird. Die Echtheitsbestätigung kann dabei über die SMTP-Echtheitsbestätigung 524, POP vor SMTP 519 oder die IP-Abschirmung 522 durchgeführt werden.

Nachrichten von vertrauten IPs nicht prüfen
Per Voreinstellung sind alle Nachrichten von vertrauten IP-Adressen 520 von der SPF-Prüfung ausgenommen

SPF-Einträge zwischenspeichern
Per Voreinstellung speichert MDaemon die SPF-Richtliniendaten für alle Domänen zwischen, die MDaemon aufgrund der DNS-Abfrage erhalten hat. Falls Sie nicht wünschen, dass diese Daten zwischengespeichert werden, deaktivieren Sie diese Option.

Cache
Ein Klick auf dieses Steuerelement öffnet den SPF-Cache.

Ausnahmeliste
Durch Anklicken dieses Steuerelements rufen Sie die Ausschlussliste für das SPF auf. In dieser Liste können Sie IP-Adressen, E-Mail-Adressen und Domänen erfassen, die von der SPF-Prüfung ausgenommen werden sollen. Bei E-Mail-Adressen wird dabei die im SMTP-Protokolldialog übermittelte E-Mail-Adresse ausgewertet, nicht aber die Absender-Kopfzeile ("From") der Nachrichten. Um eine Domäne in diese Ausnahmeliste aufzunehmen, stellen Sie dem Domänennamen die Zeichenkette "spf" voran. MDaemon bezieht die SPF-Einträge der so erfassten Domänen in alle SPF-Prüfungen ein und nutzt dazu den MDaemon-eigenen Tag "wlinclude:<Domäne>". Hierdurch können Sie auch etwa genutzte Backup-MX-Anbieter als gültige SPF-Quelle für alle Absender verwenden.

SPF-gesteuerte Behandlung von Nachrichten

Falls die Prüfung das Ergebnis "FAIL" ergibt,

...Fehler 550 senden
Diese Option bewirkt, dass der Server der Gegenstelle einen Fehler 550 meldet, falls das Ergebnis der SPF-Abfrage "Fail" ist.

...und danach Verbindung trennen
Diese Option bewirkt, dass der Mailserver die Verbindung mit der Gegenstelle sofort nach senden des Fehlers 550 trennt.#

...wird folgender Wert zur Spam-Filter-Bewertung addiert
Die hier angegebene Punktzahl wird der Spam-Bewertung einer Nachricht hinzugerechnet, wenn ihre Prüfung über SPF fehlschlägt.

Bei Nachrichten von gültigen Absendern auf der Liste zugelassener Domänen ...wird folgender Wert zur Spam-Filter-Bewertung addiert
Der hier angegeben Wert wird der Spam-Bewertung für die Nachricht hinzugerechnet, falls die SPF-Prüfung bestätigt, dass die Nachricht aus einer der in der Liste zugelassener Domänen[559] erfassten Domänen stammt.

Hier muss üblicherweise ein negativer Wert angegeben werden, damit der Wert der Spam-Bewertung für die zugelassenen Nachrichten verringert wird.

SPF Einstellungen

SPF-Prüfung auch für Daten aus HELO/EHLO durchführen
Diese Option bewirkt, dass die SPF-Prüfung auch für die Daten durchgeführt wird, die zu Beginn der SMTP-Verbindung mit den Befehlen HELO und EHLO übermittelt werden. Diese Option ist per Voreinstellung aktiv.

Kopfzeile "Received-SPF" in Nachrichten einfügen
Diese Option bewirkt, dass eine Kopfzeile "Received-SPF" in alle Nachrichten eingefügt wird.

...außer, wenn SPF-Verarbeitung das Ergebnis "NONE" meldet
Diese Option bewirkt, dass die Kopfzeile "Received-SPF" dann nicht in Nachrichten eingefügt wird, wenn das Ergebnis der SPF-Abfrage "none" lautet.

Bei Weiterleitung lokale Adresse für den SMTP-Umschlag nutzen
Diese Option bewirkt, dass MDaemon bei der Weiterleitung von Nachrichten eine lokale E-Mail-Adresse für den SMTP-Umschlag nutzt. Hierdurch werden einige Probleme bei der Weiterleitung von Nachrichten vermieden. Weitergeleitete Nachrichten werden üblicherweise unter der Adresse des ursprünglichen Absenders, nicht des weiterleitenden Empfängers, gesendet. In manchen Fällen kann die Nutzung einer lokalen Adresse statt der ursprünglichen nötig sein, damit der Server des Empfängers nicht die Absenderadresse irrtümlich für gefälscht hält. Diese Option ist per Voreinstellung aktiv.

Höchstzahl zulässiger Leerabfragen (mindestens 2)
Diese Option begrenzt die Anzahl der Leerabfragen, die MDaemon zulässt, bevor MDaemon einen dauerhaften Fehler meldet. Eine Leerabfrage ist eine Abfrage, auf die gemeldet wird, dass die Domäne nicht existiert oder keine Antworten gemeldet werden können. Der Wert muss mindestens 2 betragen.

4.1.2.4 DomainKeys Identified Mail

Der Begriff DomainKeys Identified Mail (DKIM) bezeichnet kryptografische Prüfverfahren für E-Mail-Nachrichten, der einer Fälschung der Absenderdaten in E-Mail-Nachrichten (dem sog. Spoofing) vorbeugen können. Da die meisten unerwünschten (Spam-) Nachrichten gefälschte Absenderangaben enthalten, kann DKIM zur Verringerung des Spam-Aufkommens stark beitragen, obwohl die zugehörigen Spezifikationen zunächst eigentlich nicht nur zur Spam-Abwehr entwickelt wurden. DKIM kann auch die Intaktheit eingehender Nachrichten sicherstellen und prüfen, ob der Inhalt einer Nachricht nach dem Versand durch den

Mail-Server, der sie signiert hat, noch geändert wurde, bevor sie dem eigenen System zuging. Kurz gefasst kann ein Server, der eine Nachricht empfängt, durch die kryptografische Prüfung über DKIM sicher stellen, dass die Nachricht von dem Mailserver stammt, der die Signatur erstellt hat, und dass ihr Inhalt während des Transports vom Absender zum Empfänger nicht verändert wurde.

DKIM verwendet Schlüsselpaare mit je einem öffentlichen und geheimen Schlüssel, um die Gültigkeit und Unversehrtheit der Nachrichten zur prüfen. Im DNS-Eintrag für den Mailserver des Absenders wird ein öffentlicher Schlüssel hinterlegt, und jede abgehende Nachricht wird durch den Mailserver mit dem zugehörigen geheimen Schlüssel signiert. Stellt ein Mailserver bei eingehenden Nachrichten fest, dass sie signiert sind, so ruft er den öffentlichen Schlüssel aus dem DNS-Eintrag des Mailservers des Absenders ab und vergleicht ihn mit der kryptografischen Signatur der eingegangenen Nachricht, um deren Gültigkeit zu prüfen. Schlägt diese Prüfung fehl, so geht der empfangende Server davon aus, dass die Nachricht eine gefälschte Absenderadresse enthält oder dass ihr Inhalt während des Transports geändert wurde. Eine Nachricht, deren Prüfung fehlgeschlagen ist, kann abgewiesen oder unter Anpassung der Spam-Bewertung angenommen werden.

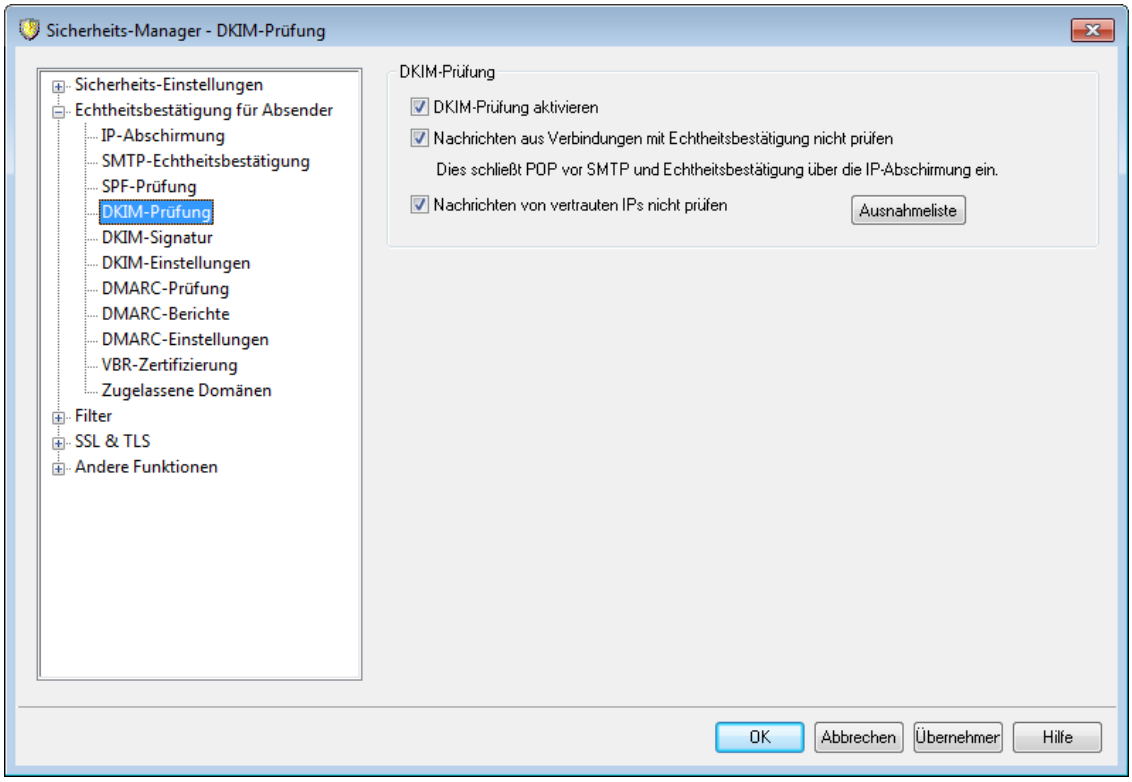
MDaemon kann mithilfe der Optionen im Abschnitt DKIM-Prüfung 531 für die kryptografische Prüfung eingehender Nachrichten eingerichtet werden. Um MDaemon so zu konfigurieren, dass abgehende Nachrichten über DomainKeys signiert werden, können die Optionen im Abschnitt DKIM-Signatur 533 verwendet werden. Sie erreichen beide Abschnitte im Menü Echtheitsbestätigung für Absender über Sicherheit » Sicherheits-Einstellungen » Echtheitsbestätigung für Absender. Die Haupt-Benutzeroberfläche 74 von MDaemon enthält eine Registerkarte DKIM (zugänglich über die Registerkarte Sicherheit), mit dessen Hilfe die Aktivität der DKIM in Echtzeit überwacht werden kann. Außerdem kann die Aktivität der KIM durch Nutzung der Optionen unter Einstellungen » Server-Einstellungen » Protokollierung » Optionen in das Protokoll aufgenommen werden.

Siehe auch:

DKIM-Prüfung 531
DKIM-Signatur 533
DKIM-Optionen 536

Nähere Informationen über DomainKeys Identified Mail erhalten Sie unter http://www.dkim.org/.

4.1.2.4.1 DKIM-Prüfung



Mithilfe der Einstellungen in diesem Konfigurationsdialog wird MDaemon so konfiguriert, dass DomainKeys-Identified-Mail-(DKIM)-Signaturen in eingehenden Nachrichten externer Absender geprüft werden. Ist diese Option aktiv, und enthält eine eingehende Nachricht eine kryptografische Signatur, so ruft MDaemon den zugehörigen öffentlichen Schlüssel aus dem DNS-Eintrag der Domäne ab, die in der Signatur bezeichnet ist. MDaemon prüft sodann anhand dieses Schlüssels die Gültigkeit der DKIM-Signatur der eingehenden Nachricht.

Besteht die DKIM-Signatur die Prüfung, so wird die Nachricht in den nächsten Arbeitsschritt des normalen Zustellvorgangs überführt. Steht die Domäne, die der Signatur entnommen wurde, auf der Liste zugelassener Domänen[559], so wirkt sich dies positiv auf die Spam-Filter-Bewertung der geprüften Nachricht aus.

Nähere Informationen über DKIM erhalten Sie unter http://www.dkim.org/.

Prüfung über DKIM

DKIM-Prüfung aktivieren
Diese Option aktiviert die Prüfung über DomainKeys-Identified-Mail für eingehende externe Nachrichten.

Nachrichten aus Verbindungen mit Echtheitsbestätigung nicht prüfen
Diese Option bewirkt, dass Nachrichten von der DKIM-Prüfung ausgenommen sind, wenn sie über eine Verbindung mit Echtheitsbestätigung übermittelt wurden. Die Echtheitsbestätigung kann dabei über die SMTP-Echtheitsbestätigung[524], POP vor SMTP[519] oder die IP-Abschirmung[522] erfolgen.

Verbindungen von vertrauten IPs nicht prüfen
Diese Option bewirkt, dass Verbindungen von vertrauten IP-Adressen[520] von der DKIM-Prüfung ausgenommen werden.

Ausnahmeliste
Ein Klick auf dieses Steuerelement öffnet die Ausschlussliste für die DKIM-Prüfung. Nachrichten von den IP-Adressen, die in dieser Liste erfasst sind, werden von der DKIM-Prüfung ausgenommen.

Kopfzeile Authentication-Results für Ergebnisse der Echtheitsbestätigung

Wird eine Nachricht über SMTP-AUTH, das SPF, DomainKeys-Identified-Mail oder DMARC echtheitsbestätigt, so fügt MDaemon in die Nachricht eine Kopfzeile "Authentication-Results" (Ergebnisse der Echtheitsbestätigung) in die Nachricht ein. Diese Kopfzeile enthält das Ergebnis der Echtheitsbestätigung. Falls MDaemon so konfiguriert ist, dass Nachrichten auch nach fehlgeschlagener Echtheitsbestätigung zur Zustellung entgegen genommen werden, so enthält die Kopfzeile Authentication-Results einen Fehlerkode, der Aufschluss gibt, warum die Echtheitsbestätigung fehlgeschlagen ist. Die Fehlerkodes wie auch die Kopfzeile selbst, müssen, da sie jeweils international genormt sind, in englischer Sprache in die Nachrichten eingefügt werden.

Diese Kopfzeile und die Protokolle zur Echtheitsbestätigung, die in diesem Abschnitt beschrieben sind, werden über die Internet Engineering Task Force (IETF) laufend weiterentwickelt. Nähere Informationen hierüber sind auf der Website der IETF unter http://www.ietf.org/ verfügbar.

DKIM-Kopfzeilen in Nachrichten für Mailinglisten

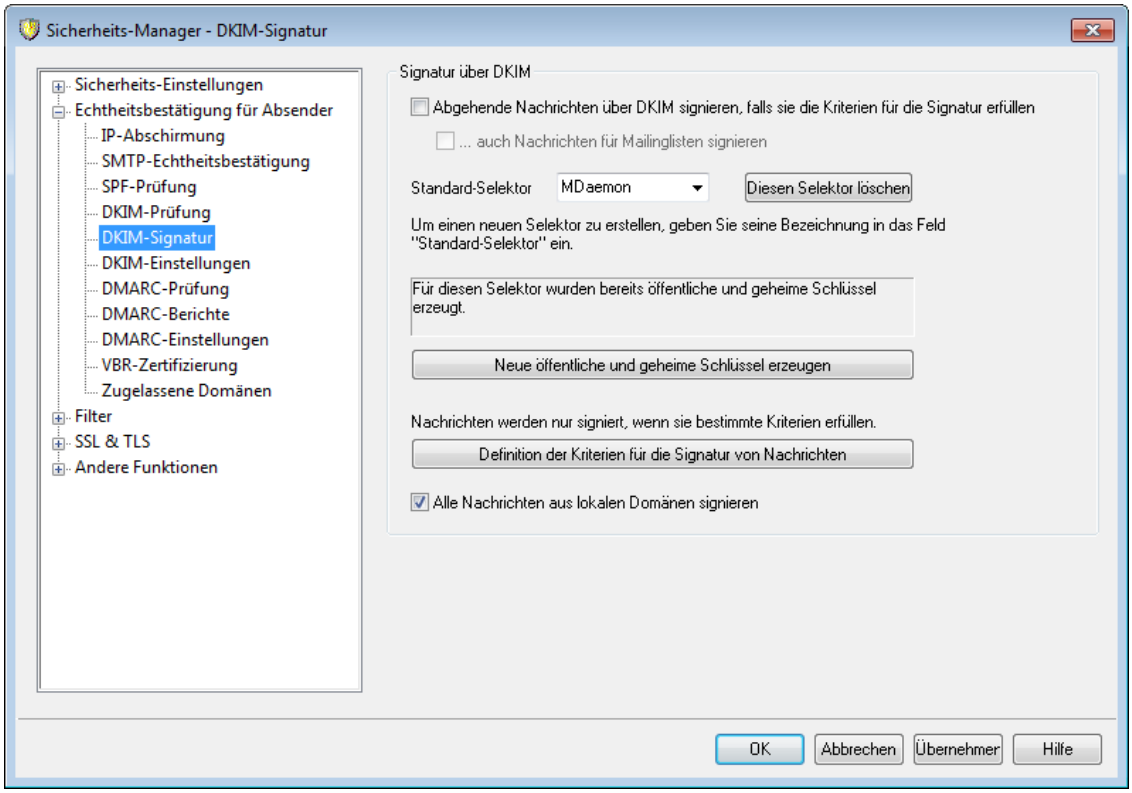
MDaemon entfernt DKIM-Signaturen grundsätzlich aus eingehenden Nachrichten, da die Signaturen durch Änderungen an den Kopfzeilen oder dem Inhalt der Nachrichten während der Verarbeitung durch Mailinglisten kompromittiert werden können. Soll MDaemon die Signaturen aus Listennachrichten nicht entfernen, so kann dies durch Bearbeiten des folgenden Eintrags in der Datei `MDaemon.ini` erreicht werden:

```
[DomainKeys]
StripSigsFromListMail=No (Nein, Voreinstellung ist "Yes", Ja)
```

Siehe auch:

DomainKeys Identified Mail 529
DKIM-Signatur 533
DKIM-Einstellungen 536

4.1.2.4.2 DKIM-Signatur



Mithilfe der Optionen im Konfigurationsdialog DKIM-Signatur können Sie MDaemon so konfiguriert werden, dass abgehende Nachrichten, die bestimmte Kriterien erfüllen, über DKIM signiert werden; Sie können auch die Kriterien bestimmen, die die Nachrichten erfüllen müssen. In diesem Dialog werden auch die Selektoren und die öffentlichen und geheimen Schlüssel für die Signatur über DKIM konfiguriert und erstellt. Beim ersten Programmstart werden ein vorgegebener Standard-Selektor ("MDaemon") und ein Schlüsselpaar aus öffentlichem und privatem Schlüssel automatisch erstellt. Alle Schlüssel sind einmalig, sie können bei zwei verschiedenen Systemen niemals gleich sein, und zwar auch dann nicht, wenn die Bezeichnung der Selektoren übereinstimmen sollte. Per Voreinstellung werden die Schlüssel mit einer Länge von 2.048 Bit erzeugt. Diese Schlüssellänge gewährleistet bereits ein hohes Maß an Sicherheit.

Signatur über DKIM

Abgehende Nachrichten über DKIM signieren, falls sie die Kriterien für die Signatur erfüllen
Diese Option bewirkt, dass abgehende Nachrichten über DomainKeys-Identified-Mail kryptografisch signiert werden. Eine abgehende Nachricht wird aber auch bei aktivierter Option nur dann signiert, falls sie die Kriterien erfüllt, die nach einem Klick auf das Steuerelement *Definition der Kriterien für die Signatur von Nachrichten* festgelegt werden können, und falls MDaemon sie über eine echtheitsbestätigte SMTP-Verbindung (SMTP-AUTH) erhalten hat. Es ist auch eine Aktion für den Inhaltsfilter verfügbar, "*Mit DKIM-Selektor signieren...*", mit deren Hilfe Nachrichten gezielt signiert werden können.

...Nachrichten für Mailinglisten signieren
Diese Option bewirkt, dass MDaemon alle abgehenden Nachrichten für Mailinglisten kryptografisch signiert. Da MDaemon hierbei jeweils alle

Nachrichten aller Mailinglisten signiert, müssen die Mailinglisten nicht mithilfe des Konfigurationsdialogs *Definition der Kriterien für die Signatur von Nachrichten* zur kryptografischen Signatur vorgesehen werden.

Die Signatur von Nachrichten für Mailinglisten macht eine Bearbeitung jeder einzelnen Nachricht durch den Inhaltsfilter erforderlich, der die Listenpost dazu aufspalten muss. Dies kann bei besonders großen Mailinglisten oder solchen mit starkem Nachrichtenverkehr die Systemleistung beeinträchtigen.

Standard-Selektor
Aus diesem Rollmenü muss der Selektor ausgewählt werden, dessen Schlüsselpaar zum Signieren abgehender Nachrichten genutzt werden soll. Falls ein neues Schlüsselpaar für einen anderen Selektor erstellt werden soll, muss der gewünschte Name für den neuen Selektor in das Feld eingetragen werden. Durch Anklicken des Steuerelements *Neue öffentliche und geheime Schlüssel erzeugen* werden die Schlüssel erzeugt. Falls nicht alle Nachrichten mit dem selben Selektor signiert werden sollen, müssen die Selektoren den zu signierenden Nachrichten durch den Menüpunkt *Definition der Kriterien für die Signatur von Nachrichten* oder über Regeln des Inhaltsfilters der oben genannten Aktion "*Mit DKIM-Selektor signieren...*" zugeordnet werden.

Diesen Selektor löschen
Durch Anklicken dieses Steuerelements können Sie einen Selektor löschen. Folgen Sie dazu den Anweisungen, die nach dem Anklicken angezeigt werden.

Neue öffentliche und geheime Schlüssel erzeugen
Ein Klick auf dieses Steuerelement erzeugt für den oben ausgewählten Selektor ein neues Schlüsselpaar mit je einem öffentlichen und geheimen Schlüssel. Nachdem das Schlüsselpaar erzeugt wurde, wird die Datei `dns_readme.txt` erzeugt und automatisch angezeigt. Diese Datei enthält beispielhafte DKIM-Daten, die nötig sind, um im DNS der eigenen Domäne die DKIM-Richtlinie und den öffentlichen Schlüssel für den angegebenen Selektor zu hinterlegen. Die Datei enthält Beispiele sowohl für den Test- als auch für den Regelbetrieb und für die Angabe, ob alle oder nur bestimmte Nachrichten aus der eigenen Domäne signiert sein müssen. Falls DKIM und der Selektor im Testbetrieb eingesetzt werden, muss die Information im Abschnitt "Testing" für Richtlinie oder Selektor genutzt werden, je nach dem, ob Richtlinie oder Selektor getestet werden. Für den Regelbetrieb müssen die Daten verwendet werden, die mit "Not Testing" gekennzeichnet sind.

Alle Schlüssel werden im Format `PEM` abgelegt; die Selektoren und die Schlüsseldateien werden im Verzeichnis `\MDaemon\Pem` nach folgendem Schema gespeichert:

```
\MDaemon\Pem\<Selector>\rsa.public - öffentlicher Schlüssel für
diesen Selektor
\MDaemon\Pem\<Selector>\rsa.private - geheimer Schlüssel für
diesen Selektor
```

Die Dateien in diesen Ordnern sind selbst nicht verschlüsselt oder verborgen. Da sie aber geheime RSA-Schlüssel enthalten, die unbefugten Personen keinesfalls zugänglich

sein sollen, muss der Systemverwalter mithilfe des Betriebssystems oder geeigneter Hilfsprogramme entsprechende Schutzmaßnahmen für die Ordner und die in ihnen enthaltenen Unterordner und Dateien ergreifen.

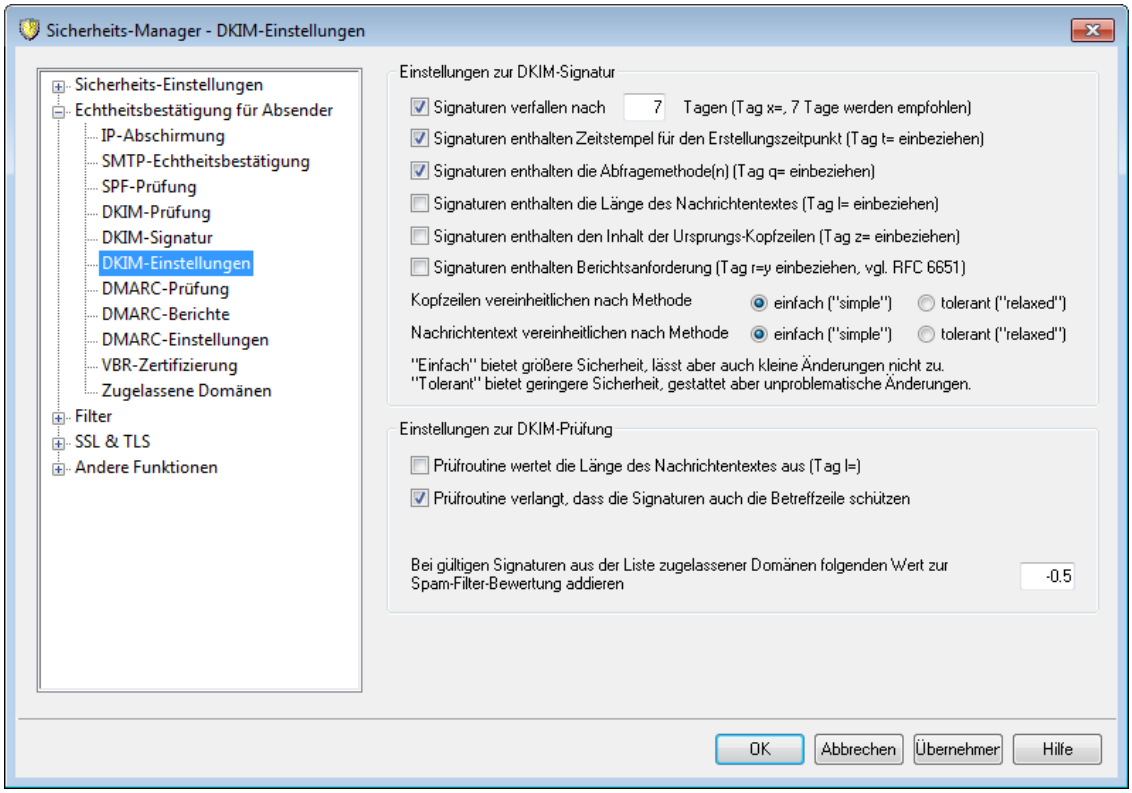
Definition der Kriterien für die Signatur von Nachrichten
Ist die Option zur Signatur abgehender Nachrichten aktiv, so kann durch Anklicken dieses Steuerelements die Datei `DKSign.dat` bearbeitet werden; Sie enthält die Liste der Domänen und Adressen, anhand derer MDaemon feststellt, ob eine abgehende Nachricht signiert werden soll. Für jede in der Liste erfasste Adresse muss auch angegeben werden, ob eine Nachricht von dieser Adresse stammen oder an sie gerichtet sein muss, damit die Nachricht signiert wird. Neben den üblicherweise verwendeten Kopfzeilen `To` und `From` sind auch weitere Kopfzeilen zulässig, wie etwa "`Reply-To`" und "`Sender`". Wahlweise kann für jeden Eintrag ein Selektor definiert werden, die zur Signatur der entsprechenden Nachrichten verwendet wird. Schließlich kann wahlweise eine Domäne als Erstellerin der Signatur angegeben werden; diese dient als Wert des Attributes "d=" in der Signatur-Kopfzeile. Dies kann etwa sinnvoll sein, wenn Nachrichten mehrerer Subdomänen signiert werden. In diesem Fall kann das Attribut "d=" dem Server des Mailempfängers mitteilen, dass die DKIM-Schlüssel im DNS-Eintrag nur einer Domäne zu finden sind. Alle Schlüssel können dann in einem Datensatz verwaltet werden, getrennte Datensätze für alle Subdomänen sind nicht erforderlich. Jokerzeichen sind für Domänennamen und E-Mail-Adressen zulässig.

Alle Nachrichten aus lokalen Domänen signieren
Diese Option bewirkt, dass alle Nachrichten, die aus lokalen Domänen stammen, vor dem Versand signiert werden. Bei Nutzung dieser Option müssen die lokalen Domänen in die Liste der Domänen, deren Nachrichten signiert werden sollen (d.h. die Datei `DKSign.dat`), nur noch dann eingetragen werden, wenn bestimmte Selektoren oder der Tag "d=" für die Signatur der Nachrichten bestimmter Domänen verwendet werden sollen. Diese Option ist per Voreinstellung aktiv.

Siehe auch:

DomainKeys Identified Mail 529
DKIM-Einstellungen 536
DKIM-Prüfung 531

4.1.2.4.3 DKIM-Einstellungen



Einstellungen zur DKIM-Signatur

Signaturen verfallen nach [xx] Tagen (Tag x=, 7 Tage werden empfohlen)
Sollen DKIM-Signaturen nur während einer bestimmten Frist als gültig betrachtet werden können, so muss diese Option aktiv sein. Die Dauer in Tagen, für welche die Signatur gültig sein soll, muss angegeben werden. Die Prüfung von Nachrichten mit verfallenen Signaturen schlägt immer fehl. Diese Option steuert den Tag "x=" der Signatur. Die voreingestellte Gültigkeit beträgt sieben Tage.

Signaturen enthalten Zeitstempel für den Erstellungszeitpunkt (Tag t= einschließen)
Diese Option bewirkt, dass der Zeitstempel für die Erstellungszeit der Signatur (Tag "t=") in die Signatur aufgenommen wird. Die Option ist per Voreinstellung aktiv.

Signaturen enthalten die Abfragemethode(n) (Tag q= einbeziehen)
Diese Option bewirkt, dass der Tag Abfragemethode ("query method") in die DKIM-Signaturen aufgenommen wird (z.B. q=dns).

Signaturen enthalten die Länge des Nachrichtentexts (Tag l= einbeziehen)
Diese Option bewirkt dass die Länge des Nachrichtentexts durch den Tag Nachrichtenlänge ("body length count") in die DKIM-Signaturen aufgenommen wird.

Signaturen enthalten den Inhalt der Ursprungs-Kopfzeilen (Tag z= einbeziehen)
Diese Option bewirkt, dass der Tag "z=" in die DKIM-Signaturen aufgenommen wird. Dieser Tag enthält eine Kopie der ursprünglichen Kopfzeilen der Nachricht; er kann daher die Signaturen beträchtlich vergrößern.

Signaturen enthalten Berichtsanforderung (Tag r=y einbeziehen)
Diese Option bewirkt, dass der Tag "r=y" in die DKIM-Signaturen aufgenommen wird. Server, die einen solchen Tag befolgen, erkennen daraus, dass der Absender einen AFRF-Fehlerbericht (Fehlerbericht über fehlgeschlagene Echtheitsbestätigung) erhalten will, falls Nachrichten geprüft werden, die zwar angeblich aus der in ihnen bezeichneten Domäne stammen, bei denen aber die DKIM-Prüfung fehlschlägt. Damit Sie diese Fehlerberichte erhalten können, müssen Sie den DNS-Einträgen der betreffenden Domäne entweder einen TXT-Eintrag mit den DKIM-Berichtsinformationen hinzufügen. Nähere Informationen hierzu finden Sie im RFC 6651, *Extensions to DomainKeys Identified Mail (DKIM) for Failure Reporting (Erweiterungen zur Fehlerberichterstattung für DomainKeys Identified Mail)*. Die diese Option erst nach Anpassung der DNS-Einträge genutzt werden kann, ist sie per Voreinstellung abgeschaltet.

Vereinheitlichung

Die Vereinheitlichung (englisch "Canonicalisation") ist ein Prozess, mit dessen Hilfe Kopfzeilen und Nachrichtentext einer Nachricht in ein bestimmtes "Standard-Format" umgesetzt werden, bevor die DKIM-Signatur erstellt wird. Dies ist erforderlich, da manche E-Mail-Server und –Relais während Verarbeitung und Transport der Nachrichten Veränderungen an ihnen vornehmen, die zwar unbedeutend sind, die Signatur der Nachrichten aber dennoch kompromittieren können. Es stehen derzeit zwei Methoden für die Vereinheitlichung im Zusammenhang mit DKIM-Signaturen zur Verfügung – einfach ("simple") und tolerant ("relaxed"). Die einfache Methode ist die strengste; sie lässt fast keine Veränderungen an den Nachrichten zu. Die tolerante Methode lässt verschiedene unbedeutende Änderungen zu.

Kopfzeilen vereinheitlichen nach Methode einfach ("simple"), tolerant ("relaxed")
Hier wird die Methode zur Vereinheitlichung ausgewählt, die bei Erstellung der Signatur auf die Kopfzeilen der Nachricht angewendet wird. Die einfache Methode gestattet keine Änderungen an den Kopfzeilen. Die tolerante Methode gestattet die Umsetzung der Namen der Kopfzeilen in Kleinschreibung, die Zusammenfassung mehrere aufeinander folgender Leerzeichen zu einem und andere unwesentliche Änderungen. Sie gestattet keine Änderungen an den Inhalten der Kopfzeilen. Per Voreinstellung ist die einfache Methode aktiv.

Nachrichtentext vereinheitlichen nach Methode einfach ("simple"), tolerant ("relaxed")
Hier wird die Methode zur Vereinfachung ausgewählt, die bei Erstellung der Signatur auf den Nachrichtentext angewendet wird. Die einfache Methode ignoriert Leerzeilen am Ende des Nachrichtentexts, andere Änderungen sind nicht zugelassen. Die tolerante Methode gestattet Leerzeilen am Ende des Nachrichtentexts, ignoriert Leerzeichen am Beginn der Zeilen, fasst mehrere aufeinander folgende Leerzeichen zu einem einzelnen Leerzeichen zusammen und gestattet andere unwesentliche Änderungen. Per Voreinstellung ist die einfache Methode aktiv.

Einstellungen zur DKIM-Prüfung

Prüfroutine wertet die Länge des Nachrichtentextes aus (Tag l=)
Ist diese Option aktiv, so beachtet MDaemon die Länge des Nachrichtentexts, wenn sie in den DKIM-Signaturen eingehender Nachrichten enthalten ist. Überschreitet die Nachrichtenlänge den Wert, der in dem entsprechenden Tag angegeben ist, so prüft MDaemon nur den Anteil, der der Länge aus der Signatur entspricht, der Rest der Nachricht wird nicht geprüft. Eine solche Veränderung

der Nachrichtengröße und der nicht geprüfte Teil der Nachricht erscheinen verdächtig, da sie darauf hindeuten, dass der Nachricht etwas hinzugefügt wurde. Ist die tatsächliche Größe der Nachricht geringer als in dem entsprechenden Tag angegeben, so schlägt die Prüfung der Signatur fehl (es wird das Ergebnis "FAIL" gemeldet). Eine geringere Größe deutet darauf hin, dass Teile der Nachricht gelöscht wurden.

Prüfroutine verlangt, dass die Signaturen auch die Betreffzeile schützen
Diese Option bewirkt, dass von DKIM-Signaturen eingehender Nachrichten verlangt wird, dass sie auch die Betreffzeile schützen müssen.

Bei gültigen Signaturen auf der Liste zugelassener Domänen folgenden Wert zur Spam-Filter-Bewertung addieren
Der hier angegebene Wert wird der Bewertung des Spam-Filters einer mit DKIM signierten Nachricht nach dem Ergebnis "Pass" hinzugefügt, falls die aus der Signatur entnommene Domäne in der Liste zugelassener Domänen[559] erfasst ist. Wird die Signatur einer Nachricht erfolgreich überprüft, und ist die Domäne aus der Signatur aber nicht in der Liste zugelassener Domänen erfasst, so wird die Bewertung des Spam-Filters nicht geändert. Die geprüfte Signatur hat dann zwar keine Auswirkung auf die Spam-Bewertung, die Nachricht durchläuft den Spam-Filter aber wie üblich und wird auch durch den Spam-Filter bewertet.

Hier sollte üblicherweise ein negativer Wert angegeben werden, sodass die Spam-Bewertung für Nachrichten verringert wird, wenn sie gültige kryptografische Signaturen enthalten und die Domäne aus der Signatur in der Liste zugelassener Domänen[559] erfasst ist Die Voreinstellung für diesen Wert beträgt –0.5.

Siehe auch:

DomainKeys Identified Mail[529]
DKIM-Prüfung[531]
DKIM-Signatur[533]

4.1.2.5 DMARC

DMARC steht für "Domain-based Message Authentication, Reporting & Conformance" (domänengestützte Echtheitsbestätigung von Nachrichten, Berichte und Überwachung der Richtlinienkonformität). DMARC ist eine Spezifikation, die missbräuchliche Nutzung von E-Mail-Nachrichten, etwa durch Spam und Phishing, eindämmen soll. DMARC soll insbesondere gefälschten Absenderangaben in der Absenderkopfzeile `From:` (Von:) der Nachrichten entgegenwirken, die Empfänger von Nachrichten über deren Absender täuschen. DMARC gestattet es den Inhabern von Domänen, das Domain Name System (DNS) zu nutzen, um Empfänger über ihre DMARC-Richtlinien zu informieren. Diese Richtlinien bestimmen die Behandlung solcher Nachrichten durch die Server der Nachrichtenempfänger, die angeblich von einem bestimmten Absender stammen, deren Absender aber nicht echtheitsbestätigt werden kann und daher möglicherweise falsch angegeben ist. Die Server der Nachrichtenempfänger rufen die Richtlinien über eine DNS-Abfrage während der Verarbeitung eingehender Nachrichten ab. Die Richtlinien können bestimmen, dass der Server des Nachrichtenempfängers Nachrichten in Quarantäne geben oder abweisen soll, falls sie nicht richtlinienkonform sind, oder dass der Server keine Maßnahmen ergreifen soll (die Nachricht wird dann normal verarbeitet). Die DNS-

Einträge für DMARC können auch Anforderungen enthalten, die Server von Nachrichtenempfängern zum Versand bestimmter Berichte veranlassen. Solche Berichte können die Anzahl der eingehenden Nachrichten angeben, die angeblich aus einer Domäne stammen, die Anteile der erfolgreich und nicht erfolgreich echtheitsbestätigten Nachrichten und Einzelheiten über fehlgeschlagene Echtheitsbestätigungsversuche. Die Leistungsmerkmale für die DMARC-Berichte können insbesondere helfen, die Effizienz der eigenen Echtheitsbestätigungsmaßnahmen für E-Mail-Nachrichten zu beurteilen, und sie geben Auskunft darüber, wie oft die eigene Domäne durch Dritte für gefälschte Absenderangaben missbraucht wird.

Der Abschnitt Echtheitsbestätigung für Absender im Menü Sicherheitseinstellungen ist in drei Konfigurationsdialoge zur Steuerung der DMARC-Prüfung und der Berichte in MDaemon untergliedert: DMARC-Prüfung, DMARC-Berichte und DMARC-Optionen.

DMARC-Prüfung 546

Während der DMARC-Prüfung fragt MDaemon die DMARC-Richtlinien durch eine DNS-Abfrage ab; diese Abfrage bezieht sich auf die Domäne in der Absenderkopfzeile `From:` (Von:) jeder eingehenden Nachricht. Die Abfrage prüft zunächst, ob die Domäne DMARC nutzt und ruft bejahendenfalls den DNS-Eintrag für DMARC 540 ab. Diese DNS-Eintrag enthält die DMARC-Richtlinie und verwandte Informationen. DMARC nutzt außerdem das SPF 527 und DKIM 531, um jede eingehende Nachricht zu prüfen, und die Prüfung durch SPF 527 oder DKIM 531 muss erfolgreich verlaufen, damit auch die DMARC-Prüfung erfolgreich sein kann. Besteht eine Nachricht diese Prüfungen, so wird sie durch den üblichen Filter- und Zustellvorgang in MDaemon normal weiterbearbeitet. Besteht eine Nachricht die Prüfung nicht, dann richtet sich ihre weitere Behandlung nach den DMARC-Richtlinien der angeblichen Absenderdomäne und danach, wie MDaemon für die Behandlung solcher Nachrichten konfiguriert ist.

Besteht eine Nachricht die DMARC-Prüfung nicht, und ist für die angebliche Absenderdomäne die DMARC-Richtlinie "`p=none`" veröffentlicht, so ergreift MDaemon keine Abwehrmaßnahmen, und die Nachricht wird normal weiterverarbeitet. Ist für die angebliche Absenderdomäne jedoch eine restriktive DMARC-Richtlinie veröffentlicht, also "`p=quarantine`" oder "`p=reject`", dann kann MDaemon die Nachricht automatisch in den Spam-Ordner des Empfängers (z.B. Junk-E-Mail) leiten. Sie können auch bestimmen, dass MDaemon die Nachricht dann abweist, wenn für die angebliche Absenderdomäne die Richtlinie "`p=reject`" veröffentlicht ist. In Nachrichten, für deren angebliche Absenderdomänen restriktive Richtlinien veröffentlicht sind, fügt MDaemon je nach veröffentlichter Richtlinie die Kopfzeilen "`X-MDDMARC-Fail-policy: quarantine`" oder "`X-MDDMARC-Fail-policy: reject`" ein. Hiermit können Sie durch den Inhaltsfilter weitere Maßnahmen auslösen, die diese Kopfzeilen auswerten und Nachrichten beispielsweise in einen besonderen Ordner zur genaueren Untersuchung leiten.

Die DMARC-Prüfung ist per Voreinstellung aktiv und wird für die meisten Einsatzgebiete von MDaemon empfohlen.

DMARC-Berichte 549

Die DMARC-Einträge, die MDaemon aus dem DNS abfragt, können Tags enthalten, durch die der Domäneninhaber anzeigt, dass er bestimmte zusammengefasste Statistik- und Fehlerberichte über die DMARC-gestützte Behandlung solcher Nachrichten erhalten will, die angeblich aus seiner Domäne stammen. Die Optionen im Konfigurationsdialog DMARC-Berichte bestimmen, ob Ihr System die angeforderten Arten von Berichten versenden soll, und welche Metadaten die Berichte enthalten

sollen. Zusammengefasste Berichte werden jeden Tag um Mitternacht (UTC-Zeit) gesendet. Fehlerberichte werden für jede Nachricht dann gesendet, wenn eine fehlgeschlagene Prüfung den Fehlerbericht auslöst. Alle Berichte werden als XML-Dateien in ZIP-Archiven versandt, die als Dateianlage an die Berichtsnachrichten angehängt werden. Es stehen verschiedene Auswertungsprogramme zur Verfügung, mit deren Hilfe die Empfänger die Berichte einsehen und auswerten können.

Per Voreinstellung versendet MDaemon keine zusammengefassten Berichte und keine Fehlerberichte. Falls Sie solche Berichte versenden lassen wollen, aktivieren Sie die entsprechenden Optionen im Konfigurationsdialog DMARC-Berichte.

DMARC-Einstellungen 553

Der Konfigurationsdialog DMARC-Optionen enthält Optionen zur Aufnahme bestimmter Daten in DKIM-Berichte, zur Protokollierung von DNS-Einträgen für DMARC und zur Aktualisierung der Liste öffentlicher Domänenendungen, die MDaemon für DMARC nutzt.

Wechselwirkung zwischen DMARC-Prüfung und Mailinglisten

DMARC soll sicherstellen, dass die Domäne in der Absenderkopfzeile `From:` eingehender Nachrichten nicht gefälscht ist sondern dem wirklichen Absender entspricht. DMARC muss daher überprüfen, ob der Server, der die Nachricht übermittelt, zum Versand von Nachrichten für die Absenderdomäne auch wirklich berechtigt ist. Bei Mailinglisten kann dies zu einem besonderen Problem führen. Es ist nämlich bei Mailinglisten üblich, dass diese die Listennachrichten für alle, auch fremde, Listenmitglieder versenden, dass dabei die Absenderkopfzeile `From:` unverändert bleibt und noch die ursprüngliche Domäne des Absenders enthält. Empfängt ein Server eine solche Listennachricht, und führt er eine DMARC-Prüfung für die Nachricht aus, dann stellt er hierbei fest, dass ein Server die Nachricht versandt hat, der eigentlich gar nicht berechtigt ist, für die Domäne in der Absenderkopfzeile `From:` Nachrichten zu versenden. Ist für die Domäne in der Absenderkopfzeile `From:` eine restriktive DMARC-Richtlinie veröffentlicht, so kann dies dazu führen, dass der Server des Empfängers die Listennachricht in Quarantäne gibt oder sogar abweist. Außerdem kann in bestimmten Fällen der Empfänger der Listennachricht automatisch aus der Mailingliste entfernt werden. Um dieses Problem zu umgehen, ersetzt MDaemon den Inhalt der Absenderkopfzeile `From:` in Listennachrichten dann durch die E-Mail-Adresse der Mailingliste, wenn für die Domäne des Absenders eine restriktive DMARC-Richtlinie veröffentlicht ist. Sie können MDaemon aber auch so konfigurieren, dass Listennachrichten aus Domänen mit restriktiven DMARC-Richtlinien abgewiesen werden. Diese Option macht es Benutzern aus Domänen mit restriktiven DMARC-Richtlinien aber unmöglich, Nachrichten in der Mailingliste zu veröffentlichen. Die Option zum Ersetzen der Absenderkopfzeile `From:` ist im Abschnitt Kopfzeilen 281 des Editors für Mailinglisten enthalten. Die Option, Nachrichten abzuweisen, ist im Abschnitt Einstellungen 278 enthalten.

Die Nutzung von DMARC für eigene MDaemon-Domänen

Die Nutzung von DMARC für eigene Domänen, die die Server der Nachrichtenempfänger in die Lage versetzt, DMARC zur Prüfung solcher Nachrichten einzusetzen, die angeblich aus den eigenen Domänen stammen, hängt von mehreren Voraussetzungen ab. Sie müssen zunächst sicherstellen, dass Sie für die betroffenen Domänen gültige DNS-Einträge für SPF und DKIM erstellt haben. SPF oder DKIM oder beide Verfahren zugleich müssen funktionsfähig eingerichtet sein,

damit DMARC nutzbar ist. Falls Sie DKIM nutzen, müssen Sie auch die Signatur von Nachrichten über DKIM 533 konfigurieren, damit MDaemon die Nachrichten der betroffenen Domänen signiert. Sie müssen außerdem für die betroffenen Domänen DNS-Einträge für DMARC anlegen. Diese Einträge sind `TXT`-Einträge in einem bestimmten, vorgegebenen Format, die die Server der Nachrichtenempfänger abfragen, um Informationen über die DMARC-Richtlinie und verschiedene weitere Parameter zu erhalten. Solche weiteren Parameter sind insbesondere die Art der Echtheitsbestätigung, die Sie nutzen, die Festlegung, ob Sie zusammengefasste Berichte erhalten wollen, und die E-Mail-Adresse, an die die Berichte gesendet werden sollen.

Ist DMARC richtig eingerichtet, und erhalten Sie XML-Berichte für DMARC, so stehen Ihnen eine Reihe von Online-Werkzeugen zur Verfügung, mit deren Hilfe Sie die Berichte auswerten und mögliche Probleme erkennen können. Zur einfacheren Handhabung steht im Verzeichnis \MDaemon\App\ auch ein Hilfsprogramm namens DMARC Reporter zur Verfügung. Nähere Informationen über seine Nutzung enthält in englischer Sprache die Datei DMARCReporterReadMe.txt.

Erstellen eines DMARC-Ressourceneintrags vom Typ TXT

Nachfolgend finden Sie einen Überblick über grundlegende und häufig genutzte Bestandteile eines DMARC-Eintrags. Nähere Informationen und Hinweise zu fortgeschrittenen Konfigurationsmöglichkeiten erhalten Sie auf der Website www.dmarc.org.

Feld "Owner" (Inhaber)

Das Feld "Owner" (es wird auch als "Name" oder "left-hand" bezeichnet) im DMARC-Ressourceneintrag muss immer den Inhalt **`_dmarc`**haben. Falls Sie die Domäne oder Subdomäne angeben wollen, auf die sich der Eintrag bezieht, so können Sie das Format **`_dmarc.domänen.name`** hierfür nutzen.

Ein Beispiel hierzu:

Ein DMARC-Eintrag für die Domäne **example.com**

`_dmarc IN TXT "v=DMARC1;p=none"`
Dieser Eintrag wirkt für E-Mail-Nachrichten von benutzer@example.com und allen Subdomänen von example.com, also beispielsweise benutzer@support.example.com.

`_dmarc.support.example.com IN TXT "v=DMARC1;p=none"`
Dieser Eintrag wirkt nur für E-Mail-Nachrichten von benutzer@support.example.com, nicht jedoch beispielsweise für benutzer@example.com.

`_dmarc.support IN TXT "v=DMARC1;p=none"`
Dieser Eintrag wirkt für E-Mail-Nachrichten von benutzer@support.example.com, benutzer@a.support.example.com, benutzer@a.b.support.example.com und so weiter.

Tags und Parameter für die DMARC-Einträge

Zwingend erforderliche Tags

Tag	Parameter	Erläuterung

v=	**DMARC1**	Dieser Tag bestimmt die Version. Er muss der erste Tag in dem Textfeld des Ressourceneintrags sein. DMARC-Tags sind üblicherweise unabhängig von Groß- und Kleinschreibung; dies gilt aber nicht für diesen Tag. Er muss immer in Großbuchstaben gesetzt sein: **DMARC1**. Ein Beispiel hierzu: `_dmarc IN TXT "v=DMARC1;p=none"`
p=	**none** **quarantine** **reject**	Dieser Tag bestimmt die Richtlinie (p steht für policy). Er muss der zweite Tag in dem Textfeld des Ressourceneintrags sein und auf den Tag **v=** folgen. **p=none** (keine) bedeutet, dass der Server des Nachrichtenempfängers auf Grundlage der DMARC-Prüfung keine Aktion vornehmen soll. Nachrichten, die die DMARC-Prüfung nicht bestehen, sollen aufgrund der nicht bestandenen DMARC-Prüfung nicht in Quarantäne gegeben oder abgewiesen werden. Sie können aber aus anderen Gründen in Quarantäne gegeben oder abgewiesen werden, etwa wegen einer Spam-Bewertung oder aufgrund anderer Sicherheitsprüfungen als DMARC. Die Nutzung der Richtlinie **p=none** wird bisweilen als Überwachungs- oder Beobachtungsmodus bezeichnet, da die Richtlinie mit dem Tag **rua=** gemeinsam verwendet werden kann, um zusammengefasste Berichte über die Nachrichten zu erhalten, gleichzeitig aber Abwehrmaßnahmen nach dem Fehlschlagen von DMARC-Prüfungen zu verhindern. Solange Sie Ihre DMARC-Implementation noch nicht ausführlich und gründlich getestet haben und sicher sind, dass Sie Abwehrmaßnahmen verlangen sollen (wie etwa durch Nutzung der restriktiveren Richtlinie **p=quarantine**), sollten Sie diese Richtlinie nutzen. **p=quarantine** (Quarantäne) bedeutet, dass der Server des Nachrichtenempfängers Nachrichten als verdächtig behandeln soll, falls diese laut Absenderkopfzeile **From:** aus Ihrer Domäne stammen, aber die DMARC-Prüfung nicht bestehen. Je nach der Konfiguration des Servers des Nachrichtenempfängers können solche Nachrichten zusätzlichen Prüfmaßnahmen unterworfen werden, auch können Sie in die Spam-Ordner der Empfänger einsortiert, an einen anderen Server geleitet oder weiteren Maßnahmen unterworfen werden. **p=reject** (abweisen) bedeutet, dass der Server des Nachrichtenempfängers alle Nachrichten abweisen soll, die die DMARC-Prüfung nicht bestehen. Manche Server sind unter Umständen so konfiguriert, dass sie solche Nachrichten entgegen der Richtlinie annehmen, sie dann aber in Quarantäne geben oder zusätzlichen Prüfmaßnahmen unterwerfen. Diese Richtlinie ist die restriktivste Richtlinie; Sie sollten sie nur dann einsetzen,

		wenn sie endgültig sicher sind, dass Ihre E-Mail-Richtlinien und ihre Infrastruktur sowie die E-Mail-Dienste, die Sie nutzen wollen, und die Benutzerkonten richtig eingerichtet sind und funktionieren. Wollen Sie Ihren Benutzern beispielsweise gestatten, Mitglieder in Mailinglisten von Drittanbietern zu werden, Weiterleitungsdienste zu nutzen, Funktionen zum "Teilen" oder Weiterleiten von Website-Inhalten oder vergleichbare Leistungsmerkmale zu nutzen, dann führt die Nutzung der Richtlinie **p=reject** mit hoher Wahrscheinlichkeit dazu, dass auch legitime Nachrichten abgewiesen werden. Es kann auch dazu führen, dass Benutzer automatisch aus Mailinglisten entfernt oder gar nicht erst in sie aufgenommen werden. Ein Beispiel hierzu: `_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:dmarc-berichte@example.net"`

Optionale Tags
Die nachfolgend aufgeführten Tags sind wahlfrei. Enthält ein Ressourceneintrag diese Tags nicht, dann werden die jeweiligen Vorgaben angenommen und verwendet

Tag	Parameter	Erläuterung
sp=	**none** **quarantine** **reject** — **Vorgabe:** Falls **sp=** nicht verwendet wird, wirkt der Tag **p=** auf die Domäne und die Subdomänen.	Dieser Tag bestimmt die Richtlinien, die für Subdomänen der Domäne wirken sollen, auf die sich der DMARC-Ressourceneintrag bezieht. Wird dieser Tag beispielsweise in einem Eintrag verwendet, der sich auf example.com bezieht, dann wirkt die Richtlinie aus dem Tag **p=** auf E-Mail-Nachrichten aus der Domäne example.com, und die Richtlinie aus dem Tag **sp=** wirkt auf E-Mail-Nachrichten aus Subdomänen von example.com, etwa mail.example.com. Wird dieser Tag nicht verwendet, so wirkt der Tag **p=** auf die Domäne und alle ihre Subdomänen. Ein Beispiel hierzu: `_dmarc IN TXT "v=DMARC1;p=quarantine;sp=reject"`

rua=	Kommagetrennte Liste der E-Mail-Adressen, an die zusammengefasste DMARC-Berichte gesendet werden sollen. Die Adressen müssen als URIs im Format **mailto:benutzer@example.com** angegeben werden.
	—
	Vorgabe: keine
	Falls dieser Tag nicht verwendet wird, werden keine zusammengefassten Berichte gesendet.
		Dieser Tag zeigt an, dass Sie zusammengefasste DMARC-Berichte von den Servern der Nachrichtenempfänger erhalten wollen, bei denen Nachrichten mit Adressen aus Ihrer Domäne in der Absenderkopfzeile **From:** eingehen. Geben Sie mindestens eine E-Mail-Adresse als URI im Format **mailto:benutzer@example.com** an, und trennen Sie mehrere URIs durch Kommata.
		Ein Beispiel hierzu:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:benutzer01@example.com,mailto:benutzer02@example.com"`
		Die E-Mail-Adressen gehören üblicherweise zu der Domäne, auf die sich der DMARC-Ressourceneintrag bezieht. Falls Sie die Berichte an eine E-Mail-Adresse in einer anderen Domäne senden wollen, dann muss die DNS-Zonendatei dieser anderen Domäne einen besonderen DMARC-Eintrag enthalten, der anzeigt, dass die Domäne die fremden DMARC-Berichte akzeptiert.
		Ein Beispielseintrag für die Domäne example.com:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:nicht-lokaler-benutzer@example.net"`
		Hierzu der erforderliche Eintrag für die Domäne example.net:
		`example.com._report._dmarc TXT "v=DMARC1"`

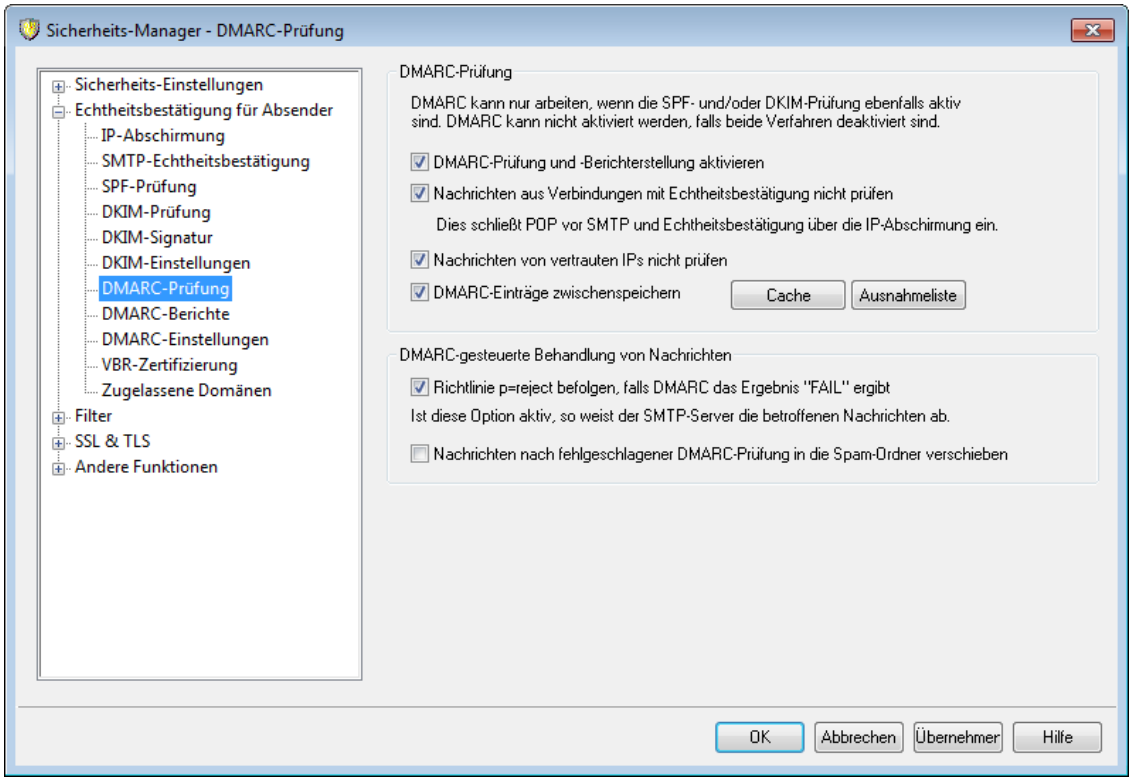
ruf=	Kommagetrennte Liste der E-Mail-Adressen, an die DMARC-Fehlerberichte gesendet werden sollen. Die Adressen müssen als URIs im Format **mailto:benutzer@example.com** angegeben werden.
	—
	Vorgabe: keine
	Falls dieser Tag nicht verwendet wird, werden keine DMARC-Fehlerberichte gesendet.
		Dieser Tag zeigt an, dass Sie DMARC-Fehlerberichte von den Servern der Nachrichtenempfänger erhalten wollen, bei denen Nachrichten mit Adressen aus Ihrer Domäne in der Absenderkopfzeile **From:** eingehen. Damit die Fehlerberichte versandt werden, müssen die Bedingungen aus dem Tag **fo=** erfüllt sein. Wird der Tag **fo=** nicht verwendet, so werden per Voreinstellung die DMARC-Fehlerberichte dann versendet, wenn bei einer Nachricht alle DMARC-Prüfungen (also SPF und DKIM) fehlschlagen. Geben Sie mindestens eine E-Mail-Adresse als URI im Format **mailto:benutzer@example.com** an, und trennen Sie mehrere URIs durch Kommata.
		Ein Beispiel hierzu:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:dmarc-failures@example.com"`
		Die E-Mail-Adressen gehören üblicherweise zu der Domäne, auf die sich der DMARC-Ressourceneintrag bezieht. Falls Sie die Berichte an eine E-Mail-Adresse in einer anderen Domäne senden wollen, dann muss die DNS-Zonendatei dieser anderen Domäne einen besonderen DMARC-Eintrag enthalten, der anzeigt, dass die Domäne die fremden DMARC-Berichte akzeptiert.
		Ein Beispielseintrag für die Domäne example.com:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:non-local-user@example.net"`
		Hierzu der erforderliche Eintrag für die Domäne example.net:
		`example.com._report._dmarc TXT "v=DMARC1"`

Ausführliche Informationen über die Spezifikation für DMARC erhalten Sie auf der Website www.dmarc.org.

Siehe auch:

DMARC-Prüfung 546
DMARC-Berichte 549
DMARC-Einstellungen 553
Mailinglisten » Einstellungen 278
Mailinglisten » Kopfzeilen 281

4.1.2.5.1 DMARC-Prüfung



DMARC-Prüfung

DMARC-Prüfung und Berichterstellung aktivieren
Ist diese Option aktiv, so fragt MDaemon die DMARC-Einträge aus dem DNS für die Domänen ab, die in den Absenderkopfzeilen `From:` der eingehenden Nachrichten als Absender genannt sind. Falls Sie die entsprechenden Optionen im Konfigurationsdialog DMARC-Berichte 549 aktivieren, sendet MDaemon auch zusammengefasste Berichte und Fehlerberichte. DMARC nutzt SPF 527 und DKIM 531 zur Echtheitsbestätigung von Nachrichten. Es muss daher mindestens eines dieser beiden Leistungsmerkmale aktiv sein, bevor DMARC genutzt werden kann. Die DMARC-Prüfung und die DMARC-Berichte sind per Voreinstellung aktiv. Ihre Nutzung empfiehlt sich in den meisten Einsatzbedingungen.

Falls Sie DMARC deaktivieren, kann dies Ihre Benutzer einem erhöhten Aufkommen an Spam, Phishing-Nachrichten und überhaupt Nachrichten mit gefälschten Absenderinformationen aussetzen. Es kann auch dazu führen, dass manche Listennachrichten Ihres Systems durch andere Server abgewiesen werden, und dass Benutzer aus Ihren Listen automatisch entfernt werden. Sie sollten DMARC daher nur dann deaktivieren, wenn Sie sich ganz sicher sind, dass Sie dieses Leistungsmerkmal nicht benötigen.

Nachrichten aus Verbindungen mit Echtheitsbestätigung nicht prüfen
Per Voreinstellung führt MDaemon für Nachrichten, die über Verbindungen mit Echtheitsbestätigung empfangen wurden, keine DMARC-Prüfung aus. Mögliche

Arten der Echtheitsbestätigung sind dabei die SMTP-Echtheitsbestätigung[524], POP vor SMTP[519] und die IP -Abschirmung[522].

Nachrichten von vertrauten IPs nicht prüfen
Per Voreinstellung führt MDaemon für Nachrichten, die von Vertrauten IP-Adressen[521] aus eingehen, keine DMARC-Prüfung aus. Um die DMARC-Prüfung auch für solche Nachrichten auszuführen, deaktivieren Sie diese Option.

DMARC-Einträge zwischenspeichern
Per Voreinstellung speichert MDaemon die Daten aus den DMARC-Ressourceneinträgen zwischen, die im Rahmen der DNS-Abfrage übermittelt wurden. Diese Zwischenspeicherung erhöht die Verarbeitungsgeschwindigkeit, wenn Nachrichten mit derselben Absenderdomäne kurz hintereinander verarbeitet werden.

Cache
Durch Anklicken dieses Steuerelements öffnen Sie die Datendatei für den DMARC-Cache, in der die DMARC-Ressourceneinträge zwischengespeichert sind.

Ausnahmeliste
Durch Anklicken dieses Steuerelements öffnen Sie die Ausnahmeliste für die DMARC-Prüfung. Eine DMARC-Prüfung unterbleibt für Nachrichten, die von IP-Adressen empfangen wurden, die in dieser Liste erfasst sind.

Die DMARC-Prüfung berücksichtigt auch die VBR-Zertifizierung[556] und die Liste zugelassener Domänen[559]. Diese Leistungsmerkmale können Nachrichten aufgrund der DKIM-Identifikationsmerkmale und der SPF-Pfade als Nachrichten behandeln, die von vertrauenswürdigen Quellen stammen. Geht beispielsweise eine Nachricht ein, die die DMARC-Prüfung nicht besteht, und hat diese Nachricht aber eine gültige DKIM-Signatur einer Domäne auf der Liste zugelassener Domänen, dann wird die Nachricht keinen aufgrund von DMARC zu treffenden Abwehrmaßnahmen unterworfen. Sie wird so behandelt, wie wenn die DMARC-Richtlinie "p=none" anwendbar wäre. Entsprechendes gilt, wenn die Prüfung des Absenders über das SPF bestätigt, dass die Nachricht von einer Domäne auf der Liste zugelassener Domänen stammt.

DMARC-gesteuerte Behandlung von Nachrichten

Richtlinie p=reject befolgen, falls DMARC das Ergebnis "FAIL" meldet
Diese Option ist per Voreinstellung aktiv. Sie bewirkt, dass die DMARC-Richtlinie `p=reject` befolgt wird, falls sie für die Domäne in der Absenderkopfzeile `From:` einer eingehenden Nachricht veröffentlicht ist und die Nachricht die DMARC-Prüfung nicht besteht. Die Nachricht wird dann während der SMTP-Verbindung abgewiesen.

Ist diese Option deaktiviert, und besteht eine Nachricht die DMARC-Prüfung nicht, so weist MDaemon die Nachricht nicht ab, sondern fügt die Kopfzeile "`X-MDDMARC-Fail-policy: reject`" in die Nachricht ein. Sie können dann mithilfe des Inhaltsfilters Aktionen für Nachrichten durchführen lassen, die diese Kopfzeile

enthalten, etwa die Nachricht zur genaueren Prüfung in einen bestimmten Ordner verschieben. Sie können auch mithilfe der Option "*Nachrichten nach Fehlschlagen der DMARC-Prüfung in die Spam-Ordner verschieben*" solche Nachrichten in die Spam-Ordner der Empfänger verschieben lassen.

Auch wenn diese Option deaktiviert ist, können Nachrichten aus anderen Gründen als der DMARC-Prüfung abgewiesen werden, etwa, wenn die Spam-Bewertung 679 den Schwellwert überschreitet.

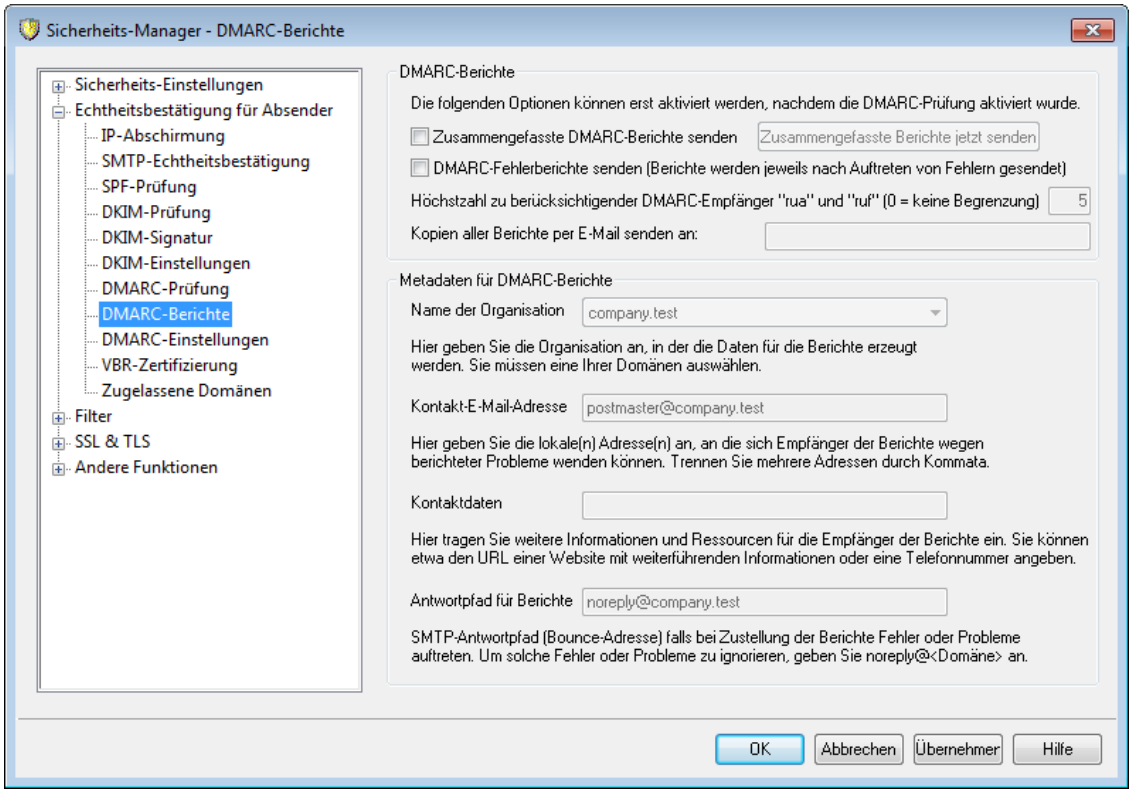
Nachrichten nach Fehlschlagen der DMARC-Prüfung in die Spam-Ordner verschieben
Diese Option bewirkt, dass MDaemon Nachrichten automatisch in die Spam-Ordner der Empfänger verschiebt, falls sie die DMARC-Prüfung nicht bestehen. Falls dieser Ordner für einen Empfänger noch nicht besteht, legt MDaemon den Ordner automatisch an, sobald er zum ersten Mal gebraucht wird.

Ist diese Option aktiv, so werden Nachrichten nur dann verschoben, wenn für die Domäne in der Absenderkopfzeile `From:` eine restriktive DMARC-Richtlinie veröffentlicht ist, also p=quarantine oder p=reject. Ist für die Domäne die Richtlinie p=none veröffentlicht, dann geht MDaemon davon aus, dass DMARC nur beobachtend betrieben wird, und dass keine Abwehrmaßnahmen getroffen werden sollen.

Siehe auch:

DMARC 538
DMARC-Berichte 549
DMARC-Einstellungen 553
Mailinglisten » Einstellungen 278
Mailinglisten » Kopfzeilen 281
Zugelassene Domänen 559

4.1.2.5.2 DMARC-Berichte



Die DMARC-Einträge, die MDaemon aus dem DNS abfragt, können Tags enthalten, durch die der Domäneninhaber anzeigt, dass er bestimmte zusammengefasste Statistik- und Fehlerberichte über die DMARC-gestützte Behandlung solcher Nachrichten erhalten will, die angeblich aus seiner Domäne stammen. Die Optionen im Konfigurationsdialog DMARC-Berichte bestimmen, ob Ihr System die angeforderten Arten von Berichten versenden soll, und welche Metadaten die Berichte enthalten sollen. Die Optionen in diesem Konfigurationsdialog stehen nur zur Verfügung, wenn die Option "*DMARC-Prüfung und -Berichterstellung*" im Konfigurationsdialog DMARC-Prüfung 546 ebenfalls aktiv ist. Die Spezifikation für DMARC verlangt außerdem due Nutzung von STARTTLS 579, sofern die Empfänger der Berichte dieses Verfahren unterstützen. Sie sollten daher STARTTLS aktivieren, falls das möglich ist.

DMARC-Berichte

Zusammengefasste DMARC-Berichte senden
Diese Option bewirkt, dass MDaemon zusammengefasste DMARC-Berichte an die Domänen sendet, die sie anfordern. Ergibt eine DNS-Abfrage nach den DMARC-Ressourceneinträgen der Domäne in der Absenderkopfzeile `From:` einer eingehenden Nachricht, dass der DMARC-Eintrag der Domäne den Tag "`rua=`" enthält (z.B. `rua=mailto:dmarc-berichte@example.com`), so zeigt dies an, dass der Inhaber der Domäne zusammengefasste DMARC-Berichte erhalten will. MDaemon speichert dann die DMARC-Daten für die Domäne und die eingehenden Nachrichten, die einen Absender der Domäne ausweisen. MDaemon speichert außerdem die E-Mail-Adressen, an die die Berichte gesandt werden sollen, das auf die Nachrichten angewendete Prüfverfahren (SPF, DKIM oder beide), das Prüfergebnis (bestanden oder nicht bestanden), den übermittelnden Server mit IP-Adresse, die angewendete DMARC-Richtlinie und weitere relevante Daten. Jeden Tag um Mitternacht (UTC-Zeit) nutzt MDaemon die gespeicherten Daten, um für die erfassten Domänen Berichte zu erstellen und sie an die angegebenen

E-Mail-Adressen zu senden. Nach dem Versand löscht MDaemon die DMARC-Daten und beginnt die Speicherung erneut.

MDaemon unterstützt nicht den DMARC-Tag "ri=", der das Intervall für den Versand der zusammengefassten Berichte festlegt. MDaemon sendet die zusammengefassten Berichte stets um Mitternacht (UTC-Zeit) an alle Domänen, für die DMARC-Daten seit dem letzten Versand neu gespeichert wurden.

Zusammengefasste Berichte jetzt senden
Durch Anklicken dieses Steuerelements können Sie die zusammengefassten Berichte auf Grundlage der derzeit gespeicherten DMARC-Daten erstellen und sofort versenden lassen. Die Berichte werden sofort versandt, und die DMARC-Daten werden anschließend gelöscht; das Verfahren gleicht dem Verfahren, das MDaemon um Mitternacht (UTC-Zeit) automatisch ausführt. Nach dem sofortigen Versand und der Löschung der DMARC-Daten beginnt MDaemon erneut mit der Speicherung der Daten und erstellt und versendet die Berichte wieder um Mitternacht (UTC-Zeit) oder wenn das Steuerelement das nächste Mal angeklickt wird, je nachdem, welches Ereignis früher eintritt.

Um aus den gespeicherten DMARC-Daten die Berichte automatisch zu erstellen und zu versenden und die Daten danach zu löschen, muss MDaemon um Mitternacht (UTC-Zeit) ausgeführt werden. Läuft MDaemon zu diesem Zeitpunkt nicht, so werden keine Berichte erstellt und die DMARC-Daten nicht gelöscht; dies wird auch nicht nachgeholt, wenn MDaemon wieder gestartet wird. Die Speicherung der DMARC-Daten wird fortgesetzt, sobald MDaemon wieder läuft, die Berichte werden aber erst wieder um Mitternacht (UTC-Zeit) oder beim nächsten Anklicken des Steuerelements "*Zusammengefasste Berichte jetzt senden*" erstellt und versandt.

DMARC-Fehlerberichte senden (Berichte werden jeweils nach Auftreten von Fehlern gesendet)
Diese Option bewirkt, dass MDaemon DMARC-Fehlerberichte an die Domänen sendet, die sie anfordern. Ergibt eine DNS-Abfrage nach den DMARC-Ressourceneinträgen der Domäne in der Absenderkopfzeile `From:` einer eingehenden Nachricht, dass der DMARC-Eintrag der Domäne den Tag "ruf=" enthält (z.B. `ruf=mailto:dmarc-fehler@example.com`), so zeigt dies an, dass der Inhaber der Domäne DMARC-Fehlerberichte erhalten will. Anders als die zusammengefassten Berichte werden die Fehlerberichte in Echtzeit unmittelbar nach dem Auftreten der sie auslösenden Fehler erstellt, und sie enthalten ausführliche Einzelheiten über den Vorgang und die Fehler, die zum Fehlschlagen der Prüfung geführt haben. Die Administratoren der betroffenen Domänen können diese Berichte verwenden, um die Fehler zu analysieren, Probleme in ihren E-Mail-Systemen und deren Konfiguration zu beseitigen und andere Probleme festzustellen, etwa auf laufende Phishing-Angriffe aufmerksam zu werden.

Der Tag "fo=" im DMARC-Eintrag einer Domäne bestimmt, auf welche Arten von Fehlern hin ein Fehlerbericht erstellt wird. Per Voreinstellung wird ein Fehlerbericht nur erstellt, wenn sowohl die SPF- wie auch die DKIM-Prüfung

fehlschlagen. Domänen können aber verschiedene Parameter im Tag "fo=" angeben und damit bestimmen, dass sie Berichte nur erhalten wollen, falls SPF fehlschlägt, falls DKIM fehlschlägt, oder falls eine Kombination der Prüfverfahren fehlschlägt. Aus diesem Grund können nach dem Fehlschlagen der DMARC-Prüfung für eine Nachricht auch mehrere Fehlerberichte erstellt werden. Ihre Zahl hängt von der Anzahl der Empfänger im Tag "ruf=", den Parameter im Tag "fo=" sowie der Anzahl fehlgeschlagener Versuche zur Echtheitsbestätigung ab, die während der Prüfung der Nachricht aufgetreten sind. Falls Sie die Anzahl der Empfänger begrenzen wollen, an die MDaemon die Berichte sendet, können Sie dazu die Option "*Höchstzahl zu berücksichtigender DMARC-Empfänger 'rua' und 'ruf'*" weiter unten nutzen.

Zur Festlegung des Formats der Fehlerberichte beachtet MDaemon nur den Tag rf=afrf (Berichte über Fehler in der Echtheitsbestätigung mithilfe des Formats für Berichte über missbräuchliche Nutzung ARF); dies entspricht auch der Vorgabe bei DMARC. Alle Berichte werden in diesem Format gesendet, und zwar auch dann, wenn der DMARC-Eintrag der betreffenden Domäne den Tag rf=iodef enthält.

Für die DMARC-Fehlerberichte unterstützt MDaemon folgende Standards vollständig: RFC 5965: Ein erweiterbares Format für E-Mail-Feedback-Berichte, RFC 6591: Berichte über Fehler in der Echtheitsbestätigung mithilfe des Formats für Berichte über missbräuchliche Nutzung ARF, RFC 6652: Berichte über Fehler bei der SPF-Verarbeitung mithilfe des Formats für Berichte über missbräuchliche Nutzung ARF, RFC 6651: Erweiterungen für Fehlerberichte bei DomainKeys Identified Mail (DKIM) und RFC 6692: Ursprungsports im Format für Berichte über missbräuchliche Nutzung ARF.

Verlangt der DMARC-Tag "fo=" auch Berichte über Fehler bei der SPF-Prüfung, so sendet MDaemon SPF-Fehlerberichte nach RFC 6522. Aus diesem Grund müssen die Erweiterungen für diese Spezifikation im SPF-Eintrag der Domäne enthalten sein. SPF-Fehlerberichte werden nicht unabhängig von der DMARC-Verarbeitung gesendet; sie werden ferner nicht gesendet, falls die Erweiterungen nach RFC 6522 fehlen.

Verlangt der DMARC-Tag "fo=" auch Berichte über Fehler bei der DKIM-Prüfung, so sendet MDaemon DKIM-Fehlerberichte nach RFC 6651. Aus diesem Grund müssen die Erweiterungen für diese Spezifikation in der Kopfzeile für die DKIM-Signatur enthalten sein, und für die Domäne muss ein gültiger TXT-Eintrag zu den DKIM-Berichten im DNS veröffentlicht sein. Die DKIM-Fehlerberichte werden nicht unabhängig von der DMARC-Verarbeitung gesendet; sie werden ferner nicht gesendet, falls die Erweiterungen nach RFC 6651 fehlen.

Höchstzahl zu berücksichtigender DMARC-Empfänger "rua" und "ruf" (0 = keine Begrenzung)
Falls Sie die Anzahl der Empfänger begrenzen wollen, an die MDaemon zusammengefasste DMARC-Berichte und DMARC-Fehlerberichte sendet, geben Sie

hier die zulässige Höchstzahl der Empfänger ein. Enthalten die Tags "rua=" oder "ruf=" im DMARC-Eintrag einer Domäne mehr Empfänger, als hier zugelassen sind, dann sendet MDaemon die Berichte an die angegebenen Empfänger in der Reihenfolge, in der sie in den Tags erscheinen, bis die Höchstzahl erreicht ist. Per Voreinstellung ist die Zahl der Empfänger nicht begrenzt.

Kopien aller Berichte per E-Mail senden an:
Falls Sie Kopien aller zusammengefassten DMARC-Berichte und DMARC-Fehlerberichte (nur bei Nutzung der Tags fo=0 und fo=1) per E-Mail an bestimmte Empfänger senden lassen wollen, tragen Sie die E-Mail-Adressen der Empfänger hier ein. Trennen Sie mehrere Adressen durch Kommata.

Metadaten für DMARC-Berichte

Die folgenden Optionen dienen dazu, Informationen und Angaben zu Ihrer Organisation, sog. Metadaten, zu erfassen, die in die DMARC-Berichte aufgenommen werden.

Name der Organisation
Dies ist die Organisation, die für die Erstellung der DMARC-Berichte verantwortlich ist. Sie müssen eine der eigenen MDaemon-Domänen angeben; Sie können die Domäne aus dem Rollmenü auswählen.

Kontakt-E-Mail-Adresse
Hier können Sie eine lokale E-Mail-Adresse angeben, mit der sich die Empfänger der Berichte bei Fragen zum Bericht in Verbindung setzen können. Trennen Sie mehrere Adressen durch Kommata.

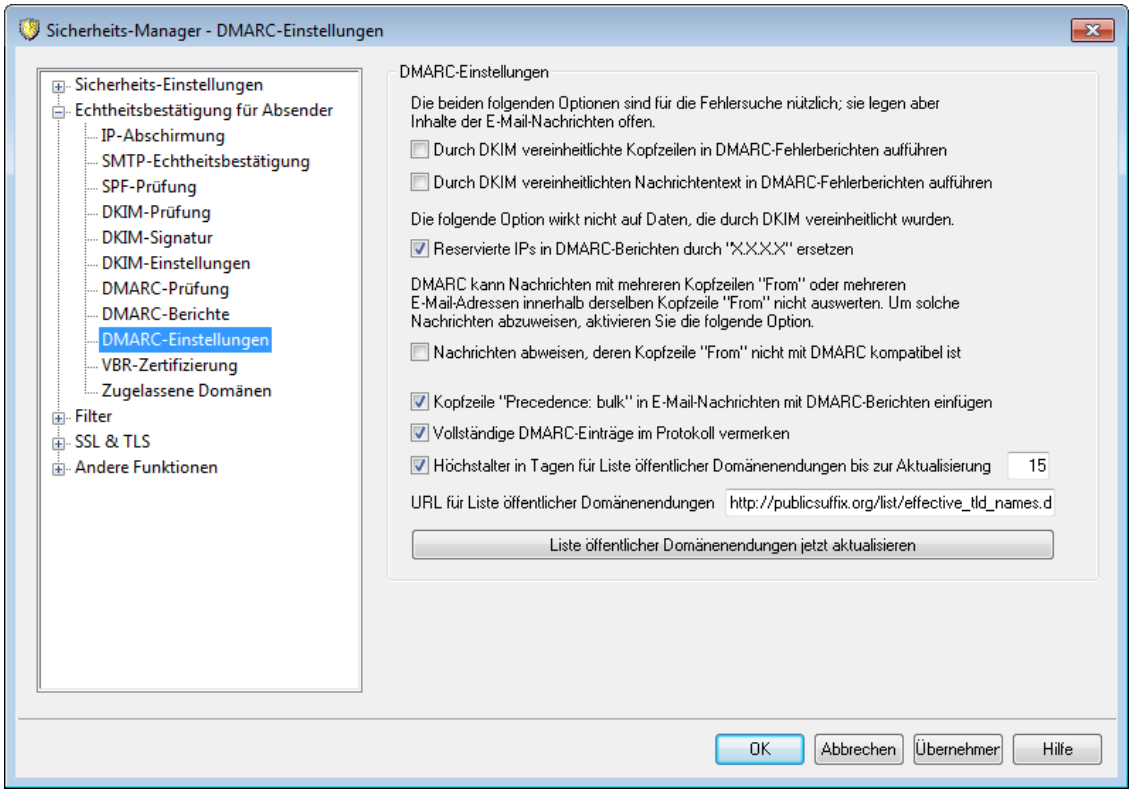
Kontaktdaten
Hier können Sie zusätzliche Kontaktdaten für die Empfänger der Berichte angeben, etwa eine Website oder Rufnummer.

Antwortpfad für Berichte
Hier können Sie den SMTP-Antwortpfad (die Bounce-Adresse) für die Nachrichten angeben, mit denen MDaemon die DMARC-Berichte versendet. Dieser Antwortpfad ist für Zustellfehler relevant; um solche Fehler zu ignorieren, geben Sie hier noreply@<meinedomäne.com> an.

Siehe auch:

DMARC 538
DMARC-Prüfung 549
DMARC-Einstellungen 553

4.1.2.5.3 DMARC-Einstellungen



DMARC-Einstellungen

Durch DKIM vereinheitlichte Kopfzeilen in DMARC-Fehlerberichten aufführen
Diese Option bewirkt, dass die durch DKIM vereinheitlichten Kopfzeilen[536] in die DMARC-Fehlerberichte[549] aufgenommen werden. Diese Option ist per Voreinstellung abgeschaltet.

Durch DKIM vereinheitlichten Nachrichtentext in DMARC-Fehlerberichten aufführen
Diese Option bewirkt, dass die durch DKIM vereinheitlichten Nachrichtentexte[536] in die DMARC-Fehlerberichte[549] aufgenommen werden. Diese Option ist per Voreinstellung abgeschaltet.

Reservierte IPs in DMARC-Berichten durch "X.X.X.X" ersetzen
Per Voreinstellung ersetzt MDaemon ihre reservierten IP-Adressen in DMARC-Berichten durch "X.X.X.X". Um Ihre reservierten IP-Adressen in den DMARC-Berichten sichtbar zu machen, deaktivieren Sie diese Option. Diese Option wirkt nicht auf durch DKIM vereinheitlichte Daten.

Vollständige DMARC-Einträge im Protokoll vermerken
Per Voreinstellung protokolliert MDaemon die vollständigen DMARC-Ressourceneinträge, die als Antwort auf die DNS-Abfrage während der DMARC-Prüfung übermittelt wurden. Um die vollständigen Ressourceneinträge nicht zu protokollieren, deaktivieren Sie diese Option.

Höchstalter der Liste öffentlicher Domänenendungen in Tagen bis zur Aktualisierung
DMARC benötigt eine Liste öffentlicher Domänenendungen, um verlässlich die richtigen Domänen festzustellen, für die DNS-Abfragen nach DMARC-Ressourceneinträgen durchzuführen sind. Per Voreinstellung aktualisiert MDaemon

die durch MDaemon gespeicherte Liste öffentlicher Domänenendungen, sobald sie ein Alter von 15 Tagen überschreitet. Durch Bearbeiten dieses Werts erreichen Sie, dass die Liste öffentlicher Domänenendungen häufiger oder seltener aktualisiert wird. Falls Sie diese Option deaktivieren, wird die Liste nicht mehr automatisch aktualisiert.

URL für Liste öffentlicher Domänenendungen
Hier wird der URL zu der Liste öffentlicher Domänenendungen festgelegt, die MDaemon zum Abruf der Liste nutzt. Per Voreinstellung nutzt MDaemon die unter http://publicsuffix.org/list/effective_tld_names.dat erreichbare Datei.

Liste öffentlicher Domänenendungen jetzt aktualisieren
Um die Liste öffentlicher Domänenendungen sofort manuell zu aktualisieren, klicken Sie auf dieses Steuerelement. Auch für diese Aktualisierung wird der *URL für Liste öffentlicher Domänenendungen* verwendet.

Siehe auch:

DMARC 538
DMARC-Prüfung 546
DMARC-Berichte 549
DMARC-Optionen 553

4.1.2.6 Zertifizierung von Nachrichten

Die Zertifizierung von Nachrichten ist eine Vorgehensweise, bei der ein Zertifizierungsdienstleister für die Legitimität der E-Mail-Nachrichten eines anderen einsteht und dessen Nachrichten zertifiziert. Vertraut der Empfänger einer Nachricht dem Zertifizierungsdienstleister, der für den E-Mail-Verkehr einer Domäne einsteht, so können die Nachrichten aus der Domäne als vertrauenswürdiger gelten als andere. Der Empfänger kann aus dem Vorhandensein der Zertifizierung entnehmen, dass sich der Absender an bestimmte Mindestanforderungen für regelkonformen Umgang mit E-Mail hält, und dass er keinen Spam und keine sonst problematischen Nachrichten versendet. Vorteil der Zertifizierung ist neben anderem, dass Nachrichten nicht fälschlich oder unnötig einer Kontrolle durch Spam-Filter unterworfen werden, die eigentlich gar nicht veranlasst wäre. Außerdem verringert die Zertifizierung die Systemressourcen, die zur Verarbeitung der Nachrichten aufgewandt werden müssen.

MDaemon unterstützt die Zertifizierung von Nachrichten durch Bereitstellung der ersten kommerziell genutzten Implementation eines neuen Internet-Protokolls namens "Vouch-By-Reference" (kurz VBR, übersetzt "Zertifizierung durch Referenz"). MDaemon Technologies arbeitet durch Mitwirkung im Domain Assurance Council (DAC) an der Entwicklung und Verbreitung dieses Protokolls mit. VBR stellt die Technik bereit, durch die Zertifizierungsdienstleister (kurz CSP vom englischen Begriff Certification Service Providers) oder "Zertifizierungsstellen" für die verantwortungsvolle Handhabung von E-Mail durch bestimmte Domänen einstehen.

Zertifizierung eingehender Nachrichten

Die Zertifizierungsfunktionen für eingehende Nachrichten, die MDaemon bereit stellt, können sehr einfach so konfiguriert werden, dass sie eingehende Nachrichten prüfen. Es genügt dazu, die Option *Eingehende Nachrichten zertifizieren* im Konfigurationsdialog VBR-Zertifizierung (Sicherheit » Sicherheits-Einstellungen » Echtheitsbestätigung für Absender » VBR-Zertifizierung) zu aktivieren und

mindestens einen Zertifizierungsdienstleister einzutragen, der für die Zertifizierung eingehender Nachrichten vertrauenswürdig ist, wie etwa `vbr.emailcertification.org`. Zertifizierte Nachrichten können von der Verarbeitung durch den Spam-Filter ausgenommen, oder ihre Spam-Bewertung kann herabgesetzt werden.

Zertifizierung abgehender Nachrichten

Bevor MDaemon Zertifizierungsdaten in abgehende Nachrichten einfügen kann, muss zunächst sichergestellt sein, dass mindestens ein Zertifizierungsdienstleister für die Zertifizierung der Nachrichten zur Verfügung steht. MDaemon Technologies erbringt für die Benutzer von MDaemon einen solchen Dienst. Nähere Informationen erhalten Sie unter www.mdaemon.com.

Um MDaemon für die Zertifizierung abgehender Nachrichten einzurichten, müssen Sie nach der Registrierung bei einem Zertifizierungsdienstleister folgende Schritte durchführen:

1. Öffnen Sie den Konfigurationsdialog VBR-Zertifizierung: Klicken Sie auf `Sicherheit » Sicherheits-Einstellungen » Echtheitsbestätigung für Absender » VBR-Zertifizierung`.
2. Aktivieren Sie "*Zertifizierungsdaten in abgehende Nachrichten einfügen*".
3. Klicken Sie auf "*Eine Domäne für die Zertifizierung von Nachrichten konfigurieren*". Hierdurch wird der Dialog für die Einrichtung der Zertifizierung geöffnet.
4. Tragen Sie den *Domänennamen* ein, dessen abgehende Nachrichten die Zertifizierungsdaten erhalten sollen.
5. Wählen Sie aus dem Rollmenü *Nachrichtentyp* den Typ der E-Mail-Nachrichten aus, den der Dienstleister für die Domäne zertifiziert, oder tragen Sie einen neuen Typ ein, falls der gewünschte Typ nicht in der Liste enthalten ist.
6. Tragen Sie mindestens einen Zertifizierungsdienstleister ein, der die abgehenden Nachrichten aus der Domäne zertifiziert. Trennen Sie mehrere Einträge durch Leerzeichen.
7. Klicken Sie auf "*OK*".
8. Konfigurieren Sie Ihren Server so, dass die abgehenden Nachrichten der Domäne durch DKIM 529 signiert werden, oder stellen Sie sicher, dass sie über einen durch SPF 527 zugelassenen Absender versandt werden; nur so ist sichergestellt, dass die Nachrichten von dem Server selbst versandt werden. Diese Absicherung ist für eine Zertifizierung unerlässlich. Eine Nachricht kann nur zertifiziert werden, wenn der Empfänger eine Möglichkeit hat, festzustellen, dass die Nachricht wirklich vom angeblichen Absender stammt.

VBR bedeutet nicht, dass die zertifizierten Nachrichten durch den Zertifizierungsdienstleister signiert oder dorthin übermittelt werden müssen. Der Dienstleister signiert und prüft keine Nachrichten als solche, er steht lediglich für den legitimen und verantwortungsvollen Umgang einer Domäne mit E-Mail-Nachrichten ein.

Nähere Informationen über die Zertifizierungsdienste, die MDaemon Technologies anbietet, erhalten Sie unter:

http://www.mdaemon.com/email-certification/

Die VBR-Spezifikation (RFC 5518) erhalten Sie in englischer Sprache hier:

http://tools.ietf.org/html/rfc5518

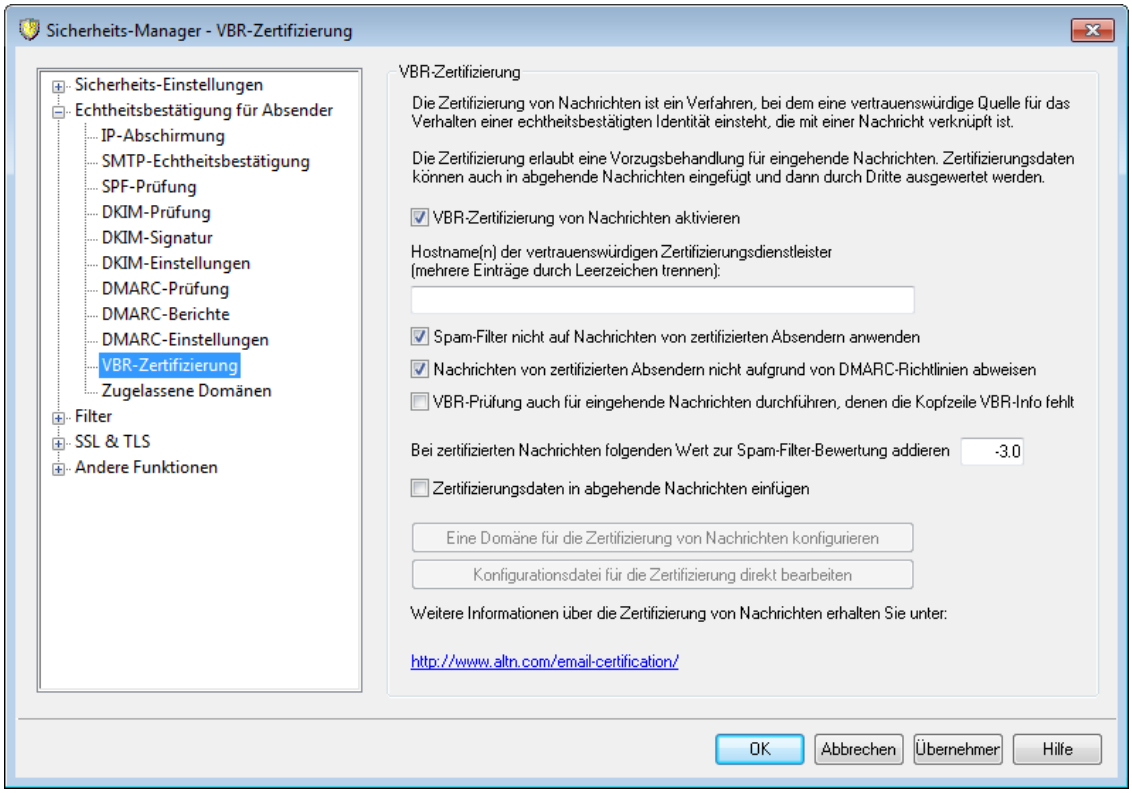
Nähere Informationen über DKIM erhalten Sie unter:

http://www.dkim.org/

Siehe auch:

VBR-Zertifizierung 556

4.1.2.6.1 VBR-Zertifizierung



Sie erreichen den Konfigurationsdialog VBR-Zertifizierung über Sicherheit » Sicherheits-Einstellungen » Echtheitsbestätigung für Absender » VBR-Zertifizierung.

VBR-Zertifizierung

VBR-Zertifizierung von Nachrichten aktivieren
Diese Option aktiviert die Zertifizierung eingehender Nachrichten. Empfängt MDaemon eine Nachricht, für die eine Zertifizierung erforderlich ist, so fragt MDaemon den vertrauenswürdigen Zertifizierungsdienstleister danach ab, ob die Nachricht tatsächlich als "zertifiziert" einzustufen ist. Trifft dies zu, so wird die Nachricht, in Abhängigkeit von den Einstellungen unten, nicht durch den Spam-Filter verarbeitet oder mit einer günstigeren Bewertung des Spam-Filters 678 versehen.

Hostname(n) der vertrauenswürdigen Zertifizierungsdienstleister (mehrere Einträge durch Kommata trennen):
In dieses Feld werden die Hostnamen der Zertifizierungsdienstleister, die vertrauenswürdig sind, eingetragen. Mehrere Einträge müssen durch Leerzeichen getrennt werden.

Spam-Filter nicht auf Nachrichten von zertifizierten Absendern anwenden
Diese Option bewirkt, dass Nachrichten von zertifizierten Absendern nicht durch den Spam-Filter verarbeitet werden.

Nachrichten von zertifizierten Absendern nicht aufgrund von DMARC-Richtlinien abweisen
Diese Option stellt sicher, dass geprüfte Nachrichten von zertifizierten Absendern nicht abgewiesen werden, falls für die Absenderdomäne stark einschränkende DMARC-Richtlinien 546 veröffentlicht sind (etwa p=quarantine oder p=reject) und die DMARC-Prüfung für die Nachrichten fehlschlägt. Die Option ist per Voreinstellung aktiv.

VBR-Prüfung auch für eingehende Nachrichten durchführen, denen die Kopfzeile VBR-Info fehlt
Diese Option bewirkt, dass die VBR-Prüfung auch bei solchen eingehenden Nachrichten durchgeführt wird, denen die Kopfzeile VBR-Info fehlt. Diese Kopfzeile ist üblicherweise erforderlich, aber die VBR-Prüfung kann möglicherweise auch durchgeführt werden, falls sie fehlt. Fehlt die Kopfzeile, so fragt MDaemon die vertrauenswürdigen Zertifizierungsdienstleister mit dem Nachrichtentyp "all" ab. Diese Option ist per Voreinstellung abgeschaltet.

Bei zertifizierten Nachrichten folgenden Wert zur Spam-Filter-Bewertung addieren
Sollen zertifiziert Nachrichten zwar nicht von der Verarbeitung durch den Spam-Filter ausgenommen werden, so kann mithilfe dieser Option festgelegt werden, welcher Punktwert zur Bewertung des Spam-Filters hinzugerechnet wird, um die Bewertung anzupassen. Der Wert sollte negativ sein, damit die Bewertung des Spam-Filters verringert wird. Die Voreinstellung beträgt "-3.0".

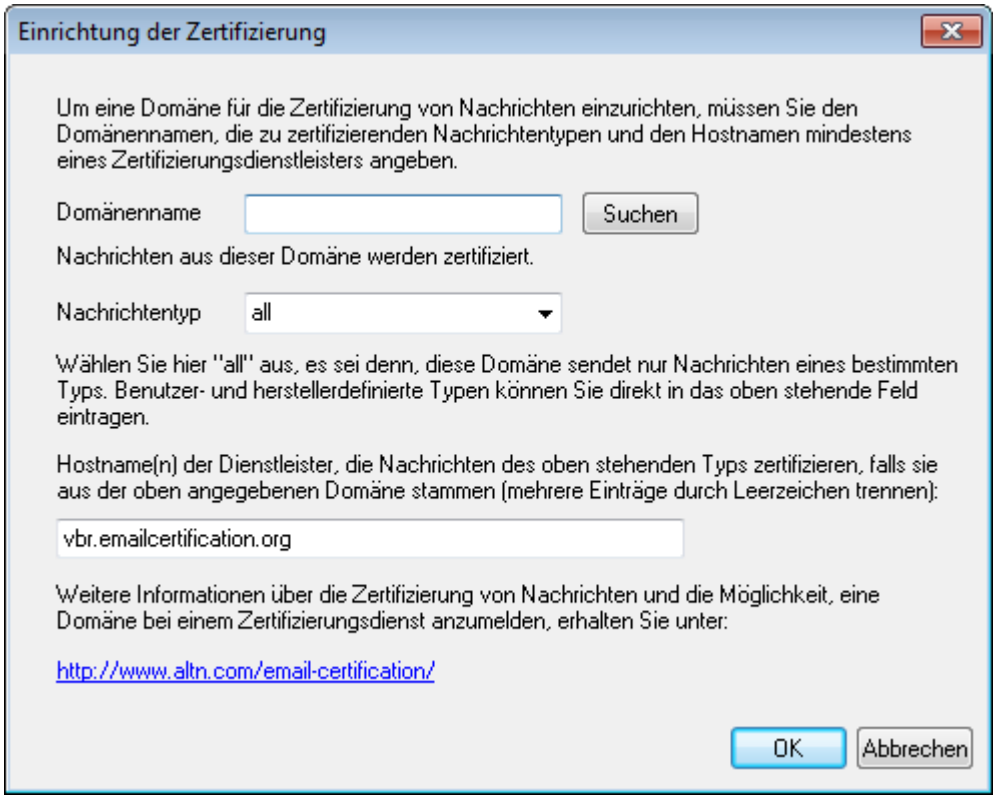
Zertifizierungsdaten in abgehende Nachrichten einfügen
Diese Option bewirkt, dass Zertifizierungsdaten in abgehende Nachrichten eingefügt werden. Nachdem die Option aktiviert wurde, muss durch Anklicken von *Eine Domäne für die Zertifizierung von Nachrichten konfigurieren* der Konfigurationsdialog für die Einrichtung der Zertifizierung aufgerufen werden. Dort werden die Domänen und die Zertifizierungsdienstleister festgelegt.

Eine Domäne für die Zertifizierung von Nachrichten konfigurieren
Nach Aktivieren der Option *Zertifizierungsdaten in abgehende Nachrichten einfügen* weiter oben muss durch Anklicken dieses Steuerelements der Konfigurationsdialog für die Einrichtung der Zertifizierung aufgerufen werden. Dort werden Domäne, Nachrichtentypen und Dienstleister für die Zertifizierung festgelegt.

Konfigurationsdatei für die Zertifizierung direkt bearbeiten
Nach Aktivieren der Option *Zertifizierungsdaten in abgehende Nachrichten einfügen* weiter oben kann die Konfigurationsdatei für die Funktion "Vouch-By-Reference" (VBR) durch Anklicken dieses Steuerelements zur direkten Bearbeitung geöffnet werden. Domänen, die bereits über den Konfigurationsdialog zur Einrichtung der Zertifizierung konfiguriert wurden, und die zugehörigen

Konfigurationsdaten, erscheinen in dieser Datei. Bestehende Einträge können bearbeitet, und neue Einträge können hinzugefügt werden.

Einrichtung der Zertifizierung



Nach Aktivieren der Option *Zertifizierungsdaten in abgehende Nachrichten einfügen* im Konfigurationsdialog Zertifizierung muss das Steuerelement *Eine Domäne für die Zertifizierung von Nachrichten konfigurieren* angeklickt werden, um diesen Konfigurationsdialog aufzurufen. Hier werden die Domäne, deren abgehende Nachrichten zertifiziert werden sollen, die zu zertifizierenden Nachrichtentypen und die Zertifizierungsdienstleister konfiguriert.

Einrichtung der Zertifizierung

Domänenname
Hier wird der Name der Domäne eingetragen, deren abgehende Nachrichten zertifiziert werden sollen.

Suchen
Wurden die Zertifizierungseinstellungen für eine bestimmte Domäne bereits konfiguriert, so kann ihr Domänenname eingegeben und auf Suchen geklickt werden; die Einstellungen der Domäne werden dann in den Konfigurationsdialog geladen.

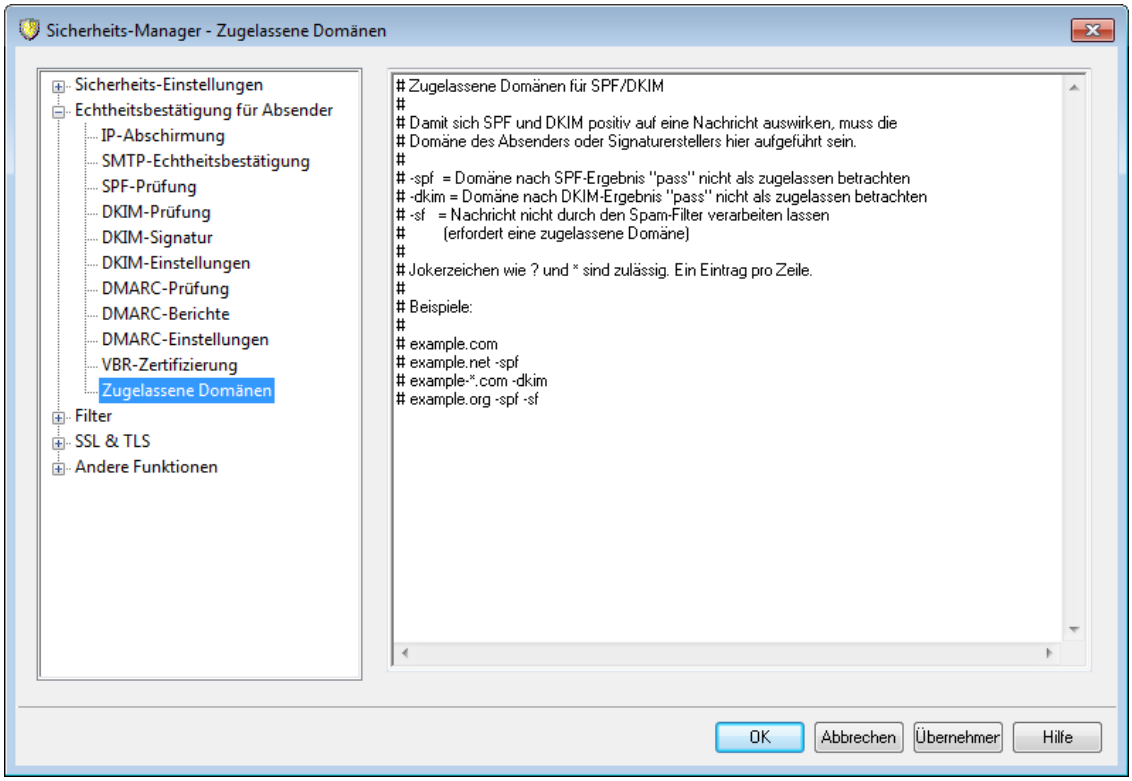
Nachrichtentyp
Aus diesem Auswahlmenü muss der Nachrichtentyp ausgewählt werden, den der Zertifizierungsdienstleister für die Domäne zertifiziert. Ist der gewünschte Typ nicht in der Liste enthalten, so muss er von Hand eingetragen werden.

Hostname(n) der Dienstleister...
In dieses Feld müssen die Hostnamen der Zertifizierungsdienstleister eingetragen werden, die die abgehenden Nachrichten der Domäne zertifizieren werden (wie etwa `vbr.emailcertification.org`). Mehrere Einträge müssen durch Leerzeichen getrennt werden.

Siehe auch:

Zertifizierung von Nachrichten 554

4.1.2.7 Zugelassene Domänen



Manche Spammer verwenden inzwischen das SPF und versehen Nachrichten mit gültigen DKIM-Signaturen. Die Tatsache, dass eine Nachricht gültig signiert ist und die Prüfung erfolgreich durchläuft, bietet daher keine Gewähr mehr dafür, dass der Empfänger die Nachricht nicht als Spam betrachtet, obwohl sie von einer gültigen Quelle stammt. Aus diesem Grund wird die Spam-Bewertung einer Nachricht aufgrund einer erfolgreichen Prüfung über SPF oder DKIM nur dann verringert, falls die Domäne aus der Signatur auch in der Liste zugelassener Domänen erfasst ist. Diese Liste ist nach ihrem Zweck eine Freigabeliste. In ihr sind Domänen erfasst, deren Nachrichten eine niedrigere Spam-Bewertung erhalten, wenn sie erfolgreich geprüft wurden.

Wird eine Nachricht, die durch eine der hier erfassten Domänen signiert ist, durch SPF oder DKIM erfolgreich geprüft, so wird ihre Spam-Bewertung anhand der Einstellungen in den Konfigurationsdialogen SPF 527 und DKIM-Prüfung 531 verringert. Für die Domänen in der Liste können jedoch auch die unten aufgeführten Befehle in beliebiger Kombination erfasst werden, falls eine oder mehrere Prüfungen die Bewertung nicht verringern sollen. Eine weitere Option verhindert die Verarbeitung einer Nachricht durch den Spam-Filter, nachdem sie erfolgreich geprüft wurde.

-spf Spam-Bewertung für Nachrichten aus dieser Domäne nach erfolgreicher Prüfung durch SPF nicht nicht verringern.

-dkim Spam-Bewertung für Nachrichten aus dieser Domäne nach erfolgreicher Prüfung durch DKIM nicht verringern.

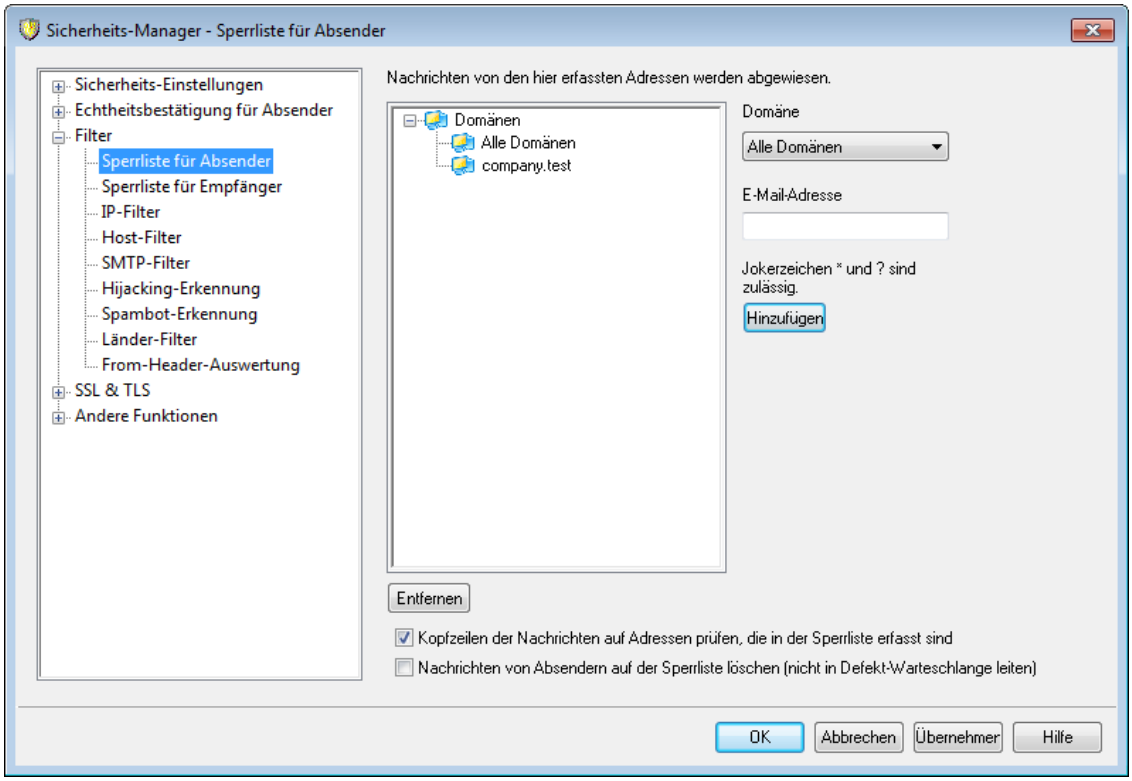
-sf Nachrichten, bei denen eine Prüfung erfolgreich abgeschlossen war, durchlaufen den Spam-Filter nicht mehr.

DMARC und die Liste zugelassener Domänen

Auch die DMARC-Prüfung[546] nutzt die Liste zugelassener Domänen, die auf Grundlage geprüfter DKIM-Identifikationsmerkmale und SPF-Pfade Nachrichten als aus vertrauenswürdigen Quellen bevorzugt behandeln kann. Geht beispielsweise eine Nachricht ein, für die die DMARC-Prüfung fehlschlägt, und hat diese Nachricht aber eine gültige DKIM-Signatur aus einer Domäne aus der Liste zugelassener Domänen, so wird die Nachricht nicht wegen der Einstellungen einer DMARC-Richtlinie abgewiesen. Die Nachricht wird dann beispielsweise so behandelt, wie wenn die Richtlinie "p=none" lautet. Entsprechendes gilt, wenn die SPF-Prüfung eine Domäne auf der Liste zugelassener Domänen trifft.

4.1.3 Filter

4.1.3.1 Sperrliste für Absender



Die Sperrliste für Absender ist über Sicherheit » Sicherheits-Einstellungen » Filter erreichbar. In dieser Liste sind alle Adressen erfasst, die keine Nachrichten über Ihren Server leiten dürfen. Geht eine Nachricht von einer der in dieser Liste erfassten Adressen ein, so wird sie während der SMTP-Verbindung abgewiesen. Dieses Leistungsmerkmal hilft, die Aktivität solcher Benutzer zu unterbinden, die Probleme verursachen. Die Adressen können für einzelne Domänen oder systemweit für alle durch MDaemon verwalteten Domänen erfasst werden.

Nachrichten von den hier erfassten Adressen werden abgewiesen.
In dieser Übersicht werden alle Adressen aufgeführt, die derzeit auf der Sperrliste erfasst sind. Sie werden getrennt nach den Domänen aufgeführt, für die sie auf der Sperrliste erfasst sind.

Domäne
Hier können Sie die Domäne auswählen, mit der eine Adresse auf der Sperrliste verknüpft werden soll. Diese Einstellung bestimmt, welche Domäne gegen den Empfang von Nachrichten von dieser Adresse aus gesperrt werden soll. Um die betreffende Adresse für das gesamte System zu sperren, wählen Sie hier "Alle Domänen" aus.

E-Mail-Adresse
Geben Sie hier die E-Mail-Adresse ein, die Sie in die Sperrliste aufnehmen möchten. Jokerzeichen sind zulässig. So verhindert der Eintrag "*@example.net" den Versand aller Nachrichten mit der Absenderdomäne "example.net". Der Eintrag "user1@*" verhindert den Versand aller Nachrichten von Adressen, die mit "user1@" beginnen, unabhängig von der Domäne, zu der sie gehören.

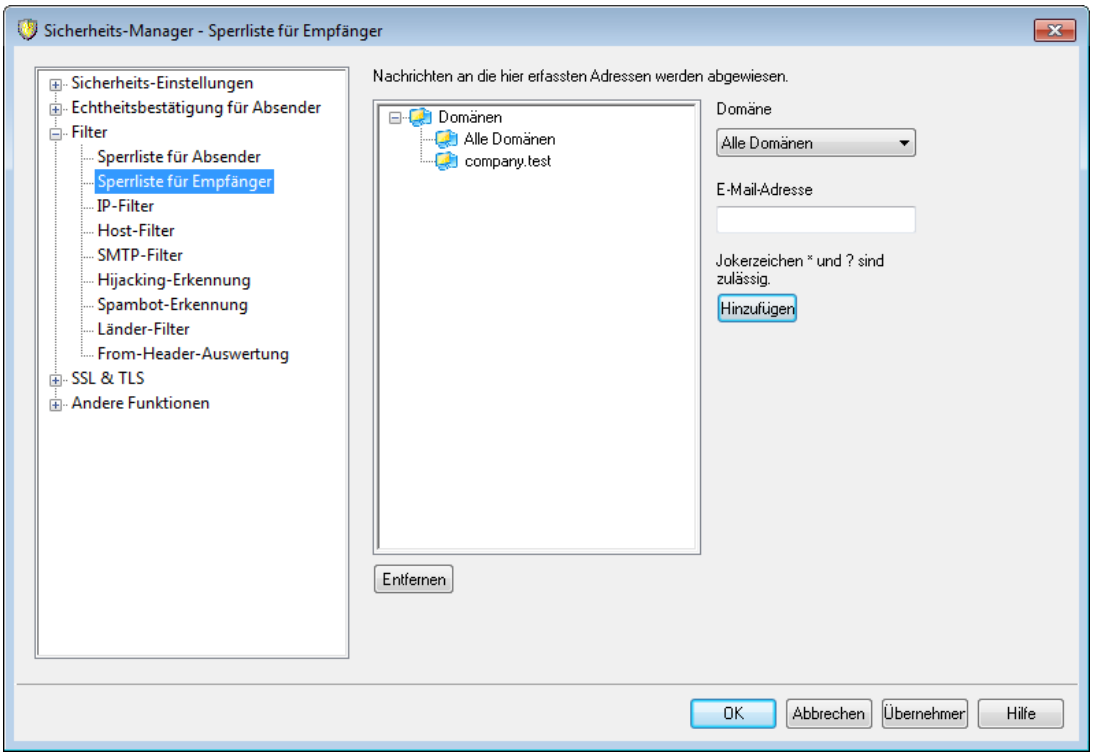
Hinzufügen
Durch Anklicken dieses Steuerelements fügen Sie die Adresse der Sperrliste hinzu.

Entfernen
Durch Anklicken dieses Steuerelements entfernen Sie den Eintrag, den Sie in der Liste ausgewählt haben.

Kopfzeilen der Nachrichten auf Adressen prüfen, die in der Sperrliste erfasst sind
Per Voreinstellung wendet MDaemon die Sperrliste auf die Daten an, die während der SMTP-Verbindung aus den Kopfzeilen From und Sender der betreffenden Nachricht entnommen wurden. Hierdurch wird verhindert, dass die Nachrichten später abgefangen und durch den MTA-Thread in die Defekt-Warteschlange verschoben werden.

Nachrichten von Absendern auf der Sperrliste löschen (nicht in Defekt-Warteschlange leiten)
Diese Option bewirkt, dass MDaemon eingehende Nachrichten von solchen Absendern löscht, die in der Sperrliste erfasst sind. Dies erfasst normale Nachrichten sowie Nachrichten, die über MultiPOP und DomainPOP eingehen. Ist die Option abgeschaltet, so werden die Nachrichten nicht gelöscht, sondern in die Defekt-Warteschlange verschoben. Die Option ist per Voreinstellung abgeschaltet.

4.1.3.2 Sperrliste für Empfänger



Die Sperrliste für Empfänger ist über Sicherheit » Sicherheits-Einstellungen » Filter erreichbar. In dieser Liste sind alle Adressen erfasst, die keine Nachrichten von Ihrem Server empfangen dürfen. Geht eine Nachricht an eine der in dieser Liste erfassten Adressen ein, so wird sie während der SMTP-Verbindung abgewiesen. Die Adressen können für einzelne Domänen oder systemweit für alle durch MDaemon verwalteten Domänen erfasst werden. Die Sperrliste für Empfänger arbeitet ausschließlich auf Grundlage der RCPT-Daten aus dem SMTP-Umschlag, nicht jedoch auf Grundlage der Kopfzeilen der Nachrichten.

Nachrichten an die hier erfassten Adressen werden abgewiesen.
In dieser Übersicht werden alle Adressen aufgeführt, die derzeit auf der Sperrliste erfasst sind. Sie werden getrennt nach den Domänen aufgeführt, für die sie auf der Sperrliste erfasst sind.

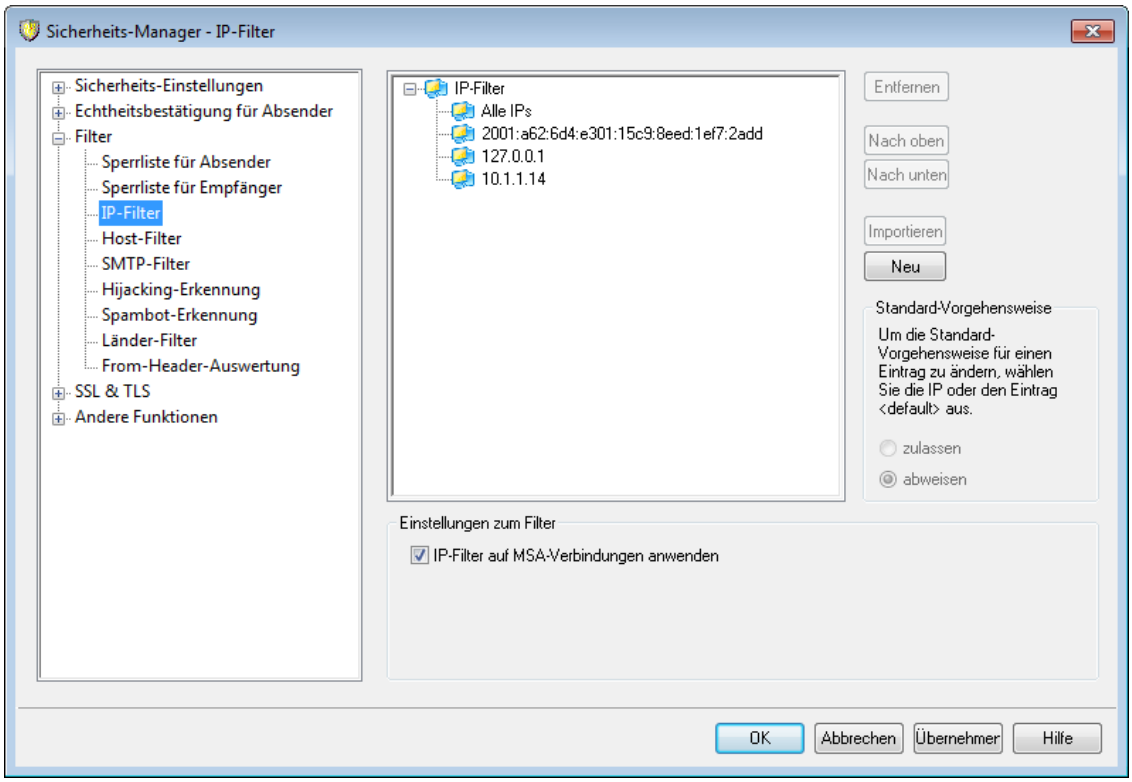
Domäne
Hier können Sie die Domäne auswählen, mit der eine Adresse auf der Sperrliste verknüpft werden soll. Diese Einstellung bestimmt, welche Domäne gegen den Versand von Nachrichten an diese Adresse gesperrt werden soll. Um die betreffende Adresse für das gesamte System zu sperren, wählen Sie hier "Alle Domänen" aus.

E-Mail-Adresse
Geben Sie hier die E-Mail-Adresse ein, die Sie in die Sperrliste aufnehmen möchten. Jokerzeichen sind zulässig. So verhindert der Eintrag "*@example.net" den Versand aller Nachrichten mit der Empfängerdomäne "example.net". Der Eintrag "user1@*" verhindert den Versand aller Nachrichten an Adressen, die mit "user1@" beginnen, unabhängig von der Domäne, zu der sie gehören.

Hinzufügen
Durch Anklicken dieses Steuerelements fügen Sie die Adresse der Sperrliste hinzu.

Entfernen
Durch Anklicken dieses Steuerelements entfernen Sie den Eintrag, den Sie in der Liste ausgewählt haben.

4.1.3.3 IP-Filter



Sie erreichen den Konfigurationsdialog IP-Filter über Sicherheit » Sicherheits-Einstellungen » Filter. Der IP-Filter enthält eine Liste von IP-Adressen, die entweder zugelassen oder gesperrt werden sollen. Von den Einstellungen in diesem Dialog hängt ab, wie der Server bei Verbindungsversuchen von den eingetragenen IP-Adressen aus reagiert. Es kann eine Adressliste eingegeben und dann festgelegt werden, dass der Server nur Verbindungen von diesen Adressen aus zulässt oder dass er alle Verbindungsversuche von diesen Adressen abweist. Die CIDR-Schreibweise und die Jokerzeichen *, # und ? sind zulässig.

Einige Beispiele hierzu:

..*.*	erfasst jede IP-Adresse
#.#.#.#	erfasst jede IP-Adresse
192.*.*.*	erfasst jede IP-Adresse, die mit 192 beginnt
192.168.*.239	erfasst jede IP-Adresse von 192.168.0.239 bis 192.168.255.239
192.168.0.1??	erfasst jede IP-Adresse von 192.168.0.100 bis 192.168.0.199

Hinzufügen neuer Einträge zum IP-Filter

Um dem IP-Filter einen neuen Eintrag hinzuzufügen, klicken Sie auf **Neu**. Es öffnet sich der Konfigurationsdialog *Neuer Eintrag im IP-Filter*.

Lokale IP-Adresse
Mit Hilfe der Auswahlliste ist festzulegen, ob sich der Eintrag für den IP-Filter auf alle lokalen IP-Adressen bezieht ("All IPs") oder ob nur eine lokale Adresse betroffen sein soll.

IP der Gegenstelle (CIDR sowie Jokerzeichen *, ? und # sind zulässig)
Hier wird die zu filternde IP-Adresse festgelegt. Der Eintrag muss in Dezimalschreibweise, durch Punkte getrennt erfolgen, da der IP-Filter nur mit numerischen IP-Adressen funktioniert. Mit dem Knopf *Hinzufügen* wird die angegebene Adresse der Filterliste angefügt.

Verbindungen zulassen
Diese Option bewirkt, dass die angegebene IP-Adresse Verbindungen mit der zugehörigen lokalen IP-Adresse herstellen kann.

Verbindungen abweisen
Diese Option bewirkt, dass die angegebene IP-Adresse keine Verbindungen mit der zugehörigen lokalen IP-Adresse herstellen kann. Die Verbindungen werden abgewiesen oder getrennt.

Hinzufügen
Durch einen Klick auf dieses Steuerelement wird der neue Eintrag der Filterliste hinzugefügt.

Entfernen
Hierdurch wird der jeweils ausgewählte Listeneintrag gelöscht.

Importieren

Mithilfe dieser Schaltfläche können Sie IP-Adressdaten aus APF- und .htaccess-Dateien importieren. Wählen Sie dazu die gewünschte IP-Adresse aus, und klicken Sie auf die Schaltfläche. Der Import der IP-Adressdaten durch MDaemon aus solchen Dateien unterliegt folgenden Einschränkungen:

- Einträge der Typen "deny from" und "allow from" werden unterstützt.
- Es werden nur IP-Adressen, nicht jedoch Domänennamen importiert.
- Die CIDR-Schreibweise ist zulässig. Unvollständige IP-Adressen sind nicht zulässig.
- Auf jeder Zeile sind beliebig viele durch Leerzeichen oder Kommata getrennte IP-Adressen zulässig. Ein Beispiel hierzu: "deny from 1.1.1.1 2.2.2.2/16", ""3.3.3.3, 4.4.4.4, 5.5.5.5".
- Zeilen, die mit # beginnen, werden ignoriert.

Entfernen

Um einen Eintrag zu entfernen, wählen Sie den Eintrag in der Liste aus, und klicken Sie auf **Entfernen**.

Standard-Vorgehensweise

Sie können eine Standard-Vorgehensweise für IP-Adressen von Gegenstellen festlegen, die noch nicht erfasst sind. Wählen Sie hierzu eine IP-Adresse aus der Liste aus, und klicken Sie danach auf **zulassen** oder **abweisen**. Ist eine Standard-Vorgehensweise bereits festgelegt, so können Sie diese Vorgehensweise ändern,

indem Sie den Eintrag "<default>" unterhalb der betreffenden IP-Adresse anklicken und danach die neue Standard-Vorgehensweise auswählen.

zulassen
Diese Option bewirkt, dass Verbindungen von allen IP-Adressen aus zugelassen sind, die nicht im IP-Filter erfasst sind.

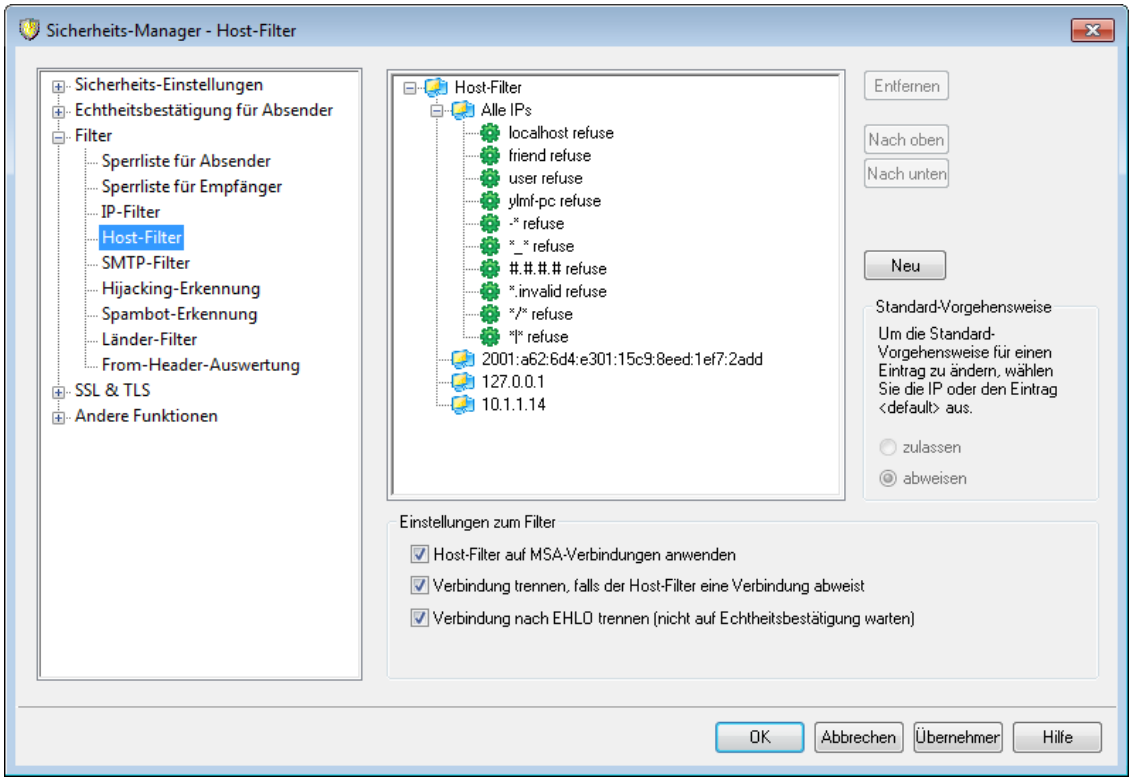
abweisen
Diese Option bewirkt, dass Verbindungen von allen IP-Adressen aus abgewiesen werden, die nicht im IP-Filter erfasst sind.

Der IP-Filter blockiert in keinem Fall vertraute IP-Adressen[520] oder lokale IP-Adressen.

Einstellungen zum Filter

IP-Filter auf MSA-Verbindungen anwenden
Diese Option bewirkt, dass der IP-Filter auch auf Verbindungen angewendet wird, die zum MSA-Port[110] des lokalen Server aufgebaut werden. Dies ist üblicherweise nicht erforderlich. Diese Option ist per Voreinstellung aktiv.

4.1.3.4 Host-Filter



Sie erreichen den Konfigurationsdialog Host-Filter über Sicherheit » Sicherheits-Einstellungen » Filter. In diesem Dialog legen Sie eine Liste von Hosts als Gegenstellen fest, und Sie bestimmen, ob der Server Verbindungen von diesen Hosts annehmen oder abweisen soll. Der Host-Filter vergleicht die EHLO- und PTR-Daten, die während der SMTP-Verbindung ermittelt werden, mit den hier angegebenen Daten.

Lokale IP-Adresse
Mit Hilfe der Auswahlliste ist festzulegen, ob sich der Eintrag für den Host-Filter auf alle lokalen IP-Adressen bezieht ("All IPs") oder ob nur eine lokale Adresse betroffen sein soll.

Host der Gegenstelle
Hier wird der zu filternde Hostname festgelegt, der für die oben ausgewählte IP-Adresse erfasst werden soll.

EHLO/PTR-Wert zulassen
Diese Option bewirkt, dass der angegebene Host Verbindungen mit der zugehörigen lokalen IP-Adresse herstellen kann.

EHLO/PTR-Wert abweisen
Diese Option bewirkt, dass der angegebene Host keine Verbindungen mit der zugehörigen lokalen IP-Adresse herstellen kann. Die Verbindungen werden abgewiesen oder, falls Sie die Option "*Verbindung trennen, sobald HELO-/PTR-Werte abgewiesen werden*" weiter unten aktivieren, getrennt.

Hinzufügen
Durch einen Klick auf dieses Steuerelement wird der neue Eintrag der Filterliste hinzugefügt.

Entfernen
Hierdurch wird der jeweils ausgewählte Listeneintrag gelöscht.

Nicht definierte Werte werden...

...zugelassen
Ist diese Option aktiv, so können alle nicht im Filter erfassten Hosts Verbindungen zur jeweiligen lokalen IP-Adresse aufbauen.

...abgewiesen
Ist diese Option aktiv, so können nur die im Filter erfassten Hosts Verbindungen zur jeweiligen lokalen IP-Adresse aufbauen.

Der Host-Filter blockiert in keinem Fall vertraute 520 oder lokale Hosts.

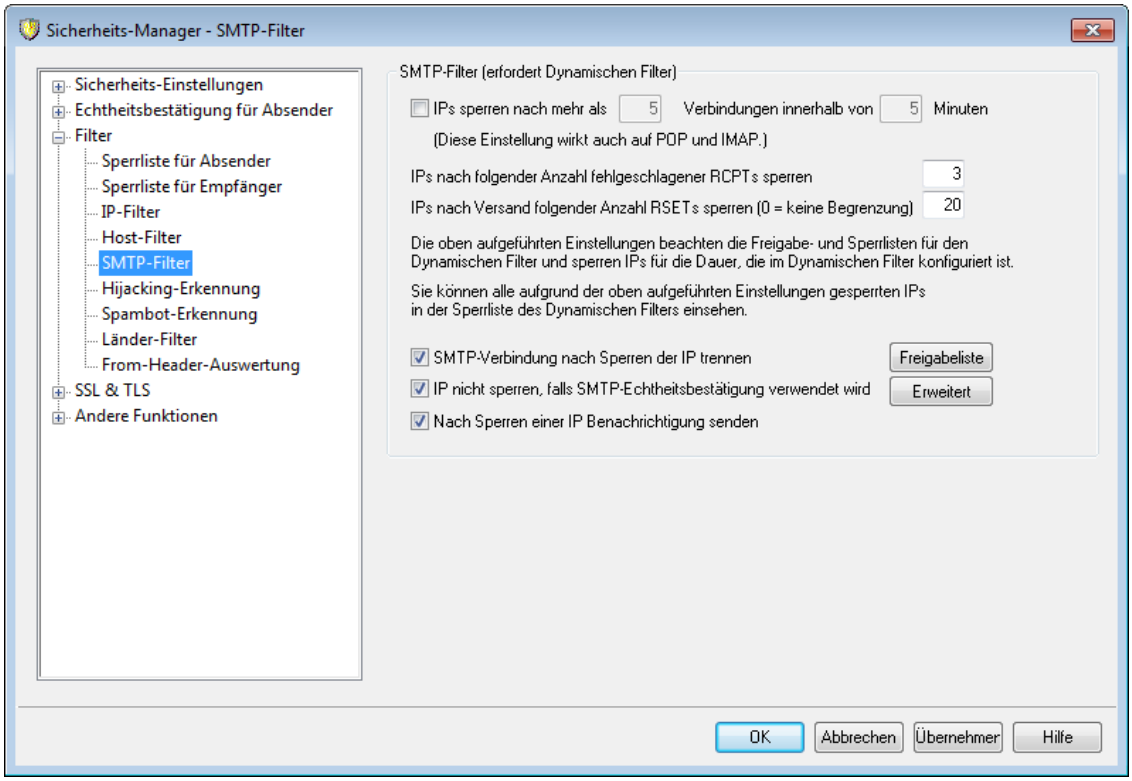
Einstellungen zum Filter

Host-Filter auf MSA-Verbindungen anwenden
Diese Option bewirkt, dass der Host-Filter auch auf Verbindungen angewendet wird, die zum MSA-Port 110 des Servers aufgebaut werden. Diese Option ist per Voreinstellung abgeschaltet.

Verbindung trennen, falls der Host-Filter eine Verbindung ablehnt
Diese Option bewirkt, dass Verbindungen sofort getrennt werden, wenn sie der Host-Filter ablehnt.

Verbindung nach EHLO trennen (nicht auf Echtheitsbestätigung warten)
Diese Option bewirkt, dass abzuweisende Verbindungen sofort nach der Phase EHLO/HELO getrennt werden. Ist diese Option nicht aktiv, so wird noch die Echtheitsbestätigung abgewartet. Diese Option ist per Voreinstellung aktiv.

4.1.3.5 SMTP-Filter



Mithilfe des SMTP-Filters können Sie die IP-Adressen solcher Gegenstellen sperren, die innerhalb eines in Minuten angegebenen Zeitraums zu viele Verbindungen mit Ihrem MDaemon-Server herstellen. Sie können auch solche IP-Adressen sperren, die zu viele fehlgeschlagene RCPT-, und die zu viele RSET-Befehle übermitteln. Der SMTP-Filter funktioniert nur, wenn der Dynamische Filter aktiv ist. Er nutzt die Dynamische Sperrliste 628 und die Dynamische Freigabeliste 626.

IPs sperren nach mehr als [X] Verbindungen innerhalb von [X] Minuten
Diese Option bewirkt, dass IP-Adressen vorübergehend gesperrt werden, sobald sie innerhalb des hier in Minuten angegebenen Zeitraums mehr als die hier angegebene Anzahl Verbindungen mit Ihrem Server hergestellt haben. Geben Sie hierzu den zu überwachenden Zeitraum und die Zahl der Verbindungen an, die in diesem Zeitraum nicht überschritten werden darf. Die Dauer der Sperre wird im Konfigurationsdialog Verfolgung fehlgeschlagener Echtheitsbestätigungen 616 festgelegt. Diese Option wirkt auch auf POP- und SMTP-Verbindungen.

IPs nach folgender Anzahl fehlgeschlagener RCPTs sperren
Diese Option bewirkt, dass IP-Adressen vorübergehend gesperrt werden, sobald sie innerhalb derselben Verbindung die hier angegebene Anzahl fehlgeschlagener RCPT-Befehle übermittelt haben, die jeweils zum Fehler "Empfänger unbekannt" geführt haben. Die Dauer der Sperre wird im Konfigurationsdialog Verfolgung fehlgeschlagener Echtheitsbestätigungen 616 festgelegt. Tritt innerhalb einer Verbindung besonders häufig der Fehler "Empfänger unbekannt" auf, so kann dies darauf hindeuten, dass es sich bei der Gegenstelle um einen Spam-Versender

handelt. Spam-Versender versuchen oft, E-Mail-Nachrichten an nicht mehr gültige oder falsche E-Mail-Adressen zuzustellen.

IPs nach Versand folgender Anzahl RSETs sperren (0 = keine Begrenzung)
Diese Option bewirkt, dass IP-Adressen vorübergehend gesperrt werden, sobald sie innerhalb derselben Verbindung die hier angegebene Anzahl von RSET-Befehlen übermittelt haben. Der Wert "0" bewirkt, dass die Höchstzahl innerhalb derselben Verbindung zulässiger RSET-Befehle nicht begrenzt wird. Der Konfigurationsdialog Server 94 im Menü Server-Einstellungen enthält eine ähnliche Option, mit deren Hilfe eine Höchstzahl zulässiger RSET-Befehle festgelegt werden kann. Die Dauer der Sperre wird im Konfigurationsdialog Verfolgung fehlgeschlagener Echtheitsbestätigungen 616 festgelegt.

SMTP-Verbindung nach Sperren der IP trennen
Diese Option bewirkt, dass MDaemon die SMTP-Verbindung trennt, sobald die IP-Adresse der Gegenstelle gesperrt wurde. Diese Option ist per Voreinstellung aktiv.

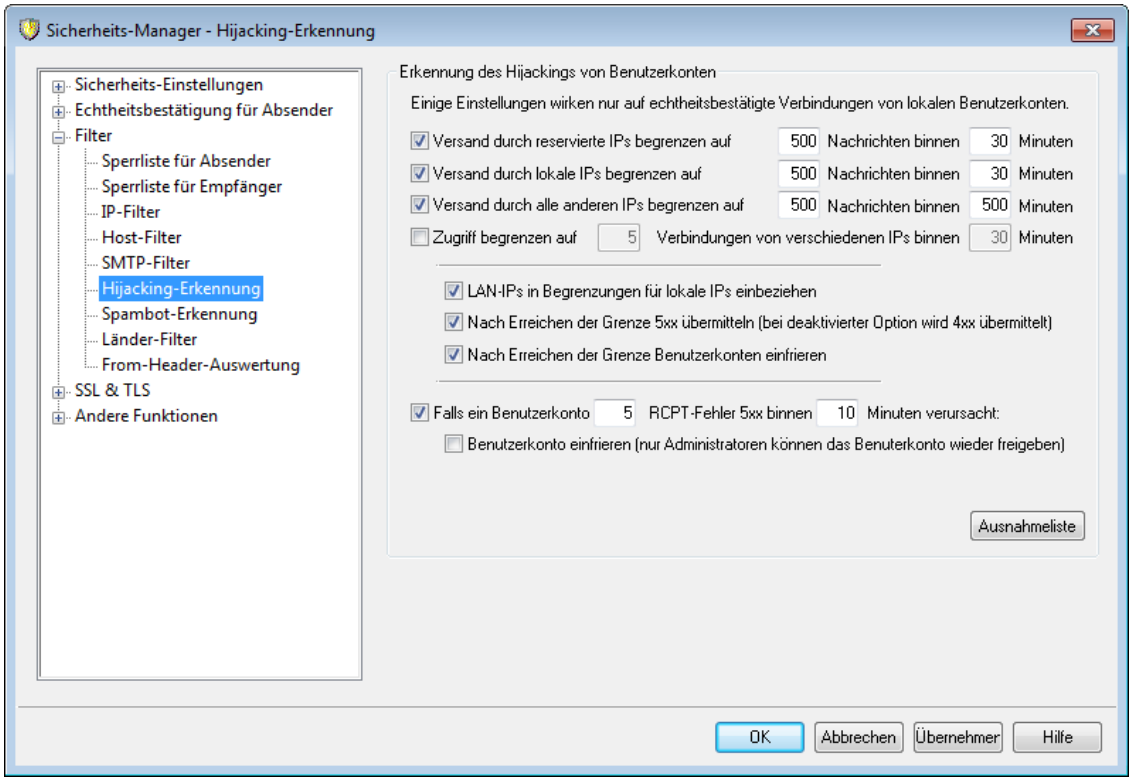
IP nicht sperren, falls SMTP-Echtheitsbestätigung verwendet wird
Diese Option bewirkt, dass Gegenstellen dann von der Behandlung durch den SMTP-Filter ausgenommen sind, wenn sie die Echtheitsbestätigung erfolgreich durchgeführt haben. Diese Option ist per Voreinstellung aktiv.

Nach Sperren einer IP Benachrichtigung senden
Wird eine IP-Adresse durch den Dynamischen Filter gesperrt, so werden die im Konfigurationsdialog für die *Berichte über gesperrte IP-Adressen* 621 konfigurierten Empfänger von dieser Sperre unterrichtet. Falls Sie solche Benachrichtigungen nach einer Sperre, die durch einen Treffer auf des SMTP-Filters veranlasst wurde, nicht wünschen, deaktivieren Sie diese Option. Diese Option ist per Voreinstellung aktiv.

Freigabeliste
Durch Anklicken dieser Schaltfläche rufen Sie die Dynamische Freigabeliste 626 auf. IP-Adressen, die in dieser Freigabeliste erfasst sind, sind von der Behandlung durch den SMTP-Filter ausgenommen.

Erweitert
Durch Anklicken dieser Schaltfläche rufen Sie den Konfigurationsdialog Dynamischer Filter 612 auf.

4.1.3.6 Hijacking-Erkennung



Erkennung des Hijackings von Benutzerkonten

Die Optionen in diesem Abschnitt dienen dazu, zu erkennen, ob ein Benutzerkonto von MDaemon möglicherweise gehijackt oder sonst kompromittiert wurde, und sodann den weiteren Versand von Nachrichten von diesem Benutzerkonto aus über Ihren Server automatisch zu unterbinden. Ein Beispiel für ein solches Hijacking ist, dass ein Spam-Versender sich die E-Mail-Adresse und das Kennwort eines Benutzerkontos verschafft; die Leistungsmerkmale zum Erkennen dieses Hijackings können dann den Spam-Versender daran hindern, von dem "gekaperten" Benutzerkonto aus massenhaft Spam- und Junk-Nachrichten über Ihren Server zu versenden. Sie können bestimmen, wie viele Nachrichten ein Benutzerkonto während einer in Minuten festgelegten Zeitspanne versenden darf, und Sie können wahlweise das Benutzerkonto sperren lassen, sobald diese Grenze erreicht wurde. Mithilfe einer *Ausnahmeliste* können Sie außerdem bestimmte Adressen von diesen Beschränkungen und Maßnahmen ausnehmen.

Die Erkennung des Hijackings von Benutzerkonten wirkt nur auf lokale Benutzerkonten und nur, soweit diese echtheitsbestätigte Verbindungen nutzen. Das Benutzerkonto des Postmasters ist von diesem Leistungsmerkmal automatisch ausgenommen.

Versand durch reservierte IPs begrenzen auf [x] Nachrichten binnen [x] Minuten
Diese Option begrenzt die Anzahl der Nachrichten, die in dem hier angegebenen Zeitraum durch MDaemon-Benutzerkonten versendet werden dürfen. Sie wirkt auf alle Nachrichten, die von reservierten IP-Adressen aus über die MDaemon-Benutzerkonten versendet werden. Die Definition der reservierten IP-Adressen

entspricht dabei weitgehend den einschlägigen RFCs (etwa 127.0.0.*, 192.168.*.*, 10.*.*.*, 172.16.0.0/12, ::1, FD00::/8, FEC0::/10 und FE80::/64).

Versand durch lokale IPs begrenzen auf [x] Nachrichten binnen [x] Minuten
Diese Option begrenzt die Anzahl der Nachrichten, die in dem hier angegebenen Zeitraum durch MDaemon-Benutzerkonten versendet werden dürfen. Sie wirkt auf alle Nachrichten, die von lokalen IP-Adressen aus über die MDaemon-Benutzerkonten versendet werden. Als lokale IP-Adressen werden dabei alle IP-Adressen behandelt, die für eine beliebige lokale MDaemon-Domäne als lokale IP-Adressen eingetragen sind.

Versand durch alle anderen IPs begrenzen auf [x] Nachrichten binnen [x] Minuten
Diese Option begrenzt die Anzahl der Nachrichten, die in dem hier angegebenen Zeitraum durch MDaemon-Benutzerkonten versendet werden dürfen. Sie wirkt auf alle Nachrichten, die von sonstigen IP-Adressen aus versandt werden, die nicht unter eine der beiden oben stehenden Einstellungen fallen.

Zugriff begrenzen auf [x] Verbindungen von verschiedenen IPs binnen [x] Minuten
Diese Option begrenzt die Anzahl der Verbindungen, die im hier angegebenen Zeitraum von verschiedenen IP-Adressen aus auf dasselbe Benutzerkonto zulässig sind. Der Arbeitsweise dieser Option liegt die Annahme zugrunde, dass in bestimmten Zeitabschnitten nicht beliebig viele Verbindungen von unterschiedlichen IP-Adressen aus mit demselben Benutzerkonto hergestellt werden. Wird beispielsweise innerhalb von fünf Minuten von 10 verschiedenen IP-Adressen aus auf dasselbe Benutzerkonto zugegriffen, so spricht dies dafür, dass es sich nicht mehr um eine normale Nutzung handelt, sondern dass das Benutzerkonto gehijackt wurde. Diese Option ist per Voreinstellung abgeschaltet.

LAN-IPs in Begrenzungen für lokale IPs einbeziehen
Diese Option bewirkt, dass LAN-IPs[610] in die Option "*Versand durch lokale IPs begrenzen...*" weiter oben einbezogen werden. Sie ist per Voreinstellung aktiv. Falls Sie die LAN-IPs nicht in die Begrenzung für lokale IPs einbeziehen wollen, deaktivieren Sie diese Option.

Nach Erreichen der Grenze 5xx übermitteln (bei deaktivierter Option wird 4xx übermittelt)
Diese Option bewirkt, dass MDaemon nach Erreichen einer oben festgelegten Grenze an das gehijackte Benutzerkonto den Meldungskode 5xx sendet. Falls Sie stattdessen einen Meldungskode 4xx senden wollen, deaktivieren Sie diese Option.

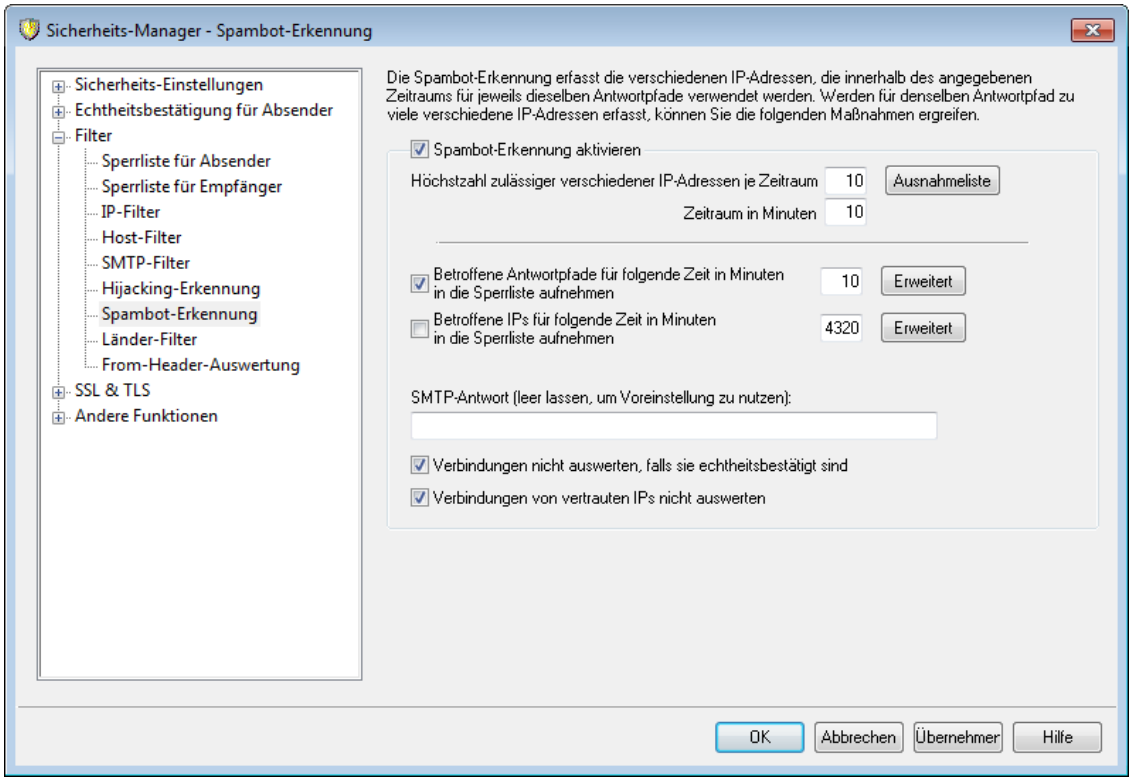
Nach Erreichen der Grenze Benutzerkonten einfrieren
Diese Option bewirkt, dass Benutzerkonten eingefroren werden, sobald einer der vorstehend bestimmten Grenzwerte überschritten ist. Tritt dieser Fall ein, so meldet der Server der Gegenstelle den Fehler 552 und trennt sofort die Verbindung; danach wird das Benutzerkonto eingefroren. Es kann dann keine Nachrichten mehr versenden und abrufen. MDaemon nimmt jedoch weiterhin die für das Benutzerkonto eingehenden Nachrichten entgegen. Der Postmaster wird per E-Mail davon informiert, dass das Benutzerkonto eingefroren wurde. Er kann durch Antwort auf die Benachrichtigung das Benutzerkonto wieder freischalten.

Falls ein Benutzerkonto [xx] RCPT-Fehler 5xx binnen [xx] Minuten verursacht
Diese Option überwacht die Anzahl der Versuche, die ein Benutzerkonto in dem hier angegebenen Zeitraum unternimmt, Nachrichten an unbekannte Empfänger zu senden. Es ist für Spam-Nachrichten charakteristisch, dass sie oft an eine große Anzahl unbekannter Empfänger versandt werden, da die Spam-Versender sie entweder an schon länger veraltete Adressen senden oder einfach Adressen durchprobieren, um auf gültige Adressen zu stoßen. Versucht ein MDaemon-Benutzerkonto daher, innerhalb eines kurzen Zeitraums Nachrichten an viele unbekannte Empfänger zu versenden, so ist dies ein guter Anhaltspunkt dafür, dass das Benutzerkonto möglicherweise kompromittiert wurde und zum Spam-Versand missbraucht wird. In Verbindung mit der Option "*Benutzerkonto einfrieren...*" weiter unten kann diese Option weiteren Schaden abwenden, indem das Benutzerkonto eingefroren wird, sobald das verdächtige Verhalten erkannt wurde. Beachte: Ungültige Empfänger, die diese Option berücksichtigt, sind Empfänger, bei denen als Antwort auf den Befehl RCPT ein Fehler 5xx gemeldet wird.

> **Benutzerkonto einfrieren (nur Administratoren können das Benutzerkonto wieder freigeben**)
> Diese Option bewirkt, dass ein Benutzerkonto eingefroren wird, sobald es die in der Option "*Falls ein Benutzerkonto [xx] RCPT-Fehler 5xx binnen [xx] Minuten verursacht*" oben definierten Schwellwerte erreicht. Der Administrator wird informiert, dass das Benutzerkonto eingefroren wurde. Er kann dann das Problem untersuchen und das Benutzerkonto wieder freigeben.

Ausnahmeliste
Mithilfe der *Ausnahmeliste* können Sie Adressen von der Erkennung des Hijackings von Benutzerkonten ausnehmen. Jokerzeichen sind zulässig. Einige Beispiele hierzu: "`newsletter@example.com`" nimmt das MDaemon-Benutzerkonto "newsletter" in der Domäne example.com aus. "`*@newsletter.example.com`" nimmt hingegen alle MDaemon-Benutzerkonten aus der Domäne newsletter.example.com aus. Das Konto des Postmasters ist von der Erkennung des Hijackings von Benutzerkonten automatisch ausgenommen.

4.1.3.7 Spambot-Erkennung



Die Spambot-Erkennung erfasst die verschiedenen IP-Adressen, die innerhalb des angegebenen Zeitraums für jeweils dieselben Antwortpfade (`SMTP MAIL`) verwendet werden. Werden für denselben Antwortpfad in einem vergleichsweise kurzen Zeitraum außergewöhnlich viele verschiedene IP-Adressen erfasst, so kann dies auf ein Spambot-Netzwerk hindeuten. Wird ein solches Spambot-Netzwerk erkannt, so wird die jeweils laufende Verbindung getrennt. Wahlweise kann auch der betroffene Antwortpfad für einen bestimmten Zeitraum in die Sperrliste aufgenommen werden. Auch die als Teil eines Spambot-Netzwerks erkannten IP-Adressen können wahlweise für einen bestimmten Zeitraum in die Sperrliste aufgenommen werden.

Spambot-Erkennung aktivieren
Diese Option aktiviert die Spambot-Erkennung. Dieses Leistungsmerkmal ist per Voreinstellung abgeschaltet.

Höchstzahl zulässiger verschiedener IP-Adressen je Zeitraum
Diese Option bestimmt, wie viele verschiedene IP-Adressen während des angegebenen Zeitraums für denselben Antwortpfad erfasst werden dürfen.

Zeitraum in Minuten
Diese Option bestimmt die Länge des Zeitraums, während dessen jeweils die Zahl der IP-Adressen je Antwortpfad gezählt wird.

Ausnahmeliste
Dieses Steuerelement öffnet die Ausnahmeliste für die Spambot-Erkennung. Sie können in die Ausnahmeliste IP-Adressen, Absender und Empfänger aufnehmen, die von der Spambot-Erkennung ausgenommen sein sollen.

Betroffene Antwortpfade für folgende Zeit in Minuten in die Sperrliste aufnehmen
Mithilfe dieser Option können Sie die Antwortpfade in die Sperrliste aufnehmen, die als Teil des Nachrichtenversands durch das Spambot-Netzwerk erkannt wurden. MDaemon nimmt Nachrichten mit solchen, in der Sperrliste erfassten, Antwortpfaden nicht mehr zur Zustellung entgegen. Die Sperre dauert jeweils die hier in Minuten angegebene Zeit. Diese Option ist per Voreinstellung abgeschaltet.

Erweitert
Dieses Steuerelement öffnet die Datendatei für Spambot-Versender. Sie enthält die jeweils gerade in der Sperrliste erfassten Antwortpfade und die Zeit, für die diese noch auf der Sperrliste verbleiben.

Betroffene IPs für folgende Zeit in Minuten in die Sperrliste aufnehmen
Mithilfe dieser Option können Sie die IP-Adressen in die Sperrliste aufnehmen, die als Teil des Nachrichtenversands durch das Spambot-Netzwerk erkannt wurden. MDaemon nimmt Nachrichten von solchen, in der Sperrliste erfassten, IP-Adressen nicht mehr zur Zustellung entgegen. Die Sperre dauert jeweils die hier in Minuten angegebene Zeit. Diese Option ist per Voreinstellung abgeschaltet.

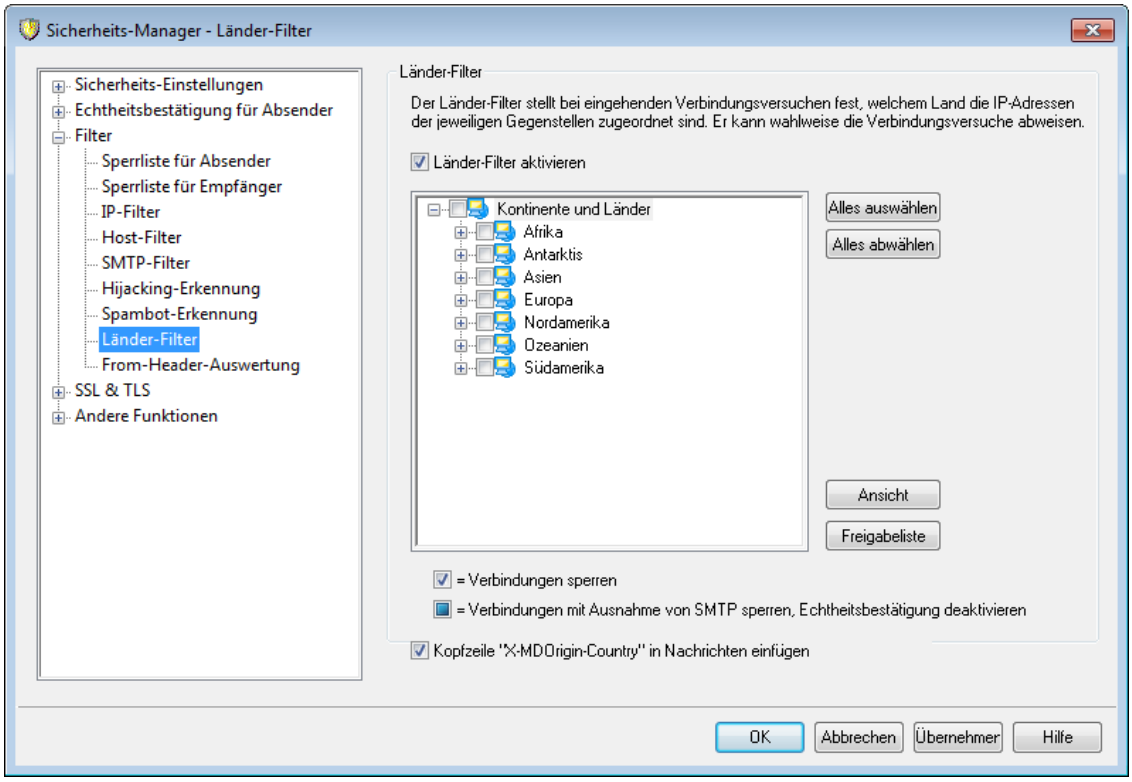
Erweitert
Dieses Steuerelement öffnet die Datendatei für Spambot-IP-Adressen. Sie enthält die jeweils gerade in der Sperrliste erfassten IP-Adressen und die Zeit, für die diese noch auf der Sperrliste verbleiben.

SMTP-Antwort (leer lassen, um Voreinstellung zu nutzen)
Mithilfe dieser Option können Sie den SMTP-Meldungstext anpassen, den MDaemon der Gegenstelle übermittelt, falls MDaemon eine Nachricht mit einem Antwortpfad oder von einer IP-Adresse auf der Sperrliste abweist. Falls hier ein Meldungstext eingetragen ist, übermittelt MDaemon dann die SMTP-Meldung "`551 5.5.1 <benutzerdefinierte SMTP-Antwort>`" anstelle der Standardmeldung. Falls Sie hier keinen Text eingeben, übermittelt MDaemon die Standardmeldung.

Verbindungen nicht auswerten, falls sie echtheitsbestätigt sind
MDaemon wertet per Voreinstellung die echtheitsbestätigten 524 Verbindungen nicht zur Spambot-Erkennung aus. Um auch die echtheitsbestätigten Verbindungen in die Auswertung einzubeziehen, deaktivieren Sie diese Option.

Verbindungen von vertrauten IPs nicht auswerten
MDaemon wertet per Voreinstellung die Verbindungen von vertrauten IP-Adressen 521 Verbindungen nicht zur Spambot-Erkennung aus. Um auch die Verbindungen von vertrauten IP-Adressen in die Auswertung einzubeziehen, deaktivieren Sie diese Option.

4.1.3.8 Länder-Filter



Länder-Filter

Der Länder-Filter ist ein auf geographische Daten gestütztes Filtersystem. Mit seiner Hilfe können Sie Verbindungsversuche für SMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery 80, XML-API, Remoteverwaltung, CalDAV/CardDAV, XMPP und Minger abweisen, falls diese Verbindungsversuche von bestimmten geographischen Regionen ausgehen, die Sie als nicht zugelassen definiert haben. MDaemon stellt fest, mit welchem Land die IP-Adressen in Verbindung stehen, von denen eingehende Verbindungen ausgehen. Verbindungen, die von gesperrten Regionen ausgehen, werden abgewiesen, und dieser Vorgang wird im Protokoll Screening vermerkt. Bei SMTP-Verbindungen kann der Länder-Filter wahlweise nur solche Verbindungen abweisen, in denen eine Echtheitsbestätigung über AUTH versucht wird. Diese Vorgehensweise ist beispielsweise dann sinnvoll, wenn Sie in einem bestimmten Land keine Benutzer haben, gleichwohl aber von dort aus Nachrichten empfangen wollen. Es werden dann nur Verbindungen abgewiesen, in denen eine Anmeldung an einem Benutzerkonto Ihres Servers versucht wird.

Das Verzeichnis `\MDaemon\Geo\` enthält Datenbankdateien, die als Hauptdatenbanken für die Zuordnung von IP-Adressbereichen zu Ländern dienen. Diese Datenbanken wurden durch MaxMind (http://www.maxmind.com) bereit gestellt. Aktualisierungen sind bei Bedarf auf der genannten Website erhältlich.

Länder-Filter aktivieren
Der Länder-Filter ist per Voreinstellung aktiv, jedoch werden in der Voreinstellung keine Regionen und Länder gesperrt. MDaemon protokolliert nur die Region und das Land, von denen die Verbindungen ausgehen. Um eine Region oder ein Land zu sperren, aktivieren Sie das Kontrollkästchen für die Region oder das Land, und klicken Sie danach auf **OK** oder **Übernehmen**. Ist der Länder-Filter aktiv, so fügt MDaemon die Kopfzeile "`X-MDOrigin-Country`" in alle Nachrichten ein. Diese Kopfzeile wird auch dann eingefügt, wenn keine Sperren bestehen, und dient dem

Inhaltsfilter und anderen Zwecken. In die Kopfzeile werden die aus zwei Buchstaben bestehenden Kennungen für Länder und Kontinente eingefügt, die im ISO-Standard 3166 definiert sind.

Alles auswählen/Alles abwählen
Mithilfe dieser Schaltflächen können Sie alle Regionen und Länder in der Liste auswählen und abwählen.

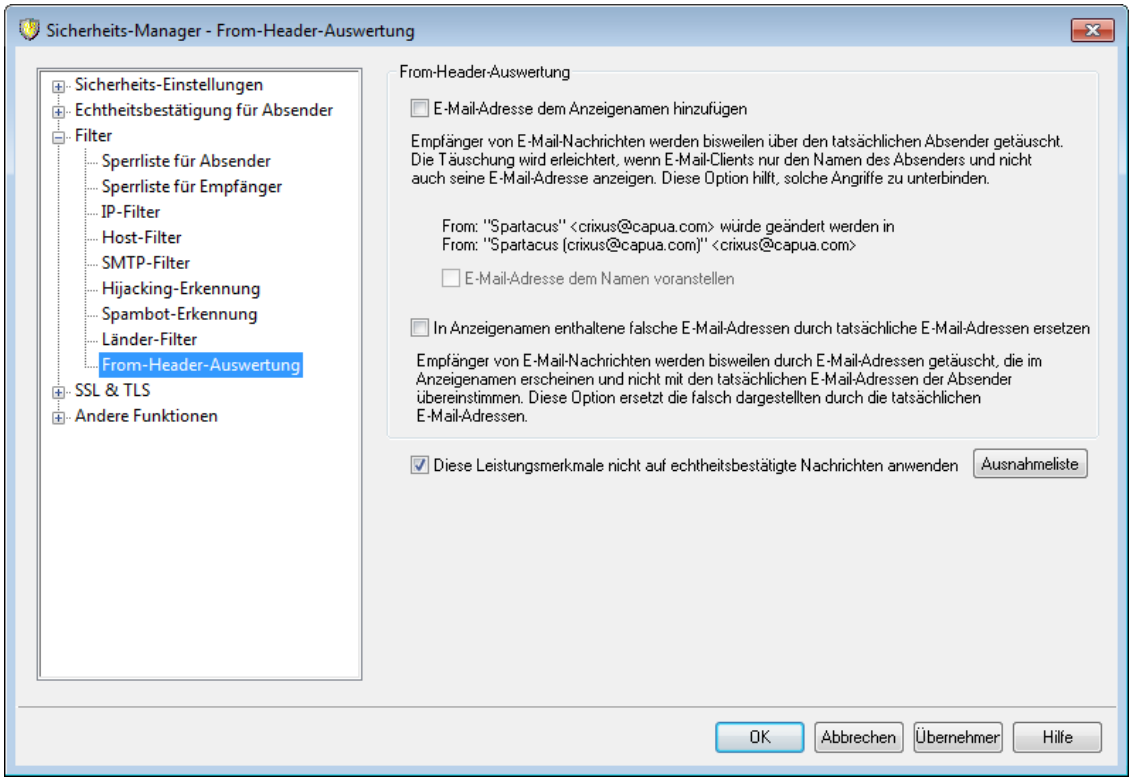
Ansicht
Durch Anklicken dieser Schaltfläche wird Ihnen eine Textdatei angezeigt, die alle derzeit durch den Länder-Filter gesperrten Länder und Regionen enthält. Haben Sie einzelne Elemente in der Liste der Länder und Regionen neu aktiviert oder deaktiviert, so ist die Schaltfläche Ansicht erst wieder verfügbar, nachdem Sie **Übernehmen** angeklickt haben.

Freigabeliste
Durch Anklicken dieser Schaltfläche wird die Freigabeliste des Dynamischen Filters 626 aufgerufen. Sie wird auch für den Länder-Filter genutzt. Falls Sie IP-Adressen von der Behandlung durch den Länder-Filter ausnehmen wollen, klicken Sie auf diese Schaltfläche, und geben Sie die IP-Adresse und die Zeitdauer an, für die Sie die IP-Adresse von der Behandlung durch den Länder-Filter ausnehmen wollen.

SMTP-Verbindungen zulassen und nur Echtheitsbestätigung unterbinden
Diese Option bewirkt, dass bei eingehenden SMTP-Verbindungen nur solche Verbindungen gesperrt werden, in denen die Gegenstelle eine Echtheitsbestätigung über AUTH versucht. Verbindungen, in denen ohne Echtheitsbestätigung nur Nachrichten übermittelt werden, bleiben zugelassen.

Kopfzeile "X-MDOrigin-Country" in Nachrichten einfügen
Ist der Länder-Filter aktiv, so fügt MDaemon die Kopfzeile "`X-MDOrigin-Country`" in alle Nachrichten ein. Diese Kopfzeile wird auch dann eingefügt, wenn keine Sperren bestehen, und dient dem Inhaltsfilter und anderen Zwecken. In die Kopfzeile werden die aus zwei Buchstaben bestehenden Kennungen für Länder und Kontinente eingefügt, die im ISO-Standard 3166 definiert sind. Falls Sie diese Kopfzeile nicht in die Nachrichten einfügen lassen wollen, deaktivieren Sie diese Option.

4.1.3.9 From-Header-Auswertung



Auswertung der Absenderkopfzeile From

Dieses Leistungsmerkmal ändert die Absenderkopfzeile "From:" eingehender Nachrichten aus Sicherheitsgründen so, dass im Namensfeld der Absenderkopfzeile, das üblicherweise nur den Namen enthält, sowohl der Name als auch die E-Mail-Adresse erscheinen. Das Leistungsmerkmal will verhindern, dass Benutzer über die Absender eingehender Nachrichten getäuscht werden und meinen, dass eine Nachricht von einer bestimmten Person stammt, wohingegen sie tatsächlich beispielsweise von einem Angreifer gesandt wurde. Eine solche Täuschung wird durch den Umstand begünstigt, dass viele E-Mail-Clients nur den Namen des Absenders und nicht auch seine E-Mail-Adresse anzeigen. Der Empfänger sieht die eigentliche E-Mail-Adresse üblicherweise erst, wenn er die Nachricht geöffnet oder einen sonstigen Vorgang durchgeführt hat, etwa, das Kontextmenü zu öffnen, oder den Mauszeiger auf dem Eintrag stehen zu lassen. Aus diesem Grund erstellen Angreifer E-Mail-Nachrichten oft so, dass in dem sichtbaren Feld der Absenderkopfzeile "From:" ein legitim erscheinender Name einer Person oder eines Unternehmens erscheint, wohingegen die E-Mail-Adresse, die Hinweise auf eine missbräuchliche Verwendung gibt, nicht angezeigt wird. So kann beispielsweise die Absenderkopfzeile "From:" einer Nachricht `"Ehrenwerte Bank und Treuhand" <langfinger.klepto@example.com>` lauten, woraufhin der E-Mail-Client nur den Teil `"Ehrenwerte Bank und Treuhand"` als Absender anzeigt. Dieses Leistungsmerkmal ändert daher den sichtbaren Teil der Absenderkopfzeile, um eine solche Täuschung offenzulegen und beide Datenelemente anzuzeigen. In dem genannten Beispiel erscheint dann der Absender beim Empfänger als `""Ehrenwerte Bank und Treuhand (langfinger.klepto@example.com)" <langfinger.klepto@example.com>"` und zeigt damit dem Empfänger an, dass die Nachricht missbräuchlich versandt wurde.

E-Mail-Adresse dem Anzeigenamen hinzufügen
Diese Option bewirkt, dass der Teil der Absenderkopfzeile "From:", der dem Empfänger angezeigt wird, in eingehenden Nachrichten geändert wird. Er enthält nach der Änderung sowohl den Namen wie auch die E-Mail-Adresse des Absenders. Durch diesen Vorgang ändert sich der Inhalt der Kopfzeile nach folgendem Schema: `"Name des Absenders" <postfach@example.com>` wird zu `"Name des Absenders (postfach@example.com)" <postfach@example.com>`. Diese Änderung wird nur in Nachrichten an lokale Benutzer durchgeführt, und sie ist per Voreinstellung abgeschaltet. Diese Option sollte umsichtig genutzt werden, da manche Benutzer eine solche Änderung des Absenders unter Umständen ablehnen, auch wenn sie ihnen bei der Erkennung missbräuchlicher Nachrichten helfen kann.

E-Mail-Adresse dem Namen voranstellen
Ist die Option *E-Mail-Adresse dem Anzeigenamen hinzufügen* weiter oben aktiv, so können Sie mithilfe dieser Option die Reihenfolge von Namen und E-Mail-Adressen in den geänderten Absenderkopfzeilen vertauschen. Die E-Mail-Adresse erscheint dann an erster Stelle. In dem oben angeführten Beispiel `"Name des Absenders" <postfach@example.com>` ergibt sich dann `"postfach@example.com (Name des Absenders)" <postfach@example.com>`.

In Anzeigenamen enthaltene falsche E-Mail-Adressen durch tatsächliche E-Mail-Adressen ersetzen
Eine weitere Taktik beim Spam-Versand ist es, in den Anzeigenamen (dies ist ein Teil der Absenderkopfzeile "From:") legitim erscheinende Namen und E-Mail-Adressen einzusetzen, obwohl die E-Mail-Adresse des tatsächlichen Absenders anders lautet. Mithilfe dieser Option können Sie in solchen E-Mail-Nachrichten die im Anzeigenamen sichtbare E-Mail-Adresse durch die tatsächliche E-Mail-Adresse des Absenders ersetzen lassen.

Diese Leistungsmerkmale nicht auf echtheitsbestätigte Nachrichten anwenden
Falls Sie die Auswertung der Absenderkopfzeile From nicht auf eingehende Nachrichten anwenden wollen, die durch MDaemon echtheitsbestätigt wurden, aktivieren Sie diese Option.

Ausnahmeliste
Mithilfe dieser Option können Sie E-Mail-Adressen in die Ausnahmeliste für die From-Header-Auswertung eintragen. Für Nachrichten, die an die dort erfassten E-Mail-Adressen gerichtet sind, werden keine Änderungen an der Absenderkopfzeile "From:" vorgenommen.

4.1.4 SSL & TLS

MDaemon unterstützt das Protokoll Secure Sockets Layer (SSL)/Transport Layer Security (TLS) für SMTP, POP und IMAP 579 sowie für die Web-Server der MDaemon-Remoteverwaltung 586 und von Webmail 582. Das SSL-Protokoll, eine Entwicklung der Netscape Communications Corporation, ist das Standardverfahren schlechthin, mit dessen Hilfe die Kommunikation zwischen Servern und Clients im Internet gesichert wird. Es unterstützt die Echtheitsbestätigung für Server, Datenverschlüsselung und wahlweise auch die Echtheitsbestätigung für Clients für TCP/IP-Verbindungen. SSL ist außerdem in allen gängigen Browsern bereits enthalten. Es genügt daher, auf dem Server ein gültiges digitales Zertifikat zu installieren, um die SSL-Funktionen des Browsers für den Zugriff auf die MDaemon-Remoteverwaltung und Webmail nutzbar zu machen.

MDaemon unterstützt für Verbindungen zu den Standardports bei Verwendung eines regulären Mailclients anstatt Webmail die Erweiterung STARTTLS über TLS für SMTP und IMAP sowie die Erweiterung STLS für POP3. Um diese Funktionen zu nutzen, muss jedoch der verwendete Mailclient nicht nur so konfiguriert sein, dass er SSL verwendet, sondern er muss die genannten Erweiterungen auch unterstützen. Dies trifft nicht auf alle Mailclients zu. Mithilfe der Abschnitte Freigabeliste für STARTTLS[590] und STARTTLS-Liste[591] in diesem Konfigurationsdialog können Sie für bestimmte Hosts und Adressen festlegen, dass diese STARTTLS nutzen müssen oder nicht nutzen dürfen.

Der Konfigurationsdialog SSL & TLS enthält weitere Abschnitte: Hierzu gehören die Konfiguration von DNSSEC[595] (DNS-Sicherheitserweiterungen, englisch DNS Security Extensions), die Konfiguration der SMTP-Erweiterungen[592] mit RequireTLS, MTA-STA und den TLS-Berichten sowie die Konfiguration von Let's Encrypt[596], die Ihnen die Nutzung der Stammzertifizierungsstelle Let's Encrypt ermöglicht.

Die Einstellungen zu den SSL-Funktionen befinden sich im Abschnitt SSL & TLS des Menüs Sicherheits-Einstellungen (erreichbar über Sicherheit » Sicherheits-Manager » SSL & TLS). Die Einstellungen zu den SSL-Ports für SMTP, POP3 und IMAP befinden sich im Abschnitt Portnummern[110] (erreichbar über Einstellungen » Server-Einstellungen).

Nähere Informationen über die Erstellung und Nutzung von SSL-Zertifikaten erhalten Sie unter:

Erstellen und Verwenden von SSL-Zertifikaten[902]

—

Das Protokoll TLS/SSL wird im Dokument RFC-4346 beschrieben: The Transport Layer Security (TLS) Protocol Version 1.1

Die SMTP-Erweiterung STARTTLS wird im Dokument RFC-3207 beschrieben: SMTP Service Extension for Secure SMTP over Transport Layer Security

Die Nutzung von TLS mit den Protokollen IMAP und POP3 wird im Dokument RFC-2595 beschrieben: Using TLS with IMAP, POP3 and ACAP

DNSSEC (die DNS-Sicherheitserweiterungen, englisch DNS Security Extensions) werden beschrieben in den Dokumenten RFC-4033: DNS Security Introduction and Requirements und RFC-4035: Protocol Modifications for the DNS Security Extensions

Eine vollständige Beschreibung von finden Sie im Dokument RFC 8689: SMTP Require TLS Option.

Die Unterstützung für MTA-STS wird beschrieben im Dokument RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

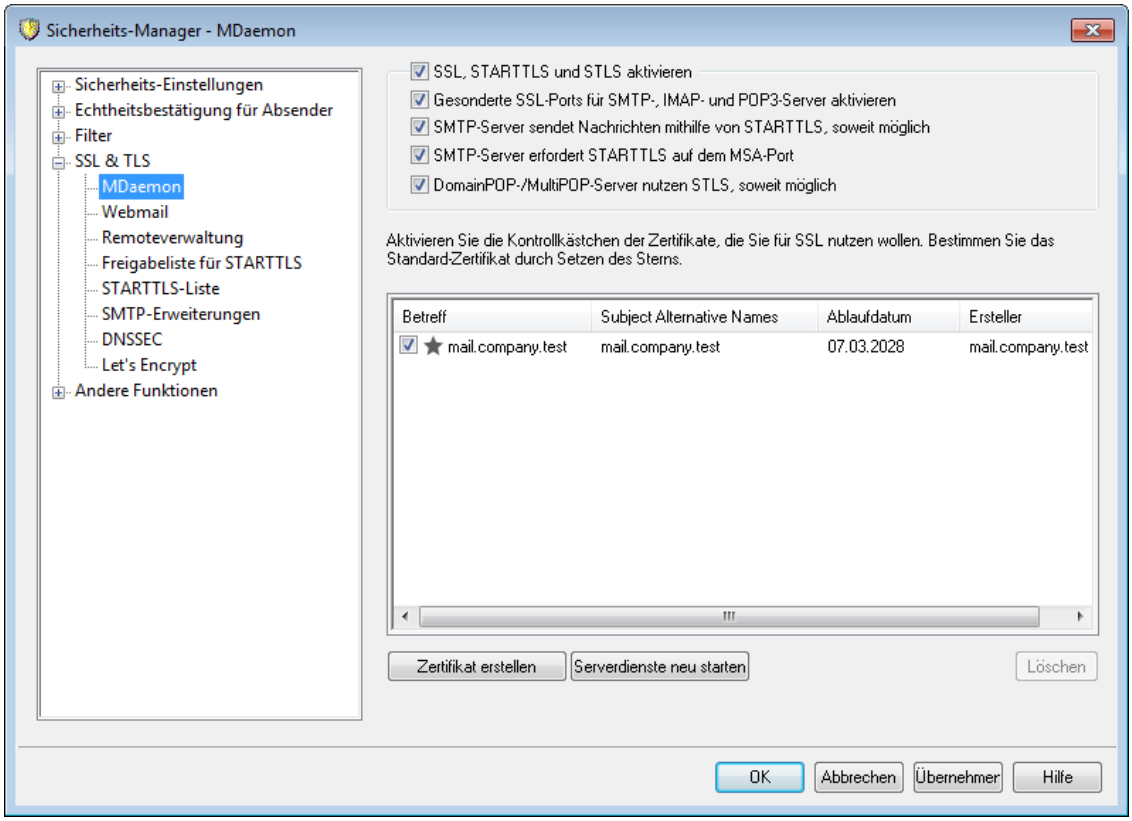
Die TLS-Berichte werden beschrieben im Dokument RFC 8460: SMTP TLS Reporting.

Die genannten Dokumente liegen in englischer Sprache vor.

Siehe auch:

SSL & TLS » MDaemon[579]
SSL & TLS » Webmail[582]
SSL & TLS » Remoteverwaltung[586]

4.1.4.1 MDaemon



SSL, STARTTLS und STLS aktivieren
Diese Option bewirkt, dass das Protokoll SSL/TLS und die Erweiterungen STARTTLS und STLS unterstützt werden. Nachdem diese Option aktiviert wurde, muss aus der Liste der Zertifikate weiter unten das zu benutzende Zertifikat ausgewählt werden.

Gesonderte SSL-Ports für SMTP-, IMAP- und POP3-Server aktivieren
Diese Option aktiviert die besonderen SSL-Ports, die im Abschnitt Portnummern 110 in der Konfiguration der Standard-Domäne definiert wurden. Clients, die auf den Standardports die Erweiterungen STARTTLS und STLS verwenden, bleiben davon unberührt. Die Option stellt lediglich zusätzliche Unterstützung für SSL zur Verfügung.

SMTP-Server sendet Nachrichten mithilfe von STARTTLS, soweit möglich
Diese Option veranlasst MDaemon, bei jedem Nachrichtenversand über SMTP zu versuchen, die Erweiterung STARTTLS zu nutzen. Unterstützt ein Server, zu dem MDaemon eine Verbindung herstellt, STARTTLS nicht, so wird die entsprechende Nachricht ohne SSL-Verschlüsselung normal zugestellt. Sie können die Nutzung von STARTTLS für einzelne Domänen durch Nutzung der Freigabeliste für STARTTLS 590 unterbinden.

SMTP-Server erfordert STARTTLS auf dem MSA-Port
Diese Option bewirkt, dass der Server für Verbindungen auf dem MSA-Port 110 STARTTLS zwingend verlangt.

DomainPOP-/MultiPOP-Server nutzen STLS, soweit möglich
Diese Option bewirkt, dass die DomainPOP- und MultiPOP-Server die Erweiterung STLS nutzen, soweit dies möglich ist.

Zertifikat zur Nutzung mit HTTPS/SSL auswählen

In dieser Liste sind Ihre SSL-Zertifikate aufgeführt. Um Zertifikate für die Nutzung durch MDaemon zu aktivieren, aktivieren Sie die zugehörigen Kontrollkästchen. Um ein Zertifikat als Standard-Zertifikat zu bestimmen, klicken Sie auf den Stern neben dem gewünschten Zertifikat. MDaemon unterstützt die Erweiterung Server Name Identification (SNI) für das Protokoll TLS. Das Leistungsmerkmal SNI (Identifizierung von Servernamen) ermöglicht die Nutzung eines eigenen Zertifikats für jeden einzelnen Hostnamen, der Ihrem Server zugeordnet ist. MDaemon prüft die aktiven Zertifikate und wählt das Zertifikat aus, in dessen Datenfeld Subject Alternative Names der jeweils angeforderte Hostname enthalten ist. (Sie legen diese Subject Alternative Names bei Erstellung des Zertifikats fest.). Falls der Client keinen bestimmten Hostnamen anfordert, oder falls MDaemon kein Zertifikat mit übereinstimmendem Hostnamen findet, nutzt MDaemon das Standard-Zertifikat. Auf der Benutzeroberfläche von MDaemon können Sie ein Zertifikat durch Doppelklick auf seinen Eintrag in der Windows-Zertifikatverwaltung öffnen und seine Eigenschaften einsehen. Diese Funktion steht in der browsergestützten Remoteverwaltung nicht zur Verfügung.

Löschen
Hierdurch wird das in der Liste ausgewählte Zertifikat gelöscht. Vor dem eigentlichen Löschvorgang erscheint ein Dialogfenster mit einer Sicherheitsabfrage, ob der Löschvorgang auch wirklich durchgeführt werden soll.

Zertifikat erstellen

Um ein SSL-Zertifikat zu erstellen, klicken Sie auf das Steuerelement Zertifikat erstellen.

Einzelheiten zu dem Zertifikat

Hostname
Hier wird der Hostname angegeben, zu dem die Benutzer eine Verbindung herstellen (z.B. "wc.example.com").

Name der Organisation/Firma
Hier wird der Name der Organisation oder der Firma eingetragen, die dieses Zertifikat besitzt.

Weitere Hostnamen (mehrere Einträge durch Kommata trennen)
Falls auf Ihrem System weitere Hostnamen konfiguriert sind, zu denen Benutzer Verbindungen herstellen, so können Sie das Zertifikat auch auf diese Hostnamen erstrecken. Geben Sie hierzu die anderen Hostnamen oder Domänennamen hier ein. Trennen Sie mehrere Einträge durch Kommata. Jokerzeichen sind zulässig, sodass sich "`*.example.com`" auf alle Subdomänen von example.com erstrecken würde (etwa "`wc.example.com`", "`mail.example.com`", usw.).

MDaemon unterstützt die Erweiterung Server Name Identification (SNI) für das Protokoll TLS. Das Leistungsmerkmal SNI (Identifizierung von Servernamen) ermöglicht die Nutzung eines eigenen Zertifikats für jeden einzelnen Hostnamen, der Ihrem Server zugeordnet ist. MDaemon prüft die aktiven Zertifikate und wählt das Zertifikat aus, in dessen Datenfeld Subject Alternative Names der jeweils angeforderte Hostname enthalten ist. Falls der Client keinen bestimmten Hostnamen anfordert, oder falls MDaemon kein Zertifikat mit übereinstimmendem Hostnamen findet, nutzt MDaemon das Standard-Zertifikat.

Länge des Schlüssels
Hier wird die gewünschte Länge des Schlüssels in Bit ausgewählt. Je länger der Schlüssel, desto besser ist der Datenaustausch gesichert. Dabei ist aber zu beachten, dass nicht alle Anwendungsprogramme Schlüssel mit einer Länge von mehr als 512 Bit verarbeiten können.

Hash-Algorithmus
Hier wird der Hash-Algorithmus ausgewählt; mögliche Algorithmen sind SHA1 und SHA2. Per Voreinstellung wird SHA2 genutzt.

Land/Region
Wählen Sie hier das Land oder die Region aus, in der sich dem oder in der sich der Server befindet.

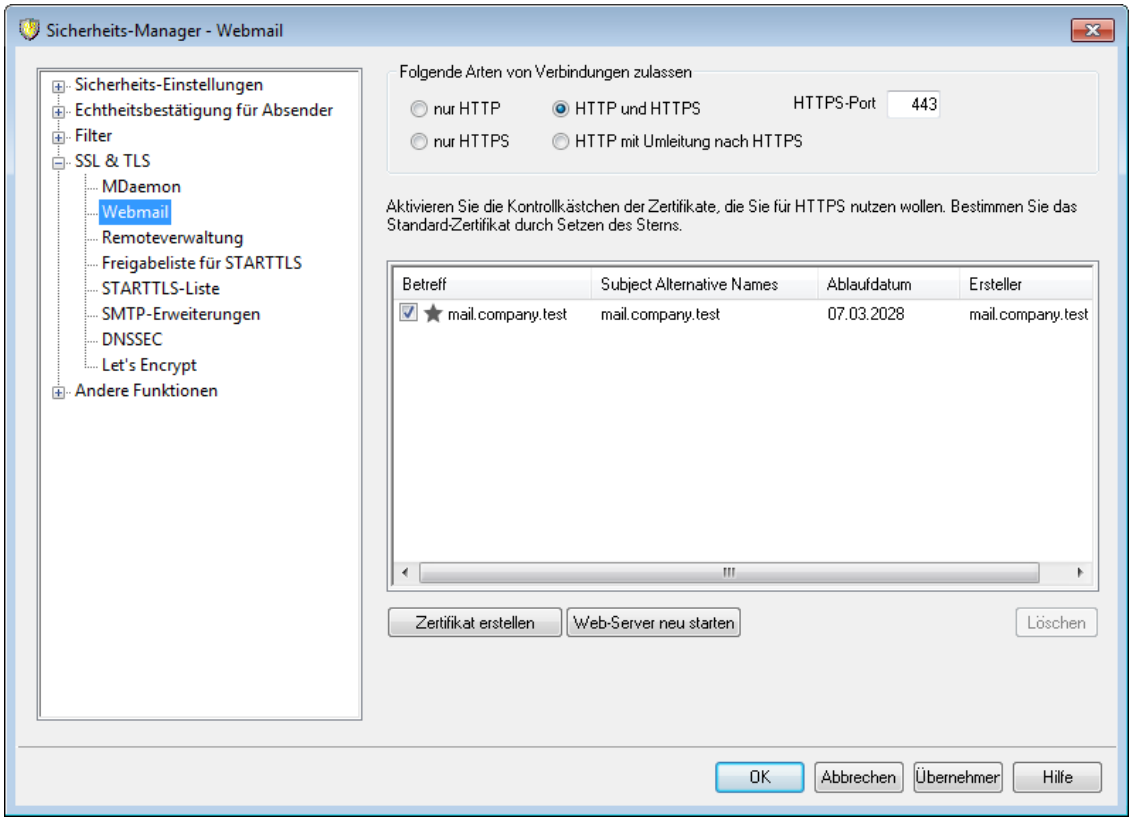
Serverdienste neu starten

Ein Klick auf dieses Steuerelement startet den Web-Server neu. Dieser Neustart ist nach jeder Änderung an einem Zertifikat erforderlich; erst danach werden neue Zertifikate genutzt.

Siehe auch:

SSL & TLS 577
Erstellen und Verwenden von SSL-Zertifikaten 902

4.1.4.2 Webmail



Der MDaemon-eigene Web-Server unterstützt das Secure-Sockets-Layer-Protokoll (SSL). SSL ist das Standardverfahren für die Sicherung webgestützter Kommunikation zwischen Server und Client. Es stellt Funktionen für die Echtheitsbestätigung des Servers, Datenverschlüsselung und zusätzliche Echtheitsbestätigung für den Client einer TCP/IP-Verbindung zur Verfügung. Da auch alle wichtigen Browser HTTPS (HTTP über SSL) unterstützen, genügt es, ein gültiges digitales Zertifikat auf dem Server zu installieren, damit beim Verbindungsaufbau eines Clients die SSL-Funktionen automatisch genutzt werden.

Die Einstellungen zu den HTTPS-Funktionen von Webmail befinden sich im Menü SSL & HTTPS, das über Einstellungen » Web- & IM-Dienste » Webmail erreichbar ist. Um die Bedienung zu vereinfachen, sind diese Einstellungen auch in dem Konfigurationsdialog "Sicherheit » Sicherheits-Manager » SSL & TLS » Webmail" gespiegelt.

Nähere Informationen über das SSL-Protokoll und die Zertifikate finden Sie unter **SSL & TLS** 577.

Diese Einstellungen wirken auf Webmail nur dann, wenn der MDaemon-eigene Web-Server verwendet wird. Ist Webmail stattdessen in die IIS oder einen anderen Web-Server eingebunden, so bleiben diese Einstellungen wirkungslos. Die Unterstützung für SSL und HTTPS muss in diesem Fall über den verwendeten Web-Server mithilfe seiner Verwaltungswerkzeuge konfiguriert werden.

Folgende Arten von Verbindungen zulassen

nur HTTP
Soll Webmail keine HTTPS-Verbindungen annehmen, so muss diese Option aktiv sein. Es sind dann nur HTTP-Verbindungen zulässig.

HTTP und HTTPS
Diese Option bewirkt, dass Webmail zwar SSL unterstützt, die Webmail-Benutzer jedoch HTTPS nicht zwingend verwenden müssen. Webmail überwacht den weiter unten konfigurierten HTTPS-Port auf eingehende Verbindungen, lässt jedoch auch normale HTTP-Verbindungen auf dem Webmail-Port zu, der im Konfigurationsdialog Web-Server 322 in der Konfiguration von Webmail definiert ist.

nur HTTPS
Diese Option bewirkt, dass Verbindungen zu Webmail ausschließlich über HTTPS hergestellt werden können. Webmail reagiert nur noch auf HTTPS-Verbindungen, nicht aber auf HTTP-Verbindungen, so lange diese Option aktiv ist.

HTTP mit Umleitung nach HTTPS
Diese Option bewirkt, dass HTTP-Verbindungen auf den HTTPS-Port umgeleitet und dann als HTTPS-Verbindungen weiter geführt werden.

HTTPS-Port
Hier wird der TCP-Port eingetragen, den Webmail auf eingehende SSL-Verbindungen überwachen soll. Die Grundeinstellung für den SSL-Port ist 443. Wird dieser SSL-Standardport verwendet, so muss beim Aufruf des URLs von Webmail keine Portnummer angegeben werden (z.B. entspricht "https://example.com" dem URL "https://example.com:443").

Diese Portnummer ist nicht dieselbe, die Webmail im Bereich Web-Server 322 im Konfigurationsdialog für Webmail zugewiesen wurde. Falls HTTP-Verbindungen zu Webmail weiterhin zugelassen sein sollen, müssen sie jenen anderen Port verwenden, sonst ist kein Verbindungsaufbau möglich. HTTPS-Verbindungen müssen hingegen auf dem HTTPS-Port hergestellt werden.

Zertifikat zur Nutzung mit HTTPS/SSL auswählen

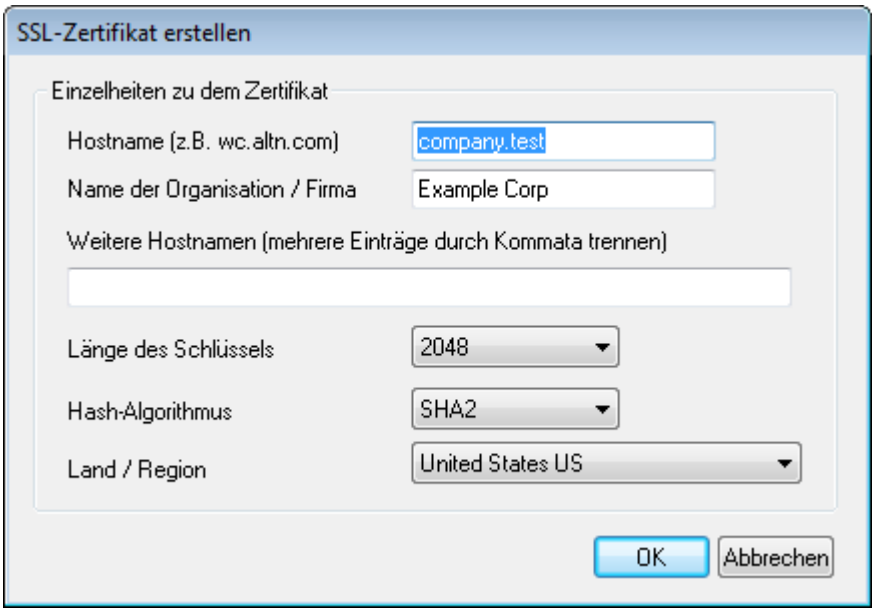
In dieser Liste sind Ihre SSL-Zertifikate aufgeführt. Um Zertifikate für die Nutzung durch MDaemon zu aktivieren, aktivieren Sie die zugehörigen Kontrollkästchen. Um ein Zertifikat als Standard-Zertifikat zu bestimmen, klicken Sie auf den Stern neben dem gewünschten Zertifikat. MDaemon unterstützt die Erweiterung Server Name Identification (SNI) für das Protokoll TLS. Das Leistungsmerkmal SNI (Identifizierung von Servernamen) ermöglicht die Nutzung eines eigenen Zertifikats für jeden einzelnen Hostnamen, der Ihrem Server zugeordnet ist. MDaemon prüft die aktiven Zertifikate und wählt das Zertifikat aus, in dessen Datenfeld Subject Alternative Names der jeweils angeforderte Hostname enthalten ist. (Sie legen diese Subject Alternative Names bei Erstellung des Zertifikats fest.). Falls der Client keinen bestimmten Hostnamen anfordert, oder falls MDaemon kein Zertifikat mit übereinstimmendem Hostnamen findet, nutzt MDaemon das Standard-Zertifikat. Auf

der Benutzeroberfläche von MDaemon können Sie ein Zertifikat durch Doppelklick auf seinen Eintrag in der Windows-Zertifikatverwaltung öffnen und seine Eigenschaften einsehen. Diese Funktion steht in der browsergestützten Remoteverwaltung nicht zur Verfügung.

Löschen
Hierdurch wird das in der Liste ausgewählte Zertifikat gelöscht. Vor dem eigentlichen Löschvorgang erscheint ein Dialogfenster mit einer Sicherheitsabfrage, ob der Löschvorgang auch wirklich durchgeführt werden soll.

Zertifikat erstellen

Um ein SSL-Zertifikat zu erstellen, klicken Sie auf das Steuerelement Zertifikat erstellen.



Einzelheiten zu dem Zertifikat

Hostname
Hier wird der Hostname angegeben, zu dem die Benutzer eine Verbindung herstellen (z.B. "wc.example.com").

Name der Organisation/Firma
Hier wird der Name der Organisation oder der Firma eingetragen, die dieses Zertifikat besitzt.

Weitere Hostnamen (mehrere Einträge durch Kommata trennen)
Falls auf Ihrem System weitere Hostnamen konfiguriert sind, zu denen Benutzer Verbindungen herstellen, so können Sie das Zertifikat auch auf diese Hostnamen erstrecken. Geben Sie hierzu die anderen Hostnamen oder Domänennamen hier ein. Trennen Sie mehrere Einträge durch Kommata. Jokerzeichen sind zulässig, sodass sich "`*.example.com`" auf alle Subdomänen von example.com erstrecken würde (etwa "`wc.example.com`", "`mail.example.com`", usw.).

MDaemon unterstützt die Erweiterung Server Name Identification (SNI) für das Protokoll TLS. Das

> Leistungsmerkmal SNI (Identifizierung von Servernamen) ermöglicht die Nutzung eines eigenen Zertifikats für jeden einzelnen Hostnamen, der Ihrem Server zugeordnet ist. MDaemon prüft die aktiven Zertifikate und wählt das Zertifikat aus, in dessen Datenfeld Subject Alternative Names der jeweils angeforderte Hostname enthalten ist. Falls der Client keinen bestimmten Hostnamen anfordert, oder falls MDaemon kein Zertifikat mit übereinstimmendem Hostnamen findet, nutzt MDaemon das Standard-Zertifikat.

Länge des Schlüssels
Hier wird die gewünschte Länge des Schlüssels in Bit ausgewählt. Je länger der Schlüssel, desto besser ist der Datenaustausch gesichert. Dabei ist aber zu beachten, dass nicht alle Anwendungsprogramme Schlüssel mit einer Länge von mehr als 512 Bit verarbeiten können.

Hash-Algorithmus
Hier wird der Hash-Algorithmus ausgewählt; mögliche Algorithmen sind SHA1 und SHA2. Per Voreinstellung wird SHA2 genutzt.

Land/Region
Wählen Sie hier das Land oder die Region aus, in der sich dem oder in der sich der Server befindet.

Web-Server neu starten

Ein Klick auf dieses Steuerelement startet den Web-Server neu. Dieser Neustart ist nach jeder Änderung an einem Zertifikat erforderlich; erst danach werden neue Zertifikate genutzt.

Verwaltung Ihres Zertifikats mithilfe von Let's Encrypt

Let's Encrypt ist eine Zertifizierungsstelle (auch Certificate Authority, kurz CA), die mithilfe eines automatisierten Verfahrens unentgeltlich Zertifikate zur Verfügung stellt. Dieses Verfahren soll die derzeit noch weit verbreiteten und komplexen Verfahren der manuellen Erstellung, Echtheitsprüfung, Signatur, Installation und Verlängerung von Zertifikaten für die Sicherung von Websites ablösen.

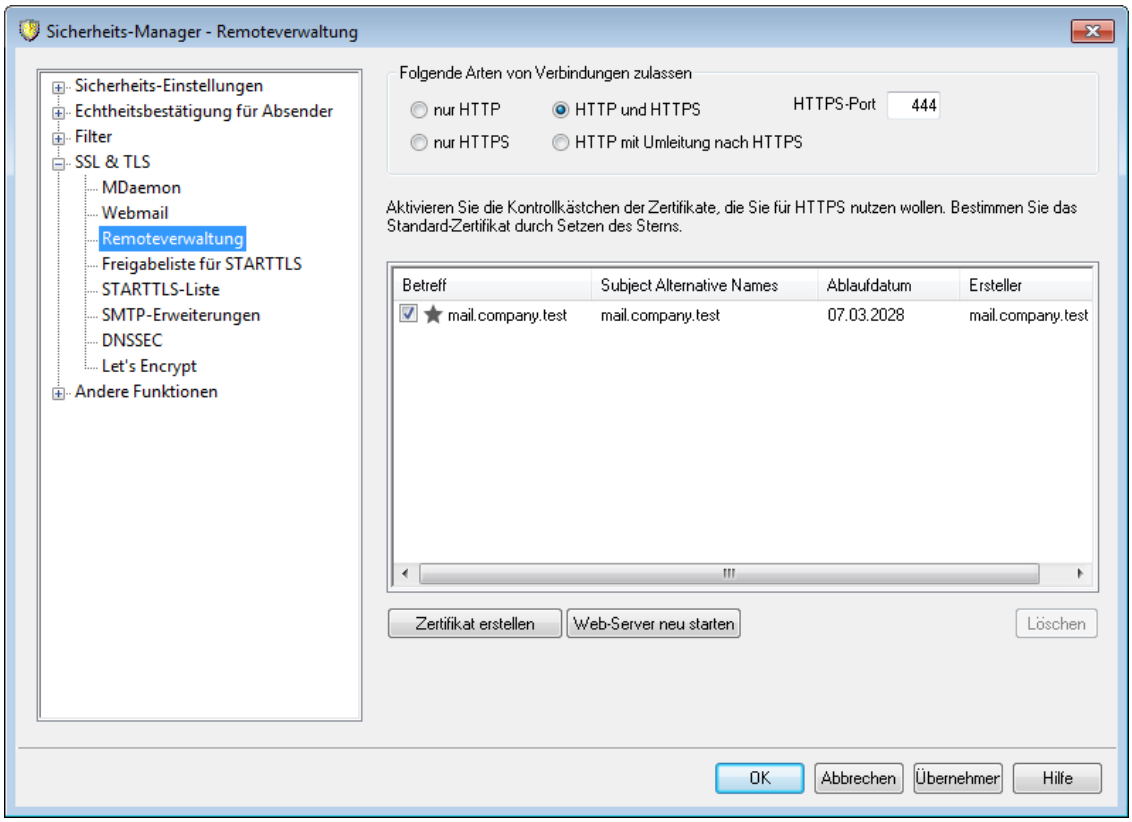
Um dieses Verfahren zu unterstützen, steht Ihnen der Konfigurationsdialog Let's Encrypt 596 zur Verfügung. Mithilfe dieses Konfigurationsdialog wird das automatische Verfahren zur Verwaltung eines Zertifikats unterstützt, das Let's Encrypt bereitstellt. Sie können hier ein PowerShell-Skript einfach konfigurieren und ausführen, das im Verzeichnis "`MDaemon\LetsEncrypt`" abgelegt ist. Wenn Sie dieses Skript ausführen, wird hierdurch das System für Let's Encrypt eingerichtet, und insbesondere werden die für die erfolgreiche Abwicklung der http-01-Challenge erforderlichen Dateien in das HTTP-Verzeichnis von Webmail kopiert. Das Skript nutzt als Domäne für das Zertifikat den SMTP-Hostnamen 184 der Standard-Domäne 181 und fügt etwa konfigurierte *Weitere Hostnamen* ein, ruft das Zertifikat ab, importiert es in Windows, und konfiguriert MDaemon so, dass das Zertifikat für MDaemon, Webmail und die Remoteverwaltung genutzt wird. Darüber hinaus erstellt das Skript im Verzeichnis "`MDaemon\Logs\`" die Protokolldatei `LetsEncrypt.log`. Diese Protokolldatei wird immer dann, wenn das Skript ausgeführt wird, gelöscht und neu erstellt. Sie beinhaltet Datum und Uhrzeit, wann das Skript ausgeführt wurde.

Falls Sie eine *E-Mail-Adresse des Administrators für Benachrichtigungen* angegeben haben, werden im Fehlerfall Benachrichtigungen an diese Adresse versandt. Nähere Informationen finden Sie im Abschnitt Let's Encrypt 596.

Siehe auch:

SSL & TLS 577
Erstellen und Verwenden von SSL-Zertifikaten 902

4.1.4.3 Remoteverwaltung



Der MDaemon-eigene Web-Server unterstützt das Secure-Sockets-Layer-Protokoll (SSL). SSL ist das Standardverfahren für die Sicherung webgestützter Kommunikation zwischen Server und Client. Es stellt Funktionen für die Echtheitsbestätigung des Servers, Datenverschlüsselung und zusätzliche Echtheitsbestätigung für den Client einer TCP/IP-Verbindung zur Verfügung. Da auch alle wichtigen Browser HTTPS (HTTP über SSL) unterstützen, genügt es, ein gültiges digitales Zertifikat auf dem Server zu installieren, damit beim Verbindungsaufbau eines Clients die SSL-Funktionen automatisch genutzt werden.

Die Einstellungen zu den HTTPS-Funktionen von WorldClient befinden sich im Menü SSL & HTTPS, das über Einstellungen » Web- & IM-Dienste » Remoteverwaltung erreichbar ist. Um die Bedienung zu vereinfachen, sind diese Einstellungen auch in dem Konfigurationsdialog "Sicherheit » Sicherheits-Einstellungen » SSL & TLS » Remoteverwaltung" gespiegelt.

Nähere Informationen über das SSL-Protokoll und die Zertifikate finden Sie unter

SSL & TLS 577.

Diese Einstellungen wirken auf die Remoteverwaltung nur dann, wenn der MDaemon-eigene Web-Server verwendet wird. Ist die Remoteverwaltung stattdessen in die IIS oder einen anderen Web-Server eingebunden, so bleiben diese Einstellungen wirkungslos. Die Unterstützung für SSL und HTTPS muss in diesem Fall über den verwendeten Web-Server mithilfe seiner Verwaltungswerkzeuge konfiguriert werden.

Folgende Arten von Verbindungen zulassen

nur HTTP
Soll die Remoteverwaltung keine HTTPS-Verbindungen annehmen, so muss diese Option aktiv sein. Es sind dann nur HTTP-Verbindungen zulässig.

HTTP und HTTPS
Diese Option bewirkt, dass die Remoteverwaltung zwar SSL unterstützt, die Benutzer der Remoteverwaltung jedoch HTTPS nicht zwingend verwenden müssen. Die Remoteverwaltung überwacht den weiter unten konfigurierten HTTPS-Port auf eingehende Verbindungen, lässt jedoch auch normale HTTP-Verbindungen auf dem Remoteverwaltungs-Port zu, der im Konfigurationsdialog Web-Server 352 in der Konfiguration der Remoteverwaltung definiert ist.

nur HTTPS
Diese Option bewirkt, dass Verbindungen zur Remoteverwaltung ausschließlich über HTTPS hergestellt werden können. Die Remoteverwaltung reagiert nur noch auf HTTPS-Verbindungen, nicht aber auf HTTP-Verbindungen, so lange diese Option aktiv ist.

HTTP mit Umleitung nach HTTPS
Diese Option bewirkt, dass HTTP-Verbindungen auf den HTTPS-Port umgeleitet und dann als HTTPS-Verbindungen weiter geführt werden.

HTTPS-Port
Hier wird der TCP-Port eingetragen, den die Remoteverwaltung auf eingehende SSL-Verbindungen überwachen soll. Die Grundeinstellung für den SSL-Port ist 444. Wird dieser SSL-Standardport verwendet, so muss beim Aufruf des URLs für die Remoteverwaltung keine Portnummer angegeben werden (z.B. entspricht "https://example.com" dem URL "https://example.com:444").

Diese Portnummer ist nicht dieselbe, die der Remoteverwaltung im Bereich Web-Server 352 im Konfigurationsdialog für die Remoteverwaltung zugewiesen wurde. Falls HTTP-Verbindungen zur Remoteverwaltung weiterhin zugelassen sein sollen, müssen sie jenen anderen Port verwenden, sonst ist kein Verbindungsaufbau möglich. HTTPS-Verbindungen müssen hingegen auf dem HTTPS-Port hergestellt werden.

Zertifikat zur Nutzung mit HTTPS/SSL auswählen

In dieser Liste sind Ihre SSL-Zertifikate aufgeführt. Um Zertifikate für die Nutzung durch MDaemon zu aktivieren, aktivieren Sie die zugehörigen Kontrollkästchen. Um ein Zertifikat als Standard-Zertifikat zu bestimmen, klicken Sie auf den Stern neben dem gewünschten Zertifikat. MDaemon unterstützt die Erweiterung Server Name Identification (SNI) für das Protokoll TLS. Das Leistungsmerkmal SNI (Identifizierung von Servernamen) ermöglicht die Nutzung eines eigenen Zertifikats für jeden einzelnen Hostnamen, der Ihrem Server zugeordnet ist. MDaemon prüft die aktiven Zertifikate und wählt das Zertifikat aus, in dessen Datenfeld Subject Alternative Names der jeweils angeforderte Hostname enthalten ist. (Sie legen diese Subject Alternative Names bei Erstellung des Zertifikats fest.). Falls der Client keinen bestimmten Hostnamen anfordert, oder falls MDaemon kein Zertifikat mit übereinstimmendem Hostnamen findet, nutzt MDaemon das Standard-Zertifikat. Auf der Benutzeroberfläche von MDaemon können Sie ein Zertifikat durch Doppelklick auf seinen Eintrag in der Windows-Zertifikatverwaltung öffnen und seine Eigenschaften einsehen. Diese Funktion steht in der browsergestützten Remoteverwaltung nicht zur Verfügung.

Löschen
Hierdurch wird das in der Liste ausgewählte Zertifikat gelöscht. Vor dem eigentlichen Löschvorgang erscheint ein Dialogfenster mit einer Sicherheitsabfrage, ob der Löschvorgang auch wirklich durchgeführt werden soll.

Zertifikat erstellen

Um ein SSL-Zertifikat zu erstellen, klicken Sie auf das Steuerelement Zertifikat erstellen.

Hostname

Hier wird der Hostname angegeben, zu dem die Benutzer eine Verbindung herstellen (z.B. "wc.example.com").

Name der Organisation/Firma
Hier wird der Name der Organisation oder der Firma eingetragen, die dieses

Zertifikat besitzt.

Weitere Hostnamen (mehrere Einträge durch Kommata trennen)
MDaemon unterstützt derzeit noch nicht mehrere Zertifikate für verschiedene Domänen; alle Domänen müssen sich dasselbe Zertifikat teilen. Falls noch weitere Hostnamen vorhanden sind, zu denen die Benutzer Verbindungen herstellen dürfen, und falls sich das Zertifikat auch auf diese Hostnamen erstrecken soll, so müssen sie hier eingetragen werden. Mehrere Einträge werden durch Kommata getrennt. Jokerzeichen sind zulässig, sodass sich "*.example.com" auf alle Subdomänen von example.com erstrecken würde (etwa "`wc.example.com`", "`mail.example.com`", usw.).

Länge des Schlüssels
Hier wird die gewünschte Länge des Schlüssels in Bit ausgewählt. Je länger der Schlüssel, desto besser ist der Datenaustausch gesichert. Dabei ist aber zu beachten, dass nicht alle Anwendungsprogramme Schlüssel mit einer Länge von mehr als 512 Bit verarbeiten können.

Hash-Algorithmus
Hier wird der Hash-Algorithmus ausgewählt; mögliche Algorithmen sind SHA1 und SHA2. Per Voreinstellung wird SHA2 genutzt.

Land/Region
Wählen Sie hier das Land oder die Region aus, in der sich dem oder in der sich der Server befindet.

Web-Server neu starten

Ein Klick auf dieses Steuerelement startet den Web-Server neu. Dieser Neustart ist nach jeder Änderung an einem Zertifikat erforderlich; erst danach werden neue Zertifikate genutzt.

Verwaltung Ihres Zertifikats mithilfe von Let's Encrypt

Let's Encrypt ist eine Zertifizierungsstelle (auch Certificate Authority, kurz CA), die mithilfe eines automatisierten Verfahrens unentgeltlich Zertifikate zur Verfügung stellt. Dieses Verfahren soll die derzeit noch weit verbreiteten und komplexen Verfahren der manuellen Erstellung, Echtheitsprüfung, Signatur, Installation und Verlängerung von Zertifikaten für die Sicherung von Websites ablösen.

Um dieses Verfahren zu unterstützen, steht Ihnen der Konfigurationsdialog Let's Encrypt 596 zur Verfügung. Mithilfe dieses Konfigurationsdialog wird das automatische Verfahren zur Verwaltung eines Zertifikats unterstützt, das Let's Encrypt bereitstellt. Sie können hier ein PowerShell-Skript einfach konfigurieren und ausführen, das im Verzeichnis "`MDaemon\LetsEncrypt`" abgelegt ist. Wenn Sie dieses Skript ausführen, wird hierdurch das System für Let's Encrypt eingerichtet, und insbesondere werden die für die erfolgreiche Abwicklung der http-01-Challenge erforderlichen Dateien in das HTTP-Verzeichnis von Webmail kopiert. Das Skript nutzt als Domäne für das Zertifikat den SMTP-Hostnamen 184 der Standard-Domäne 181 und fügt etwa konfigurierte *Weitere Hostnamen* ein, ruft das Zertifikat ab, importiert es in Windows, und konfiguriert MDaemon so, dass das Zertifikat für MDaemon, Webmail und die Remoteverwaltung genutzt wird. Darüber hinaus erstellt das Skript im Verzeichnis "`MDaemon\Logs\`" die Protokolldatei `LetsEncrypt.log`. Diese Protokolldatei wird immer dann, wenn das Skript ausgeführt wird, gelöscht und neu erstellt. Sie beinhaltet Datum und Uhrzeit, wann das Skript ausgeführt wurde. Falls Sie eine *E-Mail-Adresse des Administrators für Benachrichtigungen* angegeben

haben, werden im Fehlerfall Benachrichtigungen an diese Adresse versandt. Nähere Informationen finden Sie im Abschnitt Let's Encrypt 596.

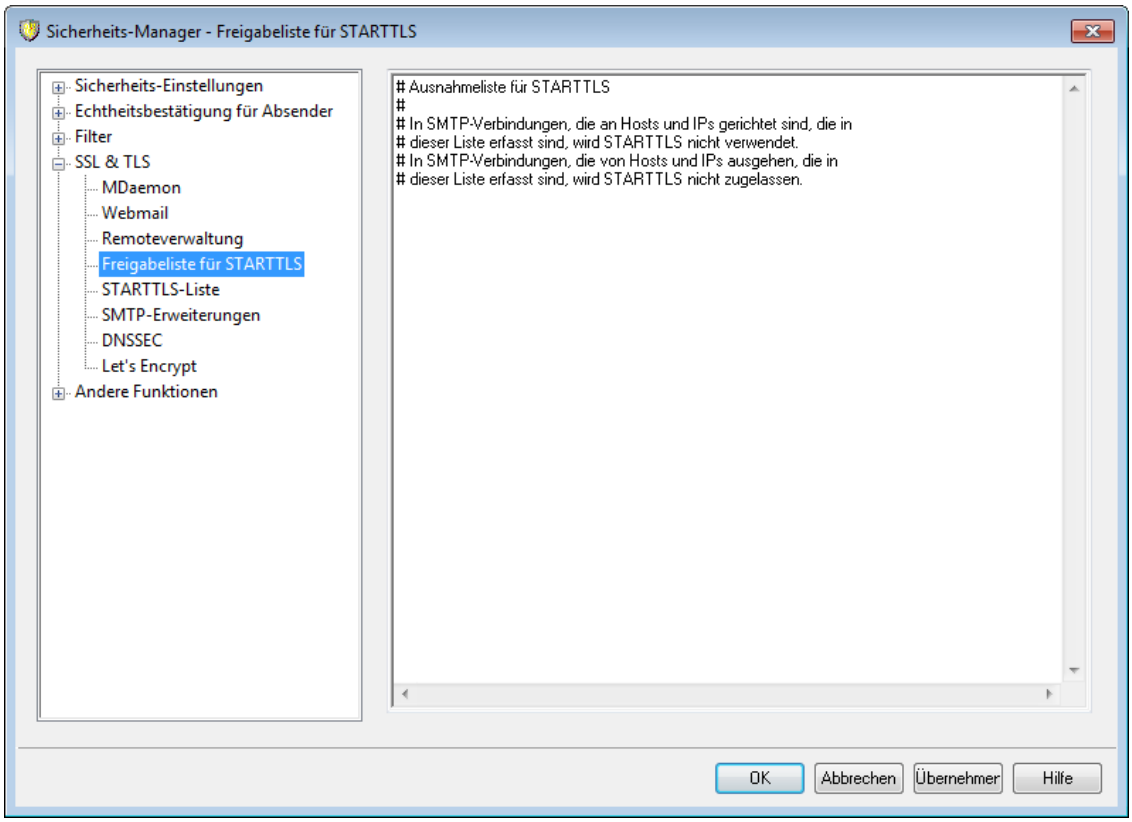
Nähere Informationen über SSL und Zertifikate erhalten Sie unter:

Die Einbindung der Remoteverwaltung in die IIS 359
SSL & TLS 577
Erstellen und Nutzung von SSL-Zertifikaten 902

Nähere Informationen über die Remoteverwaltung erhalten Sie unter:

Fernwartung 350
Remoteverwaltung » Web-Server 352
Vorlagen-Manager » Web-Dienste 795
Benutzerkonten-Editor » Web-Dienste 720

4.1.4.4 Freigabeliste für STARTTLS



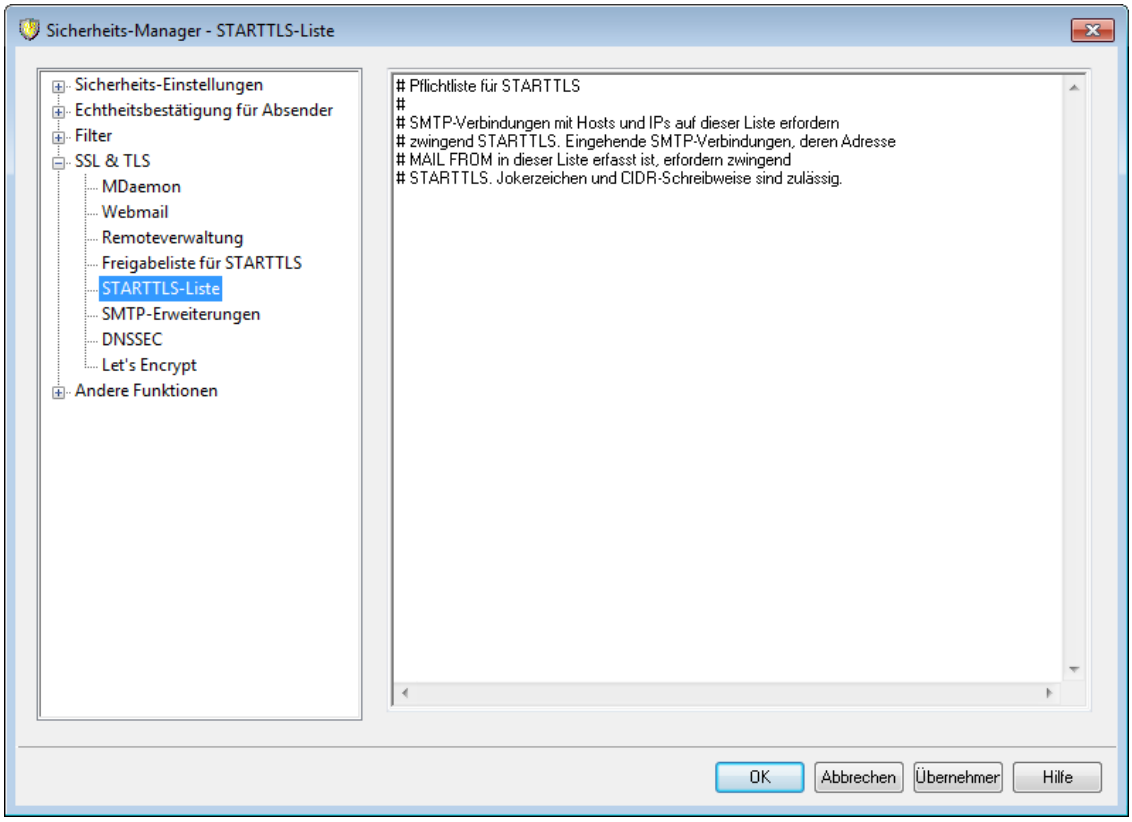
Mithilfe dieser Liste können Sie verhindern, dass bei Verbindungen mit den hier angegebenen Hosts oder IP-Adressen die Erweiterung STARTTLS verwendet wird.

Die Einträge in der Freigabeliste für STARTTLS gehen den Einträgen in der STARTTLS-Liste 591 und der Option *SMTP-Server erfordert STARTTLS auf dem MSA-Port* 579 vor.

Die SMTP-Erweiterung STARTTLS wird in dem Dokument RFC 3207 beschrieben, das unter folgender Adresse erhältlich ist:

http://www.rfc-editor.org/rfc/rfc3207.txt

4.1.4.5 STARTTLS-Liste

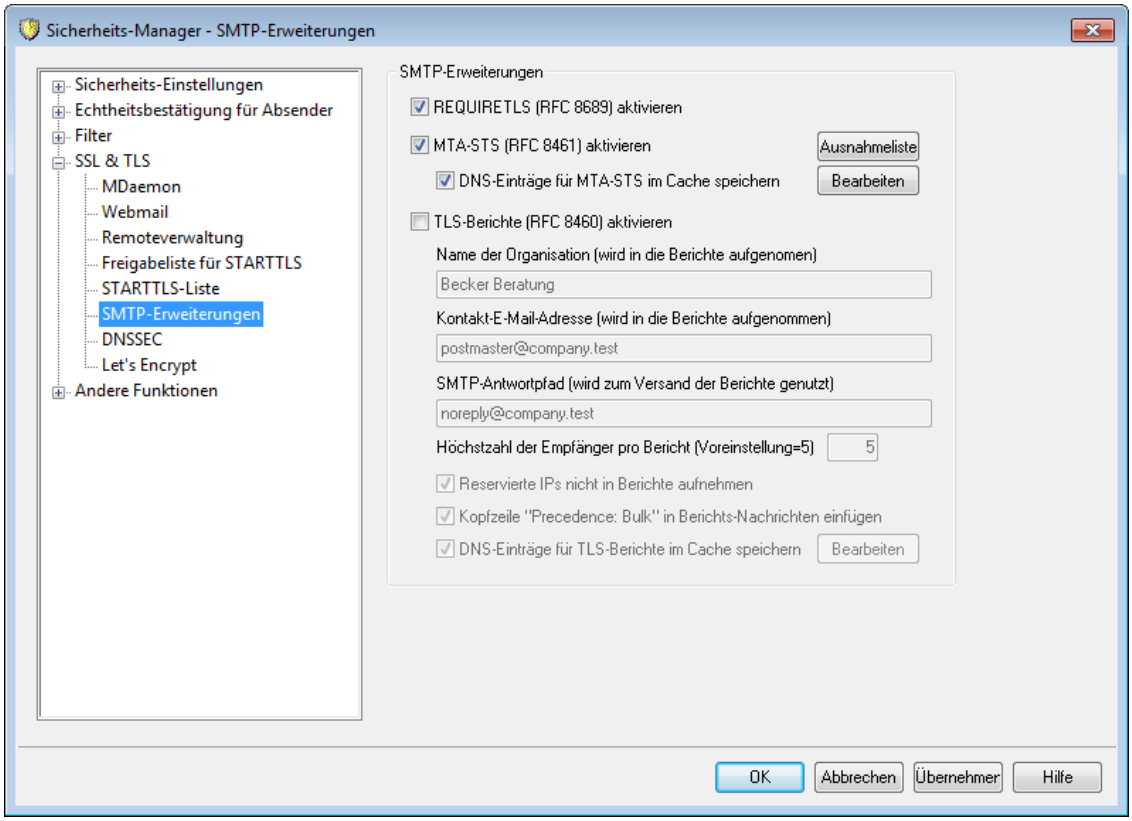


Mithilfe dieses Konfigurationsdialogs können Sie Hosts, IP-Adressen und Adressen aus dem Befehl MAIL FROM bestimmen, für die die Nutzung von STARTTLS erzwungen wird. Ohne STARTTLS können die so bezeichneten Gegenstellen keine Nachrichten mit Ihrem Server austauschen.

Die SMTP-Erweiterung STARTTLS wird in dem Dokument RFC-3207 beschrieben, das unter folgender Adresse erhältlich ist:

http://www.rfc-editor.org/rfc/rfc3207.txt

4.1.4.6 SMTP-Erweiterungen



SMTP-Erweiterungen

REQUIRETLS (RFC 8689) aktivieren
Mithilfe von RequireTLS können Sie festlegen, welche Nachrichten **zwingend** über TLS-geschützte Verbindungen übermittelt werden **müssen**. Steht TLS für die Übermittlung einer solchen Nachricht nicht zur Verfügung, oder sind die Parameter, die während des TLS-Verbindungsaufbaus und für die beteiligten Zertifikate übermittelt werden, nicht akzeptabel, so werden die Nachrichten zurückgeleitet und nicht etwa ohne TLS zugestellt. Eine vollständige Beschreibung für RequireTLS finden Sie in englischer Sprache unter RFC 8689: SMTP Require TLS Option.

RequireTLS ist per Voreinstellung aktiv. RequireTLS wirkt jedoch nur auf solche Nachrichten, die aufgrund der neuen Aktion des Inhaltsfilters 651 des Inhaltsfilters "*Nachricht für REQUIRETLS kennzeichnen...*" ("*Flag message for REQUIRETLS...*") besonders gekennzeichnet werden, oder die an nach dem Schema `<Postfach>+requiretls@Domäne.TLD` aufgebaute E-Mail-Adressen (z.B. `arvel+requiretls@mdaemon.com`) versandt werden. Regeln des Inhaltsfilters für die genannte Kennzeichnung müssen Sie selbst erstellen. Alle anderen Nachrichten werden so verarbeitet, als ob das Leistungsmerkmal nicht aktiv wäre. Nachrichten, für die RequireTLS aktiv ist, können nur dann erfolgreich versandt werden, wenn bestimmte Bedingungen alle erfüllt sind. Ist auch nur eine Bedingung nicht erfüllt, so werden die Nachrichten nicht etwa über eine unverschlüsselte Verbindung übermittelt sondern an den Absender zurückgeleitet. Folgende Bedingungen sind zu erfüllen:

- RequireTLS muss aktiv sein.

- Die fragliche Nachricht muss so gekennzeichnet sein, dass für sie die RequireTLS-Anforderungen einschlägig sind, und zwar entweder mithilfe des Inhaltsfilters oder durch Adressierung nach dem Schema "<Postfach>+requiretls@...".
- DNS-Abfragen für die MX-Hosts der Empfänger müssen mithilfe von DNSSEC 595 durchgeführt werden (hierzu finden Sie nähere Informationen weiter unten).
- Die Verbindung mit dem empfangenden Host muss mithilfe von SSL (STARTTLS) gesichert sein.
- Das SSL-Zertifikat des empfangenden Hosts muss mit dem MX-Hostnamen übereinstimmen und eine Vertrauenskette zu einer vertrauenswürdigen Stammzertifizierungsstelle (CA) aufweisen.
- Der Mailserver des Empfängers muss REQUIRETLS unterstützen und dies in der Antwort auf den Befehl EHLO bekannt geben.

RequireTLS verlangt DNSSEC-Abfragen nach den MX-Einträgen der Empfänger oder die Prüfung der MX-Einträge durch MTA-STS. Sie können DNSSEC konfigurieren 595 und dabei angeben, nach welchen Kriterien die DNSSEC-Abfragen erfolgen. Der IP-Cache 115 von MDaemon berücksichtigt jetzt die DNSSEC-Konfiguration und die entsprechenden Prüfungen. Die Hinweise am Beginn der Datendatei für die MX-Hosts 108 wurden entsprechend aktualisiert. DNSSEC verlangt entsprechend konfigurierte DNS-Server, die Sie selbst bereitstellen müssen. Deren Konfiguration ist nicht Gegenstand dieser Hilfedatei.

MTA-STS (RFC 8461) aktivieren
Die Unterstützung für MTA-STS ist per Voreinstellung aktiv. Sie finden eine Beschreibung dieses Leistungsmerkmals in englischer Sprache unter RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

Das Verfahren SMTP MTA Strict Transport Security (abgekürzt MTA-STS, Verfahren für erzwungene Transportverschlüsselung für SMTP-Mailserver) gestattet es Anbietern von E-Mail-Dienstleistungen, bekannt zu geben, dass sie durch Transport Layer Security (TLS) transportverschlüsselte SMTP-Verbindungen unterstützen. Darüber hinaus können sie festlegen, dass SMTP-Server, die Nachrichten an sie übermitteln wollen, die Übermittlung von Nachrichten an solche MX-Hosts ablehnen sollen, die TLS mit einem vertrauenswürdigen Server-Zertifikat nicht unterstützen. Um MTA-STS für Ihre eigene Domäne zu konfigurieren, ist zunächst eine Richtliniendatei erforderlich. Diese Richtliniendatei muss über HTTPS von einem URL abrufbar sein, der nach dem Schema https://mta-sts.Domäne.TLD/.well-known/mta-sts.txt gebildet ist. An die Stelle "Domäne.TLD" ist dabei Ihr eigener Domänenname zu setzen. Der Inhalt der Richtliniendatei muss Einträge des folgenden Formats enthalten:

```
version: STSv1
mode: testing
mx: mail.domain.tld
max_age: 86400
```

Als "mode" (Modus) können Sie "none" (kein MTA-STS), "testing" (MTA-STS im Versuchsbetrieb) und "enforce" (Richtlinie ist verpflichtend) einsetzen. Für jeden Ihrer MX-Hostnamen soll eine eigene Zeile "mx" enthalten sein. Subdomänen können Sie durch Jokerzeichen erfassen, etwa "*.Domäne.TLD". Der Gültigkeitszeitraum für den Eintrag (max_age) wird in Sekunden angegeben. Häufig verwendete Werte hierfür sind 86400 (dies entspricht einem Kalendertag) und 604800 (dies entspricht einer Woche).

Weiter ist ein DNS-Eintrag des Typs TXT erforderlich. Dieser Eintrag muss unter _mta-sts.Domäne. TLD abrufbar sein. An die Stelle "Domäne.TLD" ist dabei Ihr eigener Domänenname zu setzen. Der Eintrag muss dem folgenden Format entsprechen:

```
v=STSv1; id=20200206T010101;
```

Der Wert der "id" muss immer dann geändert werden, wenn sich der Inhalt der Richtliniendatei ändert. Es ist üblich, als "id" einen Zeitstempel zu verwenden.

Ausnahmeliste
Mithilfe dieser Liste können Sie einzelne Domänen von MTA-STS ausnehmen.

DNS-Einträge für MTA-STS im Cache speichern
MDaemon speichert per Voreinstellung die DNS-Einträge für MTA-STS im Cache. Um die Cache-Datei einzusehen und zu bearbeiten, klicken Sie auf das Steuerelement **Bearbeiten**.

TLS-Berichte (RFC 8460) aktivieren
Die TLS-Berichte sind per Voreinstellung deaktiviert. Sie finden eine Beschreibung dieses Leistungsmerkmals in englischer Sprache unter RFC 8460: SMTP TLS Reporting.

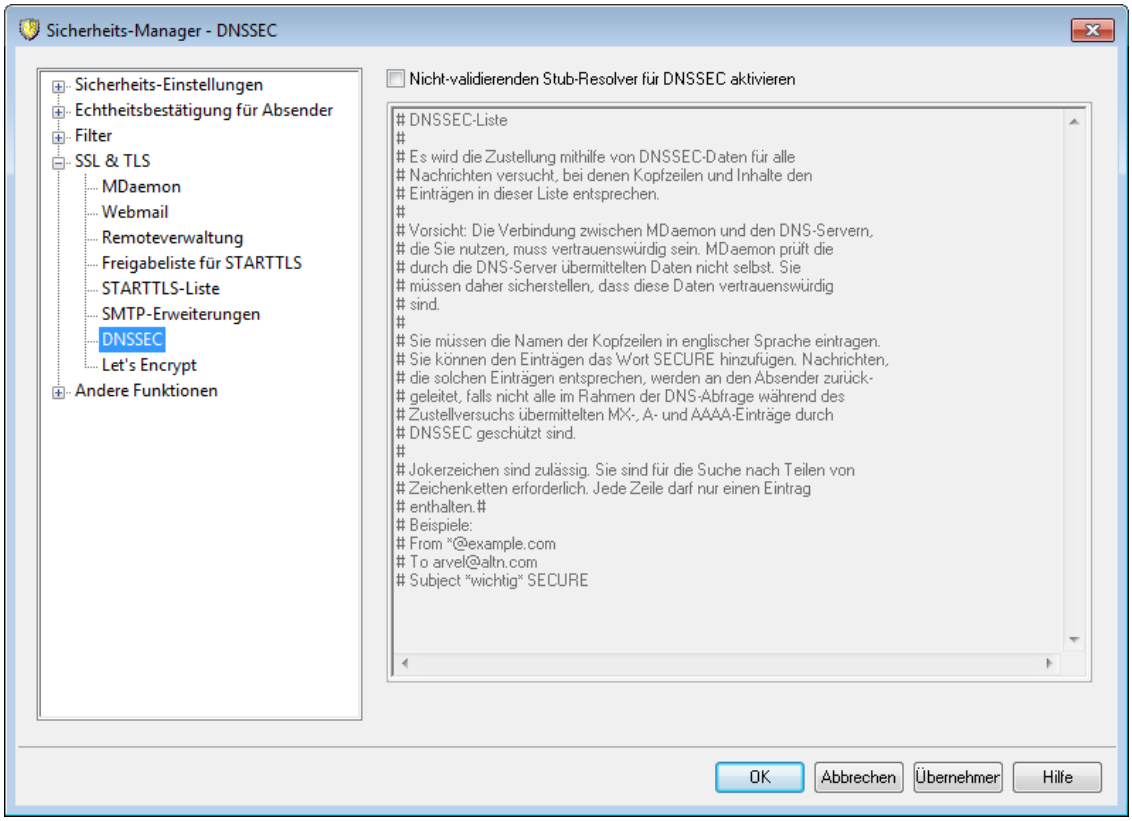
Mithilfe des Leistungsmerkmals zur Berichterstellung über SMTP TLS, kurz "TLS-Berichte" genannt, können Domänen, die MTA-STS einsetzen, Benachrichtigungen erhalten, falls der Abruf der Richtliniendatei für MTA-STS oder die Herstellung einer verschlüsselten Verbindung mittels STARTTLS fehlschlagen. Wenn dieses Leistungsmerkmal aktiv ist, sendet MDaemon einmal täglich einen Bericht an alle Domänen, an die MDaemon während des zurückliegenden Tages Nachrichten versandt oder zu versenden versucht hat, und für die MTA-STS aktiv ist.

Um die TLS-Berichte für Ihre Domäne zu aktivieren, aktivieren Sie die DKIM-Signatur, und erstellen Sie einen DNS-Eintrag des Typs TXT nach dem Schema `_smtp._tls.Domäne.TLD`, wobei "Domäne.TLD" Ihr Domänenname ist. Der DNS-Eintrag muss folgendem Format entsprechen:

```
v=TLSRPTv1; rua=mailto:postfach@domäne.tld
```

An die Stelle "Postfach@Domäne.TLD" müssen Sie die E-Mail-Adresse setzen, an die die Berichte für Ihre Domäne gesandt werden sollen.

4.1.4.7 DNSSEC



Mithilfe der Option DNSSEC (DNS Security Extensions, Sicherheitserweiterungen für DNS) kann MDaemon als nicht-validierender, sicherheitsbewusster Stub-Resolver ("Non-Validating Security-Aware Stub Resolver") arbeiten. Die RFCs 4033 und 4035 definieren einen solchen Resolver als eine Einheit, die DNS-Abfragen übermittelt, DNS-Antworten empfängt, und einen angemessen gesicherten Kanal zu einem sicherheitsbewussten rekursiv arbeitenden Nameserver aufbauen kann, der diese Dienste für den sicherheitsbewussten Stub-Resolver erbringt". Dies bedeutet, dass MDaemon in den DNS-Abfragen den DNSSEC-Dienst von Ihren DNS-Servern anfordern kann, das Kennzeichen für echtheitsbestätigte Daten (AD, Authentic Data) in den Abfragen setzen und die Antworten auf sein Vorhandensein prüfen kann. Hierdurch wird während der Verarbeitung von DNS-Daten zusätzliche Sicherheit geschaffen; da aber noch nicht alle DNS-Server und Top-Level-Domänen DNSSEC unterstützen, kann diese zusätzliche Sicherheit nur für einen Teil der anfallenden Nachrichten wirksam werden.

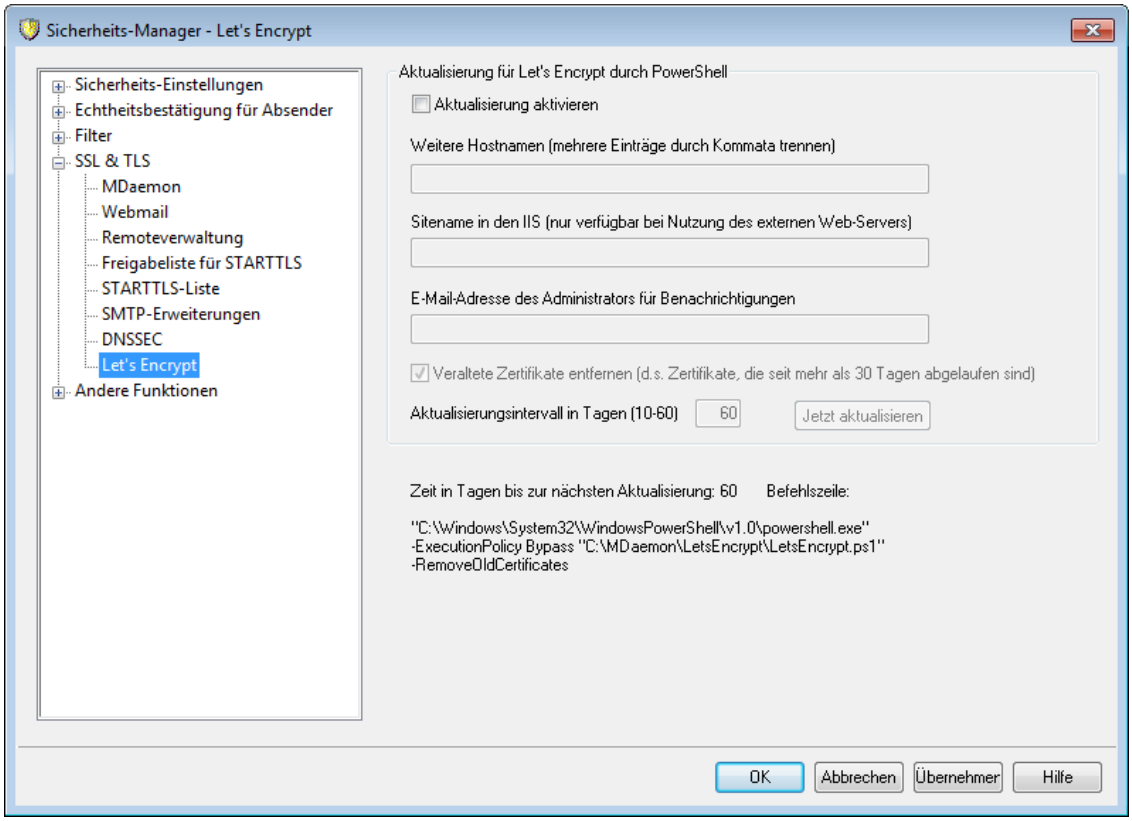
DNSSEC wirkt auch nach der Aktivierung nur auf Nachrichten, die den festgelegten Auswahlkriterien entsprechen. Sie können daher flexibel bestimmen, in welchem Umfang DNSSEC genutzt werden soll. Auf diesem Konfigurationsdialog können Sie Kombinationen aus "`Kopfzeile` und `Inhalt`" bestimmen. MDaemon fordert dann bei der DNS-Abfrage DNSSEC für alle Nachrichten an, die den hierdurch bestimmten Kriterien entsprechen. Enthalten die DNS-Antworten keine echtheitsbestätigten Daten, so führt dies grundsätzlich nicht zu negativen Folgen, und MDaemon fällt nur auf normalen DNS-Betrieb zurück. Hiervon abweichend können Sie DNSSEC für bestimmte Nachrichten *zwingend erforderlich* machen, indem Sie der Kombination aus Kopfzeile und Inhalt das Schlüsselwort "SECURE" hinzusetzen (etwa `To *@example.net SECURE`). Enthalten bei Nachrichten, die solchen Kriterien entsprechen, die DNS-Antworten keine echtheitsbestätigten Daten, so werden diese Nachrichten an die Absender zurückgeleitet. **Beachte:** DNSSEC-Abfragen nehmen mehr Zeit in Anspruch und sind ressourcenintensiver als normale DNS-Abfragen,

außerdem wird DNSSEC noch nicht durch alle Server unterstützt. MDaemon ist daher per Voreinstellung nicht darauf konfiguriert, für alle Nachrichten DNSSEC zu verwenden. Falls Sie DNSSEC für jede Nachricht verwenden wollen, fügen Sie in diesem Konfigurationsdialog den Eintrag "`To *`" hinzu.

Falls DNSSEC genutzt wurde, enthalten die Protokolle über die Übermittlung von Nachrichten zu Beginn einen entsprechenden Hinweis, und "DNSSEC" erscheint in den Protokollen neben den echtheitsbestätigten Daten.

> MDaemon ist ein nicht-validierender Stub-Resolver. Dies bedeutet, dass MDaemon zwar echtheitsbestätigte DNS-Daten von Ihrem DNS-Server anfordern, aber nicht selbst prüfen kann, ob die Daten, die hierauf zurückgemeldet werden, tatsächlich sicher sind. Um das Leistungsmerkmal DNSSEC richtig einzusetzen, müssen Sie daher sicherstellen, dass die Verbindung zu Ihrem DNS-Server vertrauenswürdig ist, etwa, weil er auf dem localhost oder in einem sicheren Netzwerk oder einer sicheren Umgebung ausgeführt wird.

4.1.4.8 Let's Encrypt



Verwaltung Ihres Zertifikats mithilfe von Let's Encrypt

Wenn Sie die Leistungsmerkmale SSL/TLS und HTTPS 577 für MDaemon 579, Webmail 582 und die Remoteverwaltung 586 nutzen wollen, müssen Sie hierfür über ein SSL/TLS-Zertifikat verfügen. Solche Zertifikate sind kleine Datendateien, die durch Zertifizierungsstellen, auch Certificate Authorities (kurz CA) genannt, ausgestellt werden. Sie ermöglichen Clients oder Browsern die Prüfung, dass diese tatsächlich

mit dem gewünschten Server verbunden sind, und sie ermöglichen die Nutzung von SSL, TLS und HTTPS, um die Verbindung zwischen Client und Server durch Verschlüsselung zu schützen. Let's Encrypt ist eine Zertifizierungsstelle, die mithilfe eines automatisierten Verfahrens unentgeltlich Zertifikate zur Verfügung stellt. Dieses Verfahren soll die derzeit noch weit verbreiteten und komplexen Verfahren der manuellen Erstellung, Echtheitsprüfung, Signatur, Installation und Verlängerung von Zertifikaten für die Sicherung von Websites ablösen.

Mithilfe dieses Konfigurationsdialog wird das automatische Verfahren zur Verwaltung eines Zertifikats unterstützt, das Let's Encrypt bereitstellt. Sie können hier ein PowerShell-Skript einfach konfigurieren und ausführen, das im Verzeichnis "`MDaemon\LetsEncrypt`" abgelegt ist. Wenn Sie dieses Skript ausführen, wird hierdurch das System für Let's Encrypt eingerichtet, und insbesondere werden die für die erfolgreiche Abwicklung der http-01-Challenge erforderlichen Dateien in das HTTP-Verzeichnis von Webmail kopiert. Das Skript nutzt als Domäne für das Zertifikat den SMTP-Hostnamen[184] der Standard-Domäne[181] und fügt etwa konfigurierte *Weitere Hostnamen* ein, ruft das Zertifikat ab, importiert es in Windows, und konfiguriert MDaemon so, dass das Zertifikat für MDaemon, Webmail und die Remoteverwaltung genutzt wird. Darüber hinaus erstellt das Skript im Verzeichnis "`MDaemon\Logs\`" die Protokolldatei `LetsEncrypt.log`. Diese Protokolldatei wird immer dann, wenn das Skript ausgeführt wird, gelöscht und neu erstellt. Sie beinhaltet Datum und Uhrzeit, wann das Skript ausgeführt wurde. Falls Sie eine *E-Mail-Adresse des Administrators für Benachrichtigungen* angegeben haben, werden im Fehlerfall Benachrichtigungen an diese Adresse versandt.

Das Skript erfordert PowerShell 5.1 und das .Net Framework 4.7.2. Aus diesem Grund kann es nicht auf Microsoft Windows 2003 ausgeführt werden. Webmail[322] muss auf Port 80 arbeiten. Das Skript funktioniert nicht, wenn Sie für Ihre Standard-Domäne einen SMTP-Hostnamen[184] (z.B. einen FQDN) eingerichtet haben, der nicht auf den MDaemon-Server verweist.

Aktualisierung für Let's Encrypt durch PowerShell

Aktualisierung aktivieren
Diese Option bewirkt, dass mithilfe des Skripts für Let's Encrypt automatisch ein SSL/TLS-Zertifikat erstellt und aktualisiert wird. Das Zertifikat wird, je nach der Einstellung für die Option *Aktualisierungsintervall in Tagen*, alle 10 bis 60 Tage erneuert.

Weitere Hostnamen (mehrere Einträge durch Kommata trennen)
Falls das Zertifikat weitere (alternative) Hostnamen enthalten soll, tragen Sie diese Hostnamen in dieses Textfeld ein. Trennen Sie mehrere Einträge durch Kommata. Der SMTP-Hostname für die Standard-Domäne braucht in dieser Liste nicht aufgeführt zu werden. Ist beispielsweise Ihre Standard-Domäne "`example.com`", und ist für sie der SMTP-Hostname "`mail.example.com`" konfiguriert, und wollen Sie zusätzlich zu diesem Hostnamen den weiteren Hostnamen "`imap.example.com`" in das Zertifikat aufnehmen lassen, so tragen Sie hier nur "`imap.example.com`" ein. Falls Sie keine weiteren Hostnamen in das Zertifikat aufnehmen lassen wollen, lassen Sie dieses Feld leer. **Beachte:** Falls Sie weitere Hostnamen angeben, muss Let's Encrypt für alle diese Hostnamen eine HTTP-Challenge erfolgreich abschließen können, da sonst nicht bestätigt werden könnte, dass der betreffende Hostname durch Ihren Server kontrolliert

wird. Schlägt auch nur eine dieser Challenges fehl, so schlägt auch der gesamte Verarbeitungsvorgang fehl.

Sitename in den IIS (nur verfügbar bei Nutzung des externen Web-Servers)
Falls Sie Webmail in die IIS eingebunden haben, geben Sie hier den IIS-Sitenamen an. Das Zertifikat kann in den IIS nur dann automatisch eingerichtet werden, wenn die Microsoft Web Scripting Tools installiert sind.

E-Mail-Adresse des Administrators für Benachrichtigungen
Falls Sie wünschen, dass ein Administrator über Fehler während einer Let's-Encrypt-Aktualisierung informiert wird, geben Sie hier seine E-Mail-Adresse an.

Veraltete Zertifikate entfernen (d.s. Zertifikate, die seit mehr als 30 Tagen abgelaufen sind)
MDaemon entfernt per Voreinstellung alle veralteten Zertifikate. Veraltete Zertifikate sind solche Zertifikate, die seit mehr als 30 Tagen abgelaufen sind. Falls Sie nicht wünschen, dass veraltete Zertifikate automatisch entfernt werden, deaktivieren Sie diese Option.

Aktualisierungsintervall in Tagen (10-60)
Mithilfe dieser Option legen Sie fest, in welchem Intervall das Zertifikat aktualisiert werden soll. Mögliche Intervalle reichen von 10 bis 60 Tage. Die Voreinstellung beträgt 60 Tage.

Jetzt aktualisieren
Durch Anklicken dieser Schaltfläche führen Sie das Skript sofort aus.

4.1.5 Andere Funktionen

4.1.5.1 Schutz gegen Rückstreuung - Übersicht

Rückstreuung

Als "Rückstreuung" (engl. "Backscatter") bezeichnet man Antworten auf E-Mail-Nachrichten, die bei Benutzern des lokalen Systems eingehen, obwohl diese Benutzer die Ursprungsnachrichten gar nicht versendet hatten. Rückstreuung tritt auf, wenn Spam oder durch Viren versandte Nachrichten einen "Antwort-Pfad" mit gefälschter Absenderadresse enthalten. Wird eine solche Nachricht durch den Server eines Empfängers abgewiesen, oder hat der Empfänger eine Abwesenheitsmeldung aktiviert, so wird die jeweilige Antwortnachricht an die gefälschte Adresse gesandt. Dies kann zu zahlreichen falschen Statusnachrichten und Nachrichten von Autobeantwortern führen, die die Postfächer der Benutzer belegen. Spam-Versender und Viren-Programmierer nützen diesen Umstand bisweilen gezielt aus, um Denial-of-Service-Angriffe gegen E-Mail-Server durchzuführen; sie lösen dazu gezielt eine Flut von Nachrichten aus, die von Servern weltweit ausgeht.

Die Lösung, die MDaemon bietet

Um die Rückstreuung zu bekämpfen, enthält MDaemon eine Funktion zum Schutz gegen Rückstreuung. Sie bewirkt, dass Statusnachrichten und Nachrichten von Autobeantwortern nur dann an die Benutzer weitergeleitet werden, wenn die Benutzer die Ursprungsnachrichten selbst versandt haben. Dazu dient ein Hashverfahren mit geheimem Schlüssel, das einen bestimmten uhrzeitabhängigen Kode in den "Antwort-Pfad" der abgehenden Nachrichten einfügt. Tritt bei der Zustellung einer solchen Nachricht ein Problem auf, und wird sie zurück geleitet,

oder geht eine automatisch erzeugte Antwort mit dem Antwort-Pfad "mailer-daemon@..." oder NULL, so erkennt MDaemon den vorher eingefügten Kode und stellt dadurch fest, dass es sich um eine legitime Antwort auf eine Nachricht handelt, die tatsächlich von einem lokalen Benutzerkonto aus versandt wurde. Enthält die Adresse den besonderen Kode nicht, oder ist der Kode mehr als sieben Tage alt, kann MDaemon die Nachricht als ungültig behandeln und abweisen.

Sie erreichen den Konfigurationsdialog Schutz gegen Rückstreuung[599] im Menü Sicherheit von MDaemon unter Sicherheit » Sicherheits-Einstellungen » Andere Funktionen » Schutz gegen Rückstreuung.

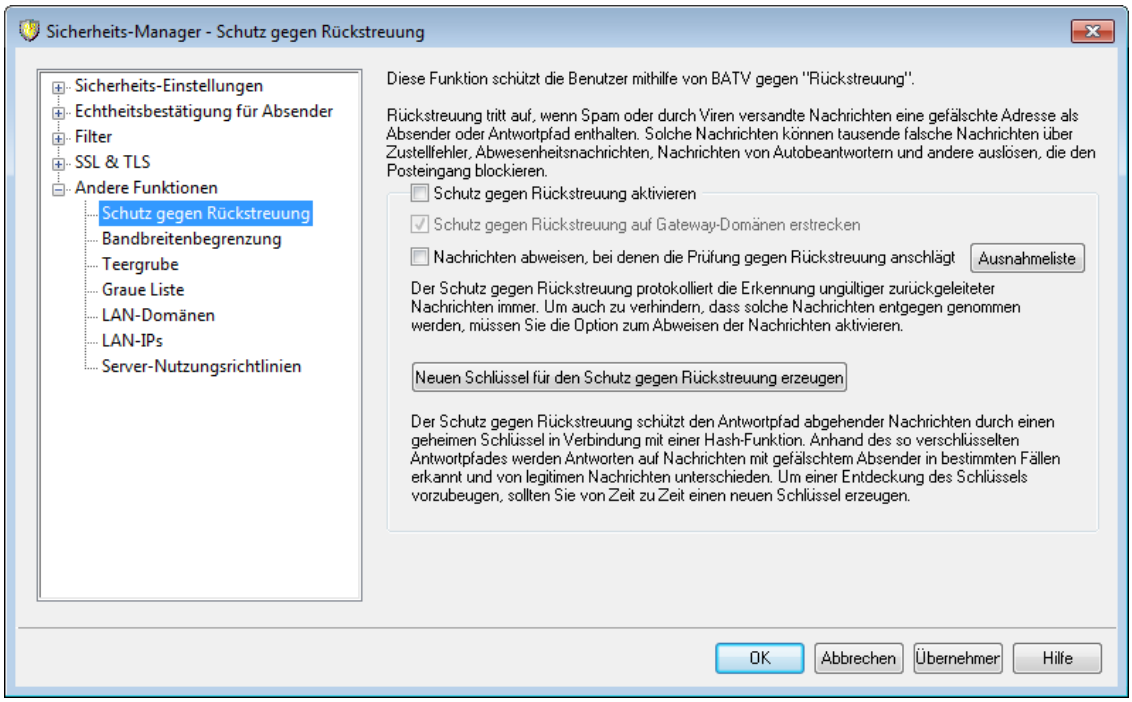
Der Schutz gegen Rückstreuung implementiert die Technik "Bounce Address Tag Validation" (kurz BATV, übersetzt Gültigkeitsprüfung von Adressen bei zurücklaufenden Nachrichten durch Tags). Nähere Informationen über BATV erhalten Sie unter:

http://www.mipassoc.org/batv/

Siehe auch:

Schutz gegen Rückstreuung[599]

4.1.5.1.1 Schutz gegen Rückstreuung



Schutz gegen Rückstreuung

Schutz gegen Rückstreuung aktivieren
Diese Option bewirkt, dass zum Schutz gegen Rückstreuung in die Adresse des Antwortpfades jeder abgehenden Nachricht ein besonderer Kode eingefügt wird. MDaemon erzeugt diesen besonderen Kode mithilfe des geheimen Schlüssels, der in der Datei rsa.private im Verzeichnis PEM_batv\ unter dem MDaemon-Verzeichnis abgelegt ist. Der Kode ist sieben Tage lang gültig. Eingehende Statusnachrichten oder andere automatisch erzeugte Nachrichten (mit dem

Antwortpfad "mailer-daemon@..." oder NULL) müssen einen gültigen, nicht verfallenen Kode enthalten, ansonsten schlägt die Prüfung fehl.

Wird diese Option deaktiviert, so fügt MDaemon den Kode zum Schutz gegen Rückstreuung nicht mehr in abgehende Nachrichten ein. MDaemon prüft aber eingehende Statusnachrichten und automatisch erzeugte Nachrichten weiterhin und stellt damit sicher, dass Nachrichten mit gültigem Kode nicht irrtümlich abgewiesen werden.

Schutz gegen Rückstreuung auf Gateway-Domänen erstrecken
Ist der Schutz gegen Rückstreuung aktiv, so kann er durch diese Option auch auf Domänen erstreckt werden, für die MDaemon als Gateway oder Backup-Server arbeitet (siehe Domänen-Gateways 250).

Nachrichten abweisen, bei denen die Prüfung gegen Rückstreuung anschlägt
Diese Option bewirkt, dass Statusnachrichten oder andere automatisch erzeugte Nachrichten abgewiesen werden, falls sie die Prüfung gegen Rückstreuung nicht bestehen. Nachrichten mit dem Antwort-Pfad "mailer-daemon@..." oder NULL bestehen die Prüfung nicht, falls sie den besonderen Kode nicht enthalten oder falls sie einen Kode enthalten, dessen siebentägige Gültigkeit abgelaufen ist. Der Schutz gegen Rückstreuung arbeitet sehr zuverlässig; falsche positive Treffer oder "Grauzonen" gibt es nicht. Eine Nachricht ist sicher gültig oder ungültig. Aus diesem Grund kann eine Fehlfunktion beim Abweisen ungültiger Nachrichten nicht auftreten, so lange sichergestellt ist, dass alle abgehenden Nachrichten aller Benutzerkonten den besonderen Kode enthalten. In allen Fällen, auch wenn Nachrichten trotz nicht bestandener Prüfung nicht abgewiesen werden, wird das Ergebnis der Prüfung gegen Rückstreuung in die Protokolldatei SMTP-in.log eingetragen. Eingehende Nachrichten für Gateways werden nur dann abgewiesen, wenn die Option *Schutz gegen Rückstreuung auf Gateway-Domänen erstrecken* weiter oben aktiv ist.

Die Option zum Abweisen von Nachrichten sollte erst etwa eine Woche nach Aktivieren des Schutzes gegen Rückstreuung ebenfalls aktiviert werden. In der Zwischenzeit können immer noch Statusnachrichten oder automatisch erzeugte Nachrichten auf solche Nachrichten hin eingehen, die vor Aktivierung des Schutzes gegen Rückstreuung versandt worden waren. Würden ungültige Nachrichten sofort abgewiesen, wären auch die erwünschten Statusnachrichten und automatisch erzeugten Nachrichten hiervon betroffen. Nach etwa einer Woche hingehen sollte es gefahrlos möglich sein, mit dem Abweisen zu beginnen. Dieselbe Vorsichtsmaßnahme ist nach dem Erzeugen eines neuen Schlüssels angebracht; der alte Schlüssel sollte nicht sofort gelöscht sondern noch für sieben Tage beibehalten werden, wie es MDaemon empfiehlt (siehe *Neuen Schlüssel für Schutz gegen Rückstreuung erzeugen* weiter unten).

Ausnahmeliste
Durch Anklicken dieses Steuerelements rufen Sie die Ausnahmeliste für den Schutz gegen Rückstreuung auf. In dieser Liste können Sie alle IP-Adressen

und Domänen erfassen, die vom Schutz gegen Rückstreuung ausgenommen sein sollen.

Neuen Schlüssel für Schutz gegen Rückstreuung erzeugen
Ein Klick auf dieses Steuerelement erzeugt einen neuen Schlüssel für den Schutz gegen Rückstreuung. MDaemon nutzt diesen Schlüssel, um die besonderen Kodes zu erzeugen und zu prüfen, die in abgehende Nachrichten eingefügt werden. Der Schlüssel wird in einer Datei mit Namen `rsa.private` im Verzeichnis `PEM\_batv\` unter dem MDaemon-Verzeichnis abgelegt. Beim Erzeugen eines neuen Schlüssels erscheint ein Dialogfenster, das den Benutzer darüber informiert, dass der bisherige Schlüssel noch für sieben Tage beibehalten und zur Prüfung genutzt wird, falls der Benutzer ihn nicht sofort löschen will. In den meisten Fällen sollte hier "Nein" angeklickt werden, damit der Schlüssel für weitere sieben Tage beibehalten wird. Wird der Schlüssel sofort gelöscht, so könnte dies dazu führen, dass einige Nachrichten die Prüfung gegen Rückstreuung nicht bestehen, da sie noch einen Kode enthalten, der mithilfe des gelöschten Schlüssels erzeugt wurde.

Falls der Postverkehr über verschiedene Server verteilt abgewickelt wird, kann es erforderlich sein, denselben Schlüssel durch alle anderen Server oder Mail Transfer Agents (MTAs) nutzen zu lassen.

Siehe auch:

Schutz gegen Rückstreuung - Übersicht 598

4.1.5.2 Bandbreitenbegrenzung - Übersicht

Die Funktionen zur Bandbreitenbegrenzung gestatten die Überwachung und Steuerung der von MDaemon genutzten Übertragungsbandbreite durch Drosselung der Übertragungsgeschwindigkeit. Die gewünschte Geschwindigkeit für Verbindungen und die einzelnen Serverdienste lässt sich so beeinflussen; für alle wichtigen Serverdienste von MDaemon sind nach Domänen sowie Domänen-Gateways getrennte Einstellungen möglich. Auch Verbindungen im lokalen Netzwerk lassen sich durch Wahl der entsprechenden Option "Local traffic "("Lokaler Datenverkehr") aus einem Rollmenü beeinflussen. Die hier vorgenommenen Einstellungen wirken sich auf Verbindungen aus, die entweder von einer lokalen IP-Adresse oder einem lokalen Domänennamen ausgehen oder zu diesen hergestellt werden.

Die Bandbreitenbegrenzung kann entweder nach Verbindungen oder Serverdiensten getrennt gesteuert werden. Bei Steuerung nach Verbindungen wird jede einzelne Verbindung unabhängig von den anderen auf die ihr zugewiesene Übertragungsgeschwindigkeit gedrosselt. Mehrere gleichzeitig bestehende Verbindungen, die jeweils von demselben Serverdienst genutzt werden, können dabei die Datenrate überschreiten, die einem bestimmten Serverdienst zugewiesen ist. Arbeitet die Bandbreitenbegrenzung nach Serverdiensten getrennt, so überwacht MDaemon die gesamte Übertragungsgeschwindigkeit aller gleichzeitig bestehenden Verbindungen, die von demselben Serverdienst genutzt werden, und weist jeder Verbindung einen gleich großen Anteil an der gesamten für den Serverdienst zulässigen Bandbreite zu. Die entsprechende Begrenzung wirkt sich also von der Zahl unabhängig auf alle Verbindungen des jeweils gesteuerten Serverdienstes aus.

Soll die Bandbreitenbegrenzung auch Domänen-Gateways erfassen, so muss sie hierfür etwas anders arbeiten als bei normalen Domänen, da mit Domänen-Gateways

keine bestimmte IP-Adresse verknüpft ist. MDaemon muss den Parameter auswerten, der mit dem RCPT-Befehl übermittelt wurde, um festzustellen, ob eine eingehende SMTP-Verbindung an den Gateway gerichtet ist. Falls dies zutrifft, werden die Regeln für die Bandbreitenbegrenzung bei eingehenden SMTP-Verbindungen angewendet. Wegen der Beschränkungen des SMTP-Protokolls greift die Bandbreitenbegrenzung auch dann für eine Verbindung insgesamt ein, wenn nur ein einziger Empfänger einer an mehrere Adressaten gerichteten Nachricht an ein Domänen-Gateway gerichtet ist.

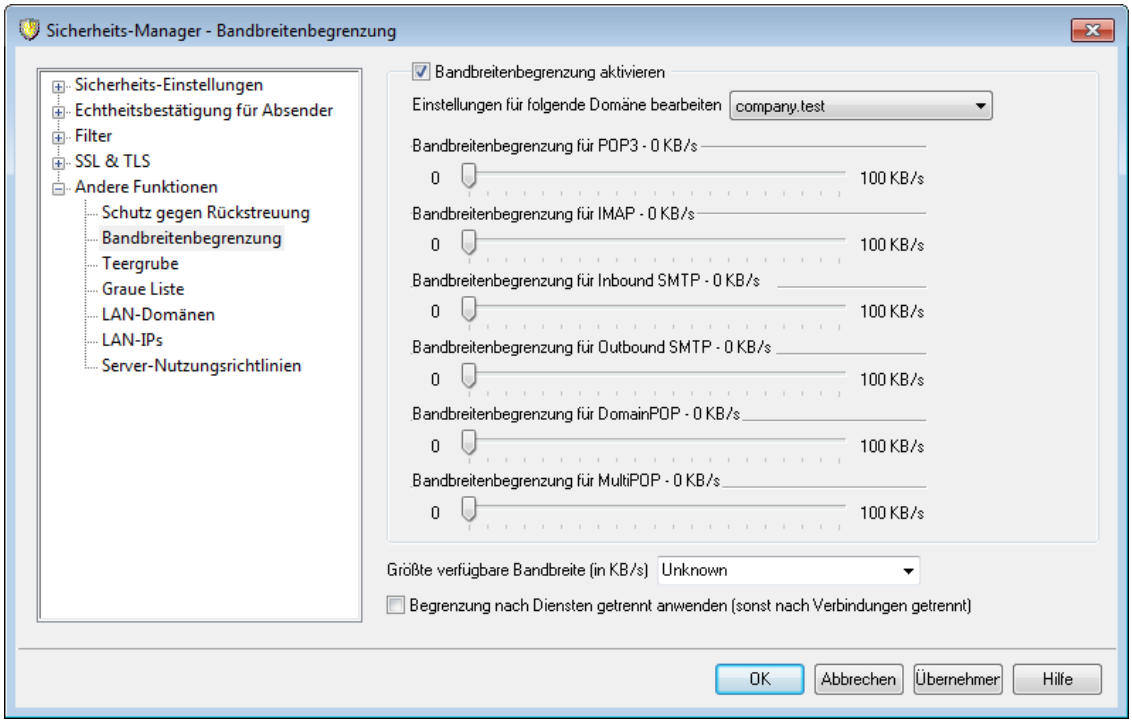
Das System zur Bandbreitenbegrenzung rechnet in Kilobyte pro Sekunde (KB/s). Der Wert 0 bewirkt, dass die Geschwindigkeit, mit der eine Verbindung (oder ein Serverdienst) arbeitet, nicht gedrosselt wird und demzufolge die gesamte verfügbare Bandbreite nutzen darf. Der Wert 10 beispielsweise veranlasst MDaemon, die Übertragungsgeschwindigkeit so zu drosseln, dass sie höchstens 10 KB/s erreicht und diesen Wert nur geringfügig überschreitet.

Zu Beginn einer Verbindung können Spitzen im Übertragungsvolumen auftreten, welche die gesetzten Werte überschreiten. Die Bandbreitenbegrenzung wirkt sich im Verlauf der Verbindung aus, und nach kurzer Zeit wird die Verbindung auf die gewünschte Bandbreite gedrosselt.

Siehe auch:

Bandbreitenbegrenzung 602
LAN-IP-Adressen 610

4.1.5.2.1 Bandbreitenbegrenzung



Bandbreitenbegrenzung aktivieren
Um die Funktionen zur Bandbreitenbegrenzung zu nutzen, aktivieren Sie diese Option.

Einstellungen für folgende Domäne bearbeiten
Aus diesem Rollmenü wird zunächst die gewünschte Domäne ausgewählt. Ihre Einstellungen für die einzelnen Serverdienste können anschließend getrennt von den Einstellungen für die anderen Domänen bearbeitet werden. Der Wert 0 in einem Feld bewirkt, dass die Übertragungsbandbreite dieses Serverdienstes nicht begrenzt wird. Der letzte Eintrag im Rollmenü lautet "Local traffic" ("Lokaler Datenverkehr"). Die Einstellungen zur Bandbreitenbegrenzung für diesen Eintrag bestimmen die Übertragungsbandbreite für den lokalen Datenverkehr (also Verbindungen innerhalb des LAN, die nicht zu externen Gegenstellen aufgebaut werden). Im Konfigurationsdialog LAN-IP-Adressen 610 werden die IP-Adressen eingetragen, die als lokal im Sinne des lokalen Datenverkehrs behandelt werden sollen.

Dienste

Bandbreitenbegrenzung für [Serverdienst] – [xx] KB/s
Nach Auswahl einer Domäne aus dem Rollmenü werden die Bandbreitenbeschränkungen für die einzelnen Serverdienste dieser Domäne mit Hilfe der hier aufgeführten Steuerelemente festgelegt. Der Wert 0 bewirkt, dass die Bandbreite für den betreffenden Serverdienst nicht begrenzt wird. Ein anderer Wert als 0 gibt in Kilobyte pro Sekunde die höchstzulässige Bandbreite für den betreffenden Serverdienst an.

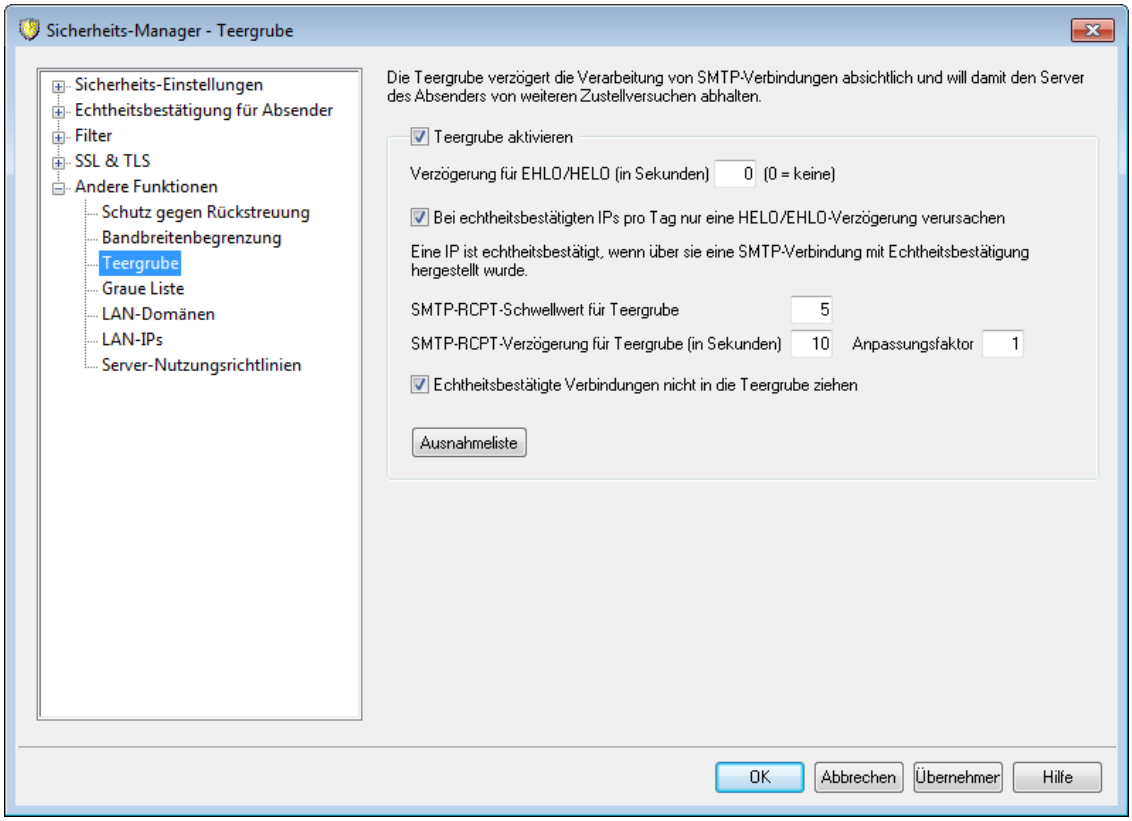
Größte verfügbare Bandbreite (KB/s)
Aus diesem Rollmenü muss die maximale Übertragungsgeschwindigkeit der benutzten Internet-Verbindung in Kilobyte pro Sekunde ausgewählt werden.

Begrenzung nach Diensten getrennt anwenden (sonst nach Verbindungen getrennt)
Diese Option bewirkt, dass die Bandbreitenbegrenzung nach Serverdiensten und nicht, wie vorgegeben, nach Verbindungen getrennt arbeitet. Bei der Steuerung nach Serverdiensten wird die Übertragungsbandbreite, die einem Dienst zugewiesen ist, unter allen Verbindungen, die dieser Dienst nutzt, gleichmäßig aufgeteilt. Die gesamte Bandbreite, die beispielsweise durch mehrere IMAP-Clients, die gleichzeitig Verbindungen zum Server aufbauen, genutzt wird, kann daher den Wert nie überschreiten, der dem Serverdienst IMAP zugewiesen wurde. Die Begrenzung ist von der Anzahl der gleichzeitig mit dem Server verbundenen Clients unabhängig. Bei einer Begrenzung nach Verbindungen hingegen kann keine IMAP-Verbindung für sich allein, wohl aber können mehrere gleichzeitig bestehende Verbindungen in der Summe ihrer Bandbreiten den pro einzelner Verbindung festgesetzten Wert überschreiten.

Siehe auch:

Bandbreitenbegrenzung - Übersicht 601

4.1.5.3 Teergrube



Sie erreichen die Teergrube im Menü Sicherheit über Sicherheit » Sicherheits-Einstellungen » Andere Funktionen » Teergrube.

Die Teergrube kann eine Verbindung gezielt verlangsamen, sobald eine vorher eingestellte Anzahl von RCPT-Befehlen von dem Absender der Nachricht empfangen wurde. Dies soll Spam-Versender von dem Versuch abhalten, große Mengen unerwünschter E-Mail ("Spam") durch das eigene System zu versenden. Einstellbar sind dabei sowohl die Anzahl der RCPT-Befehle als Schwellwert für die Aktivierung der Teergrube als auch die Zeit in Sekunden, für die immer dann eine Verzögerung verursacht wird, wenn ein neuer Befehl der Gegenstelle in der fraglichen Verbindung empfangen wurde. Der Hintergedanke dieser Vorgehensweise ist, dass ein so geschütztes System für Spam-Versender uninteressant wird, weil der Versand jeder einzelnen Nachricht extrem lange dauert, und dass Spam-Versender dadurch von weiteren Versuchen abgehalten werden, unerwünschte Post über das System zu versenden.

Teergrube aktivieren
Dieses Kontrollkästchen aktiviert die Teergrube.

Verzögerung für EHLO/HELO (in Sekunden)
Diese Option verzögert die Antwort des Servers auf die SMTP-Befehle EHLO/HELO. Die Verzögerung dieser Antworten um nur etwa 10 Sekunden kann durch ein geringeres Spam-Aufkommen bereits erheblich Systemlast und Verarbeitungszeit sparen. Spammer sind oft auf eine sehr schnelle Zustellung ihrer Nachrichten angewiesen und warten daher nicht lange auf die Antwort auf EHLO/HELO-Befehle. Auch bei einer nur kurzen Verzögerung warten die Programme, die Spammer zum Nachrichtenversand nutzen, manchmal die Antwort nicht ab, sondern geben den Zustellversuch auf und versuchen es beim nächsten

Server. Verbindungen auf dem MSA-Port (der im Abschnitt Portnummern 110 des Konfigurationsdialogs Server-Einstellungen eingestellt wird), sind von dieser Verzögerung nicht betroffen. Die Voreinstellung für diese Option ist 0, sodass die Antworten auf EHLO/HELO-Befehle nicht verzögert werden.

Bei echtheitsbestätigten IPs pro Tag nur eine HELO/EHLO-Verzögerung verursachen
Soll für Verbindungen mit Echtheitsbestätigung, die von derselben IP-Adresse ausgehen, nur eine EHLO/HELO-Verzögerung pro Tag eintreten, so muss diese Option aktiv sein. Bei der ersten Nachricht, die von der IP-Adresse aus übermittelt wird, tritt die Verzögerung ein, bei allen weiteren Nachrichten derselben IP-Adresse jedoch nicht mehr.

SMTP-RCPT-Schwellwert für Teergrube
Hier wird die Anzahl der SMTP-Befehle RCPT angegeben, die während einer SMTP-Verbindung von der jeweiligen Gegenstelle gesendet werden dürfen. Erst bei Überschreiten dieser Schwelle wird die Teergrube aktiv. Ist hier etwa der Wert 10 eingestellt, und versucht der Absender, eine Nachricht an 20 Benutzer zu versenden (dazu wären 20 RCPT-Befehle nötig), so führt MDaemon die ersten 10 Befehle normal aus und verzögert nach jedem weiteren empfangenen Befehl den Protokolldialog um die Zeit, die im Feld *SMTP-RCPT-Verzögerung für Teergrube* eingegeben wird.

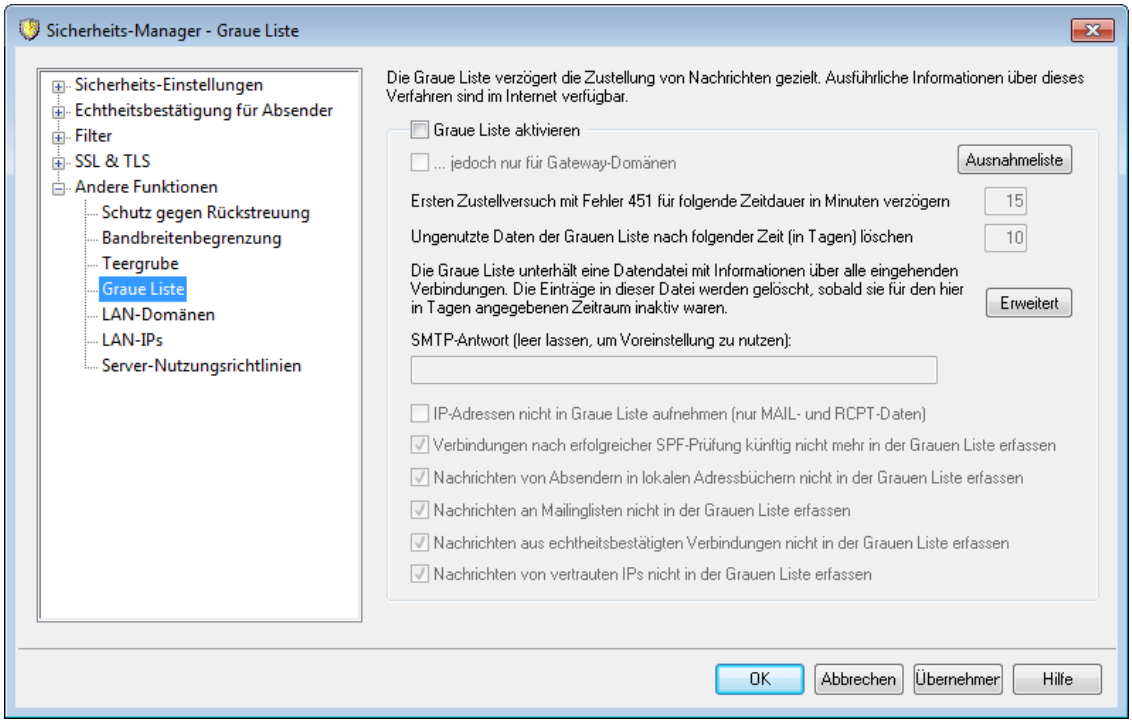
SMTP-RCPT-Verzögerung für Teergrube (in Sekunden)
Sobald der oben konfigurierte *SMTP-RCPT-Schwellwert für Teergrube* von einer Gegenstelle überschritten wird, verzögert MDaemon den Protokolldialog nach jedem weiteren RCPT-Befehl um die hier in Sekunden angegebene Zeit, so lange die Verbindung besteht.

Anpassungsfaktor
Dieser Wert ist ein Multiplikator, der die Verzögerung durch die Teergrube mit der Zeit erhöht. Wird der Schwellwert für die Aktivierung der Teergrube erreicht, und wird daraufhin die jeweilige Verbindung durch die Teergrube verzögert, so wird jede Verzögerungszeit mit dem Anpassungsfaktor multipliziert, um den Wert für die nächste Verzögerung in dieser Verbindung zu erhalten. Betragen die Verzögerungszeit zum Beispiel 10 und der Anpassungsfaktor 1.5, so dauert die erste Verzögerung 10 Sekunden, die zweite 15, die dritte 22.5, dann 33.75, und so weiter (also 10 x 1.5 = 15, 15 x 1.5 = 22.5 usw.).Die Voreinstellung für den Anpassungsfaktor ist 1; hierdurch wird die Verzögerungszeit nicht erhöht.

Echtheitsbestätigte Verbindungen nicht in die Teergrube ziehen
Diese Option bewirkt, dass Absender nicht von der Teergrube erfasst werden, wenn sie Verbindungen mit Echtheitsbestätigung nutzen.

Ausnahmeliste
Durch Anklicken dieser Schaltfläche rufen Sie die Dynamische Freigabeliste 626 auf, die auch für die Teergrube genutzt wird. In dieser Ausnahmeliste können Sie die IP-Adressen bestimmen, die von der Behandlung durch die Teergrube ausgenommen sind.

4.1.5.4 Graue Liste



Sie erreichen die Graue Liste im Menü Sicherheit über Sicherheit » Sicherheits-Einstellungen » Andere Funktionen » Graue Liste.

Die Graue Liste ist eine Technik zur Bekämpfung von Spam. Sie nutzt die Tatsache, dass SMTP-Server die Zustellung von Nachrichten wiederholt, bei deren erstem Zustellversuch der Server des Empfängers den Fehlerkode für einen vorübergehenden Fehler gemeldet hat (etwa "Bitte versuchen Sie es später erneut." oder "Please try again later."). Wird diese Technik genutzt, und trifft eine Nachricht von einer Gegenstelle ein, die nicht bereits in einer Freigabeliste erfasst oder dem System bislang nicht bekannt war, so werden Absender und Empfänger der Nachricht und die IP-Adresse des zustellenden Servers protokolliert; danach wird die Nachricht während der SMTP-Übertragung unter Hinweis auf einen vorübergehenden Fehler abgewiesen. Während eines bestimmten Zeitraums (beispielsweise 30 Minuten) werden auch erneute Zustellversuche unter Hinweis auf einen vorübergehenden Fehler abgewiesen. Da Spam-Versender üblicherweise keinen erneuten Zustellversuch unternehmen, wenn eine Nachricht abgewiesen wird, kann die Graue Liste das Spam-Aufkommen deutlich senken. Selbst wenn ein Spam-Versender jedoch einen erneuten Zustellversuch unternimmt, könnte er in der Zwischenzeit durch eine andere Technik zur Spam-Abwehr identifiziert werden (wie etwa die Sperrlisten für DNS 704), und die Nachrichten würden trotz erneutem Zustellversuch aufgrund anderer Kriterien abgewiesen werden. Bei Nutzung dieser Technik muss jedoch bedacht werden, dass nicht nur die Zustellung von Spam, sondern auch die legitimer Nachrichten, durch diese Technik verzögert wird. Es ist auch wichtig, zu bedenken, dass sich nicht vorhersagen lässt, wie lange der Server des Absenders wartet, bis er einen neuen Zustellversuch unternimmt. Daher kann das absichtliche Abweisen einer Nachricht auch unter Hinweis auf einen vorübergehenden Fehler und unter Verwendung des entsprechenden Fehlerkodes die Zustellung einer Nachricht um wenige Minuten oder sogar einen ganzen Tag verzögern.

Die Nutzung der Grauen Liste bringt einige bekannte Probleme und unerwünschte Nebenwirkungen mit sich, und der Konfigurationsdialog enthält Einstellungen, die das Verhalten der Grauen Liste in solchen Situationen steuern.

Zunächst wird in manchen Domänen ein ganzer Pool an Mailservern zum Versand abgehender Nachrichten eingesetzt. Hierbei könnte jeder Zustellversuch von einem anderen Mailserver ausgeführt und damit fälschlich nicht als erneuter Zustellversuch für eine vorher abgewiesene Nachricht, sondern als erster Zustellversuch einer neuen Nachricht erkannt werden. Hierdurch vervielfacht sich die Zeit, bis ein Zustellversuch erfolgreich durchgeführt werden kann, da jeder neue Zustellversuch als eigene Nachricht in der Grauen Liste erfasst wird. Bei Absenderdomänen, die das SPF nutzen, kann die SPF-Abfrage dieses Problem lösen. Außerdem kann durch eine entsprechende Option die IP-Adresse des Mailservers des Absenders ignoriert werden. Diese Einstellung verringert zwar die Wirksamkeit der Grauen Liste, sie löst aber die genannten Probleme im Zusammenhang mit Serverpools vollständig.

Weiter führt die Nutzung der Grauen Liste üblicherweise zu großen Datenbanken, da alle eingehenden Verbindungen erfasst werden müssen. MDaemon verringert die Notwendigkeit der Erfassung von Verbindungen, soweit es möglich ist, indem die Bearbeitung der Grauen Liste gegen Ende des SMTP-Verarbeitungsdurchlaufs stattfindet. MDaemon kann daher alle anderen Techniken zur Spam-Abwehr einsetzen, bevor eine Verbindung in der Grauen Liste erfasst wird. Dadurch wird die Datenbankgröße für die Graue Liste deutlich verringert, und da die Datenbank komplett im Hauptspeicher gehalten wird, ist die Leistungsfähigkeit des Servers nur wenig eingeschränkt.

Schließlich sind mehrere Einstellungen vorhanden, mit deren Hilfe sich die Wirkungen der Grauen Liste auf legitime Nachrichten nach Möglichkeit verringern lässt. So lassen sich Nachrichten an Mailinglisten von der Grauen Liste ausschließen. Weiter verfügt die Graue Liste über eine eigene Freigabeliste, in der IP-Adressen und Adressen von Absendern und Empfängern erfasst werden können, die von der Grauen Liste ausgenommen sein sollen. Außerdem kann das private Adressbuch eines jeden Benutzerkontos als Freigabeliste genutzt werden; Nachrichten an einen Benutzer sind dann von der Grauen Liste ausgenommen, wenn die Absender im privaten Adressbuch des Benutzers eingetragen sind.

Nähere Informationen über die Technik der Grauen Liste im Allgemeinen erhalten Sie auf der Website von Even Harris unter:

http://projects.puremagic.com/greylisting/

Graue Liste

Graue Liste aktivieren
Diese Option aktiviert die Nutzung der Grauen Liste für MDaemon.

...jedoch nur für Gateway-Domänen
Diese Option bewirkt, dass die Graue Liste Nachrichten nur erfasst, wenn sie an Gateway-Domänen gerichtet sind.

Ausnahmeliste
Dieses Steuerelement öffnet die Ausnahmeliste, in der Absender, Empfänger und IP-Adressen eingetragen werden können, die von der Bearbeitung durch die Graue Liste ausgenommen sein sollen.

Ersten Zustellversuch mit Fehler 451 für folgende Zeitdauer in Minuten verzögern
Der hier einzustellende Wert gibt in Minuten an, wie lange erneute Zustellversuche nach dem ersten Versuch durch die Graue Liste vorübergehend

abgewiesen werden sollen. Während dieser Zeit werden alle weiteren Zustellversuche abgewiesen, wenn die zu ihnen gehörende Kombination aus Server, Absender und Empfänger (eine sog. Dreiergruppe der Grauen Liste) bereits in der Grauen Liste erfasst ist. Nach Ablauf dieser Zeit werden Zustellversuche der erfassten Kombination aus Server, Absender und Empfänger erst dann wieder abgewiesen, wenn der Eintrag in der Datenbank der Grauen Liste verfallen ist.

Dauer in Tagen, bis ungenutzte Einträge in der Grauen Liste verfallen
Nachdem die erste Sperrdauer für die Graue Liste für eine bestimmte Dreiergruppe abgelaufen ist, werden keine weiteren Nachrichten durch die Graue Liste verzögert, auf die diese Dreiergruppe passt. Werden jedoch von dieser Dreiergruppe für die hier in Tagen angegebene Zeitdauer überhaupt keine Nachrichten mehr empfangen, so verfällt der Datenbankeintrag der Grauen Liste für diese Dreiergruppe. Spätere Zustellversuche führen zur Erstellung eines neuen Eintrags, für den dann wieder die oben angegebene Sperrzeit gilt.

Erweitert
Dieses Steuerelement öffnet die Datenbankdatei für die Graue Liste, in der direkt Änderungen vorgenommen werden können.

SMTP-Antwort (leer lassen, um Voreinstellung zu nutzen)
In dieses Textfeld können Sie einen benutzerdefinierten Text eintragen, den MDaemon als Teil der SMTP-Meldung nach dem Schema "`451 <your custom text>`" übermittelt. Die Voreinstellung, die genutzt wird, falls hier kein Text eingetragen ist, lautet "`451 Greylisting enabled, try again in X minutes`". Sie können in diesem Text beispielsweise einen URL übermitteln, der zu einer genaueren Beschreibung der Verfahrensweise der Grauen Liste führt.

IP-Adressen nicht in Graue Liste aufnehmen (nur MAIL- und RCPT-Daten)
Diese Option bewirkt, dass die IP-Adresse des Mailservers des Absenders nicht in der Grauen Liste erfasst wird. Dies löst zwar das oben näher ausgeführte Problem im Zusammenhang mit Serverpools, verringert aber auch die Wirksamkeit der Grauen Liste.

Verbindungen nach erfolgreicher SPF-Prüfung künftig nicht mehr in der Grauen Liste erfassen
Ist diese Option aktiv, so werden Nachrichten dann nicht als erste sondern als erneute Zustellversuche behandelt, wenn Absender und Empfänger, nicht jedoch der Server des Absenders mit einer Dreiergruppe übereinstimmen, durch eine SPF-Abfrage aber festgestellt werden kann, dass der Server des Absenders neben dem in der Dreiergruppe erfassten Server Nachrichten für die Absenderdomäne versenden darf. In diesem Fall wird auch kein zusätzlicher Eintrag in der Datenbank angelegt.

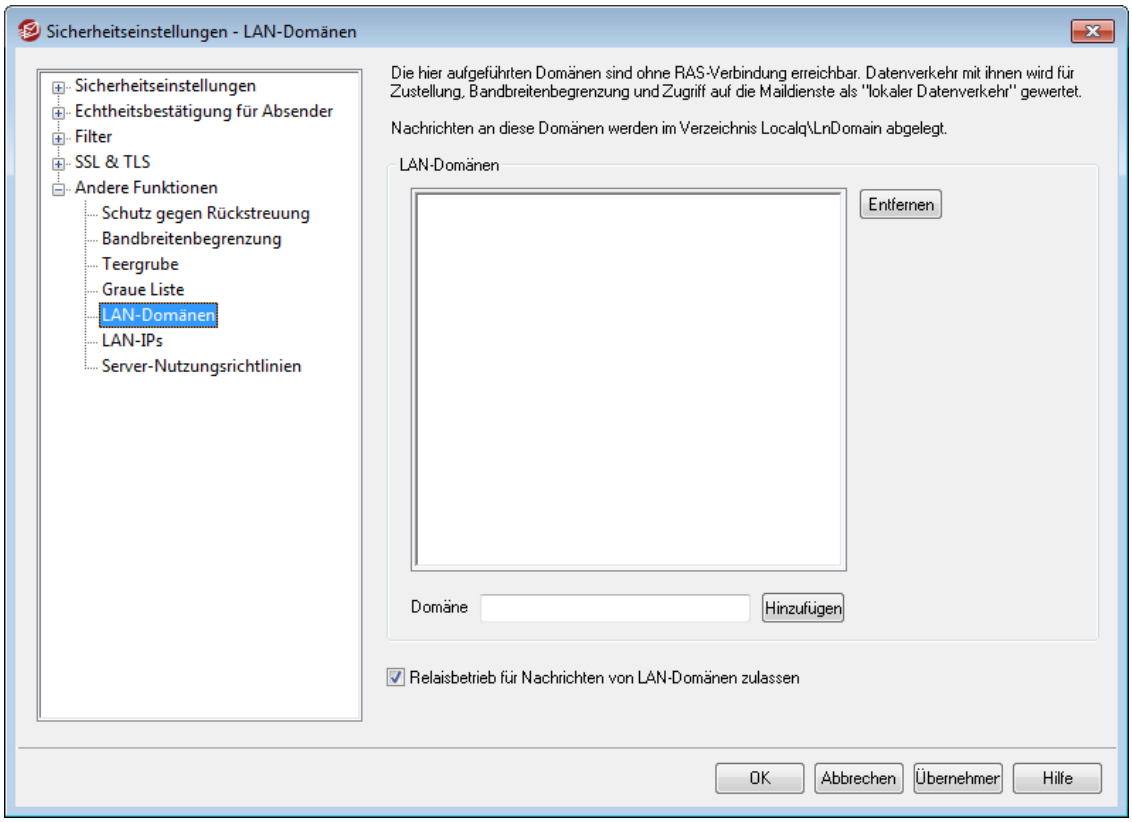
Nachrichten von Absendern in lokalen Adressbüchern nicht in der Grauen Liste erfassen
Diese Option bewirkt, dass eine Nachricht von der Bearbeitung durch die Graue Liste ausgenommen sind, wenn ihr Absender im Adressbuch des Empfängers eingetragen ist.

Nachrichten an Mailinglisten nicht in der Grauen Liste erfassen
Diese Option bewirkt, dass Nachrichten an Mailinglisten nicht durch die Graue Liste verarbeitet werden.

Nachrichten aus echtheitsbestätigten Verbindungen nicht in der Grauen Liste erfassen
Diese Option bewirkt, dass Nachrichten aus Verbindungen mit Echtheitsbestätigung nicht durch die Graue Liste verarbeitet werden.

Nachrichten von vertrauten IPs nicht in der Grauen Liste erfassen
Diese Option bewirkt, dass Nachrichten dann nicht in der Grauen Liste erfasst werden, wenn sie von vertrauten IP-Adressen aus gesendet werden.

4.1.5.5 LAN-Domänen



LAN-Domänen

MDaemon betrachtet die hier erfassten Domänen als Teil Ihres lokalen Netzwerks (LAN, local area network). MDaemon geht daher davon aus, dass keine RAS-Verbindung oder sonstige Internetverbindung erforderlich ist, um Nachrichten an diese Domänen zu übermitteln.

Domäne
Um eine Domäne in die Liste aufzunehmen, tragen Sie den Domänennamen in dieses Feld ein, und klicken Sie danach auf *Hinzufügen*.

Hinzufügen
Nachdem Sie in das Feld *Domäne* einen Domänennamen eingetragen haben, klicken Sie auf dieses Steuerelement, um die Domäne in die Liste aufzunehmen.

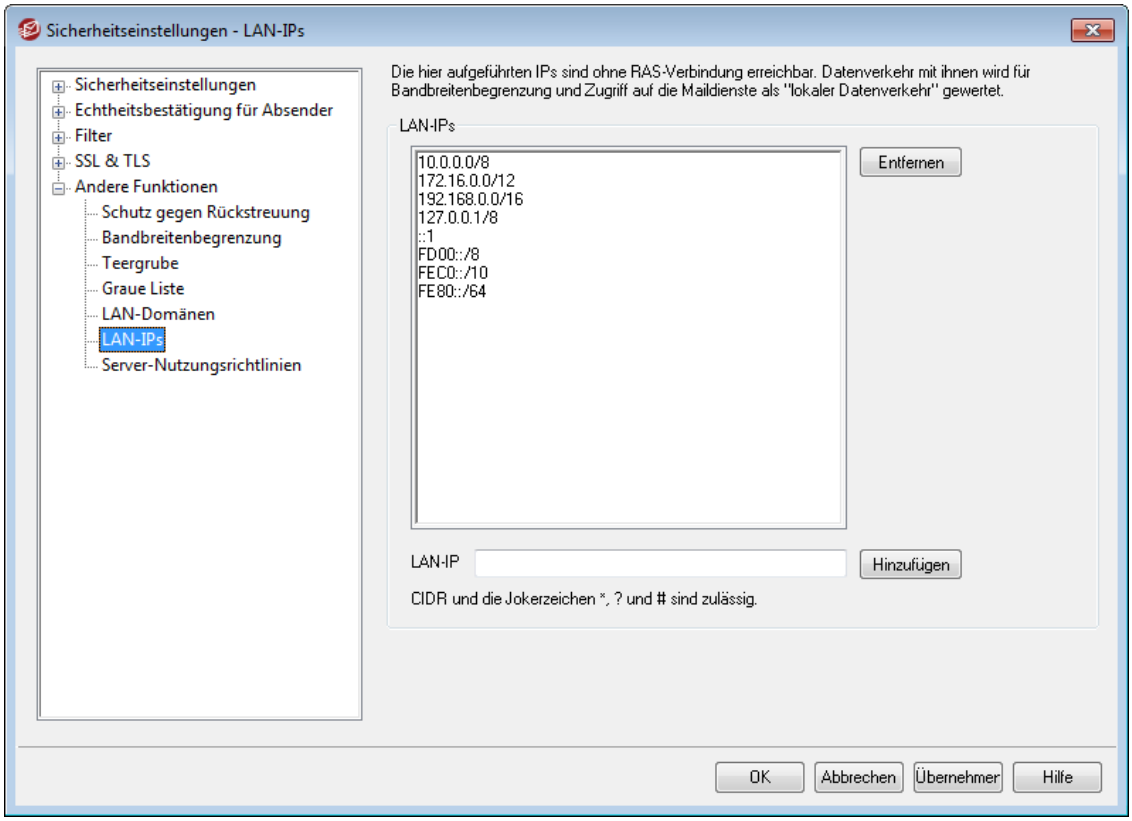
Entfernen
Um eine Domäne aus der Liste zu entfernen, wählen Sie die Domäne in der Liste aus, und klicken Sie dann auf dieses Steuerelement.

Relaisbetrieb für Nachrichten von LAN-Domänen zulassen
Ist diese Option aktiv, so führt MDaemon für die hier erfassten Domänen den Relaisbetrieb durch. Diese Option eröffnet eine gewisse Kontrolle über den Nachrichtenverkehr aus diesen und in diese Domänen.

Siehe auch:

LAN-IPs 610

4.1.5.6 LAN-IPs



LAN-IPs

Die Funktionen dieses Konfigurationsdialogs sind an die Funktionen des Konfigurationsdialogs LAN-Domänen 609 angelehnt. MDaemon betrachtet die hier erfassten IP-Adressen als Teil Ihres lokalen Netzwerks (LAN, local area network). MDaemon geht daher davon aus, dass keine RAS-Verbindung oder sonstige Internetverbindung erforderlich ist, um Nachrichten an diese IP-Adressen zu übermitteln. Verkehr mit diesen IP-Adressen wird im Rahmen der Bandbreitenbegrenzung wie lokaler Datenverkehr behandelt. Außerdem können Verbindungen mit diesen IP-Adressen, da sie als lokal betrachtet werden, von verschiedenen Sicherheitsmaßnahmen und Maßnahmen zur Spam-Abwehr und den damit verbundenen Beschränkungen ausgenommen werden.

Entfernen
Um eine IP-Adresse aus der Liste zu entfernen, wählen Sie die IP-Adresse in der Liste aus, und klicken Sie dann auf dieses Steuerelement.

LAN-IP
Um eine IP-Adresse in die Liste aufzunehmen, tragen Sie die IP-Adresse in dieses Feld ein, und klicken Sie danach auf *Hinzufügen*. Jokerzeichen, wie etwa 127.0.*.*, sind zugelassen.

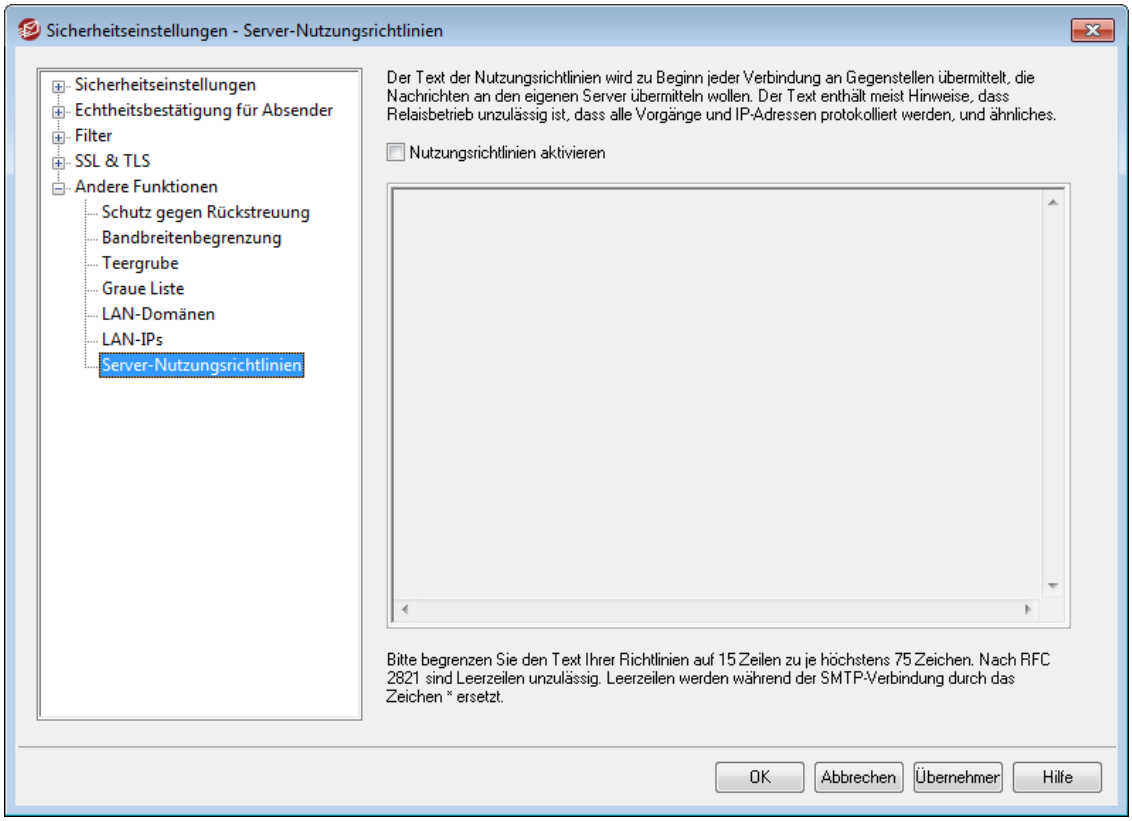
Hinzufügen
Nachdem Sie in das Feld *LAN-IP* eine IP-Adresse eingetragen haben, klicken Sie auf dieses Steuerelement, um die IP-Adresse in die Liste aufzunehmen.

Voreinstellung
Durch Anklicken dieses Steuerelements ersetzen Sie alle in der Liste erfassten LAN-IPs durch Voreinstellungen, die die reservierten IP-Adressbereiche abdecken. Bevor die Liste tatsächlich ersetzt wird, erscheint noch eine Sicherheitsabfrage.

Siehe auch:

LAN-Domänen 609

4.1.5.7 Server-Nutzungsrichtlinien



Erstellen von Nutzungsrichtlinien für SMTP-Verbindungen
Mithilfe dieses Konfigurationsdialogs können die Nutzungsrichtlinien für das eigene System definiert werden. Der eingegebene Text wird in der Datei `policy.dat` im MDaemon-Verzeichnis `\app\` gespeichert und zu Beginn jeder SMTP-Verbindung an die Gegenstelle übermittelt, bevor diese mit der Übermittlung von Nachrichten beginnt. Gängige Beispiele für solche Nutzungsrichtlinien sind "`Relaisbetrieb ist auf diesem System gesperrt`" und "`Unbefugte Nutzung verboten`". Die einzelnen Zeilen des Textes müssen nicht mit den Steuerzeichen

"220" oder "220-" beginnen. MDaemon verarbeitet jede Textzeile mit und ohne diese vorangestellten Steuerzeichen richtig.

Ein Beispieltext für die Nutzungsrichtlinien, der Hinweise zum Relaisbetrieb enthält, würde während einer SMTP-Verbindung folgendermaßen ausgegeben werden:

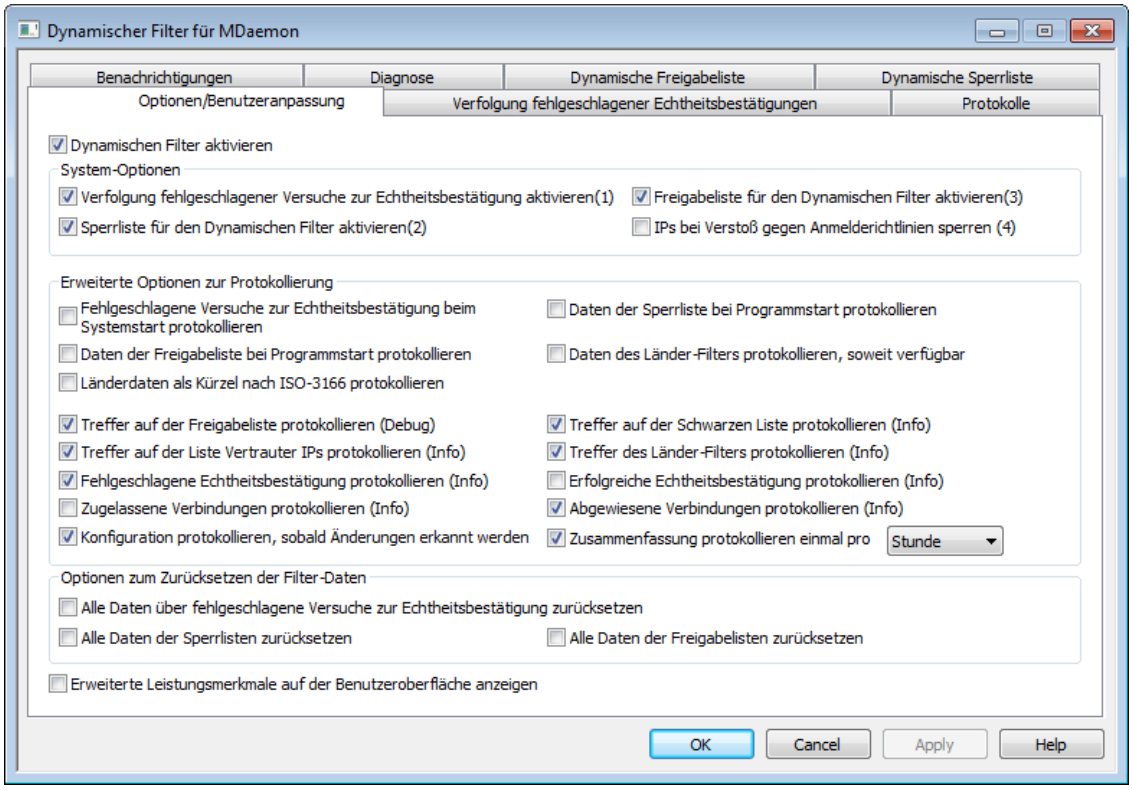
```
220-MDaemon Technologies ESMTP MDaemon
220-Unzulaessiger Relaisbetrieb ist gesperrt.
220-Falls Sie kein entsprechend berechtigter
220-Beutzer unseres Servers sind, duerfen Sie
220-dieses System nicht für Relaisbetrieb verwenden.
220
HELO example.com...
```

Die Datei POLICY.DAT darf nur aus druckbarem ("printable") ASCII-Text bestehen. Die Länge ihrer einzelnen Zeilen ist auf je 512 Zeichen begrenzt; es empfiehlt sich aber dringend, höchstens 75 Zeichen pro Zeile zu schreiben. Die Datei darf höchstens 5.000 Byte groß sein. Größere Dateien zeigt MDaemon nicht an.

Der Text der Nutzungsrichtlinien sollte, wenn er in der jeweiligen Landessprache abgefasst ist, aus Gründen der Verständlichkeit immer auch in englischer Sprache wiedergegeben werden, damit sein Inhalt auch von Gegenstellen verstanden wird, die die Landessprache nicht beherrschen.

4.2 Dynamischer Filter

4.2.1 Optionen/Benutzeranpassung



Mithilfe des Dynamischen Filters kann MDaemon bestimmte Muster in eingehenden Verbindungen nachverfolgen, hieraus verdächtige Aktivität erkennen und entsprechend reagieren. Sie können IP-Adressen (oder Adressbereiche) gegen weitere Verbindungen sperren[616], falls in Verbindungen von diesen IP-Adressen aus mehrfach innerhalb eines bestimmten Zeitraums fehlgeschlagene Versuche zur Echtheitsbestätigung ausgehen. Sie können auch Benutzerkonten einfrieren[616], falls von Gegenstellen für diese zu oft in zu kurzer Zeit fehlgeschlagene Versuche zur Echtheitsbestätigung durchgeführt werden. Werden IP-Adressen gesperrt und Benutzerkonten eingefroren, so geschieht dies nur vorübergehend. Die IP-Adressen werden für eine vorbestimmte Zeit gesperrt, und die eingefrorenen Benutzerkonten können nach einer vorbestimmten Zeit automatisch wieder freigegeben werden. Die entsprechenden Festlegungen trifft der Administrator.

Dynamischen Filter aktivieren
Diese Option aktiviert die Leistungsmerkmale des Dynamischen Filters. Sie können diesen Dienst auch im Abschnitt Server im Navigationsbereich der Benutzeroberfläche von MDaemon aktivieren und deaktivieren.

System-Optionen

Verfolgung fehlgeschlagener Versuche zur Echtheitsbestätigung aktivieren
Diese Option bewirkt, dass der Dynamische Filter fehlgeschlagene Versuche zur Echtheitsbestätigung für die auf der Registerkarte Protokolle[620] festgelegten Protokolle nachverfolgt und die Aktionen ausführt, die auf der Registerkarte Verfolgung fehlgeschlagener Echtheitsbestätigungen[616] festgelegt sind. Diese Option ist per Voreinstellung aktiv.

Sperrliste für den Dynamischen Filter aktivieren
Diese Option ermöglicht es dem Dynamischen Filter, IP-Adressen und -Adressbereiche in die Sperrliste aufzunehmen. Sie können die Sperrliste auf der Registerkarte Dynamische Sperrliste[628] verwalten. Diese Option ist per Voreinstellung aktiv.

Freigabeliste für den Dynamischen Filter aktivieren
Diese Option ermöglicht es dem Dynamischen Filter, IP-Adressen und -Adressbereiche durch Aufnahme in die Freigabeliste von der Behandlung durch den Dynamischen Filter auszunehmen. Sie können die Freigabeliste auf der Registerkarte Dynamische Freigabeliste[626] verwalten. Diese Option ist per Voreinstellung aktiv.

IPs bei Verstoß gegen Anmelderichtlinien sperren
Per Voreinstellung verlangt MDaemon, dass die Benutzerkonten bei der Anmeldung nicht nur den Postfachnamen aus ihrer E-Mail-Adresse sondern die vollständige E-Mail-Adresse als Anmeldenamen verwenden (so müssen sie "`benutzer1@example.com`" und nicht nur "`benutzer1`" verwenden). Diese Vorgehensweise wird durch die Option "*POP-/IMAP-Server verlangen zur Echtheitsbestätigung die vollständige E-Mail-Adresse*" auf der Seite System[495] gesteuert. Ist diese Option aktiv, so können Sie auch die Option *IPs bei Verstoß gegen Anmelderichtlinien sperren* aktivieren. Es werden dann alle IP-Adressen gesperrt, von denen aus Anmeldungen ohne vollständige E-Mail-Adresse versucht werden. Diese Option ist per Voreinstellung abgeschaltet.

Erweiterte Optionen zur Protokollierung

Fehlgeschlagene Versuche zur Echtheitsbestätigung beim Systemstart protokollieren
Diese Option bewirkt, dass die Daten über fehlgeschlagene Versuche zur Echtheitsbestätigung[616], die der Dynamische Filter derzeit speichert, beim Systemstart in das Protokoll geschrieben werden. Diese Option ist per Voreinstellung abgeschaltet.

Daten der Sperrliste bei Programmstart protokollieren
Diese Option bewirkt, dass die Daten der Dynamischen Sperrliste[628], die der Dynamische Filter derzeit speichert, beim Systemstart in das Protokoll geschrieben werden. Diese Option ist per Voreinstellung abgeschaltet.

Daten der Freigabeliste bei Programmstart protokollieren
Diese Option bewirkt, dass die Daten der Dynamischen Freigabeliste[626], die der Dynamische Filter derzeit speichert, beim Systemstart in das Protokoll geschrieben werden. Diese Option ist per Voreinstellung abgeschaltet.

Daten des Länder-Filters protokollieren, soweit verfügbar
Diese Option bewirkt, dass die Daten zum Ursprung der Verbindung für jede Verbindung protokolliert werden, soweit sie verfügbar sind.

Länderdaten als Kürzel nach ISO-3166 protokollieren
Diese Option bewirkt, dass für die Länder und Regionen nicht die vollen Namen sondern die aus zwei Buchstaben bestehenden, im ISO-Standard 3166 definierten Kennungen protokolliert werden.

Alle Treffer auf den Freigabelisten protokollieren
Diese Option fügt dem Protokoll des Dynamischen Filters immer dann einen Eintrag hinzu, wenn eine eingehende Verbindung von einer Adresse aus hergestellt wird, die in der Dynamischen Freigabeliste[626] erfasst ist.

Alle Treffer auf den Sperrlisten protokollieren
Diese Option fügt dem Protokoll des Dynamischen Filters immer dann einen Eintrag hinzu, wenn eine eingehende Verbindung von einer Adresse aus hergestellt wird, die in der Dynamischen Sperrliste[628] erfasst ist.

Alle Treffer auf der Liste Vertrauter IPs protokollieren
Diese Option fügt dem Protokoll des Dynamischen Filters immer dann einen Eintrag hinzu, wenn eine eingehende Verbindung von einer Adresse aus hergestellt wird, die in der Liste Vertrauter IP-Adressen[521] erfasst ist.

Alle Treffer des Länder-Filters protokollieren
Diese Option fügt dem Protokoll des Dynamischen Filters immer dann einen Eintrag hinzu, wenn eine eingehende Verbindung durch den Länder-Filter[574] abgewiesen wird.

Alle fehlgeschlagenen Versuche zur Echtheitsbestätigung protokollieren
Diese Option fügt dem Protokoll des Dynamischen Filters immer dann einen Eintrag hinzu, wenn in einer eingehenden Verbindung die Echtheitsbestätigung fehlschlägt.

Alle erfolgreichen Echtheitsbestätigungen protokollieren
Diese Option fügt dem Protokoll des Dynamischen Filters immer dann einen Eintrag hinzu, wenn in einer eingehenden Verbindung die Echtheitsbestätigung erfolgreich durchgeführt wurde. Diese Option ist per Voreinstellung abgeschaltet.

Alle zugelassenen Verbindungen protokollieren
Diese Option fügt dem Protokoll des Dynamischen Filters immer dann einen Eintrag hinzu, wenn eine eingehende Verbindung die Prüfung durch den Dynamischen Filter bestanden hat und daher zugelassen wurde. Diese Option ist per Voreinstellung abgeschaltet.

Alle abgewiesenen Verbindungen protokollieren
Diese Option fügt dem Protokoll des Dynamischen Filters immer dann einen Eintrag hinzu, wenn eine eingehende Verbindung durch den Dynamischen Filter abgewiesen wurde. Diese Option ist per Voreinstellung abgeschaltet.

Konfiguration protokollieren, sobald Änderungen erkannt werden
Diese Option protokolliert alle Einstellungen der Konfiguration des Dynamischen Filters, sobald Änderungen erkannt werden, die von externen Stellen aus vorgenommen werden, etwa durch manuelle Bearbeitung der INI-Datei. Normale Änderungen werden im Detailgrad INFO protokolliert.

Zusammenfassung protokollieren einmal pro [Tag | Stunde | Minute]
Diese Option protokolliert eine Zusammenfassung der Statistiken des Dynamischen Filters in den hier angegebenen Intervallen. Per Voreinstellung werden die Statistiken einmal pro Stunde protokolliert.

Optionen zum Zurücksetzen der Filter-Daten

Alle Daten über fehlgeschlagene Versuche zur Echtheitsbestätigung zurücksetzen
Um alle Daten des Dynamischen Filters über fehlgeschlagene Versuche zur Echtheitsbestätigung zurückzusetzen, aktivieren Sie dieses Kontrollkästchen, und klicken Sie danach auf **Übernehmen** oder **OK**. Die Daten werden dann unmittelbar zurückgesetzt.

Alle Daten der Sperrlisten zurücksetzen
Um alle Daten der Sperrliste des Dynamischen Filters zurückzusetzen, aktivieren Sie dieses Kontrollkästchen, und klicken Sie danach auf **Übernehmen** oder **OK**. Die Daten werden dann unmittelbar zurückgesetzt.

Alle Daten der Freigabelisten zurücksetzen
Um alle Daten der Freigabeliste des Dynamischen Filters zurückzusetzen, aktivieren Sie dieses Kontrollkästchen, und klicken Sie danach auf **Übernehmen** oder **OK**. Die Daten werden dann unmittelbar zurückgesetzt.

Erweiterte Leistungsmerkmale auf der Benutzeroberfläche anzeigen

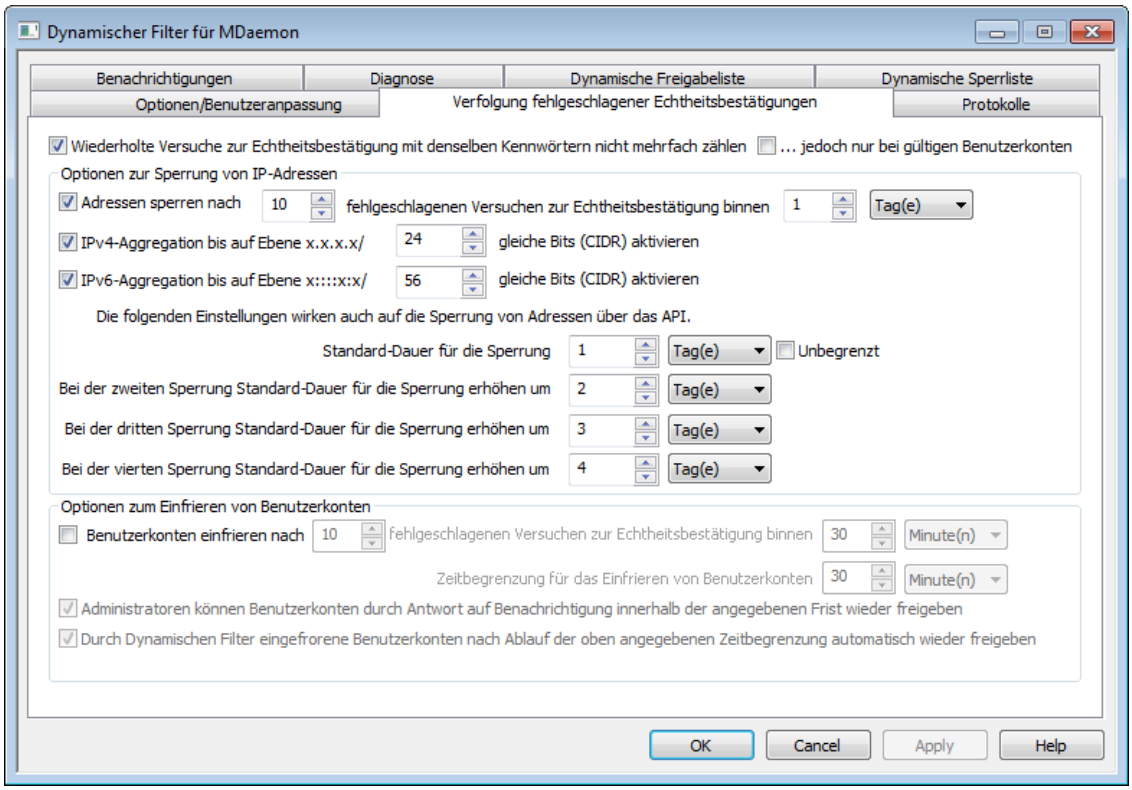
Diese Option bewirkt, dass auf der Benutzeroberfläche Optionen für zusätzliche, erweiterte Leistungsmerkmale des Dynamischen Filters erscheinen. Änderungen an dieser Option werden erst nach einem Neustart von MDaemon oder der genutzten Konfigurationsverbindung wirksam. Die Option fügt dem Konfigurationsdialog für den Dynamischen Filter auch die Registerkarte NAT-Ausnahmen für Domäne 630 hinzu. Sie können hier bestimmte IP-Adressen und IP-Adressbereiche bestimmen, die von der Behandlung durch den Dynamischen Filter ausgenommen sein sollen. Die Option fügt weiter dem Menü für den Dynamischen

Filter in der Symbolleiste mehrere Verknüpfungen hinzu. Der Eintrag für den Dynamischen Filter im Navigationsbereich wir um eine Option erweitert, mit deren Hilfe der Dynamische Filter angehalten werden kann, ohne ihn zu deaktivieren. Diese Option ist insbesondere hilfreich, um den Zugriff von Clients auf den Dienst zu unterbinden, während Sie seine Konfiguration bearbeiten.

Siehe auch:

Verfolgung fehlgeschlagener Echtheitsbestätigungen 616
Dynamische Freigabeliste 626
Dynamische Sperrliste 628
NAT-Ausnahmen für Domäne 630
Protokolle 620
Länder-Filter 574
SMTP-Filter 567

4.2.2 Verfolgung fehlgeschlagener Echtheitsbestätigungen



Wiederholte Versuche zur Echtheitsbestätigung mit denselben Kennwörtern nicht mehrfach zählen

Diese Option wirkt auf auf die Optionen zur Sperrung von IP-Adressen und die Optionen zum Einfrieren von Benutzerkonten, die weiter unten dargestellt sind. Sie ist per Voreinstellung aktiv. Sie bewirkt, dass mehrere aufeinander folgende fehlgeschlagene Versuche zur Echtheitsbestätigung, in denen immer dasselbe falsche Kennwort verwendet wird, nur einmal und nicht mehrfach gezählt werden. Sie werden daher auch nicht auf die Höchstzahl fehlgeschlagener Versuche zur Echtheitsbestätigung angerechnet, bei deren Überschreiten IP-Adressen gesperrt und Benutzerkonten eingefroren werden. Mehrere aufeinander folgende fehlgeschlagene Versuche zur Echtheitsbestätigung mit immer demselben falschen

Kennwort können beispielsweise auftreten, wenn sich das Kennwort für ein Benutzerkonto geändert hat oder es wegen Überschreiten der Gültigkeit ungültig geworden ist, der Benutzer das Kennwort aber noch nicht geändert hat und der Client automatisch immer wieder versucht, sich mit dem jetzt ungültigen Kennwort anzumelden.

... jedoch nur bei gültigen Benutzerkonten
Diese Option bewirkt, dass wiederholte Versuche zur Echtheitsbestätigung mit denselben Kennwörtern nur dann nicht mehrfach gezählt werden, wenn dabei die Anmeldung an einem gültigen Benutzerkonto versucht wird. Ein Beispiel zur Vorgehensweise, wenn dies Option aktiv ist: Aktualisiert ein Benutzer ein geändertes Kennwort auf einem Client, lässt es aber auf einem anderen Client unverändert, so versucht dieser andere Client, sich mit dem veralteten Kennwort anzumelden. Diese Anmeldeversuche schlagen fehl. Sie werden aber nicht mehrfach gezählt, da jeweils ein gültiger Benutzername übermittelt wird. Versucht dagegen ein Bot die Anmeldung und probiert dabei dasselbe Kennwort in Kombination mit wahllosen nicht bestehenden Anmeldenamen aus, dann werden diese Anmeldeversuche mehrfach gezählt. Das Kennwort ist im Beispiel zwar stets gleich, aber die Anmeldenamen sind nicht gültig. Der Bot wird daher gesperrt, sobald die Höchstzahl der zulässigen fehlgeschlagenen Anmeldeversuche erreicht ist.

Optionen zur Sperrung von IP-Adressen

Adressen sperren nach [x] fehlgeschlagenen Versuchen zur Echtheitsbestätigung binnen [x] [Minuten | Stunden | Tagen]
Diese Option bewirkt, dass IP-Adressen vorübergehend gesperrt werden, sobald Sie innerhalb des hier angegeben Zeitraums die hier angegebene Zahl fehlgeschlagener Versuche zur Echtheitsbestätigung erreicht haben. Geben Sie hierzu die Zeitdauer in Minuten, Stunden oder Tagen und die Höchstzahl zulässiger fehlgeschlagener Versuche zur Echtheitsbestätigung innerhalb dieses Zeitraums an.

IPv4-Aggregation bis auf Ebene x.x.x.x/ [x] gleiche Bits (CIDR) aktivieren
Diese Option sperrt einen IPv4-Adressbereich, falls die fehlgeschlagenen Versuche zur Echtheitsbestätigung nicht von derselben sondern von mehreren nahe beieinander liegenden Adressen ausgehen.

IPv6-Aggregation bis auf Ebene x::::x:x/ [x] gleiche Bits (CIDR) aktivieren
Diese Option sperrt einen IPv6-Adressbereich, falls die fehlgeschlagenen Versuche zur Echtheitsbestätigung nicht von derselben sondern von mehreren nahe beieinander liegenden Adressen ausgehen.

Sperrdauern bei mehreren Sperrungen

In diesem Abschnitt werden die Zeiträume angegeben, für die IP-Adressen und IP-Adressbereiche durch den Dynamischen Filter gesperrt werden, sobald sie die festgelegte Höchstzahl fehlgeschlagener Versuche zur Echtheitsbestätigung erreicht haben. Per Voreinstellung erhöht sich die Sperrdauer mit jeder Sperre, wobei der jeder Sperre zugeordnete Wert jeweils der Standard-Dauer für die Sperre hinzugerechnet wird. Per Voreinstellung beträgt die Sperrdauer einen Tag. Diese Sperrdauer tritt ein, wenn eine IP-Adresse oder ein IP-Adressbereich zum ersten Mal gesperrt wird. Werden später dieselbe IP-Adresse oder derselbe IP-Adressbereich erneut gesperrt, so beträgt die Gesamt-Sperrdauer die Summe der Standard-Dauer für die Sperrung und des Werts, um den sich die Standard-Dauer jeweils erhöht. Im Beispiel beträgt daher die Sperrdauer bei der zweiten Sperrung drei, bei der dritten

Sperrung vier und bei der vierten Sperrung fünf Tage. Auch bei allen weiteren Sperrungen nach der vierten Sperrung wird jeweils der Wert für die vierte Sperrung herangezogen.

Standard-Dauer für die Sperrung
Hier wird der Zeitraum festgelegt, für den eine IP-Adresse oder ein IP-Adressbereich gegen weitere Verbindungen mit MDaemon gesperrt wird, sobald von der IP-Adresse oder dem IP-Adressbereich aus die oben festgelegte Höchstzahl fehlgeschlagener Versuche zur Echtheitsbestätigung erreicht wurde. Die Voreinstellung beträgt 1 Tag. Dieser Wert gilt dann, wenn nicht aufgrund der folgenden Einstellungen eine Erhöhung der Standard-Dauer eintritt.

Bei der zweiten Sperrung Standard-Dauer für die Sperrung erhöhen um
Hier wird der Zeitraum festgelegt, um den sich die Standard-Dauer für die Sperrung einer IP-Adresse oder eines IP-Adressbereichs gegen weitere Verbindungen mit MDaemon bei der zweiten Sperrung erhöht. Die Voreinstellung beträgt 2 Tage. Dieser Wert wird der Standard-Dauer für die Sperrung hinzugerechnet.

Bei der dritten Sperrung Standard-Dauer für die Sperrung erhöhen um
Hier wird der Zeitraum festgelegt, um den sich die Standard-Dauer für die Sperrung einer IP-Adresse oder eines IP-Adressbereichs gegen weitere Verbindungen mit MDaemon bei der dritten Sperrung erhöht. Die Voreinstellung beträgt 3 Tage. Dieser Wert wird der Standard-Dauer für die Sperrung hinzugerechnet.

Bei der vierten Sperrung Standard-Dauer für die Sperrung erhöhen um
Hier wird der Zeitraum festgelegt, um den sich die Standard-Dauer für die Sperrung einer IP-Adresse oder eines IP-Adressbereichs gegen weitere Verbindungen mit MDaemon bei der vierten Sperrung und allen weiteren Sperrungen erhöht. Die Voreinstellung beträgt 4 Tage. Dieser Wert wird der Standard-Dauer für die Sperrung hinzugerechnet.

Unbegrenzt
Diese Option bewirkt, dass IP-Adressen nach Überschreiten der Höchstzahl zulässiger fehlgeschlagener Versuche zur Echtheitsbestätigung dauerhaft gesperrt werden. Die in den weiteren Optionen konfigurierten Sperrdauern sind dann nicht anwendbar.

Optionen zum Einfrieren von Benutzerkonten

Benutzerkonten einfrieren nach [x] fehlgeschlagenen Versuchen zur Echtheitsbestätigung binnen [x] [Minuten | Stunden | Tagen]
Diese Option bewirkt, dass der Status eines Benutzerkontos[714] automatisch auf *eingefroren* gesetzt wird, sobald für das Benutzerkonto innerhalb des hier festgelegten Zeitraums die hier festgelegte Höchstzahl fehlgeschlagener Versuche zur Echtheitsbestätigung erreicht ist. MDaemon nimmt eingehende Nachrichten auch für eingefrorene Benutzerkonten weiterhin zur Zustellung an. Eine Anmeldung an dem Benutzerkonto zum Versand oder Abruf von Nachrichten ist aber erst dann wieder möglich, wenn der Status des Benutzerkontos wieder auf *aktiv* gesetzt und das Benutzerkonto damit wieder freigegeben ist. Diese Option ist per Voreinstellung aktiv.

Zeitbegrenzung für das Einfrieren von Benutzerkonten
Hier wird der Zeitraum festgelegt, für den das Benutzerkonto eingefroren bleibt, bevor es automatisch wieder freigegeben wird. Diese Option ist nur wirksam, wenn auch die Option *Durch Dynamischen Filter eingefrorene Benutzerkonten nach Ablauf der oben angegebenen Zeitbegrenzung automatisch wieder freigeben* weiter unten aktiv ist.

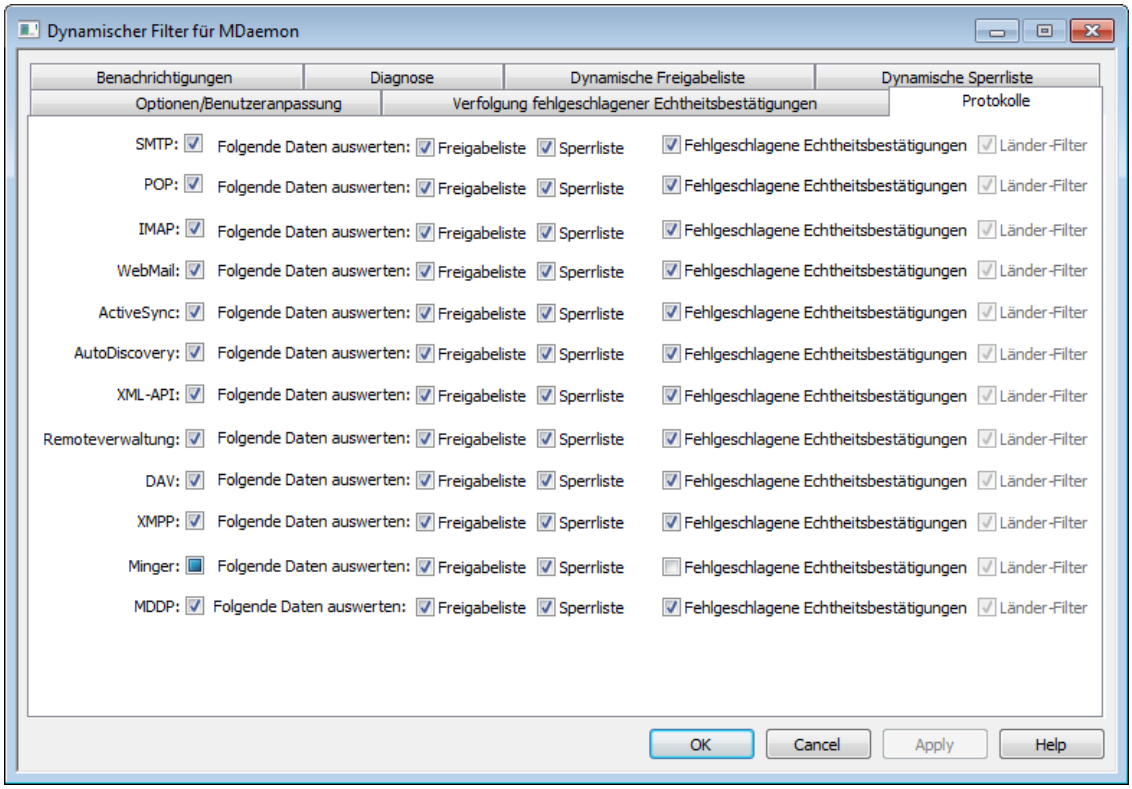
Administratoren können Benutzerkonten durch Antwort auf Benachrichtigung innerhalb der angegebenen Frist wieder freigeben
Wird ein Benutzerkonto durch den Dynamischen Filter eingefroren, so erhält der Administrator per Voreinstellung hierüber eine Benachrichtigung per E-Mail. Ist diese Option aktiv, so kann der Administrator den Status des Benutzerkontos auf *aktiv* setzen und so das Benutzerkonto wieder freigeben, indem er auf diese Benachrichtigung antwortet. Diese Option ist per Voreinstellung aktiv. Sie erfordert, dass auf der Registerkarte Benachrichtigungen 621 die Optionen für Berichte über eingefrorene Benutzerkonten aktiv sind.

Durch Dynamischen Filter eingefrorene Benutzerkonten nach Ablauf der oben angegebenen Zeitbegrenzung automatisch wieder freigeben
Diese Option bewirkt, dass eingefrorene Benutzerkonten nach Ablauf der *Zeitbegrenzung für das Einfrieren von Benutzerkonten* automatisch wieder freigegeben werden. Diese Option ist per Voreinstellung deaktiviert.

Siehe auch:

Optionen/Benutzeranpassung 612
Dynamische Freigabeliste 626
Dynamische Sperrliste 628
Benachrichtigungen 621

4.2.3 Protokolle

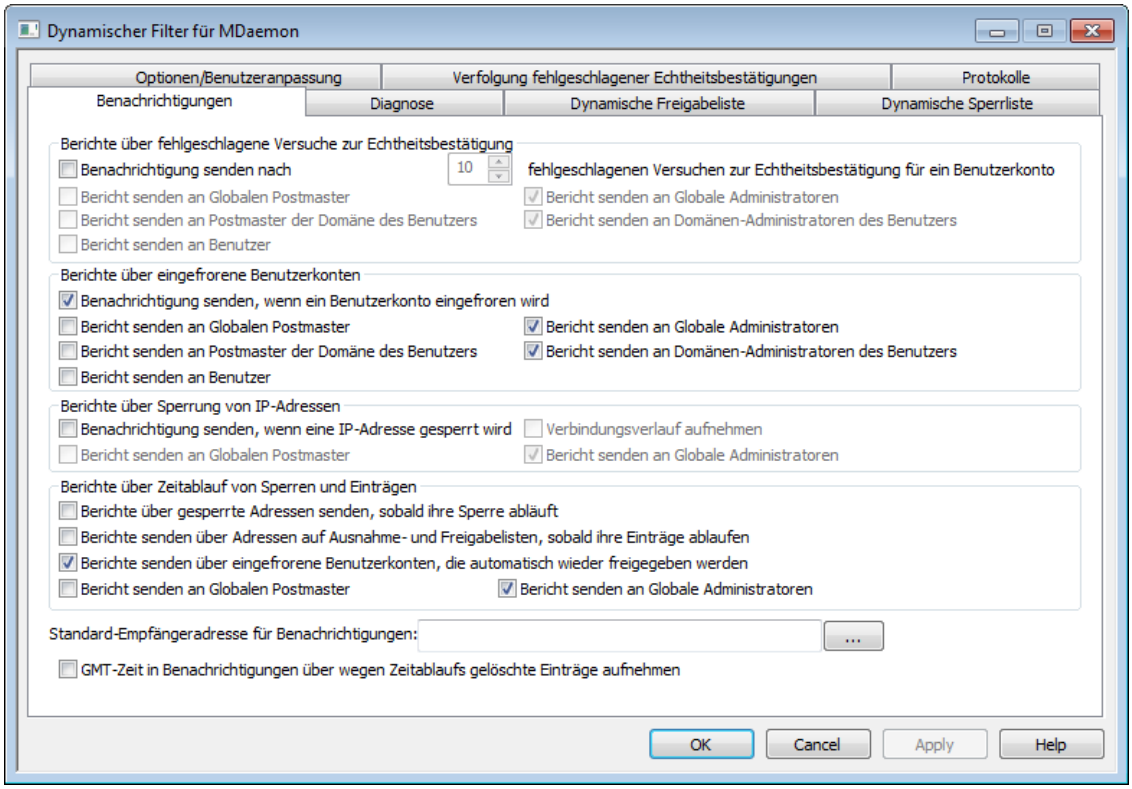


Per Voreinstellung wirkt der Dynamische Filter auf die folgenden Protokolle: SMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery 80, das Verwaltungs-API, die MDaemon-Remoteverwaltung, WebDAV und CalDAV, XMPP und Minger. Mithilfe der Optionen auf der Registerkarte Protokolle können Sie bestimmen, bei welchen Arten eingehender Verbindungen die Dynamische Freigabeliste 626 und die Dynamische Sperrliste 628 abgefragt werden, die fehlgeschlagenen Versuche zur Echtheitsbestätigung verfolgt 616 und der Länder-Filter 574 angewendet werden sollen. Per Voreinstellung sind die Optionen zur Verfolgung fehlgeschlagener Echtheitsbestätigungen für Minger nicht aktiv und im Übrigen alle Optionen dieses Konfigurationsdialogs aktiv.

Siehe auch:

Verfolgung fehlgeschlagener Echtheitsbestätigungen 616
Dynamische Freigabeliste 626
Dynamische Sperrliste 628

4.2.4 Benachrichtigungen



Berichte über fehlgeschlagene Versuche zur Echtheitsbestätigung

Benachrichtigung senden nach [x] fehlgeschlagenen Versuchen zur Echtheitsbestätigung für ein Benutzerkonto
Diese Option bewirkt, dass MDaemon den Postmaster oder andere ausgewählte Empfänger per E-Mail benachrichtigt, wenn für ein Benutzerkonto die hier angegebene Anzahl aufeinander folgender, fehlgeschlagener Versuche zur Echtheitsbestätigung erreicht ist. Falls keinem der angegebenen Empfänger eine gültige E-Mail-Adresse zugeordnet werden kann, wird die Benachrichtigung an die im Feld *Standard-Empfängeradresse für Benachrichtigungen* eingetragene Adresse versandt. Ist die *Standard-Empfängeradresse* nicht angegeben, so wird in diesem Fall keine Benachrichtigung versandt. Die Option ist per Voreinstellung aktiv, und ihr voreingestellter Wert beträgt 10.

Bericht senden an Globalen Postmaster
Diese Option bewirkt, dass die Berichte per E-Mail an den Globalen Postmaster 827 versandt werden. Diese Option ist per Voreinstellung aktiv.

Bericht senden a Globale Administratoren
Diese Option bewirkt, dass die Berichte per E-Mail an die Globalen Administratoren 757 versandt werden.

Bericht senden an Postmaster der Domäne des Benutzers
Diese Option bewirkt, dass die Berichte per E-Mail an den Postmaster der Domäne 827 versandt werden, zu der das betroffene Benutzerkonto gehört.

Bericht senden an Domänen-Administratoren des Benutzers
Diese Option bewirkt, dass die Berichte per E-Mail an den Domänen-Administratoren[757] der Domäne versandt werden, zu der das betroffene Benutzerkonto gehört.

Bericht senden an Benutzer
Diese Option bewirkt, dass die Berichte per E-Mail an den betroffenen Benutzer selbst versandt werden.

Berichte über eingefrorene Benutzerkonten

Benachrichtigung senden, wenn ein Benutzerkonto eingefroren wird
Diese Option bewirkt, dass MDaemon den Postmaster oder andere ausgewählte Empfänger per E-Mail benachrichtigt, wenn ein Benutzerkonto wegen zu vieler fehlgeschlagener Versuche zur Echtheitsbestätigung[616] eingefroren wurde. Falls keinem der angegebenen Empfänger eine gültige E-Mail-Adresse zugeordnet werden kann, wird die Benachrichtigung an die im Feld *Standard-Empfängeradresse für Benachrichtigungen* eingetragene Adresse versandt. Ist die *Standard-Empfängeradresse* nicht angegeben, so wird in diesem Fall keine Benachrichtigung versandt. Die Option ist per Voreinstellung aktiv.

Bericht senden an Globalen Postmaster
Diese Option bewirkt, dass die Berichte per E-Mail an den Globalen Postmaster[827] versandt werden. Diese Option ist per Voreinstellung aktiv.

Bericht senden a Globale Administratoren
Diese Option bewirkt, dass die Berichte per E-Mail an die Globalen Administratoren[757] versandt werden.

Bericht senden an Postmaster der Domäne des Benutzers
Diese Option bewirkt, dass die Berichte per E-Mail an den Postmaster der Domäne[827] versandt werden, zu der das betroffene Benutzerkonto gehört.

Bericht senden an Domänen-Administratoren des Benutzers
Diese Option bewirkt, dass die Berichte per E-Mail an den Domänen-Administratoren[757] der Domäne versandt werden, zu der das betroffene Benutzerkonto gehört.

Bericht senden an Benutzer
Diese Option bewirkt, dass die Berichte per E-Mail an den betroffenen Benutzer selbst versandt werden.

Berichte über Sperrung von IP-Adressen

Benachrichtigung senden, wenn eine IP-Adresse gesperrt wird (auch wenn die Sperre über API veranlasst wird)
Diese Option bewirkt, dass MDaemon den Postmaster oder andere ausgewählte Empfänger per E-Mail benachrichtigt, wenn ein Benutzerkonto durch den Dynamischen Filter eingefroren wurde. Falls keinem der angegebenen Empfänger eine gültige E-Mail-Adresse zugeordnet werden kann, wird die Benachrichtigung an die im Feld *Standard-Empfängeradresse für Benachrichtigungen* eingetragene Adresse versandt. Ist die *Standard-Empfängeradresse* nicht angegeben, so wird in diesem Fall keine Benachrichtigung versandt. Die Option ist per Voreinstellung aktiv.

This option causes MDaemon to send a notification message to a postmaster or other selected recipient any time an account is blocked by the Dynamic Screening system. If none of the selected addresses can be resolved, MDaemon will send the message to the Default Notification Address designated below. If no address has been specified, the message will not be sent. The option is enabled by default.

Bericht senden an Globalen Postmaster
Diese Option bewirkt, dass die Berichte per E-Mail an den Globalen Postmaster[827] versandt werden. Diese Option ist per Voreinstellung aktiv.

Bericht senden a Globale Administratoren
Diese Option bewirkt, dass die Berichte per E-Mail an die Globalen Administratoren[757] versandt werden.

Berichte über Zeitablauf von Sperren und Einträgen

Berichte über gesperrte Adressen senden, sobald ihre Sperre abläuft
Diese Option bewirkt, dass MDaemon die ausgewählte Empfänger per E-Mail benachrichtigt, wenn eine gesperrte IP-Adresse wegen Zeitablaufs aus der Dynamischen Sperrliste[628] gelöscht wurde. Die Option ist per Voreinstellung aktiv.

Berichte senden über Adressen auf Ausnahme- und Freigabelisten, sobald ihre Einträge ablaufen
Diese Option bewirkt, dass MDaemon die ausgewählte Empfänger per E-Mail benachrichtigt, wenn eine gesperrte IP-Adresse wegen Zeitablaufs aus der Dynamischen Freigabeliste[626] gelöscht wurde. Die Option ist per Voreinstellung aktiv.

Berichte senden über eingefrorene Benutzerkonten, die automatisch wieder freigegeben wurden
Diese Option bewirkt, dass MDaemon die ausgewählte Empfänger per E-Mail benachrichtigt, wenn ein eingefrorenes Benutzerkonto nach Ablauf der *Zeitbegrenzung für das Einfrieren von Benutzerkonten* automatisch wieder freigegeben[616] wurde. Die Option ist per Voreinstellung aktiv.

Bericht senden an Globalen Postmaster
Diese Option bewirkt, dass die Berichte per E-Mail an den Globalen Postmaster[827] versandt werden. Diese Option ist per Voreinstellung aktiv.

Bericht senden a Globale Administratoren
Diese Option bewirkt, dass die Berichte per E-Mail an die Globalen Administratoren[757] versandt werden.

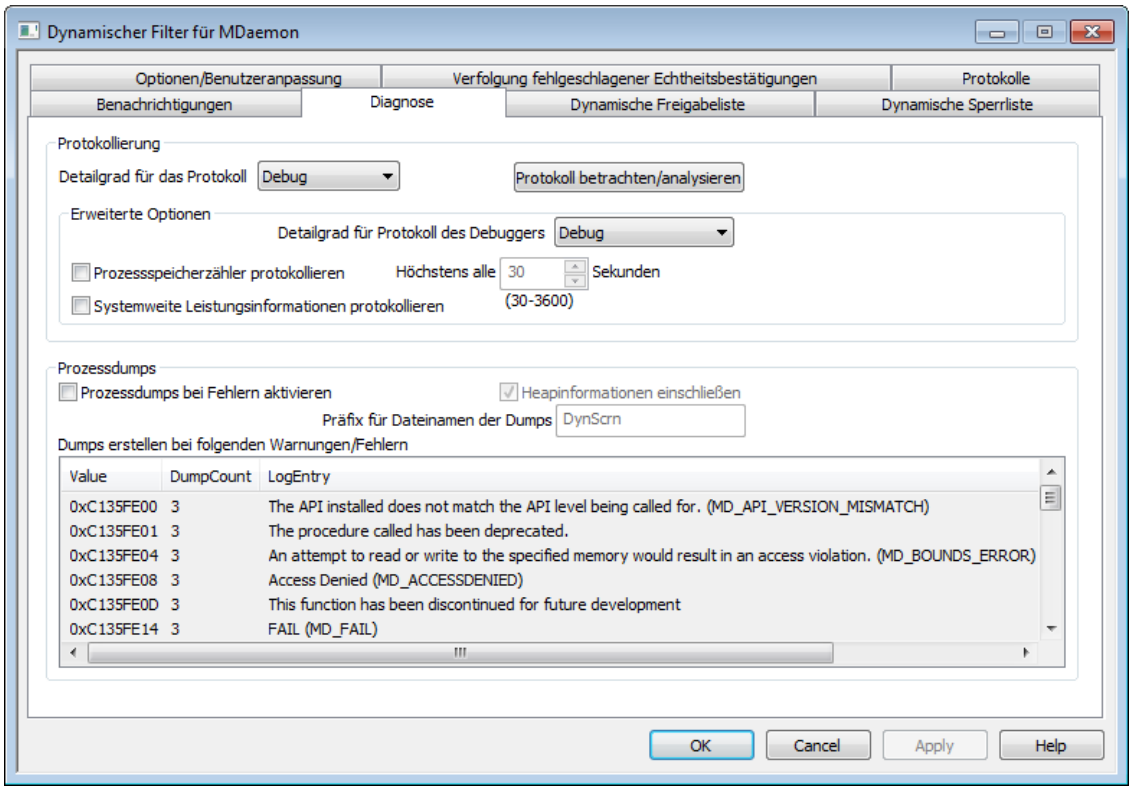
Standard-Empfängeradresse für Benachrichtigungen
Hier wird die E-Mail-Adresse festgelegt, an die die ausgewählten Berichte gesendet werden, falls keine anderen Empfänger ausgewählt sind, oder falls den ausgewählten Empfängern keine gültigen E-Mail-Adressen zugeordnet werden können. Können keine gültigen E-Mail-Adressen zugeordnet werden, und ist keine *Standard-Empfängeradresse für Benachrichtigungen* eingetragen, so werden keine Benachrichtigungen versandt.

GMT-Zeit in Benachrichtigungen über wegen Zeitablaufs gelöschte Einträge aufnehmen
Per Voreinstellung beziehen sich die Zeitangaben in den Berichten, die Informationen über den Zeitpunkt der Löschung eines Eintrags wegen Zeitablaufs enthalten, auf die Zeitzone, in der der Server selbst betrieben wird. Diese Option erweitert die Zeitangaben um die Zeit in der Zeitzone GMT. Dies ist insbesondere dann hilfreich, wenn Ihre Administratoren in verschiedenen Zeitzonen arbeiten.

Siehe auch:

Optionen/Benutzeranpassung 612
Verfolgung fehlgeschlagener Echtheitsbestätigungen 616

4.2.5 Diagnose



Dieser Konfigurationsdialog enthält erweiterte Optionen, die üblicherweise nur zur Fehlersuche im Dynamischen Filter oder zur Bereitstellung von Daten für den technischen Support gebraucht werden.

Protokollierung

Detailgrad für das Protokoll
Der Cluster-Dienst von MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info	Dies ist ein Detailgrad mit üblichem Umfang. Es werden allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.
Warnung	Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.
Fehler	Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.
kritisch	Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.
Keine	Es werden nur Starten und Beenden des Dienstes protokolliert.

Protokolldatei betrachten/analysieren
Durch Anklicken dieses Steuerelements öffnet sich der erweiterte Protokollbetrachter für MDaemon. Per Voreinstellung werden die Protokolle im Verzeichnis "..\MDaemon\Logs\" gespeichert.

Erweiterte Optionen

Detailgrad für Protokoll des Debuggers
Diese Option bestimmt den geringsten zulässigen Detailgrad für die Protokolldaten, die an den Debugger übermittelt werden. Die auswählbaren Detailgrade sind dieselben wie in der Tabelle weiter oben.

Prozessspeicherzähler protokollieren
Mithilfe dieser Option können prozessspezifische Informationen über Speicher, Handle und Threads protokolliert werden. Diese Informationen sind hilfreich, um Probleme mit der Zuweisung von Ressourcen und vergleichbare Probleme zu diagnostizieren. Die Protokolleinträge werden nur ausgegeben, wenn die Daten sich seit der letzten Protokollierung geändert haben.

Systemweite Leistungsinformationen protokollieren
Mithilfe dieser Option können systemweite Leistungsdaten protokolliert werden. Diese Informationen sind hilfreich, um Probleme mit der Zuweisung von Ressourcen und vergleichbare Probleme zu diagnostizieren. Die Protokolleinträge werden nur ausgegeben, wenn die Daten sich seit der letzten Protokollierung geändert haben.

Höchstens alle [xx] Sekunden
Diese Option begrenzt die Häufigkeit, mit der die Prozess- und Leistungsinformationen protokolliert werden.

Prozessdumps

Prozessdumps bei Fehlern aktivieren
Diese Option bewirkt die Erstellung von Prozessdumps in den Fällen, in denen die weiter unten angegebenen Warnungen und Fehler auftreten.

Heapinformationen einschließen
Per Voreinstellung werden die Heapinformationen in die Prozessdumps aufgenommen. Falls Sie dies nicht wünschen, deaktivieren Sie dieses Kontrollkästchen.

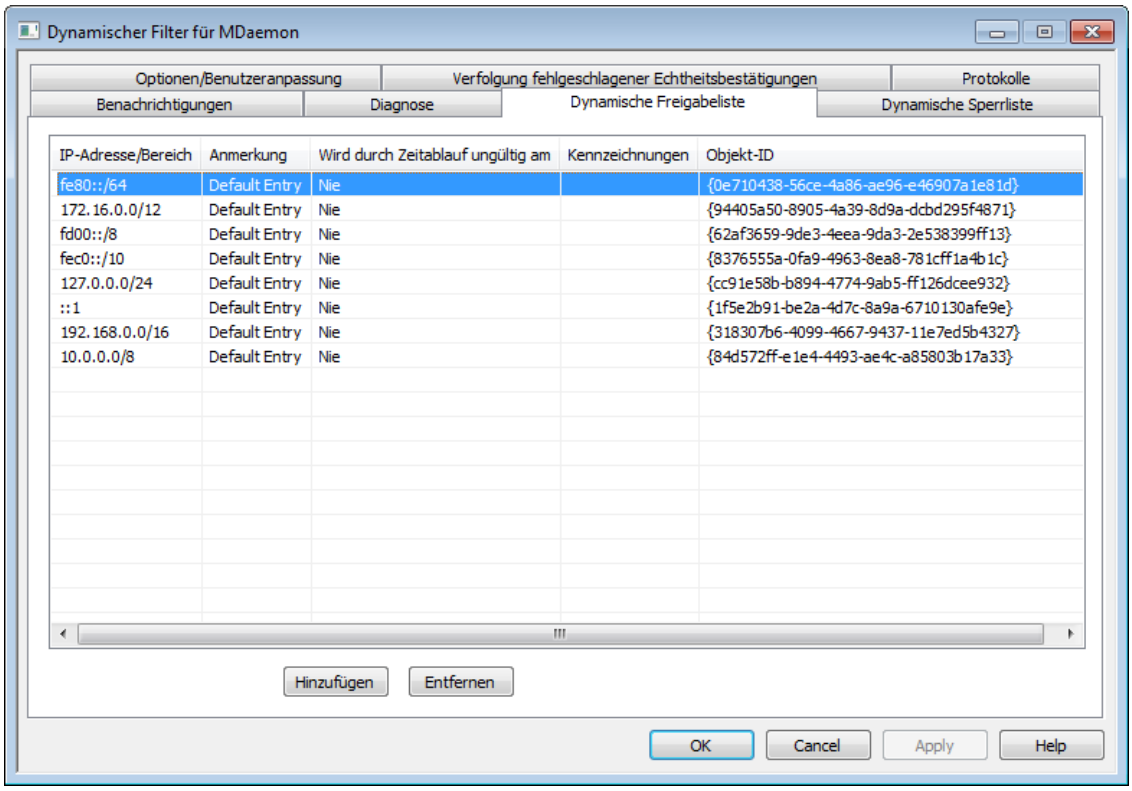
Präfix für Dateinamen der Dumps
Die Dateinamen der Dump-Dateien beginnen mit dem hier angegeben Text. Der Präfix lautet per Voreinstellung "AirSync".

Dumps erstellen bei folgenden Warnungen/Fehlern
Um diese Einträge zu bearbeiten, öffnen Sie durch Rechtsklick in diesem Bereich das Kontextmenü. Mithilfe der dann erscheinenden Menüeinträge *Eintrag hinzufügen, Eintrag bearbeiten* und *Eintrag löschen* können Sie die Liste der Fehler und Warnungen verwalten, die das Erstellen von Prozessdumps auslösen. Für jeden Eintrag können Sie die Anzahl der zulässigen Prozessdumps angeben; wird diese Zahl erreicht, so wird der Eintrag deaktiviert.

Siehe auch:

Dynamischer Filter » Optionen/Benutzeranpassung 612

4.2.6 Dynamische Freigabeliste

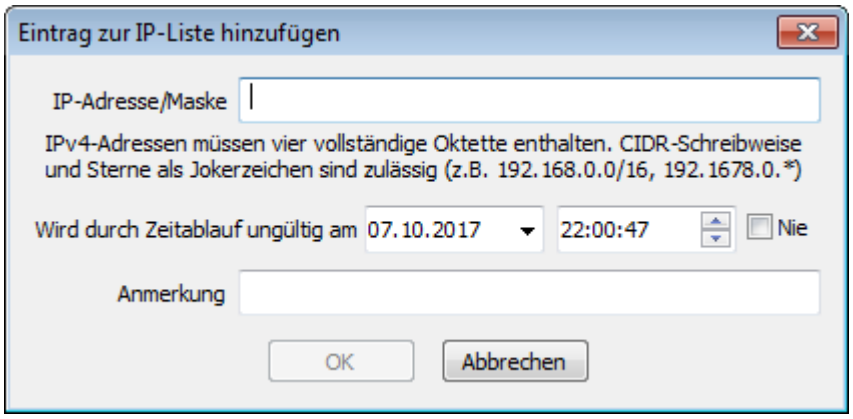


In der Dynamischen Freigabeliste sind die IP-Adressen und -Adressbereiche erfasst, die von der Behandlung durch den Dynamischen Filter ausgenommen sind und daher nicht gegen Versuche gesperrt werden, Verbindungen mit MDaemon herzustellen. Sie können Einträge in die Freigabeliste aufnehmen, indem Sie auf die Schaltfläche **Hinzufügen** klicken. Jeder Eintrag enthält die betroffene IP-Adresse oder den betroffenen IP-Adressbereich, Datum und Uhrzeit, zu denen der Eintrag automatisch wieder gelöscht wird, Anmerkungen, die Sie zu dem Eintrag erfassen wollen, und eine Objekt-ID. Statt eines Zeitpunks für die automatische Löschung kann auch "**Nie**" ausgewählt werden; solche Einträge verbleiben dauerhaft in der Dynamischen Freigabeliste. Die Dynamische Freigabeliste gilt auch für die Leistungsmerkmale SMTP-Filter 567, Länder-Filter 574 und Teergrube 604.

Hinzufügen von Einträgen zur Dynamischen Freigabeliste

Um der Liste einen neuen Eintrag hinzuzufügen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf **Hinzufügen**. Hierdurch öffnet sich das Eingabefenster **Eintrag zur IP-Liste hinzufügen**.



2. Geben Sie die gewünschte IP-Adresse oder den gewünschten IP-Adressbereich ein.
3. Wählen Sie Datum und Uhrzeit, zu denen der Eintrag wegen Zeitablaufs automatisch wieder gelöscht werden soll, oder klicken Sie auf **Nie**.
4. Geben Sie eine Anmerkung zu dem Eintrag ein, falls gewünscht.
5. Klicken Sie auf **OK**.

Entfernen von Einträgen aus der Liste

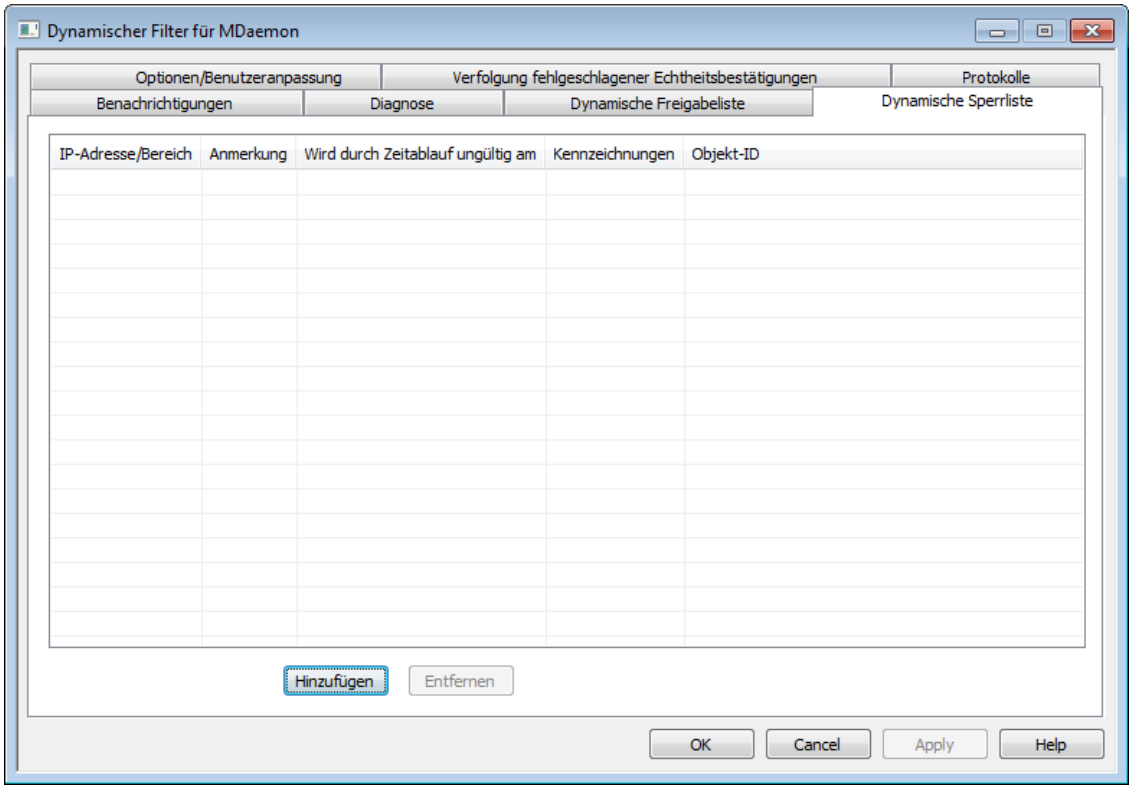
Um einen Eintrag oder mehrere Einträge aus der Liste zu entfernen, gehen Sie folgendermaßen vor:

1. Wählen Sie den Eintrag oder die Einträge, die Sie aus der Liste entfernen wollen. Um mehrere Einträge auszuwählen, halten Sie die Taste Strg gedrückt, während Sie die gewünschten Einträge anklicken.
2. Klicken Sie auf **Entfernen**.

Siehe auch:

Optionen/Benutzeranpassung 612
Verfolgung fehlgeschlagener Echtheitsbestätigungen 616
Dynamische Sperrliste 628
Protokolle 620

4.2.7 Dynamische Sperrliste

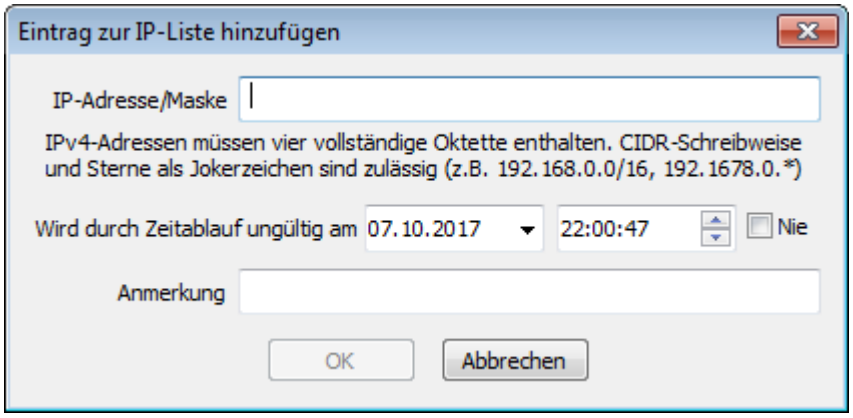


In der Dynamischen Sperrliste sind die IP-Adressen und -Adressbereiche erfasst, die der Dynamische Filter gegen Versuche sperrt, Verbindungen mit MDaemon herzustellen. Einträge können mithilfe der Optionen zur Verfolgung fehlgeschlagener Echtheitsbestätigungen[616] und des SMTP-Filters[567] automatisch in die Sperrliste aufgenommen werden. Sie können Einträge auch manuell erfassen, indem Sie auf die Schaltfläche **Hinzufügen** klicken. Jeder Eintrag enthält die betroffene IP-Adresse oder den betroffenen IP-Adressbereich, Datum und Uhrzeit, zu denen der Eintrag automatisch wieder gelöscht wird, Anmerkungen, die Sie zu dem Eintrag erfassen wollen, und eine Objekt-ID. Statt eines Zeitpunks für die automatische Löschung kann auch "**Nie**" ausgewählt werden; solche Einträge verbleiben dauerhaft in der Dynamischen Sperrliste.

Hinzufügen von Einträgen zur Dynamischen Sperrliste

Um der Liste einen neuen Eintrag hinzuzufügen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf **Hinzufügen**. Hierdurch öffnet sich das Eingabefenster **Eintrag zur IP-Liste hinzufügen**.



2. Geben Sie die gewünschte IP-Adresse oder den gewünschten IP-Adressbereich ein.
3. Wählen Sie Datum und Uhrzeit, zu denen der Eintrag wegen Zeitablaufs automatisch wieder gelöscht werden soll, oder klicken Sie auf **Nie**.
4. Geben Sie eine Anmerkung zu dem Eintrag ein, falls gewünscht.
5. Klicken Sie auf **OK**.

Entfernen von Einträgen aus der Liste

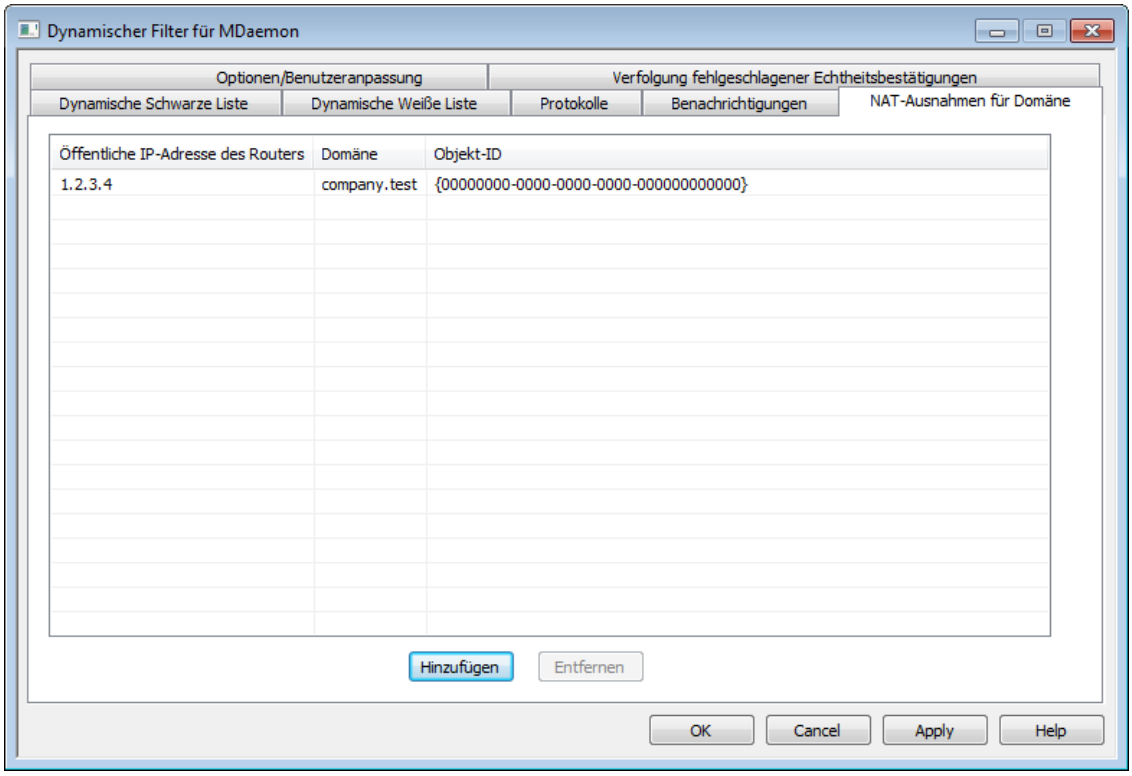
Um einen Eintrag oder mehrere Einträge aus der Liste zu entfernen, gehen Sie folgendermaßen vor:

1. Wählen Sie den Eintrag oder die Einträge, die Sie aus der Liste entfernen wollen. Um mehrere Einträge auszuwählen, halten Sie die Taste Strg gedrückt, während Sie die gewünschten Einträge anklicken.
2. Klicken Sie auf **Entfernen**.

Siehe auch:

Optionen/Benutzeranpassung 612
Verfolgung fehlgeschlagener Echtheitsbestätigungen 616
Dynamische Freigabeliste 626
Protokolle 620

4.2.8 NAT-Ausnahmen für Domäne



Dieser Konfigurationsdialog ist nur zugänglich, wenn im Konfigurationsdialog Optionen/Benutzeranpassung[612] des Dynamischen Filters die Option *Erweiterte Leistungsmerkmale auf der Benutzeroberfläche anzeigen* aktiviert haben.

Dieses Leistungsmerkmal kann in solchen Anwendungsfällen hilfreich sein, in denen eine Gruppen von MDaemon-Benutzern in demselben externen Netzwerk (LAN) zusammengefasst ist und für dieses Netzwerk die Netzadressumsetzung (Network Address Translation, NAT) genutzt wird. Die Nutzung der NAT führt dazu, dass alle Benutzer des Netzwerks unter derselben öffentlichen IP-Adresse auftreten. Wenn Sie diese öffentliche IP-Adresse für das externe Netzwerk, in dem die MDaemon-Benutzer zusammengefasst sind, in die Liste der NAT-Ausnahmen eintragen, können Sie dadurch verhindern, dass die öffentliche IP-Adresse und damit alle dahinterliegenden Benutzer durch den Dynamischen Filter gesperrt werden, wenn bei nur einem Benutzerkonto die Echtheitsbestätigung wegen eines falschen Kennworts fehlschlägt. Ohne die NAT-Ausnahme würde ein einziger Benutzer mit fehlerhaft konfiguriertem E-Mail-Client die Sperrung der IP-Adresse verursachen, die auch alle anderen Benutzer in dem externen Netzwerk erfassen würde. Dieser Fall kann beispielsweise eintreten, wenn ein Benutzer sein Kennwort geändert, aber vergessen hat, das geänderte Kennwort in seinen Mailclient einzutragen.

IP-Adressen, die hier erfasst sind, können aus anderen Gründen dennoch gesperrt werden, beispielsweise, wenn Bots die Anmeldung an nicht bestehenden Benutzerkonten versuchen oder falsch konfigurierte Mailclients die Anmeldung an einer MDaemon-Domäne versuchen, die mit der hier erfassten IP-Adresse nicht verknüpft ist. Falls Sie eine IP-Adresse vollständig von der Bearbeitung durch den Dynamischen Filter ausschließen wollen, müssen Sie die IP-Adresse in die Dynamische Freigabeliste[626] eintragen.

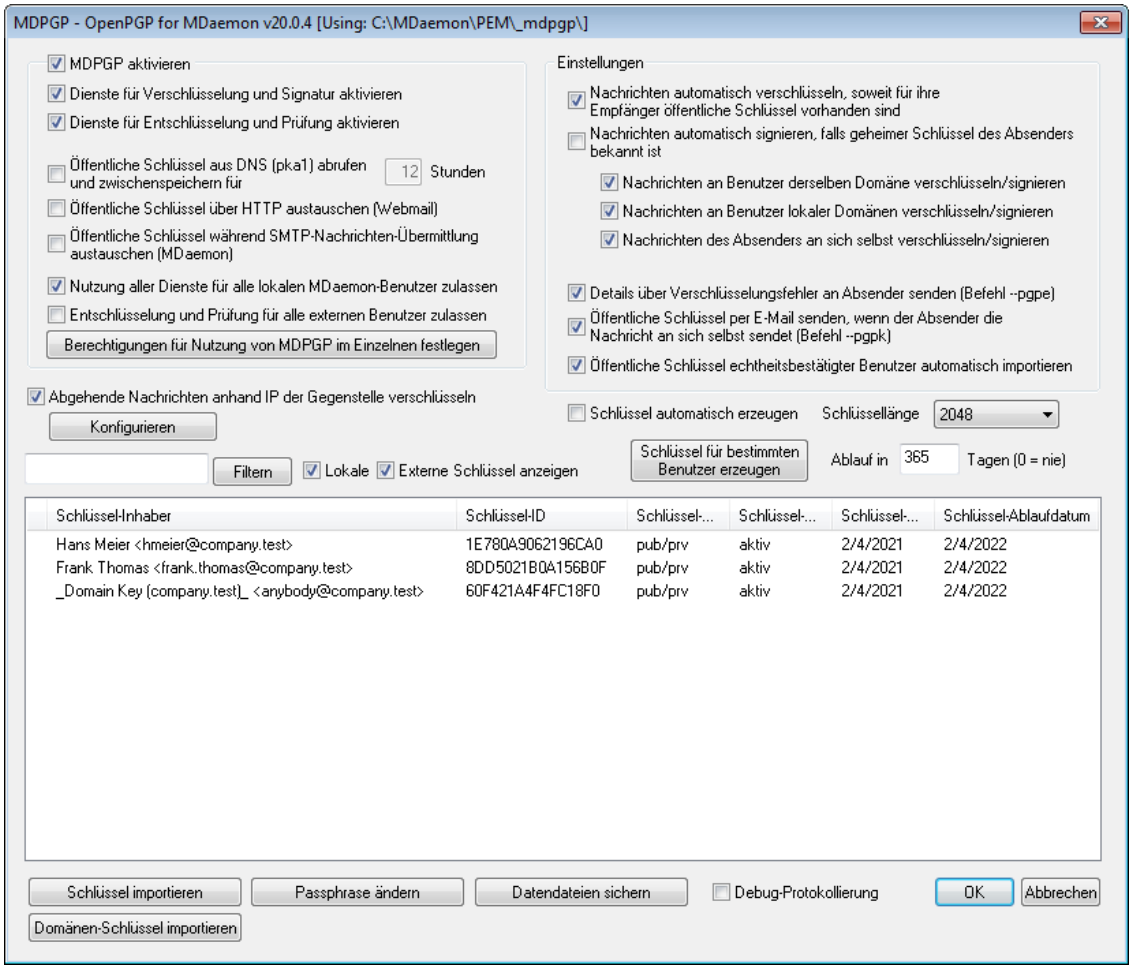
Hinzufügen einer NAT-Ausnahme für eine Domäne

Um eine NAT-Ausnahme hinzuzufügen, klicken Sie auf **Hinzufügen**. Geben Sie danach die *Öffentliche IP-Adresse des Routers* ein, unter der das externe Netzwerk nach außen auftritt, und wählen Sie die MDaemon-*Domäne* aus, deren Benutzer unter der angegebenen IP-Adresse Verbindungen herstellen. Klicken Sie zum Abschluss auf **OK**.

Siehe auch:

Optionen/Benutzeranpassung 612

4.3 MDPGP



OpenPGP ist ein standardisiertes Verfahren zum Austausch verschlüsselter Daten. Es stehen zahlreiche OpenPGP-Plugins für Mailclients zur Verfügung, mit deren Hilfe die Benutzer verschlüsselte Nachrichten senden und empfangen können. MDPGP ist eine in MDaemon integrierte OpenPGP-Komponente, die Ihren Benutzern Leistungsmerkmale für Verschlüsselung, Entschlüsselung und grundlegende Funktionen zur Schlüsselverwaltung zur Verfügung stellt, ohne dass die Benutzer hierzu Plugins in ihren E-Mail-Clients nutzen müssen.

MDPGP verschlüsselt und entschlüsselt Nachrichten nach einem asymmetrischen Verfahren mit öffentlichen und geheimen ("privaten") Schlüsseln. Will ein Benutzer mithilfe von MDPGP eine verschlüsselte Nachricht an einen Empfänger übermitteln, dann verschlüsselt MDPGP diese Nachricht mithilfe eines Schlüssels, den der

Empfänger dem Absender zuvor zur Verfügung gestellt haben, und der in MDPGP importiert worden sein muss. Dieser Schlüssel wird als öffentlicher Schlüssel des Empfängers bezeichnet. Will ein externer Absender einem Empfänger auf dem MDaemon-Server eine verschlüsselte Nachricht übermitteln, so muss der Empfänger diesem Absender ebenfalls zuvor seinen öffentlichen Schlüssel zur Verfügung gestellt haben. Dieser Schlüsselaustausch ist Voraussetzung für die Verschlüsselung von Nachrichten durch OpenPGP. Eine Nachricht, die nur mit dem öffentlichen Schlüssel des Empfängers verschlüsselt ist, kann nur der Empfänger mit einem weiteren, nämlich seinem geheimen Schlüssel entschlüsseln. Dieser geheime Schlüssel bleibt beim Empfänger und darf dem Kommunikationspartner nicht bekannt gemacht werden. MDPGP verwaltet die geheimen Schlüssel der Benutzer auf dem MDaemon-Server und nutzt sie zum Entschlüsseln der eingehenden Nachrichten.

MDPGP unterhält zwei Schlüsselspeicher, um die Leistungsmerkmale zu Signatur, Verschlüsselung und Entschlüsselung zur Verfügung zu stellen. Diese Schlüsselspeicher werden auch als Schlüsselringe oder Schlüsselbunde bezeichnet. Ein Schlüsselbund enthält die öffentlichen Schlüssel, der zweite Schlüsselbund enthält die geheimen Schlüssel. MDPGP kann für die eigenen Benutzer automatisch Schlüssel erzeugen, sobald sie gebraucht werden. Schlüssel können auch manuell für bestimmte Benutzer erzeugt werden. Es lassen sich auch bereits bestehende Schlüssel importieren. MDaemon kann in Nachrichten, die von lokalen Benutzern stammen und in Verbindungen mit Echtheitsbestätigung übermittelt wurden, auch automatisch nach öffentlichen Schlüsseln suchen, etwa in Dateianlagen, und diese Schlüssel automatisch importieren. Die lokalen Benutzer können so beispielsweise ihre Kommunikationspartner zur Übermittlung derer öffentlicher Schlüssel per E-Mail auffordern und sich diese Schlüssel dann selbst per E-Mail zusenden. MDPGP importiert diese Schlüssel dann in den Schlüsselbund für öffentliche Schlüssel. MDPGP speichert jeden Schlüssel nur einmal, kann aber mehrere verschiedene Schlüssel für dieselbe Adresse speichern. Geht eine Nachricht für eine Adresse ein, zu der in einem Schlüsselbund ein passender Schlüssel vorhanden ist, so signiert, verschlüsselt oder entschlüsselt MDPGP die Nachricht je nach Bedarf und in Übereinstimmung mit den hier getroffenen Einstellungen. Liegen für eine Adresse mehrere Schlüssel vor, so verwendet MDPGP zur Verschlüsselung den als bevorzugt gekennzeichneten Schlüssel. Ist kein Schlüssel als bevorzugt gekennzeichnet, so nutzt MDaemon den ersten Schlüssel. Bei der Entschlüsselung nutzt MDaemon alle für die Adresse verfügbaren Schlüssel.

Sie können die Leistungsmerkmale für Signatur und Verschlüsselung in MDPGP auf automatischen oder manuellen Betrieb konfigurieren. Im automatischen Betrieb signiert und verschlüsselt MDaemon die Nachrichten, soweit dies möglich ist. Im manuellen Betrieb signiert und verschlüsselt MDaemon die Nachrichten, falls der Absender bestimmte Befehle in die Betreffzeile der Nachrichten aufnimmt. In beiden Betriebsarten werden Nachrichten aber nur dann signiert, verschlüsselt und entschlüsselt, wenn der betreffende Benutzer die Berechtigung hat, die Leistungsmerkmale von MDPGP zu nutzen.

Die Spezifikation für OpenPGP ist in den RFCs 4880 und 3156 in englischer Sprache beschrieben.

MDPGP aktivieren

MDPGP aktivieren
MDPGP ist per Voreinstellung aktiv. MDPGP signiert, verschlüsselt und entschlüsselt Nachrichten aber erst dann, wenn Sie Schlüssel erstellt oder

bestehende Schlüssel in die Schlüsselbunde importiert haben, oder wenn Sie die Option *Schlüssel automatisch erzeugen* weiter unten aktivieren.

Dienste für Verschlüsselung und Signatur aktivieren
Nachrichten werden per Voreinstellung signiert und verschlüsselt, falls die erforderlichen Schlüssel in den Schlüsselbunden vorhanden sind. Falls Sie nicht wünschen, dass MDPGP Nachrichten signiert und verschlüsselt, deaktivieren Sie diese Option.

Nachrichten können auch dann signiert werden, wenn sie nicht verschlüsselt werden. Verschlüsselt MDPGP eine Nachricht, so signiert MDPGP die Nachricht aber immer.

Dienste für Entschlüsselung und Prüfung aktivieren
Eingehende Nachrichten werden per Voreinstellung entschlüsselt, falls der geheime Schlüssel des Empfängers verfügbar ist. MDPGP prüft außerdem die Signaturen eingehender unverschlüsselter Nachrichten. Diese Leistungsmerkmale sind aber nur aktiv, wenn Empfänger und Absender zur Nutzung der Dienste für Entschlüsselung und Prüfung berechtigt sind. Diese Berechtigung kann durch die Optionen *Nutzung aller Dienste für alle lokalen MDaemon-Benutzer zulassen* und *Berechtigungen für Nutzung von MDPGP im Einzelnen festlegen* weiter unten erteilt werden. Per Voreinstellung sind alle Benutzer entsprechend berechtigt. Falls Sie die Signaturen eingehender Nachrichten nicht prüfen lassen wollen oder eingehende Nachrichten nicht durch MDPGP entschlüsseln lassen wollen, deaktivieren Sie diese Option. Die Benutzer können dann eingehende Nachrichten in ihren Clients entschlüsseln und müssen hierzu möglicherweise besondere Plugins benutzen. Solange diese Option abgeschaltet ist, werden alle eingehenden verschlüsselten Nachrichten wie normale Nachrichten behandelt und in die Postfächer der Empfänger eingestellt.

Öffentliche Schlüssel aus DNS (pka1) abrufen und zwischenspeichern für [xx] Stunden
Diese Option bewirkt, dass MDPGP DNS-Abfragen nach den öffentlichen Schlüsseln von Nachrichten-Empfängern durchführt. Solche öffentlichen Schlüssel können in TXT-Einträgen des Formats PKA1 im DNS veröffentlicht sein. Diese Option erleichtert die Arbeit, weil sie den Abruf öffentlicher Schlüssel, die zum Verschlüsseln von Nachrichten benötigt werden, automatisiert. Ihre Benutzer müssen dann nicht zunächst die öffentlichen Schlüssel ihrer Kommunikationspartner selbst beschaffen und in den Schlüsselbund importieren, damit sie den Kommunikationspartnern verschlüsselte Nachrichten senden können. Alle Schlüssel-URIs, die im Rahmen der PKA1-Abfragen gefunden werden, werden sofort ausgewertet. Die entsprechenden Schlüssel werden abgerufen, geprüft und in den Schlüsselbund aufgenommen. Schlüssel, die in dieser Weise erfolgreich abgerufen wurden, werden in der Datei `fetchedkeys.txt` zwischengespeichert. Sie bleiben nur für die in dieser Option angegebene Dauer gültig. Ist für den PKA1-Eintrag selbst im Feld TTL (time to live, Gültigkeitsdauer) eine Gültigkeitsdauer bestimmt, so wird diese Gültigkeitsdauer ausgewertet. Unterscheiden sich die Gültigkeitsdauer aus dieser Option und die aus dem PKA1-Eintrag, so gilt die längere Gültigkeitsdauer. Der Gültigkeitszeitraum aus dieser Option stellt damit den Mindestzeitraum dar, für den der Schlüssel zwischengespeichert wird. Die Voreinstellung beträgt 12 Stunden. Der niedrigste zulässige Wert beträgt 1 Stunde.

Sie können auch eigene öffentliche Schlüssel im DNS veröffentlichen. Hierzu müssen Sie TXT-Einträge in einem bestimmten Format erstellen. Ein Beispiel hierzu: Für den Benutzer `frank@example.com` mit der Schlüssel-ID `0A2B3C4D5E6F7G8H` erstellen Sie im DNS der Domäne "`example.com`" einen Eintrag des Typs `TXT` mit dem Inhalt "`frank._pka.example.com`" (Sie ersetzen das Zeichen `@` aus der E-Mail-Adresse durch die Zeichenkette "`._pka.`"). Die Daten für den `TXT`-Eintrag haben dann etwa folgendes Format "`v=pka1; fpr=<vollständiger Fingerabdruck des Schlüssels>; uri=<Webmail-URL>/WorldClient.dll?view=mdpgp&k=0A2B3C4D5E6F7G8H`". Dabei setzen Sie für den `<vollständigen Fingerabdruck des Schlüssels>` den vollständigen, aus 40 Zeichen (20 Byte) bestehenden, Fingerabdruck des Schlüssels ein. Den vollständigen Fingerabdruck der einzelnen Schlüssel können Sie in der Benutzeroberfläche von MDPGP einsehen. Klicken Sie dazu doppelt auf den gewünschten Schlüssel.

Öffentliche Schlüssel über HTTP austauschen (Webmail)
Diese Option gestattet es Ihnen, Webmail als einfachen Server für öffentliche Schlüssel zu verwenden. Webmail beantwortet dann Anforderungen nach den öffentlichen Schlüsseln Ihrer lokalen Benutzer. Um eine solche Anforderung zu senden, muss ein URL nach folgendem Muster verwendet werden: "`http://<Webmail-URL>/WorldClient.dll?View=MDPGP&k=<Schlüssel-ID>`". Dabei muss für den Platzhalter `<Webmail-URL>` der Pfad zu Ihrem Webmail-Server eingesetzt werden (beispielsweise "`http://webmail.example.com`"). Für den Platzhalter `<Schlüssel-ID>` muss die 16 Zeichen lange Schlüssel-ID des gewünschten Schlüssels eingesetzt werden (beispielsweise "`0A1B3C4D5E6F7G8H`"). Die Schlüssel-ID besteht aus den letzten 8 Byte des Fingerabdrucks des Schlüssels und enthält insgesamt 16 Zeichen.

Öffentliche Schlüssel während SMTP-Nachrichten-Übermittlung austauschen (MDaemon)
Diese Option ermöglicht die automatische Übermittlung öffentlicher Schlüssel während der Übermittlung von Nachrichten über SMTP. Ist sie aktiv, so befolgt der SMTP-Server von MDaemon den SMTP-Befehl RKEY. Übermittelt MDaemon eine E-Mail-Nachricht an eine Gegenstelle, die RKEY unterstützt, so bietet MDaemon dieser Gegenstelle an, den aktuellen und bevorzugten öffentlichen Schlüssel des Absenders der Nachricht zusätzlich zu der Nachricht selbst ebenfalls zu übermitteln. Die Gegenstelle antwortet dann entweder, dass der Schlüssel bereits bekannt ist und nicht erneut benötigt wird (Meldung "250 2.7.0 Key already known", *Schlüssel schon bekannt*), oder dass der Schlüssel benötigt wird. Im zweiten Fall übermittelt MDaemon den Schlüssel sofort im ASCII-Armored-Format (auf Meldung der Gegenstelle "354 Enter key, end with CRLF.CRLF", *Schlüssel übermitteln, beenden mit CRLF.CRLF*). Die Übermittlung entspricht dabei technisch der Übermittlung einer E-Mail-Nachricht. Schlüssel mit abgelaufener Gültigkeit und widerrufene Schlüssel werden keinesfalls übermittelt. Verfügt MDaemon über mehrere Schlüssel für den Absender, so bietet MDaemon immer den als bevorzugt gekennzeichneten Schlüssel an. Ist kein Schlüssel als bevorzugt gekennzeichnet, so bietet MDaemon den ersten gefundenen Schlüssel an. Sind keine gültigen Schlüssel verfügbar, so wird keine Übermittlung

durchgeführt. Es werden nur Schlüssel angeboten, die lokalen Benutzern zugeordnet sind.

Die Übermittlung der öffentlichen Schlüssel erfolgt während der SMTP-Verbindung, über die auch die zugehörige Nachricht übermittelt wird. Öffentliche Schlüssel, die auf diesem Weg übermittelt werden, werden nur akzeptiert, falls die zugehörige Nachricht alle folgenden Voraussetzungen erfüllt: Die Nachricht muss mit einer gültigen DKIM -Signatur[533] der Domäne versehen sein, zu der der Schlüsselinhaber gehört. Der Tag i= muss dabei die Adresse des Schlüsselinhabers enthalten, und diese Adresse muss genau der Adresse aus der Absenderkopfzeile From: entsprechen. Es darf nur eine Absenderkopfzeile From: vorhanden sein. Der Schlüsselinhaber wird dem Schlüssel selbst entnommen. Die Nachricht muss durch einen Host zugestellt werden, der in den SPF-Einträgen[527] der Absenderdomäne enthalten ist. Der Schlüsselinhaber muss zur Nutzung von RKEY berechtigt sein. Hierzu müssen in der Regeldatei von MDPGP entsprechende Einträge entweder für den Schlüsselinhaber selbst oder für die gesamte Domäne enthalten sein (Anweisungen hierzu enthält die Datei selbst), die bestimmen, dass die Domäne für Zwecke des Schlüsselaustauschs vertrauenswürdig ist. Die Prüfung, ob die Voraussetzungen erfüllt sind, laufen automatisch ab, und hierzu müssen die DKIM[529] und die SPF-Prüfung[527] zwingend aktiv sein.

Das Protokoll für MDPGP weist die Ergebnisse und die Einzelheiten für alle Schlüssel aus, die importiert und gelöscht werden, und zwar auch für die während der SMTP-Verbindung übermittelten Schlüssel. Die eigentliche Übermittlung der Schlüssel während der SMTP-Verbindung wird im Protokoll für SMTP vermerkt.

Nutzung aller Dienste für alle lokalen MDaemon-Benutzer zulassen
Per Voreinstellung können alle lokalen MDaemon-Benutzerkonten alle MDPGP-Dienste nutzen, die Sie in diesem Konfigurationsdialog aktiviert haben, also Signatur, Verschlüsselung, Entschlüsselung und Prüfung. Falls Sie einzelnen Benutzern die Nutzung dieser Dienste nicht oder die Nutzung nicht aller Dienste gestatten wollen, können Sie diese Benutzer mithilfe der Schaltfläche "*Berechtigungen für Nutzung von MDPGP im Einzelnen festlegen*" weiter unten genau bestimmen. Falls Sie nur einzelnen bestimmten lokalen Benutzern die Nutzung der MDPGP-Dienste gestatten wollen, deaktivieren Sie diese Option, und legen Sie die einzelnen Berechtigungen mithilfe der Schaltfläche "*Berechtigungen für Nutzung von MDPGP im Einzelnen festlegen*" weiter unten fest.

Entschlüsselung und Prüfung für alle externen Benutzer zulassen
Per Voreinstellung kann jede für ein lokales Benutzerkonto eingehende Nachricht eines externen Absenders entschlüsselt werden, falls MDPGP den geheimen Schlüssel des lokalen Empfängers kennt. Darüber hinaus prüft MDPGP die Signaturen in eingehenden Nachrichten externer Absender.

Falls die die Nachrichten bestimmter externer Absender nicht entschlüsseln und prüfen wollen, können Sie diese externen Absender mithilfe der Schaltfläche "*Berechtigungen für Nutzung von MDPGP im Einzelnen festlegen*" weiter unten bestimmen. Falls Sie nur die Nachrichten einzelner bestimmter externer Absender durch MDPGP entschlüsseln und prüfen lassen wollen, deaktivieren Sie diese Option, und legen Sie mithilfe der Schaltfläche "*Berechtigungen für Nutzung von MDPGP im Einzelnen festlegen*" weiter unten die externen Absender fest, deren Nachrichten entschlüsselt und geprüft werden sollen.

Berechtigungen für Nutzung von MDPGP im Einzelnen festlegen
Durch Anklicken dieser Schaltfläche öffnet sich die Datei `rules.txt`, in der Sie für einzelne Benutzer die Berechtigungen zur Nutzung von MDPGP festlegen können. Mithilfe dieser Datei können Sie festlegen, wer Nachrichten signieren, verschlüsseln und entschlüsseln lassen darf. Sie können auch einzelne Benutzer von der Nutzung dieser Leistungsmerkmale ausschließen. Mithilfe des Eintrags "`+*@example.com`" können Sie beispielsweise allen Benutzern der Domäne `example.com` die Verschlüsselung von Nachrichten gestatten, dann aber mithilfe des Eintrags "`-frank@example.com`" den Benutzer `frank@example.com` von der Nutzung dieses Leistungsmerkmals gezielt ausschließen. Sie finden am Beginn der Datei `rules.txt` einen Hinweistext mit Beispielen und Erläuterungen.

Hinweise zur Datei Rules.txt und ihrer Syntax

- Die Verschlüsselung kann nur für solche Nachrichten durchgeführt werden, die von Benutzern des eigenen MDaemon-Servers stammen und in Verbindungen mit SMTP-Echtheitsbestätigung übermittelt werden. Sie können auch externe Adressen angeben, die die Verschlüsselungs-Dienste nicht nutzen dürfen. Nachrichten an solche externen Adressen verschlüsselt MDPGP auch dann nicht, wenn der zugehörige öffentliche Schlüssel verfügbar ist.
- Falls Einträge in der Datei `rules.txt` der globalen Option "*Nutzung aller Dienste für alle lokalen MDaemon-Benutzer zulassen*" widersprechen, gehen die Einträge und Einstellungen der Datei `rules.txt` vor.
- Falls zwischen den Einträgen in der Datei `rules.txt` und der systemweiten Option "*Entschlüsselung und Prüfung für alle externen Benutzer zulassen*" Widersprüche bestehen, gehen die Einträge in der Datei `rules.txt` der systemweiten Option vor.
- Zeilen, die mit # beginnen, werden nicht ausgewertet.
- Trennen Sie mehrere E-mail-Adressen auf derselben Zeile durch Leerzeichen.
- Jokerzeichen (* und ?) sind in E-Mail-Adressen zulässig.
- MDPGP signiert zwar Nachrichten immer dann, wenn MDPGP sie auch verschlüsselt, die Berechtigung zur Nutzung der Verschlüsselung umfasst aber nicht auch die Berechtigung zum Signieren unverschlüsselter Nachrichten. Benutzerkonten können unverschlüsselte Nachrichten nur dann signieren, wenn sie über die Berechtigung zum Signieren verfügen.
- Jeder E-Mail-Adresse muss eines der folgenden Steuerzeichen vorangestellt werden:

+ (Plus) - Die Adresse darf MDPGP zur Verschlüsselung nutzen.

- (Minus) - Die Adresse darf MDPGP **nicht** zur Verschlüsselung nutzen.

! (Ausrufezeichen) - Die Adresse darf MDPGP zur Entschlüsselung nutzen.

~ (Tilde) - Die Adresse darf MDPGP **nicht** zur Entschlüsselung nutzen.

^ (Caret) - Die Adresse darf MDPGP zum Signieren nutzen.

= (Istgleich) - Die Adresse darf MDPGP **nicht** zum Signieren nutzen.

$ (Dollar) - Die Adresse darf MDPGP zur Prüfung von Signaturen nutzen.

& (Und-Zeichen) - Die Adresse darf MDPGP **nicht** zur Prüfung von Signaturen nutzen.

Einige Beispiele hierzu:

`+*@*` — Alle Benutzer aller Domänen dürfen verschlüsseln.

`!*@*` — Alle Benutzer aller Domänen dürfen entschlüsseln.

`^*@*` — Alle Benutzer aller Domänen dürfen signieren.

`^*@example.com` — Alle Benutzer der Domäne `example.com` dürfen verschlüsseln.

`+frank@example.com ~frank@example.com` — Dieser Benutzer darf verschlüsseln aber nicht entschlüsseln.

`+GROUP:VerschlüsselungsBenutzer` — Die Mitglieder der MDaemon-Gruppe `VerschlüsselungsBenutzer` dürfen verschlüsseln.

`^GROUP:Signatoren` — Die Mitglieder der MDaemon-Gruppe `Signatoren` dürfen signieren.

Betriebsarten für Verschlüsselung und Signatur

Automatische Betriebsart

Mithilfe der Optionen im Abschnitt *Einstellungen* können Sie MDPGP so konfigurieren, dass Nachrichten berechtigter Benutzerkonten automatisch signiert und verschlüsselt werden. Versendet ein Benutzerkonto eine Nachricht in einer Verbindung mit Echtheitsbestätigung, und kennt MDPGP den erforderlichen Schlüssel, so wird die Nachricht in Abhängigkeit von den folgenden Einstellungen signiert oder verschlüsselt.

Im Abschnitt *Manuelle Betriebsart* weiter unten sind Steuerkodes für die Betreffzeile beschrieben. Diese Steuerkodes haben immer Vorrang vor den Einstellungen für die automatische Betriebsart. Sind also einzelne Optionen für die automatische Betriebsart deaktiviert, so können Benutzerkonten, die zum Signieren und Verschlüsseln von Nachrichten berechtigt sind, Nachrichten immer mithilfe der Steuerkodes signieren und verschlüsseln lassens.

Einstellungen

Nachrichten automatisch verschlüsseln, soweit für ihre Empfänger öffentliche Schlüssel vorhanden sind
Per Voreinstellung verschlüsselt MDPGP abgehende Nachrichten aller zur Verschlüsselung berechtigten Benutzerkonten, falls die geheimen Schlüssel der Empfänger bekannt sind. Falls Sie die Nachrichten nicht automatisch verschlüsseln lassen wollen, deaktivieren Sie diese Option. Berechtigte Benutzer können auch bei deaktivierter Option ihre Nachrichten mithilfe der unten beschriebene Steuerkodes verschlüsseln lassen.

Nachrichten automatisch signieren, falls geheimer Schlüssel des Absenders bekannt ist
Diese Option bewirkt, dass MDPGP abgehende Nachrichten aller zur Signatur berechtigten Benutzerkonten, deren geheime Schlüssel bekannt sind, automatisch signiert. Berechtigte Benutzer können auch bei deaktivierter Option ihre Nachrichten mithilfe der unten beschriebene Steuerkodes signieren lassen.

Nachrichten an Benutzer derselben Domäne verschlüsseln/signieren
Ist MDPGP zum automatischen Signieren und Verschlüsseln von Nachrichten konfiguriert, so bewirkt diese Option, dass MDPGP auch Nachrichten zwischen Benutzern derselben Domäne signiert und verschlüsselt, soweit die erforderlichen Schlüssel bekannt sind. Diese Option ist per Voreinstellung aktiv.

Nachrichten an Benutzer lokaler Domänen verschlüsseln/signieren
Ist MDPGP zum automatischen Signieren und Verschlüsseln von Nachrichten konfiguriert, so bewirkt diese Option, dass MDPGP auch Nachrichten zwischen Benutzern der lokalen MDaemon-Domänen signiert und verschlüsselt, soweit die erforderlichen Schlüssel bekannt sind. Werden auf dem MDaemon-Server beispielsweise die Domänen "example.com" und "example.net" betrieben, so werden Nachrichten zwischen den Benutzern dieser Domänen automatisch verschlüsselt oder signiert. Diese Option ist per Voreinstellung aktiv.

Nachrichten des Absenders an sich selbst verschlüsseln/signieren
Ist MDPGP zum automatischen Signieren und Verschlüsseln von Nachrichten konfiguriert, so verschlüsselt und signiert MDPGP auch Nachrichten, die der Absender an sich selbst sendet (z.B. frank@example.com an frank@example.com). Ist das betreffende Benutzerkonto zum Verschlüsseln und Entschlüsseln berechtigt (dies ist per Voreinstellung der Fall), so bedeutet dies, dass MDPGP die Nachricht entgegennimmt, verschlüsselt, sofort wieder entschlüsselt und in den Posteingang des Benutzers einstellt. Ist das betreffende Benutzerkonto nur zum Verschlüsseln, nicht aber zum Entschlüsseln berechtigt, so verschlüsselt MDPGP die Nachricht und stellt sie dann noch verschlüsselt in den Posteingang des Empfängers ein, der gleichzeitig der Absender ist. Diese Option ist per Voreinstellung aktiv.

Manuelle Betriebsart

Sie die oben beschriebenen Optionen *Nachrichten automatisch signieren...* und *Nachrichten automatisch verschlüsseln...* deaktiviert, so wird MDPGP in der manuellen Betriebsart betrieben. MDPGP signiert und verschlüsselt Nachrichten dann nur, wenn sie von berechtigten Benutzern in Verbindungen mit Echtheitsbestätigung übermittelt werden und die folgenden Steuerkodes in der Betreffzeile enthalten.

--pgps Die Nachricht wird signiert, falls möglich. Der Steuerkode darf am Beginn oder Ende der Betreffzeile erscheinen.

--pgpe Die Nachricht wird verschlüsselt, falls möglich. Der Steuerkode darf am Beginn oder Ende der Betreffzeile erscheinen.

--pgpx Die Nachricht **muss zwingend** verschlüsselt werden. Falls die Nachricht nicht verschlüsselt werden kann, etwa, weil der öffentliche Schlüssel des Empfängers nicht bekannt ist, dann wird die Nachricht nicht zugestellt sondern an den Absender

zurückgeleitet. Der Steuerkode darf am Beginn oder Ende der Betreffzeile erscheinen.

--pgpk Dem Absender wird sein eigener öffentlicher Schlüssel zugesandt. Hierzu setzt der betreffende Benutzer den Steuerkode an den Beginn der Betreffzeile und sendet die Nachricht an sich selbst. MDPGP sendet dem Benutzer dann seinen öffentlichen Schlüssel per E-Mail.

--pgpk<E-Mail> Dem Absender wird der öffentliche Schlüssel zu der angegebenen E-Mail-Adresse zugesandt. Hierzu setzt der betreffende Benutzer den Steuerkode an den Beginn der Betreffzeile und sendet die Nachricht an sich selbst. MDPGP sendet dem Benutzer dann den öffentlichen Schlüssel zu der angegebenen Adresse per E-Mail.

Ein Beispiel hierzu:

```
Betreff: --pgpk<frank@example.com>
```

Schlüsselverwaltung

Die Optionen in der unteren Hälfte des Konfigurationsdialogs für MDPGP dienen der Verwaltung der öffentlichen und geheimen Schlüssel. Für jeden Schlüssel erscheint ein Eintrag. Durch Rechtsklick auf einen Eintrag öffnet sich ein Kontextmenü, aus dem Sie den Schlüssel exportieren, löschen, sperren und entsperren können. Wenn Sie den Schlüssel exportieren, wird er im Verzeichnis `\MDaemon\Pem\_mdpgp\exports\` gespeichert, und Sie können den öffentlichen Schlüssel wahlweise auch an eine E-Mail-Adresse senden lassen. Mithilfe der Optionen *Lokale/Externe Schlüssel anzeigen* und *Filtern* können Sie bestimmte Adressen und Gruppen leichter auffinden.

Details über Verschlüsselungsfehler an Absender senden (Befehl --pgpe)
Diese Option bewirkt, dass ein Absender über Fehler bei der Verschlüsselung informiert wird, falls er den Befehl --pgpe verwendet hat und danach die Verschlüsselung fehlschlägt (etwa, weil kein öffentlicher Schlüssel des Empfängers vorliegt). Diese Option ist per Voreinstellung abgeschaltet, sodass per Voreinstellung auch keine Benachrichtigungen versandt werden.

Öffentliche Schlüssel per E-Mail senden, wenn der Absender die Nachricht an sich selbst sendet (Befehl --pgpk)
Diese Option bewirkt, dass externe Benutzer die öffentlichen Schlüssel interner Benutzer per E-Mail anfordern können. Sie können E-Mail-Nachrichten an das Systemkonto des MDaemon-Servers (z.B. MDaemon@example.com) senden, die in der Betreffzeile den Befehl "--pgpk<E-Mail-Adresse> enthalten (z.B. `--pgpk<frank@example.com>`). Falls der öffentliche Schlüssel für die angegebene E-Mail-Adresse vorhanden ist, sendet MDaemon diesen Schlüssel an den Absender zurück. Diese Option ist per Voreinstellung abgeschaltet.

Öffentliche Schlüssel echtheitsbestätigter Benutzer automatisch importieren
Diese Option bewirkt, dass MDPGP in E-Mail-Nachrichten, die Benutzer in Verbindungen mit Echtheitsbestätigung übermittelt haben, nach öffentlichen Schlüsseln sucht und sie in den Schlüsselbund importiert. Die Schlüssel müssen als Dateianlagen im Format ASCII armor vorliegen. Hierdurch können die Benutzer die öffentlichen Schlüssel ihrer Kommunikationspartner einfach in den

Schlüsselbund importieren lassen, indem sie sich die öffentlichen Schlüssel selbst per E-Mail senden. Falls Sie den automatischen Import von Schlüsseln nicht wünschen, deaktivieren Sie diese Option. Diese Option ist per Voreinstellung aktiv.

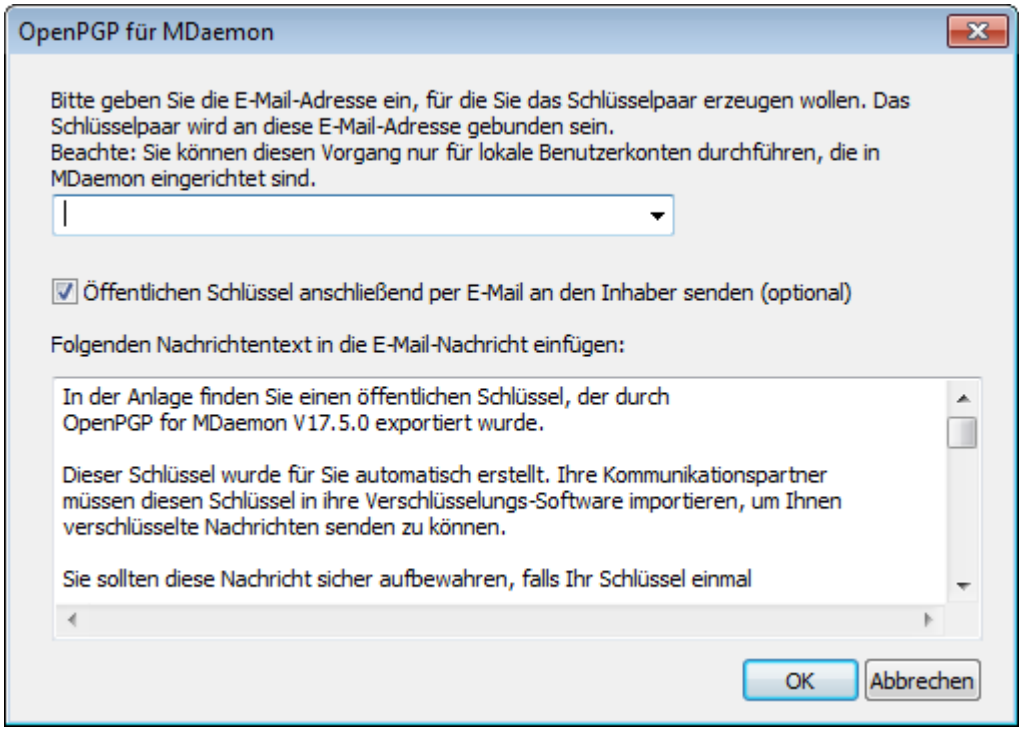
Schlüssel automatisch erzeugen
Diese Option bewirkt, dass MDPGP automatisch für jeden MDaemon-Benutzer ein Schlüsselpaar mit öffentlichem und geheimem Schlüssel erzeugt. MDPGP erzeugt die Schlüssel nicht alle gleichzeitig, vielmehr erstellt MDPGP immer erst dann ein Schlüsselpaar, wenn eine Nachricht für den Benutzer verarbeitet wird. Diese Option ist per Voreinstellung abgeschaltet, um die Systemressourcen zu schonen und das unnötige Erzeugen von Schlüsseln für solche Benutzer zu vermeiden, die MDPGP möglicherweise gar nicht nutzen.

Schlüssellänge
Diese Option bestimmt die Schlüssellänge der Schlüssel in Bit, die MDPGP erzeugt. Sie können als Schlüssellänge 1024, 2048 und 4096 wählen. Die Voreinstellung beträgt 2048 Bit.

Ablauf in [x] Tagen (0=nie)
Diese Option legt die Gültigkeitsdauer für die durch MDPGP erzeugten Schlüssel fest. Nach Ablauf dieser Gültigkeitsdauer werden die Schlüssel ungültig. Der Wert 0 bewirkt, dass die Schlüssel unbefristet gültig sind. Der Wert beträgt per Voreinstellung 0.

Schlüssel für bestimmten Benutzer erzeugen
Um ein Schlüsselpaar aus öffentlichem und geheimem Schlüssel für ein bestimmtes Benutzerkonto zu erstellen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf **Schlüssel für bestimmten Benutzer erzeugen**.
2. Wählen Sie aus dem Dropdown-Menü das gewünschte Benutzerkonto aus. Falls Sie einen Schlüssel erzeugen wollen, der für alle Benutzerkonten der Domäne verwendet wird, wählen Sie aus der Liste die Option "_Domain Key (domain.tld)_ <anybody@domain.tld>" aus.
3. **Falls gewünscht:** Aktivieren Sie das Kontrollkästchen *Öffentlichen Schlüssel anschließend per E-Mail an den Inhaber senden...*, falls Sie den Schlüssel dem betreffenden Benutzer als Dateianlage per E-Mail senden lassen wollen.
4. Klicken Sie auf **OK**.



Abgehende Nachrichten anhand IP der Gegenstelle verschlüsseln
Falls Sie einen bestimmten Schlüssel zur Verschlüsselung aller Nachrichten verwenden wollen, die an eine bestimmte IP-Adresse gerichtet sind, aktivieren Sie diese Option, und klicken Sie dann auf **Konfigurieren**, um die Konfigurationsdatei für die Transportverschlüsselung aufzurufen. In dieser Datei können Sie die IP-Adressen und die zugehörigen Schlüssel-IDs erfassen. Nachrichten, die über abgehende SMTP-Verbindungen an die hier erfassten Gegenstellen übermittelt werden, werden unmittelbar vor der Übermittlung mit dem der IP-Adresse zugeordneten Schlüssel verschlüsselt. Falls die Nachricht bereits mit einem anderen Schlüssel verschlüsselt wurde, wird dieser Schritt übersprungen.

Schlüssel importieren
Falls Sie eine Schlüsseldatei manuell in MDPGP importieren wollen, klicken Sie auf diese Schaltfläche, wählen Sie die Datei aus, und klicken Sie danach auf **Öffnen**. Beim Import eines geheimen Schlüssel müssen Sie den zugehörigen öffentlichen Schlüssel nicht gesondert importieren, da er bereits im geheimen Schlüssel enthalten ist. Ist der geheime Schlüssel durch eine Passphrase geschützt, so fragt MDPGP die Passphrase während des Imports ab. Ohne die Passphrase kann der geheime Schlüssel nicht importiert werden. Nach dem Import des geheimen Schlüssels ändert MDPGP die Passphrase des geheimen Schlüssels in die Passphrase, die MDPGP gerade verwendet.

Domänen-Schlüssel importieren
Falls Ihnen ein Schlüssel für die Verschlüsselung aller an eine bestimmte Domäne gerichteten E-Mail-Nachrichten zur Verfügung gestellt wurde, können Sie diesen Schlüssel mithilfe dieses Steuerelements importieren. Klicken Sie dazu auf das Steuerelement, geben Sie den Domänennamen ein, klicken Sie auf **OK**, suchen Sie die Datei `public.asc` mit dem Domänen-Schlüssel auf, und klicken Sie auf **Öffnen**. Hierdurch wird der Domänen-Schlüssel in die Liste aufgenommen, und es wird eine Regel des Inhaltsfilters erstellt, die die Verschlüsselung aller

abgehenden Nachrichten für diese Domäne unabhängig von dem Absender durchführt.

Passphrase ändern
Geheime Schlüssel sind immer durch eine Passphrase geschützt. Um einen geheimen Schlüssel zu importieren, müssen Sie seine Passphrase angeben. Nach dem Export eines geheimen Schlüssels bleibt der Schlüssel durch die Passphrase geschützt und kann an anderer Stelle nur importiert werden, wenn die Passphrase bekannt ist. Die Standard-Passphrase, die MDPGP nutzt, lautet **MDaemon**. Aus Sicherheitsgründen sollten Sie diese Passphrase ändern, sobald Sie MDPGP eingerichtet haben. Jeder geheime Schlüssel, den MDPGP erzeugt oder importiert, wird mit dieser Passphrase gesichert; bestehende Passphprases werden beim Import entsprechend geändert. Sie können die Passphrase jederzeit durch Anklicken von **Passphrase ändern** im Konfigurationsdialog für MDPGP ändern. Nach einer Änderung wird jeder geheime Schlüssel im Schlüsselbund aktualisiert, und seine Passphrase wird auf die neue Passphrase geändert.

Datendateien sichern
Durch Anklicken dieser Schaltfläche erstellen Sie Sicherheitskopien der Datendateien, die die Schlüsselbunde enthalten, nämlich `Keyring.private` und `Keyring.public`. Per Voreinstellung werden die Sicherheitskopien in "`\MDaemon\Pem\_mdpgp\backups`" abgelegt; ihren Dateinamen werden Datum und Dateiendung `.bak` hinzugefügt.

- Weitergeleitete Nachrichten werden nicht verschlüsselt.
- Nachrichten von Autobeantwortern werden nicht verschlüsselt.
- Schlüsselserver, Verzeichnisdienste und der Widerruf von Schlüsseln werden nur im Rahmen der Optionen "*Öffentliche Schlüssel aus DNS (pka1) abrufen und zwischenspeichern für [xx] Stunden*" und "*Öffentliche Schlüssel über HTTP senden (WorldClient)*" unterstützt..
- Die Aktion Verschlüsseln des Inhaltsfilters wirkt nicht auf Nachrichten, die bereits verschlüsselt sind. Die Aktionen Verschlüsseln und Entschlüsseln werden nur bei entsprechender Berechtigung und MDPGP-Konfiguration wirksam.
- Die Dropdown-Liste, in der die MDaemon-Benutzerkonten angezeigt werden, zeigt per Voreinstellung die ersten 500 Benutzerkonten. Um alle Benutzerkonten anzeigen zu lassen, können Sie in der Datei `plugins.dat` den Eintrag `MaxUsersShown=0` setzen. Hierdurch kann sich bei sehr umfangreichen Benutzerlisten die Ladezeit erhöhen.
- `MDPGPUtil.exe` steht als Befehlszeilenwerkzeug zur Verfügung und kann mithilfe von Befehlszeilenparametern entschlüsseln und verschlüsseln. Um Hilfe zu diesem Programm zu erhalten, führen Sie MDPGPUtil von der Befehlszeile aus ohne Parameter aus.

4.4 Outbreak Protection

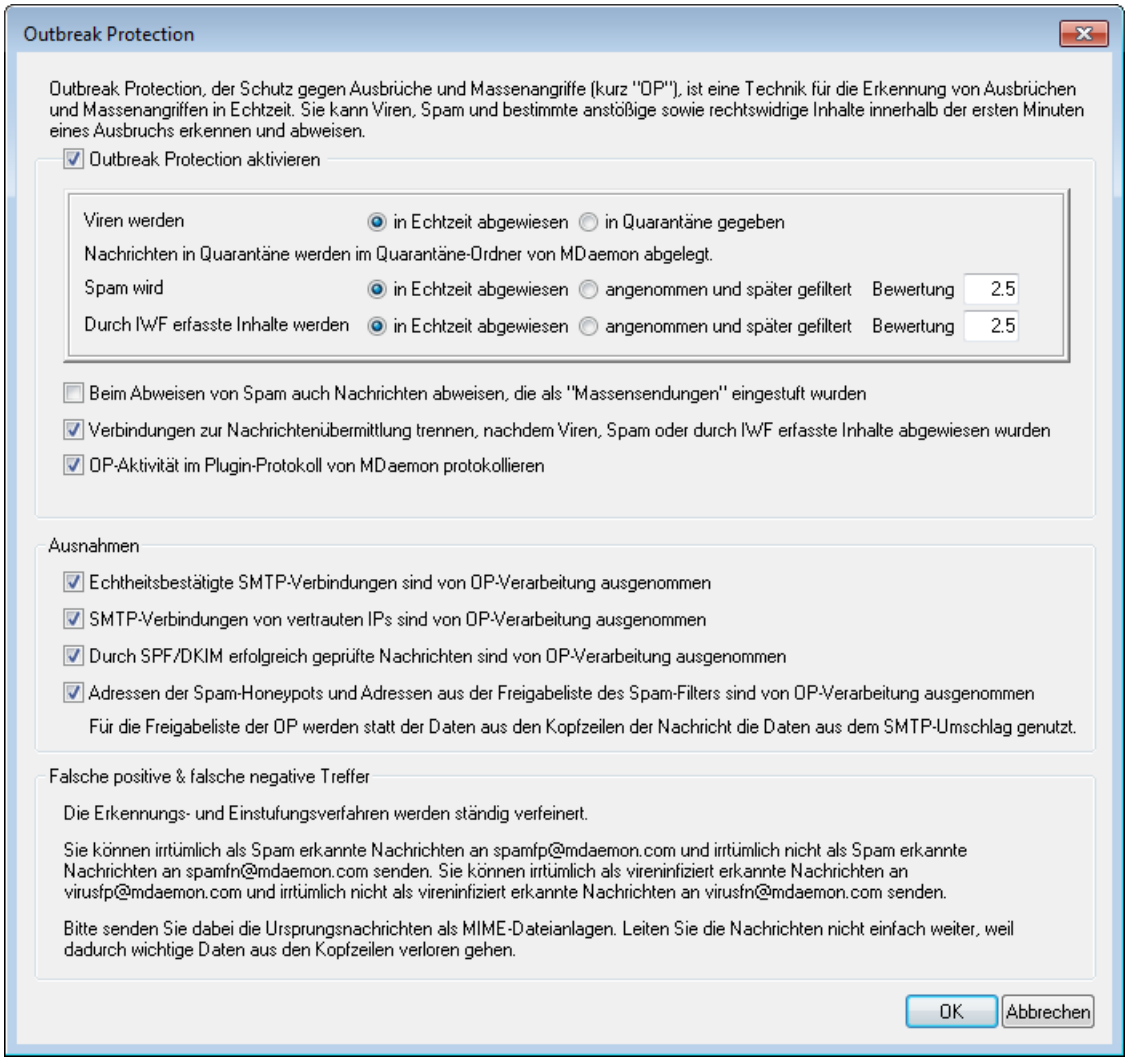
Die Outbreak Protection (OP), der Schutz gegen Massenangriffe, ist Teil des optional erhältlichen Leistungsmerkmals MDaemon AntiVirus 671. Wenn Sie MDaemon AntiVirus erstmals aktivieren, beginnt hierdurch ein 30 Tage dauernder Testzeitraum. Lizenzen für dieses Leistungsmerkmal können Sie über Ihren autorisierten Reseller für MDaemon oder auf der Website www.mdaemon.com kaufen.

Sie erreichen den Konfigurationsdialog für die Outbreak Protection (OP) über das Menü Sicherheit auf der Benutzeroberfläche von MDaemon (Sicherheit » Outbreak Protection... oder Strg+Umschalt+1). Die OP ist ein revolutionäres, in Echtzeit arbeitendes System zum Schutz gegen Spam, Viren und Phishing. Seine Technologie kann die durch MDaemon getragene E-Mail-Infrastruktur vorausschauend, automatisch und binnen weniger Minuten nach Beginn eines Massenangriffs schützen.

Die Outbreak Protection arbeitet vollständig unabhängig von den Inhalten; sie stützt sich insbesondere nicht auf eine nur lexikalische Analyse von Nachrichten-Inhalten. Aus diesem Grund benötigt sie keine heuristischen Regeln, keinen Inhaltsfilter und keine Aktualisierung von Signaturen. Sie ist kann daher auch nicht durch zusätzlich eingestreuten gezielt ablenkenden Text, bewusste Abweichungen von der Normschreibweise, Strategien des Social Engineerings, Sprachbarrieren und Unterschieden in der verwendeten Kodierung umgangen werden. Die OP stützt sich auf die durch Cyren entwickelten Techniken zur Erkennung wiederkehrender Verhaltensmuster ("Recurrent Pattern Detection") und zum Schutz in Echtzeit ("Zero-Hour"). Die OP wertet Nachrichtenstrukturen und die Charakteristik der Nachrichtenübermittlung über SMTP mathematisch aus und analysiert dabei Muster der Übermittlung von E-Mail-Nachrichten. Die so gewonnenen Datenmuster werden mit ähnlichen Mustern verglichen, die aus Millionen von E-Mail-Nachrichten weltweit gewonnen, analysiert und in Echtzeit verglichen werden. **Beachte:** Die OP übermittelt nie die eigentlichen Inhalte der Nachrichten, und die Inhalte der Nachrichten lassen sich auch nicht aus den gewonnenen Datenmustern herleiten.

Da die Nachrichten weltweit in Echtzeit analysiert werden, kann der Schutz binnen Minuten, oft binnen Sekunden, nach Beginn eines neuen Massenangriffs oder Ausbruchs bereit gestellt werden. Bei Viren ist dieses Schutzniveau besonders wichtig, da die Hersteller herkömmlicher AntiVirus-Lösungen oft erst Stunden nach Beginn eines Massenangriffs aktualisierte Virensignaturen prüfen und bereit stellen können, und da es noch länger dauern kann, bis solche Aktualisierungen dann im Wirkbetrieb eingesetzt werden. Während dieser Zeiträume sind Server ohne Outbreak Protection für den jeweiligen Massenangriff verwundbar. Bei Spam-Nachrichten stellt sich die Situation vergleichbar dar; es kostet oft Zeit und Aufwand, Spam zu analysieren und hieraus funktionssichere Filterregeln zu erstellen, damit die Spam-Nachrichten von herkömmlichen heuristischen und inhaltsgestützten Systemen erkannt werden können.

Es ist jedoch wichtig, zu bedenken, dass das Leistungsmerkmal Outbreak Protection keinen Ersatz für herkömmliche Techniken zur Abwehr von Viren, Spam und Phishing darstellt. Vielmehr bietet die OP eine zusätzliche besondere Schutzschicht, die die bestehenden heuristischen, Signatur- und Inhalts-gestützten Techniken in MDaemon ergänzt. Insbesondere ist die OP darauf ausgerichtet, umfangreiche Massenangriffe und Ausbrüche zu behandeln, wohingegen bereits länger bekannte, nur im Einzelfall auftretende oder besonders zielgerichtete Nachrichten durch die herkömmlichen Leistungsmerkmale besser erkannt werden können.



Outbreak Protection

Outbreak Protection aktivieren

Diese Option aktiviert Outbreak Protection auf dem Server. Eingehende Nachrichten werden dann analysiert, um festzustellen, ob sie Teil eines laufenden Massenangriffs mit oder Ausbruchs von Viren, Spam oder Phishing sind. Die folgenden Optionen in diesem Konfigurationsmenü legen fest, wie mit Nachrichten zu verfahren ist, wenn sie als Teil eines Massenangriffs erkannt werden. Auch die Absender, deren Nachrichten von der Prüfung auf Massenangriffe ausgenommen sein sollen, werden hier festgelegt.

Viren werden...

in Echtzeit abgewiesen

Falls gewünscht ist, dass Nachrichten bereits während der SMTP-Übertragung abgewiesen werden, wenn festgestellt wird, dass sie Teil eines Virenangriffs sind, so muss diese Option aktiv sein. Die Nachrichten werden dann weder in Quarantäne gegeben noch an ihre Empfänger zugestellt; sie werden direkt vom Server abgewiesen.

in Quarantäne gegeben

Diese Einstellung bewirkt, dass Nachrichten auch dann entgegen genommen werden, wenn sie als Teil eines Massenangriffs erkannt werden. Die

Nachrichten werden dann zwar nicht abgewiesen, aber auch nicht an die Empfänger zugestellt. Statt dessen werden sie in Quarantäne gegeben und im Quarantäne-Ordner abgelegt.

Spam wird...

in Echtzeit abgewiesen
Sollen Nachrichten durch den Server bereits während der Zustellung abgewiesen werden, wenn der Schutz gegen Massenangriffe bestätigt hat, dass sie Teil eines Massenangriffs mit Spam sind, so muss diese Option aktiv sein. Die Nachrichten werden dann nicht als Spam gekennzeichnet und zugestellt, sie werden direkt während der SMTP-Übermittlung durch den Server abgewiesen. Nachrichten, die der Schutz gegen Massenangriffe als "Massensendung" ("bulk") einstuft, werden durch diese Funktion nur dann abgewiesen, wenn die Option Beim Abweisen von Spam auch Nachrichten abweisen, die als "Massensendungen" eingestuft werden aktiv ist. Nachrichten, die der Schutz gegen Massenangriffe als "Massensendungen" einstuft, können einfach Teil bestimmter sehr umfangreicher Mailinglisten oder sonstiger weit verbreiteter Inhalte sein, sodass der Empfänger solche Nachrichten nicht als Spam ansehen muss. Aus diesem Grund sollten Massensendungen normalerweise durch den Schutz gegen Massenangriffe nicht abgewiesen oder mit einer ungünstigeren Spam-Bewertung versehen werden.

angenommen und später gefiltert
Diese Option bewirkt, dass Nachrichten angenommen werden, auch wenn der Schutz gegen Massenangriffe bestätigt, dass die Nachrichten Teil eines Massenangriffs mit Spam sind. Die Nachrichten können dann durch Spam- und Inhaltsfilter verarbeitet werden. Die Nachrichten werden durch den Schutz gegen Massenangriffe nicht abgewiesen; ihre Spam-Bewertung wird in Übereinstimmung mit den Einstellungen zur Spam-Bewertung weiter unten angepasst.

Die Einstellung *angenommen und später gefiltert* bewirkt zwar, dass der Schutz gegen Massenangriffe die Nachrichten nicht selbst direkt abweist, verhindert aber nicht, dass MDaemon Nachrichten seinerseits während der SMTP-Übertragung abweist, falls der Spam-Filter entsprechend konfiguriert ist und die Spam-Bewertung den im Konfigurationsdialog Spam-Filter 679 eingestellten Schwellwert überschreitet.

Bewirkt die Bewertungs-Einstellung weiter unten beispielsweise, dass die Spam-Bewertung einer Nachricht 15,0 beträgt, und ist der Spam-Filter so konfiguriert, dass er Nachrichten mit einer Bewertung ab 15,0 bereits während der SMTP-Übertragung abweist, dann wird die Nachricht bereits während der Übermittlung abgewiesen, nicht aber angenommen und später gefiltert.

Bewertung
Bei Nutzung der Option *angenommen und später gefiltert* wird der hier eingetragene Wert der Spam-Bewertung einer Nachricht hinzugerechnet, falls der Schutz gegen Massenangriffe bestätigt, dass die Nachricht Teil eines Massenangriffs mit Spam ist.

Durch IWF erfasste Inhalte

Die folgenden Optionen beziehen sich auf Inhalte, die durch die Internet Watch Foundation (IWF) als Verweise auf Sites erkannt werden, die den Missbrauch von Kindern bildlich darstellen (etwa Sites mit Kinderpornographie). Sie ermöglichen es dem Schutz gegen Massenangriffe, eine URL-Liste zu nutzen, die die IWF bereitstellt, und damit Nachrichten zu erkennen und zu kennzeichnen, die auf die fraglichen Inhalte verweisen. Die IWF betreibt eine unabhängige Anlaufstelle, bei der möglicherweise rechtswidrige Online-Inhalte, insbesondere Kinderpornographie, weltweit gemeldet werden können. Die IWF arbeitet mit der Polizei, verschiedenen Behörden, der Online-Industrie im weiteren Sinne und der Öffentlichkeit zusammen, um die Verfügbarkeit rechtswidriger Online-Inhalte zu bekämpfen. Die URL-Liste der IWF wird täglich aktualisiert und um neue Sites erweitert, die Bilder von Kindesmissbrauch anbieten.

Viele Unternehmen und sonstige Organisationen haben interne Richtlinien, die bestimmen, welche Arten von Inhalten ihre Angestellten und Mitarbeiter per E-Mail senden und empfangen dürfen. Insbesondere pornographische und rechtswidrige Inhalte sind dabei oft verboten. In vielen Ländern sind darüber hinaus Versand und Empfang solcher Inhalte gesetzlich unzulässig. Die folgenden Funktionen können dabei helfen, die Einhaltung solcher Regelungen und Gesetze sicherzustellen.

Nähere Informationen über die IWF sind verfügbar unter:

http://www.iwf.org.uk/

Durch IWF erfasste Inhalte werden...

in Echtzeit abgewiesen
Diese Option bewirkt, dass eingehende Nachrichten bereits während der SMTP-Übermittlung abgewiesen werden, falls sie Inhalte enthalten, die durch die IWF erfasst sind.

angenommen und später gefiltert
Diese Option bewirkt, dass die Spam-Bewertung von Nachrichten verschlechtert wird, falls sie Inhalte enthalten, die durch die IWF erfasst sind. Die Nachrichten werden dann nicht abgewiesen. Die Bewertung wird um den im Feld *Bewertung* festgelegten Wert erhöht.

Bewertung
Ist die Option *angenommen und später gefiltert* weiter oben aktiv, so wird der Spam-Filter-Bewertung der Nachrichten der hier festgelegte Wert hinzugerechnet, falls sie Inhalte enthalten, die durch die IWF erfasst sind.

Beim Abweisen von Spam auch Nachrichten abweisen, die als "Massensendungen" eingestuft werden
Der Schutz gegen Massenangriffe spricht gelegentlich auf Nachrichten an, die als Spam angesehen werden können, obwohl sie nicht durch einen bekannten Spam-Versender oder ein Bot-Netz versandt wurden. Dies kann insbesondere auf legitime Newsletter und Mailinglisten zutreffen. Der Schutz gegen Massenangriffe stuft solche Nachrichten nicht als "Spam (bestätigt)" ("Spam [confirmed]") sondern als "Spam (Massenversand)" ("Spam [bulk]") ein. Um die Abwehrfunktionen des Schutzes gegen Massenangriffe auch auf den Massenversand anzuwenden, muss diese Option aktiv sein. Ist die Option nicht aktiv, so beziehen sich die Abwehrmaßnahmen nur auf bestätigten Spam. Soll auf einem System Massen-E-Mail empfangen werden, und können die Quellen oder

die Empfänger nicht in die Freigabelisten eingetragen werden, so kann es erforderlich sein, diese Option zu deaktivieren und Nachrichten zunächst anzunehmen, wenn ihre Quelle nicht einwandfrei als Spam-Versender identifiziert wurde.

Verbindungen zur Nachrichtenübermittlung trennen, nachdem Viren, Spam oder durch IWF erfasste Inhalte abgewiesen wurden
Diese Option bewirkt, dass eine Verbindung zur Nachrichtenübermittlung getrennt wird, nachdem eine Nachricht abgewiesen wurde, weil sie Viren enthielt, als Spam eingestuft wurde, oder durch die IWF erfasste Inhalte enthielt.

OP-Aktivität im Plugin-Protokoll von MDaemon protokollieren
Soll die Aktivität des Schutzes gegen Massenangriffe im Plugin-Protokoll erfasst werden, so muss diese Option aktiv sein.

Ausnahmen

Echtheitsbestätigte SMTP-Verbindungen sind von OP-Verarbeitung ausgenommen
Ist diese Option aktiv, so sind SMTP-Verbindungen mit Echtheitsbestätigung von der Bearbeitung durch den Schutz gegen Massenangriffe ausgenommen. Der Schutz wird für Nachrichten aus echtheitsbestätigten Verbindungen nicht wirksam.

SMTP-Verbindungen von vertrauten IPs sind von OP-Verarbeitung ausgenommen
Ist diese Option aktiv, so sind Verbindungen, die von vertrauten IP-Adressen ausgehen, von der Bearbeitung durch den Schutz gegen Massenangriffe ausgenommen. Der Schutz wird für Nachrichten, die von vertrauten IP-Adressen aus übermittelt werden, nicht wirksam.

Durch SPF/DKIM erfolgreich geprüfte Nachrichten sind von OP-Verarbeitung ausgenommen
Diese Option bewirkt, dass Nachrichten von der Verarbeitung durch den Schutz gegen Massenangriffe ausgenommen sind, falls sie durch SPF oder DKIM erfolgreich geprüft wurden und die Absenderdomäne in der Liste zugelassener Domänen 559 erfasst ist.

Adressen der Spam-Honeypots und Adressen aus der Freigabeliste des Spam-Filters sind von OP-Verarbeitung ausgenommen
Diese Option bewirkt, dass die Spam-Honeypots 709 und die Freigabelisten des Spam-Filters von der Verarbeitung durch Outbreak Protection ausgenommen sind. "Freigabelisten" bezieht sich dabei auf die Empfänger oder den Parameter des Befehls RCPT, der während der SMTP-Verbindung übermittelt wird. Die Freigabelisten für Absender beziehen sich dabei auf den Absender oder den Parameter des Befehls MAIL, der während der SMTP-Verbindung übermittelt wird. Diese Vorgänge werden nicht durch Inhalte aus den Kopfzeilen der Nachrichten gesteuert.

Falsche positive und falsche negative Treffer

Falsche positive Treffer, die dazu führen, dass normale Nachrichten irrtümlich als Teil eines Massenangriffs erkannt werden, sollten, wenn überhaupt, nur sehr selten auftreten. Sollte es doch zu einem falschen positiven Treffer kommen, so kann der Systemverwalter die fälschlich erkannte Nachricht im Falle falscher positiver Treffer bei Spam und Phishing an **spamfp@mdaemon.com** und bei Viren an **virusfp@mdaemon.com** übermitteln, sodass Alt-N die Erkennungs- und Einstufungsverfahren verfeinern kann.

Falsche negative Treffer, die dazu führen, dass Nachrichten irrtümlich nicht als Teil eines Massenangriffs erkannt werden, werden häufiger auftreten als falsche positive Treffer. Dabei ist aber zu beachten, dass der Schutz gegen Massenangriffe nicht darauf ausgelegt ist, alle Spam-Nachrichten, Virenangriffe und ähnliche Nachrichten abzufangen; er bietet lediglich eine weitere Schutzschicht, die sich speziell gegen Massenangriffe richtet. Alte Nachrichten, besonders auf die Empfänger abgestimmte Nachrichten und ähnliches erkennt der Schutz gegen Massenangriffe unter Umständen nicht. Solche Nachrichten sollten aber durch die anderen Funktionen von AntiVirus und MDaemon, die in der Verarbeitungskette später wirksam werden, erkannt werden. Sollte ein falscher negativer Treffer auftreten, kann der Systemverwalter jedoch auch solche Nachrichten im Falle falscher negativer Spam- und Phishing-Nachrichten an **spamfn@mdaemon.com** und bei Viren an **virusfn@mdaemon.com** senden, damit auch hier die Erkennungs- und Einstufungsverfahren verbessert werden können.

Werden falsch eingestufte Nachrichten an Alt-N übermittelt, so sollen sie als MIME-Dateianlage versandt und nicht einfach weitergeleitet werden, sonst gehen Kopfzeilen und andere für die Einstufung entscheidende Daten verloren.

4.5 Inhaltsfilter und AntiVirus

Der Inhaltsfilter

Der Inhaltsfilter Inhaltsfilter[649] (Sicherheit » Inhaltsfilter) kann sehr vielseitig eingesetzt werden: er kann Spam filtern, vireninfizierte Nachrichten abfangen, bevor sie an ihrem eigentlichen Ziel ankommen, bestimmte Nachrichten an einen oder mehrere Benutzer zusätzlich senden, den Nachrichten Hinweistexte anfügen, Kopfzeilen hinzufügen und löschen, Datei-Anlagen entfernen, Nachrichten löschen und vieles mehr. Regeln für den Inhaltsfilter werden vom Administrator festgelegt und können wegen ihrer Vielseitigkeit in vielen Situationen benützt werden. Die Einsatzmöglichkeiten werden dabei fast nur von dem Einfallsreichtum des Systemverwalters begrenzt. Es sollte durchaus experimentiert werden, um die ganze Palette der Anwendungen zu erforschen.

MDaemon AntiVirus (MDAV)

Bei Nutzung des Leistungsmerkmals MDaemon AntiVirus, das gesondert zu lizensieren ist, erscheinen zwei zusätzliche Abschnitte im Konfigurationsdialog des Inhaltsfilters: Virenprüfung[671] und AV-Aktualisierung[675]. In diesen Abschnitten können Sie die Leistungsmerkmale von AntiVirus direkt konfigurieren und bestimmen, welche Aktionen MDaemon ausführt, wenn Viren erkannt werden. MDAV verfügt über zwei Module für die Virenprüfung: Cyren Anti-Virus und ClamAV. Sie können Nachrichten wahlweise nur durch eine oder durch beide Module prüfen lassen, um die Sicherheit zu erhöhen. MDAV enthält auch den Schutz gegen Ausbrüche und Massenangriffe, die Outbreak Protection[643]. Dieses Leistungsmerkmal hängt nicht von Heuristik oder Signaturen ab und unterscheidet sich hierdurch von herkömmlichen Schutzmechanismen. Es ist stattdessen darauf ausgelegt, Spam, Phishing und Virenangriffe, die Teil eines Massenangriffs sind, zu erkennen; solche Angriffe werden bisweilen durch herkömmliche Schutzmechanismen nicht erkannt.

Wenn Sie MDaemon AntiVirus zum ersten Mal aktivieren[671], beginnt damit zugleich ein 30 Tage dauernder Testzeitraum. Falls Sie eine Lizenz für dieses Leistungsmerkmal erwerben wollen, setzen Sie sich mit Ihrem autorisierten Reseller für

MDaemon in Verbindung, oder suchen Sie www.mdaemon.com auf.

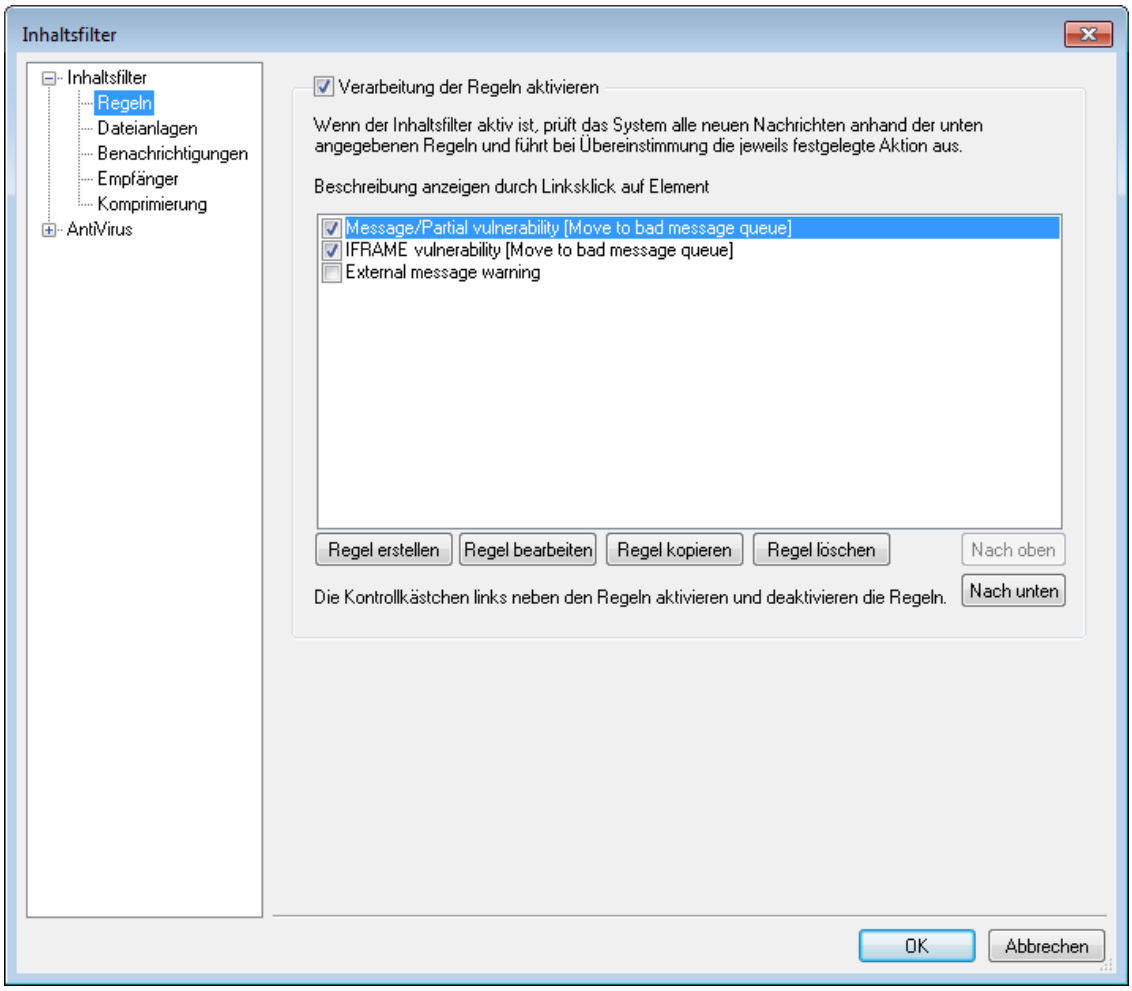
Siehe auch:

Der Editor für den Inhaltsfilter 649
Erstellen einer neuen Regel für den Inhaltsfilter 651
Bearbeiten einer bestehenden Regel für den Inhaltsfilter 657
Nutzung Regulärer Ausdrücke in den Regeln des Inhaltsfilters 657

Virenprüfung 671
AntiVirus-Aktualisierung 675
Outbreak Protection 643

4.5.1 Der Editor für den Inhaltsfilter

4.5.1.1 Regeln



Alle Nachrichten, die MDaemon verarbeitet, durchlaufen zu irgendeiner Zeit eine Nachrichten-Warteschlange. Ist der Inhaltsfilter aktiv, so verarbeitet er jede Nachricht, bevor sie die jeweilige Warteschlange verlässt. Am Ende der Verarbeitung steht dann fest, wie mit der Nachricht weiter verfahren wird.

Der Inhaltsfilter ignoriert alle Nachrichten, deren Dateiname mit dem Buchstaben "P" beginnt. Alle anderen Nachrichten werden hingegen verarbeitet. Nach der Verarbeitung ändert MDaemon den ersten Buchstaben des Dateinamens nach "P", sodass der Inhaltsfilter jede Nachricht nur einmal verarbeitet.

Regeln für den Inhaltsfilter

Verarbeitung der Regeln aktivieren
Die Auswahl dieser Option aktiviert den Inhaltsfilter. Alle durch MDaemon verarbeiteten Nachrichten passieren vor der Zustellung den Inhaltsfilter.

Bestehende Regeln des Inhaltsfilters

In diesem Abschnitt erscheinen alle bestehenden Regeln für den Inhaltsfilter; neben jeder Regel erscheint ein Kontrollkästchen, mit dessen Hilfe sie aktiviert und deaktiviert werden kann. Um für eine bestimmte Regel die Beschreibung im intern verwendeten Skript-Format anzuzeigen, müssen die Regel angeklickt werden und der Mauszeiger über ihr stehen bleiben. Durchläuft eine Nachricht den Inhaltsfilter, so werden die Regeln in der Reihenfolge angewendet, in der sie hier erscheinen. So können die Regeln leicht und flexibel neu angeordnet werden.

Ein Beispiel hierzu: Besteht eine Regel, die alle Nachrichten mit dem Text "Das ist Spam!" löscht und eine ähnliche Regel, die solche Nachrichten an den Postmaster weiter leitet, so können beide Regeln auf ein- und dieselbe Nachricht angewandt werden, wenn sie nur in der richtigen Reihenfolge stehen. Dabei darf natürlich keine Regel "Keine weiteren Regeln abarbeiten" weiter oben in der Regelliste stehen. Eine solche Regel müsste an das Ende der Liste verschoben werden; dann können alle Nachrichten, die den Text "Das ist Spam!" enthalten, erst an den Postmaster

In MDaemon lassen sich Regeln definieren, die mehrere Vorgänge auf einmal ausführen sowie und/oder-("`and/or`")-Operatoren verwenden. Für das oben angeführte Beispiel lässt sich daher statt mehreren einzelnen auch eine einzige kombinierte Regel anlegen, die alle gewünschten Aufgaben - und mehr - ausführen kann.

Regel erstellen
Mit diesem Knopf wird der Editor für die Erstellung einer neuen Regel[651] aufgerufen.

Regel bearbeiten
Diese Option öffnet einen Editor, in dem die jeweils ausgewählte Regel bearbeitet[657] wird.

Regel kopieren
Durch einem Klick auf dieses Steuerelement wird die gewählte Regel kopiert, sodass der Liste eine zweite identische Regel hinzugefügt wird. Diese neue Regel erhält einen Standardnamen nach dem Schema "Copy of ("Kopie von") [ursprüngliche Regel]". Dies ist sinnvoll, wenn mehrere ähnliche Regeln erstellt

werden sollen. Man legt nur eine "Grundregel" an, kopiert sie mehrfach und ändert dann die Kopien, wo nötig.

Regel löschen
Hiermit wird die jeweils gewählte Regel aus dem Inhaltsfilter gelöscht. Vorher wird aber noch eine Bestätigung für den Löschvorgang abgefragt.

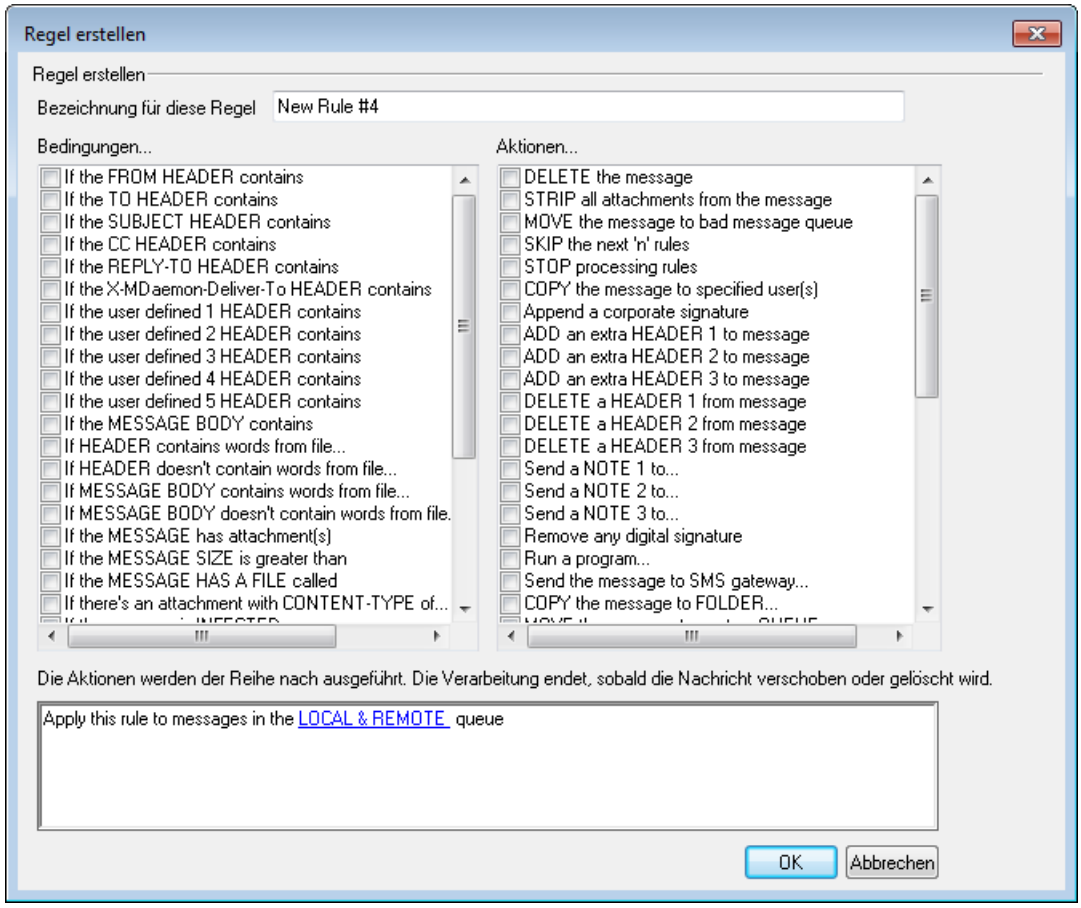
Nach oben
Hiermit wird die gewählte Regel weiter nach oben verschoben.

Nach unten
Hiermit wird die gewählte Regel weiter nach unten verschoben.

Siehe auch:

Erstellen einer neuen Regel für den Inhaltsfilter 651
Bearbeiten einer bestehenden Regel für den Inhaltsfilter 657
Nutzung Regulärer Ausdrücke in den Filterregeln 657

4.5.1.1.1 Erstellen einer neuen Regel für den Inhaltsfilter



In diesem Dialogfenster werden neue Regeln für den Inhaltsfilter angelegt. Es wird durch einen Klick auf das Steuerelement *Regel erstellen* im Konfigurationsdialog des Inhaltsfilters im vorherigen Fenster geöffnet.

Regel erstellen

Bezeichnung für diese Regel
Hier sollte ein Name eingetragen werden, der die neue Regel möglichst gut beschreibt. Vorgabe ist ein Name nach dem Schema "Neue Regel #n".

Bedingungen...

In diesem Textfeld erscheinen die Bedingungen, die der neuen Regel hinzugefügt werden können. Jede gewünschte Bedingung wird durch einen Klick in das entsprechende Auswahlfeld markiert und erscheint dann in dem Abschnitt Beschreibung der Regel weiter unten. Die meisten Bedingungen benötigen noch zusätzliche Daten, die nach einem Klick auf den Hyperlink der betreffenden Bedingung eingegeben werden können.

If the [HEADER] contains ("Falls die [Kopfzeile] ... enthält")—Mit diesen Optionen kann die Bedingung auf den verschiedenen Kopfzeilen aufgebaut werden. Der zu suchende Text muss noch angegeben werden. Diese Bedingung unterstützt jetzt Reguläre Ausdrücke. Siehe Nutzung regulärer Ausdrücke in den Bedingungen des Inhaltsfilters 657.

If the user defined [# HEADER] contains ("Falls die benutzerdefinierte [Kopfzeile] ... enthält")—Hiermit lässt sich die Regel auf benutzerdefinierte Kopfzeilen aufbauen. Der Name der Kopfzeile und der darin zu suchende Text müssen noch angegeben werden. Diese Bedingung unterstützt jetzt Reguläre Ausdrücke. Siehe Nutzung regulärer Ausdrücke in den Bedingungen des Inhaltsfilters 657.

If the MESSAGE BODY contains ("Falls der Nachrichtentext ... enthält")—Diese Option legt den Nachrichtentext als Bedingung fest. Auch hier muss der zu suchende Text noch angegeben werden. Diese Bedingung unterstützt jetzt Reguläre Ausdrücke. Siehe Nutzung regulärer Ausdrücke in den Bedingungen des Inhaltsfilters 657.

If the MESSAGE has Attachment(s) ("Falls die Nachricht Datei-Anlagen hat")—Ist diese Option gewählt, so prüft die Regel, ob die Nachricht Datei-Anlagen hat oder nicht. Weitere Informationen werden nicht benötigt.

If the MESSAGE SIZE is greater than ("Falls die Nachricht größer ist als")—Hiermit wird die Regel von der Nachrichtengröße abhängig gemacht. Die Größe muss in kB angegeben werden; die Voreinstellung ist 10 kB.

If the MESSAGE HAS A FILE called ("Falls die Nachricht eine Datei-Anlage mit Namen ... hat")—Diese Option sucht nach einer Datei-Anlage mit einem bestimmten Dateinamen, der noch angegeben werden muss. Jokerzeichen wie *.exe und *.* sind zulässig.

If message is INFECTED... ("Falls die Nachricht infiziert ist")—Diese Bedingung wird erfüllt, wenn MDaemon feststellt, dass eine Nachricht mit einem Virus infiziert ist.

If the EXIT CODE from a previous run process is equal to("Falls die Schlussmeldung eines vorher ausgeführten Prozesses gleich ... ist")—Verwendet eine vorher abgearbeitete Regel

die Aktion "Programm ausführen", so kann diese Bedingung feststellen, ob der Prozess eine bestimmte Schlussmeldung gegeben hat.

If the MESSAGE IS DIGITALLY SIGNED ("Falls die Nachricht digital signiert ist")—Diese Regel erfasst alle digital signierten Nachrichten. Weitere Informationen sind nicht nötig.

If SENDER is a member of GROUP... ("Ist der ABSENDER Mitglied der GRUPPE")—Diese Bedingung trifft auf Nachrichten zu, die von einem Benutzerkonto ausgehen, das Mitglied der in der Regel bezeichneten Gruppe ist.

If RECIPIENT is a member of GROUP... ("Ist der EMPFÄNGER Mitglied der GRUPPE")— Diese Bedingung trifft auf Nachrichten zu, die an ein Benutzerkonto gerichtet sind, das Mitglied der in der Regel bezeichneten Gruppe ist.

If ALL MESSAGES ("Für alle Nachrichten")—Mit dieser Option betrifft die Regel alle Nachrichten. Weitere Informationen sind nicht nötig. Es werden alle Nachrichten erfasst, es sei denn, sie werden vorher von einer Regel "Weiterbearbeitung abbrechen" oder von der Aktion "Nachricht löschen") erfasst.

Aktionen...

MDaemon kann die hier aufgeführten Aktionen durchführen, falls eine Nachricht den Bedingungen für eine Regel entspricht. Manche Aktionen erfordern zusätzliche Informationen, die nach einem Klick auf den Hyperlink der betreffenden Aktion angegeben werden können.

Delete Message ("Nachricht löschen")—Mit dieser Aktion wird die Nachricht gelöscht.

Strip All Attachments From Message ("Datei-Anlagen aus der Nachricht entfernen")—Diese Option entfernt sämtliche Datei-Anlagen von der Nachricht.

Move Message To Bad Message Queue ("Nachricht in Defekt-Warteschlange verschieben")—Hiermit wird die Nachricht in die Warteschlange für defekte Nachrichten kopiert oder verschoben.

Skip n Rules ("n Regeln überspringen")—Mit dieser Aktion wird die definierte Anzahl von Regeln übersprungen. Das ist nützlich, wenn eine Regel nur unter bestimmten Umständen Anwendung finden soll.

Ein Beispiel hierzu: Nachrichten mit dem Wort "Spam" sollen gelöscht werden, solche mit den Wörtern "Guter Spam" hingegen nicht. Um dies zu ermöglichen, legt man eine Regel an, die Nachrichten mit dem Wort "Spam" löscht, und eine weitere, in der Reihenfolge davor, die festlegt "wenn die Nachricht "Guter Spam" enthält, dann 1 Regel überspringen".

Stop Processing Rules ("Keine weiteren Regeln abarbeiten")—Diese Aktion bricht die Abarbeitung weiterer Regeln sofort ab.

Copy Message To Specified User(s) ("Nachricht auch an die angegebenen Benutzer leiten")—Damit wird eine Kopie der Nachricht an

zusätzliche Empfänger geleitet. Die Adressen der Empfänger müssen noch angegeben werden.

Append a corporate signature ("Unternehmens-Signatur anfügen")—Hiermit können der Nachricht ein kleiner Textbaustein oder der Inhalt einer Datei als Fußtext hinzugefügt werden. Es steht eine Option für die Nutzung von HTML zur Verfügung; hiermit können Sie in Ihrer Signatur HTML-Kode nutzen. Diese Aktion unterstützt die Signatur-Makros[136] des Typs `$CONTACT...$`.

Ein Beispiel hierzu: Mit dieser Regel könnte der Text "Diese Nachricht stammt aus meiner Firma. Bitte richten Sie alle Beschwerden und Fragen an user01@example.com" hinzugefügt werden.

Add Extra Header Item To Message ("Der Nachricht die zusätzliche Kopfzeile hinzufügen")—Diese Aktion fügt der Nachricht eine zusätzlich Kopfzeile an. Der Name und der Inhalt dieser Kopfzeile müssen hier angegeben werden.

Delete A Header Item From Message ("Kopfzeile löschen")—Diese Aktion entfernt eine Kopfzeile aus der Nachricht. Der Name dieser Kopfzeile muss noch angegeben werden.

Send Note To... ("Benachrichtigung an...")—Hiermit wird eine Nachricht an eine bestimmte Adresse gesendet. Absender, Empfänger, Betreff und ein kleiner Text können dazu angegeben werden. Es kann auch die Originalnachricht als Datei-Anlage mitgeschickt werden. **Beachte:** Diese Aktion überspringt alle Nachrichten, die keinen Antwortpfad enthalten. Sie kann daher beispielsweise auch nicht auf Nachrichten über den Zustellstatus (DSN) wirken.

Ein Beispiel hierzu: Man kann eine Regel anlegen, die alle Nachrichten mit dem Text "Das ist Spam!" in das Defekt-Verzeichnis verschiebt, und eine weitere, die jemanden von diesem Vorgang benachrichtigt.

Remove Digital Signature ("Digitale Signatur löschen")—Mit dieser Aktion wird eine etwa vorhandene digitale Signatur aus der Nachricht gelöscht.

Run Process... ("Programm ausführen")—Hiermit wird ein bestimmtes Programm ausgeführt, wenn die Nachricht der Bedingung entspricht. Pfad- und Dateiname des Programms müssen noch angegeben werden. Mit dem Makro $MESSAGEFILENAME$ kann man den Namen der Nachricht an das Programm übergeben. Es muss ausgewählt werden, ob MDaemon für eine bestimmte Zeit oder ohne Begrenzung angehalten wird, während das Programm läuft, und ob das Programm nötigenfalls abgebrochen wird und in einem versteckten Fenster laufen soll.

Send Message Through SMS Gateway Server... ("Nachricht an das SMS-Gateway senden")—Mit dieser Option wird die Nachricht an ein SMS-Gateway weitergeleitet. Der Name oder die IP-Adresse des Gateways und die Telefonnummer für den Versand der Nachricht müssen noch angegeben werden.

Copy Message to Folder... ("Nachricht in Ordner kopieren")—Diese Option legt eine Kopie der Nachricht in dem angegebenen Verzeichnis ab.

MOVE the messages to custom QUEUE... ("Nachricht in benutzerdefinierte Warteschlange verschieben")—Mithilfe dieser Aktion kann die Nachricht in eine oder mehrere benutzerdefinierte Warteschlangen verschoben werden. Werden die Nachrichten in Warteschlangen für externe Post verschoben, so können Zeitpläne, die mit diesen Warteschlangen verknüpft sind, steuern, wann die Nachrichten zugestellt werden.

Add Line To Text File ("Der Textdatei eine Zeile hinzufügen")—Diese Option bewirkt, dass eine Textzeile an eine bestimmte Textdatei angefügt wird. Bei Auswahl dieser Vorgehensweise müssen der Pfad zur Datei und der hinzuzufügende Text angegeben werden. Dabei sind bestimmte Makros von MDaemon zulässig; diese veranlassen den Inhaltsfilter, Informationen wie Absender, Empfänger, Nachrichten-ID u.a. dynamisch einzufügen. Ein Klick auf den Knopf "Makros" im Fenster "Add line to text file" ("Der Textdatei eine Zeile hinzufügen") zeigt die Liste zulässiger Makros an.

[Copy][Move] Message to Public Folders... ("Nachricht in öffentliche Ordner [kopieren][verschieben]")—Hiermit wird eine Nachricht in einen oder mehrere öffentliche Ordner kopiert oder verschoben.

Search and Replace Words in a Header ("Wörter in einer Kopfzeile suchen und ersetzen")—Diese Option durchsucht die ausgewählte Kopfzeile nach bestimmten Wörtern und kann diese, falls ein Treffer erzielt wird, löschen oder ersetzen. Beim Anlegen dieser Regel muss die Verknüpfung "specify information" ("Informationen angeben") in der Beschreibung für die Regel, um das Fenster "Kopfzeilen - Suchen und Ersetzen" zu öffnen; dort werden die gewünschten Kopfzeilen und die zu ändernden oder löschenden Wörter angegeben. Diese Aktion unterstützt jetzt Reguläre Ausdrücke. Siehe Nutzung regulärer Ausdrücke in den Bedingungen des Inhaltsfilters 657.

Search and Replace Words in the Message Body ("Wörter im Nachrichtentext suchen und ersetzen")—Diese Option durchsucht den Nachrichtentext und kann jeden gewünschten Text ersetzen. Diese Aktion unterstützt jetzt Reguläre Ausdrücke. Siehe Nutzung regulärer Ausdrücke in den Bedingungen des Inhaltsfilters 657.

Jump to Rule... ("Zur Regel… springen")—Diese Aktion springt direkt zu einer anderen Regel, die in der Liste weiter unten steht. Die übrigen Regeln werden dabei übergangen.

Send an instant message... ("Instant-Message senden...")—Diese Aktion sendet eine Instant-Message an einen Empfänger, wenn die Nachricht die Bedingungen für die Regel erfüllt. Sie müssen dazu die Empfängeradresse ("To"), die Absenderadresse ("From") und den Inhalt der Nachricht angeben.

Add to Windows Event Log...("In die Windows-Ereignisanzeige eintragen..."—Diese Aktion trägt eine Zeichenkette in das Windows-Ereignisprotokoll ein. Sie können in diese Zeichenkette Makros eintragen, und Sie können sich durch Anklicken des entsprechenden Steuerelements die zulässigen Makros anzeigen lassen.

Extract attachments to folder...("Dateianlagen entpacken in den Ordner...")—Diese Aktion entnimmt Dateianlagen aus der Nachricht. Sie

müssen das Verzeichnis angeben, in das die Dateianlagen kopiert werden sollen, und Sie können die Dateianlagen wahlweise anschließend aus der Nachricht löschen lassen. Sie können auch Bedingungen festlegen, die bestimmen, welche Dateianlagen entnommen werden sollen. Kriterien hierfür sind Dateiname, Inhaltstyp und Größe der Dateianlagen.

Change message processing priority...("Rangstufe der Nachricht ändern..."—Diese Aktion ändert die Rangstufe der Nachrichten. Die Rangstufe kann "10 (dringend)" bis "90 (Wiederholung)" betragen. Die Voreinstellung beträgt "50 (normal)".

Sign with DKIM selector... ("Mit DKIM-Selektor ... signieren")—Diese Aktion bewirkt, dass eine Nachricht mit einer DKIM-Signatur[533]. versehen wird. Sie kann auch eingesetzt werden, um Nachrichten mithilfe von Regeln des Inhaltsfilters anhand bestimmter Kriterien mit anderen Selektoren als denen zu signieren, die im Konfigurationsdialog für DKIM ausgewählt wurden.

Flag message for REQUIRETLS... ("Nachricht für REQUIRETLS kennzeichnen...")—Diese Aktion kennzeichnet die Nachricht für die Nutzung von REQUIRETLS[592].

[Sign|Encrypt|Decrypt] message with the user's [Private|Public] key...("Nachricht mit [öffentlichem|geheimem] Schlüssel des Benutzers [signieren|verschlüsseln|entschlüsseln]—Diese Aktionen signieren, verschlüsseln und entschlüsseln die Nachricht mithilfe eines öffentlichen oder geheimen Schlüssels. Nähere Informationen finden Sie im Abschnitt MDPGP[631]. **Beachte:** Diese Aktionen werden auch dann ausgeführt, wenn MDPGP deaktiviert ist.

Add a warning to the top of the message...("Warnmeldung am Beginn des Nachrichtentexts einfügen...")—Diese Aktion fügt am Beginn der Nachricht eine Warnmeldung ein. Sie können die Warnmeldung im Format Nur-Text oder HTML eingeben. Für die Verwendung von HTML aktivieren Sie das Kontrollkästchen HTML verwenden. Sie können den Text auch aus einer Datei laden.

Add an attachment... ("Eine Dateianlage hinzufügen...")—Diese Aktion fügt der Nachricht eine Dateianlage hinzu, falls die Nachricht die Bedingungen der Regel erfüllt. Die Datei muss sich im Ordner `./MDaemon/CFilter/Attachments/` befinden.

Extract attachment and add link... ("Dateianlage entpacken und durch Verknüpfung ersetzen...")—Mithilfe dieser Aktion können Sie Dateianlagen aus Nachrichten entnehmen lassen, die die Bedingungen der Regel erfüllen. Die Dateianlagen werden dabei durch eine Verknüpfung ersetzt. Siehe auch: Verlinkung von Dateianlagen[364].

Beschreibung für diese Regel
In diesem Abschnitt des Konfigurationsdialogs erscheint die neue Regel im Skript-Format, wobei die Bedingungen und Aktionen als Hyperlinks dargestellt werden. Zusätzliche Informationen zu den Bedingungen und Aktionen der Regel können nach einem Klick auf den entsprechenden Hyperlink in einem Editor angegeben werden.

Siehe auch:

Editor für den Inhaltsfilter 649
Bearbeiten einer bestehenden Regel für den Inhaltsfilter 657
Nutzung Regulärer Ausdrücke in den Filterregeln 657

4.5.1.1.2 Bearbeiten einer bestehenden Regel für den Inhaltsfilter

Um eine bestehende Regel für den Inhaltsfilter zu ändern, wählen Sie sie in der Liste im Konfigurationsdialog des Inhaltsfilters aus, und klicken Sie auf *Regel bearbeiten*. Die Regel wird dann in einem eigenen Editor geöffnet, dessen Bedienung mit dem Editor zum Erstellen einer neuen Regel für den Inhaltsfilter 651 übereinstimmt.

Siehe auch:

Der Editor für den Inhaltsfilter 649
Erstellen einer neuen Regel für den Inhaltsfilter 651
Nutzung Regulärer Ausdrücke in den Regeln des Inhaltsfilters 657

4.5.1.1.3 Nutzung Regulärer Ausdrücke in den Filterregeln

Der Inhaltsfilter unterstützt die Suche anhand "Regulärer Ausdrücke" diese sind vielseitig einsetzbar, und mit ihrer Hilfe kann nicht nur nach herkömmlichen Zeichenketten sondern auch nach Text-Mustern gesucht werden. Reguläre Ausdrücke enthalten eine Kombination aus Klartext und besonderen Steuerzeichen, welche die Art der Rastersuche festlegen; sie können daher das Regelsystem des Inhaltsfilters mächtiger und treffsicherer machen.

Was versteht man unter Regulären Ausdrücken?
Reguläre Ausdrücke werden nach dem englischen Fachbegriff "Regular Expression" auch als "RegExp" abgekürzt. Ein Regulärer Ausdruck ist ein Textmuster, das aus einer Kombination von Zeichen mit besonderer Bedeutung, den sog. *Metazeichen*, und regulären alphanumerischen Zeichen, den sog. *gewöhnlichen* oder *terminalen Zeichen* (wie etwa abc, 123 und andere). Anhand des Musters wird versucht, einen Treffer in der entsprechenden Zeichenkette zu finden, wobei diese Suche erfolgreich oder erfolglos sein kann. Reguläre Ausdrücke werden hauptsächlich zur Treffersuche in normalem Text und zum Suchen und Ersetzen verwendet.

Metazeichen sind besondere Zeichen, die innerhalb Regulärer Ausdrücke bestimmte Funktionen erfüllen. Das System der Regulären Ausdrücke, das im Inhaltsfilter von MDaemon implementiert ist, gestattet die Verwendung folgender Metazeichen:

```
\ | () [] ^ $ * + ? . <>
```

Metazeichen	Beschreibung
****	Wird der Backslash ("\" oder "umgekehrter Schrägstrich") vor ein Metazeichen gesetzt, so wird das folgende Metazeichen maskiert, also als gewöhnliches Zeichen behandelt. Dies ist nötig, wenn der Reguläre Ausdruck nach einem der besonderen Zeichen suchen soll, die sonst als Metazeichen verwendet werden. Beispielsweise muss ein Ausdruck, der nach dem Pluszeichen ("+") suchen soll, dafür die Zeichenkette "\+" enthalten.

|	Das *Alternativzeichen* (auch "*Oder-Zeichen*" oder "*senkrechter Strich*" genannt) wird verwendet, wenn entweder die Zeichenkette vor oder nach dem Oderzeichen mit dem zu durchsuchenden Text übereinstimmen soll. Der Reguläre Ausdruck "abc?xyz" sucht beispielsweise nach dem Vorkommen der Zeichenketten "abc" oder "xyz".
[...]	Eine von eckigen Klammern ("[" und "]") umschlossene Zeichenkette bedeutet, dass jedes beliebige Zeichen in der Kette mit dem zu durchsuchenden Text übereinstimmen soll. Ein Bindestrich ("-") zwischen den Zeichen in Klammern definiert eine Zeichenreihe. Wird beispielsweise die Zeichenkette "abc" mit dem Regulären Ausdruck "[a-z]" durchsucht, dann ergeben sich drei Treffer: "*a*", "*b*" und "*c*". Lautet statt dessen der Suchausdruck "[az]", so ergibt sich nur ein Treffer: "*a*".
^	Das sog. "Caret" bezeichnet einen Zeilenanfang. In der Zeichenkette "abc ab a" ergibt der Suchausdruck "^a" einen Treffer, und zwar das erste Zeichen der durchsuchten Zeichenkette. Der Ausdruck "^ab" ergibt ebenfalls einen Treffer, und zwar die ersten beiden Zeichen in der durchsuchten Zeichenkette.
[^...]	Folgt das Caret ("^") direkt auf eine öffnende eckige Klammer ("["), so erfüllt es einen anderen Zweck. Es legt fest, dass die in der Klammer folgenden Zeichen keinen Treffer in der zu durchsuchenden Zeichenkette ergeben dürfen. Der Ausdruck "[^0-9]" bedeutet beispielsweise, dass das zu suchende Zeichen keine Ziffer sein darf.
(...)	Die runden Klammern beeinflussen die Reihenfolge, in der die Muster ausgewertet werden, und dient außerdem als Suchmuster, das in Ausdrücken zum *Suchen und Ersetzen* verwendet werden kann. Die Ergebnisse einer Suche durch einen Regulären Ausdruck werden zwischengespeichert und können in der Anweisung zum *Ersetzen* verwendet werden, um einen neuen Ausdruck zu bilden. Im Ausdruck zum *Ersetzen* kann das Zeichen "$0" enthalten sein; es wird durch die Zeichenketten ersetzt, die während der Suche durch den Regulären Ausdruck gefunden wurden. Findet der Suchausdruck "a(bcd)e" beispielsweise eine Zeichenkette, so ersetzt der Ausdruck "123-$0-123" den gefundenen Text durch "123-abcde-123". In ähnlicher Weise können die besonderen Zeichen "$1", "$2", "$3" usw. in dem Ausdruck verwendet werden, der Zeichenketten ersetzen soll. Diese Zeichen werden nur durch die unmittelbaren Ergebnisse des Suchmusters, nicht aber durch die vollständige gefundene Zeichenkette ersetzt. Die Zahl nach dem Backslash legt bei Regulären Ausdrücken mit mehr als einem Suchmuster fest, auf welches Suchmuster verwiesen werden soll. Lautet der Suchausdruck beispielsweise "(123)(456)", und lautet der

Ausdruck zum Ersetzen "a-$2-b-$1", so wird eine gefundene Zeichenkette durch "a-456-b-123" ersetzt, wohingegen ein Ausdruck zum Ersetzen "a-$0-b" durch "a-123456-b" ersetzt wird.

**$** Das Dollarzeichen ("$") bezeichnet ein Zeilenende. In der Zeichenkette "13 321 123" ergibt der Ausdruck "3$" einen Treffer, und zwar das letzte Zeichen der Kette. Der Ausdruck "123$" ergibt ebenfalls einen Treffer, und zwar die *letzten drei* Zeichen in der Zeichenkette.

***** Das Zeichen Stern ("*") bestimmt, dass das ihm vorausgehende Zeichen mehrmals hintereinander vorkommen darf, aber nicht vorkommen muss. Daher ergibt "1*abc" für die Zeichenketten "111abc" und "abc" jeweils einen Treffer.

+ Etwas anders als der Stern, bestimmt das Pluszeichen "+", dass das ihm vorausgehende Zeichen mindestens einmal in der Zeichenkette vorkommen muss, aber auch mehrfach vorkommen darf. Daher ergibt "1+abc" einen Treffer bei der Zeichenkette "111abc", nicht aber bei "abc".

? Das Fragezeichen ("?") bestimmt, dass das ihm vorausgehende Zeichen mehrmals vorkommen darf, aber nicht vorkommen muss. Daher ergibt "1?abc" einen Treffer für den Text "abc" sowie einen Treffer für die Zeichenkette "1abc" aus dem Text "111abc".

. Das Metazeichen Punkt (".") ergibt einen Treffer für jedes beliebige andere Zeichen. Daher ergibt ".+abc" einen Treffer für "123456abc", "a.c" ergibt einen Treffer für "aac", "abc", "acc" u.s.w.

Geeignete Bedingungen und Aktionen
Reguläre Ausdrücke dürfen in die Bedingung jeder Filterregel eingesetzt werden, die sich auf *Kopfzeilen* bezieht, also beispielsweise in jeder Regel, mit der Bedingung "`if the FROM HEADER contains`" ("Wenn die Kopfzeile Absender ... enthält"). Reguläre Ausdrücke sind auch in der Bedingung "`if the MESSAGE BODY contains`" ("Wenn der Nachrichtentext ... enthält") zulässig.

Reguläre Ausdrücke sind auch in zwei *Aktionen* der Regeln des Inhaltsfilters zulässig: "`Search and Replace Words in a Header`" ("Wörter in einer Kopfzeile suchen und ersetzen") und "`Search and Replace Words in the Message Body`" ("Wörter im Nachrichtentext suchen und ersetzen").

Reguläre Ausdrücke in den *Bedingungen* der Regeln des Inhaltsfilters arbeiten unabhängig von Groß- und Kleinschreibung und ignorieren die Schreibweise insoweit.

Die Frage, ob Reguläre Ausdrücke in *Aktionen* der Regeln des Inhaltsfilters die Groß-/Kleinschreibung beachten sollen, ist dem Benutzer überlassen. Beim Anlegen eines Regulären

Ausdrucks fragt MDaemon ab, ob die Groß- und Kleinschreibung beachtet werden soll oder nicht.

Definition eines Regulären Ausdrucks in der Bedingung einer Regel

Um für eine Regel, die sich auf eine Kopfzeile oder den Nachrichtentext bezieht, einen Regulären Ausdruck zu definieren, ist wie folgt vorzugehen:

1. Im Dialogfenster "Regel erstellen" den Listeneintrag wählen, der die gewünschte Bedingung zu Kopfzeile oder Nachrichtentext kennzeichnet, die in die Regel eingefügt werden soll.

2. In der Regel-Beschreibung am Ende des Dialogfensters "Regel erstellen" den Link "**contains specific strings**" ("enthält bestimmte Zeichenketten") der Bedingung anklicken, die in Schritt 1 ausgewählt wurde. Es öffnet sich das Fenster zur Eingabe des zu suchenden Textes.

3. Den Link "**contains**" ("enthält") im Abschnitt "Derzeit angegebene Zeichenketten..." anklicken.

4. Aus dem Rollmenü den Eintrag "**Matches Regular Expression**" ("ergibt einen Treffer aus Regulärem Ausdruck") wählen und OK anklicken.

5. Falls Hilfe bei der Definition des Regulären Ausdrucks gewünscht ist oder der Ausdruck überprüft werden soll, das Steuerelement "**Regulären Ausdruck testen**" anklicken. Falls diese Funktion nicht benötigt wird, den Regulären Ausdruck in das Textfeld eintragen, **Hinzufügen** anklicken und mit Schritt 8 fortfahren.

6. Den Regulären Ausdruck in das Feld "Suchausdruck" eintragen. Um diesen Vorgang zu vereinfachen, ist ein Kontextmenü vorgesehen, mit dessen Hilfe die gewünschten Metazeichen einfach in den Regulären Ausdruck eingesetzt werden können. Ein Klick auf den Knopf ">" öffnet das Menü. Nach Auswahl eines Menüpunkts wird das zugehörige Metazeichen in den Ausdruck eingefügt, und der Ankerpunkt für die Texteingabe wird an die Stelle im Ausdruck verschoben, die für das Zeichen erforderlich ist.

7. Gewünschten Text, anhand dessen der Ausdruck überprüft werden soll, in das entsprechende Textfeld eingeben und **Testen** anklicken. Wenn keine weiteren Tests gewünscht sind, **OK** anklicken.

8. **OK** anklicken.

9. Mit der Erstellung der Regel wie gewohnt fortfahren.

Definition eines Regulären Ausdrucks in der Aktion einer Regel

Um eine Aktion "Search and Replace Words in..." ("Wörter in ... suchen und ersetzen") für den Einsatz eines Regulären Ausdrucks zu konfigurieren, ist wie folgt vorzugehen:

1. Im Dialogfenster "Regel erstellen" den Listeneintrag wählen, der die gewünschte Aktion zum Suchen und Ersetzen von Wörtern kennzeichnet, die in die Regel eingefügt werden soll.

2. In der Regel-Beschreibung am Ende des Dialogfensters "Regel erstellen" den Link "**specify information**" ("Informationen angeben") der Aktion anklicken, die in Schritt 1 ausgewählt wurde. Es öffnet sich das Fenster zur Eingabe der Parameter zum Suchen und Ersetzen.

3. Wurde in Schritt 1 die Aktion "*Search…header*" ("Kopfzeile … durchsuchen) ausgewählt, muss die zu durchsuchende Kopfzeile aus dem Rollmenü ausgewählt oder, falls die gewünschte Kopfzeile hier nicht aufgeführt ist, in das Textfeld eingegeben werden. Wurde in Schritt 1 die Aktion "*Search…header*" ("Kopfzeile … ersetzen"), so wird dieser Schritt übersprungen.

4. Den für diese Aktion gewünschten *Suchausdruck* eintragen. Um diesen Vorgang zu vereinfachen, ist ein Kontextmenü vorgesehen, mit dessen Hilfe die gewünschten Metazeichen einfach in den Regulären Ausdruck eingesetzt werden können. Ein Klick auf den Knopf ">" öffnet das Menü. Nach Auswahl eines Menüpunkts wird das zugehörige Metazeichen in den Ausdruck eingefügt, und der Ankerpunkt für die Texteingabe wird an die Stelle im Ausdruck verschoben, die für das Zeichen erforderlich ist.

5. Den für diese Aktion gewünschten Ausdruck zum *Ersetzen* eintragen. Wie beim Suchausdruck, steht auch hier ein Kontextmenü zum Einfügen der Metazeichen zur Verfügung. Soll die gefundene Zeichenkette nicht durch anderen Text ersetzt sondern gelöscht werden, das entsprechende Textfeld leer lassen.

6. "**Groß-/Kleinschreibung prüfen**" anklicken, falls der Ausdruck nach Groß- und Kleinschreibung unterscheiden soll.

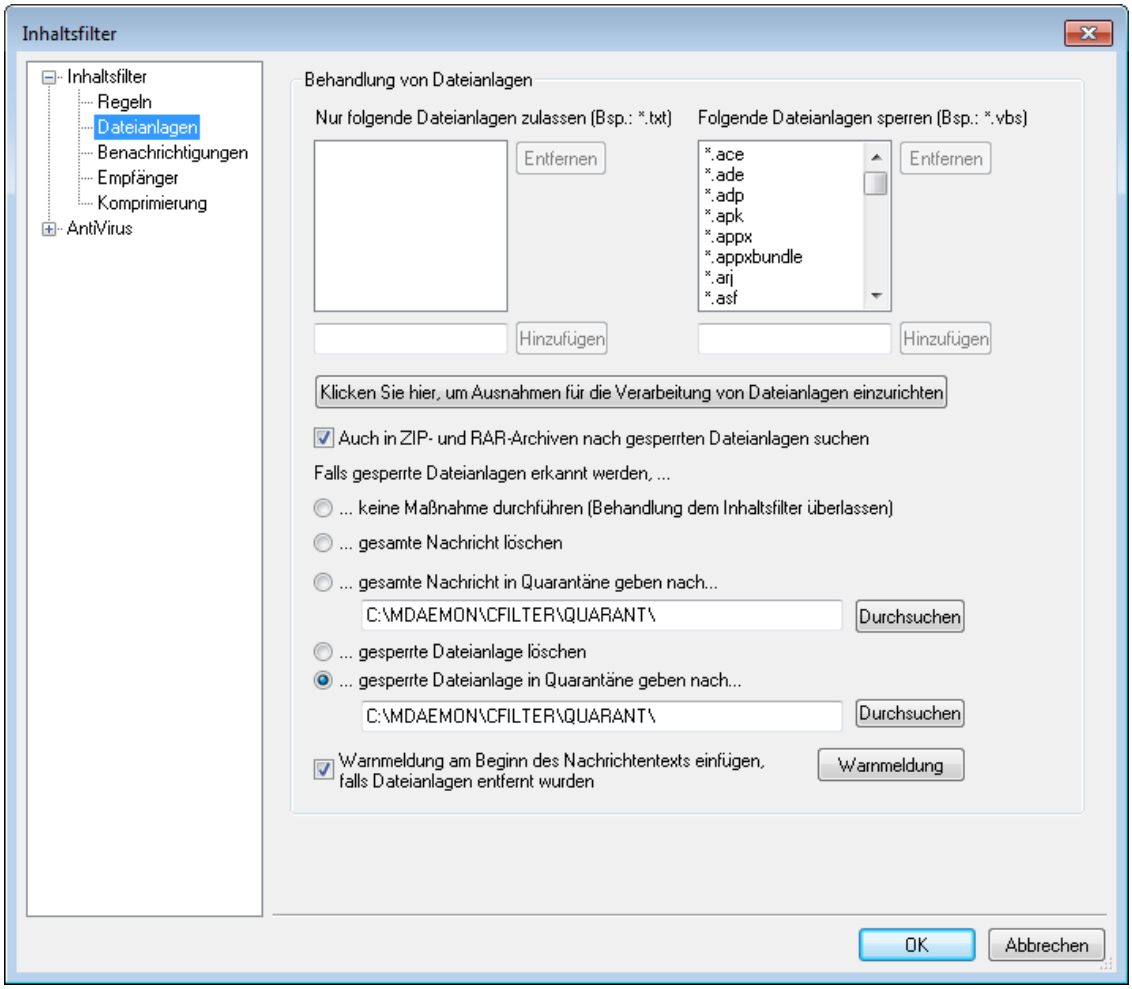
7. "Regulärer Ausdruck" anklicken, falls die zum Suchen und Ersetzen eingetragenen Zeichenketten als Reguläre Ausdrücke behandelt werden sollen; ansonsten werden diese als normale Zeichenketten behandelt, und der Inhaltsfilter sucht nach einer genauen Übereinstimmung des eingetragenen Textes, ohne die Texte als Reguläre Ausdrücke zu verarbeiten.

8. Falls der Reguläre Ausdruck nicht getestet werden soll, diesen Schritt überspringen. Falls ein Test gewünscht ist, "**Test ausführen**" anklicken. Im Fenster "Test für Funktion Suchen und Ersetzen" die Ausdrücke zum Suchen und Ersetzen sowie den Text eintragen, anhand dessen die Ausdrücke geprüft werden sollen, dann Testen anklicken. Werden keine weiteren Tests mehr gewünscht, **OK** anklicken.

9. **OK** anklicken.

10. Mit der Erstellung der Regel wie gewohnt fortfahren.

4.5.1.2 Dateianlagen



In diesem Konfigurationsdialogr können Dateianlagen zugelassen oder gesperrt werden. Gesperrte Dateianlagen werden automatisch aus den verarbeiteten Nachrichten automatisch entfernt.

Behandlung von Dateianlagen

Die unter *Folgende Dateianlagen sperren* nach Namen erfassten Dateien werden automatisch aus Nachrichten entfernt, wenn diese durch MDaemon verarbeitet werden. Falls Dateien in der Liste *Nur folgende Dateianlagen zulassen* aufgeführt sind, so werden nur diese Dateianlagen zugelassen, alle anderen Dateianlagen werden aus den Nachrichten entfernt. Nachdem die Dateianlage entfernt wurde, stellt MDaemon die Nachricht ohne die Datei normal zu. Im Konfigurationsdialog "Benachrichtigung" kann festgelegt werden, ob und welche Adressen benachrichtigt werden sollen, wenn eine gesperrte Dateianlage aufgetreten ist.

In dieser Liste sind Jokerzeichen zulässig. Der Eintrag "`*.exe`" würde z.B. bewirken, dass alle Dateianlagen mit der Namenserweiterung EXE zugelassen oder gelöscht werden. Um diesen Listen einen Eintrag hinzuzufügen, ist der Dateiname in das entsprechende Feld einzutragen und auf "Hinzufügen" zu klicken.

Klicken Sie hier, um Ausnahmen für die Verarbeitung von Dateianlagen einzurichten
Ein Klick auf dieses Steuerelement erlaubt es, Adressen anzugeben, die von der Sperre der Dateianlagen ausgenommen werden. Nachrichten an diese

ausgeschlossenen Adressen werden auch dann vollständig zugestellt, wenn sie gesperrte Dateianlagen enthalten.

Auch in ZIP- und RAR-Archiven nach gesperrten Dateien suchen
Diese Option bewirkt, dass auch komprimierte Dateien der Formate ZIP, 7-Zip und RAR nach gesperrten Dateianlagen durchsucht werden. Dies erstreckt sich auch auf alle Regeln des Inhaltsfilters, die nach bestimmten Dateinamen suchen, sodass der Inhaltsfilter einen Treffer erkennt, falls solche Dateinamen in Archiven gefunden werden.

Gesperrte Dateianlage in Quarantäne geben nach
Ein Klick auf dieses Steuerelement bewirkt, dass gesperrte Dateianlagen nicht gelöscht sondern in Quarantäne gegeben werden. Hierzu muss noch festgelegt werden, wo solche Dateien abgelegt werden sollen.

Falls gesperrte Dateianlagen erkannt werden, ...
Mithilfe der nachfolgenden Optionen legen Sie die Behandlung von Nachrichten fest, die gesperrte Dateianlagen enthalten.

...keine Maßnahme durchführen (Behandlung dem Inhaltsfilter überlassen)
Diese Option bewirkt, dass keine besondere Maßnahme für die Dateianlagen ergriffen wird. Die Behandlung richtet sich dann nach den Regeln des Inhaltsfilters 649.

...gesamte Nachricht löschen
Diese Option bewirkt, dass die gesamte Nachricht gelöscht wird, falls sie eine gesperrte Dateianlage enthält.

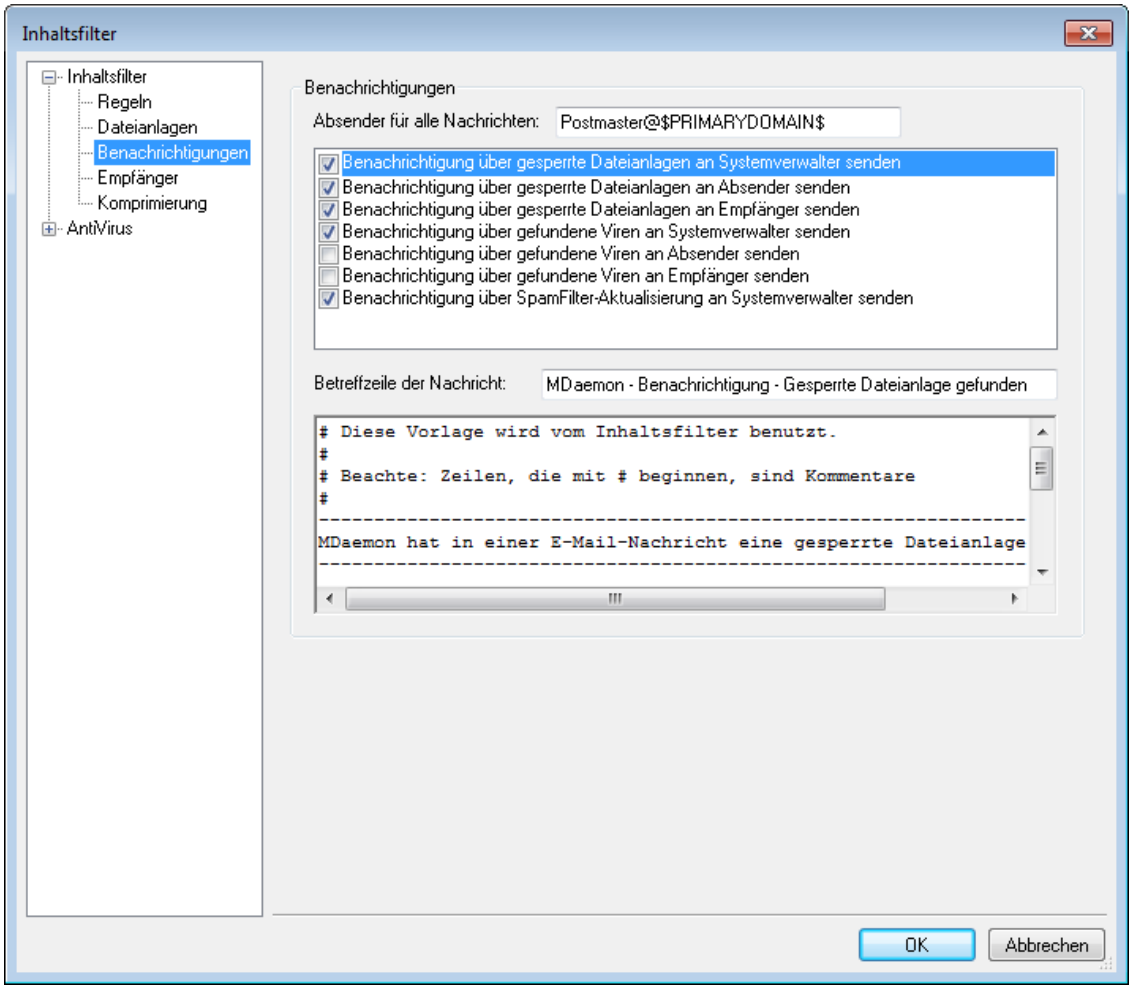
...gesamte Nachricht in Quarantäne geben nach...
Diese Option bewirkt, dass Nachrichten mit gesperrten Dateianlagen in dem angegebenen Verzeichnispfad in Quarantäne gegeben werden.

...gesperrte Dateianlage löschen
Diese Option bewirkt, dass nicht die gesamte Nachricht, sondern nur die gesperrte Dateianlage selbst gelöscht wird.

...gesperrte Dateianlage in Quarantäne geben nach...
Diese Option bestimmt, dass die gesperrte Dateianlage nicht gelöscht sondern in dem angegebenen Verzeichnispfad in Quarantäne gegeben wird. Diese Option ist per Voreinstellung aktiv.

Warnmeldung am Beginn des Nachrichtentexts einfügen, falls Dateianlagen entfernt wurden
Wenn MDaemon eine Dateianlage aus einer Nachricht entfernt, etwa, weil ein Virus gefunden wurde, dann wird am Beginn des Nachrichtentexts eine Warnmeldung eingefügt. Um die Vorlage für diese Warnmeldung zu bearbeiten, klicken Sie auf die Schaltfläche **Warnmeldung**. Diese Option ist per Voreinstellung aktiv.

4.5.1.3 Benachrichtigungen



In diesem Konfigurationsdialog wird festgelegt, wer verständigt werden soll, wenn ein Virus oder eine gesperrte Dateianlage festgestellt, und nachdem die Dateien des AntiVirus-Moduls oder des Spam-Filters aktualisiert wurden.

Benachrichtigungen

Absender für alle Nachrichten:
Hier wird die Absenderadresse eingetragen, die in den Warnnachrichten vermerkt sein soll.

Benachrichtigung über gefundene Viren an [...] senden
Geht eine Nachricht mit einer vireninfizierten Dateianlage ein, so erhalten die hier ausgewählten Empfänger eine entsprechende Warnmeldung. An Absender, Empfänger und die Adressen, die im Konfigurationsdialog Empfänger 667 definiert sind, können jeweils angepasste Nachrichten versandt werden. Um die Nachricht für einen bestimmten Eintrag anzupassen, muss dieser zunächst in der Liste ausgewählt werden. Sodann kann die Nachricht, die im unteren Teil des Fensters erscheint, geändert werden. Jedem Eintrag ist eine eigene Nachricht zugeordnet. Auf Anhieb ist dies allerdings nicht ersichtlich, da alle Texte per Voreinstellung gleich lauten.

Benachrichtigung über gesperrte Dateianlagen an [...] senden
Geht eine Nachricht mit einer gesperrten Dateianlage ein, so erhalten die hier ausgewählten Empfänger eine entsprechende Warnmeldung. An Absender, Empfänger und die Adresse, die im Konfigurationsdialog Empfänger[667] definiert sind, können jeweils angepasste Nachrichten versandt werden. Um die Nachricht für einen bestimmten Eintrag anzupassen, muss dieser zunächst in der Liste ausgewählt werden. Sodann kann die Nachricht, die im unteren Teil des Fensters erscheint, geändert werden. Jedem Eintrag ist eine eigene Nachricht zugeordnet. Auf Anhieb ist dies allerdings nicht ersichtlich, da alle Texte per Voreinstellung gleich lauten.

Benachrichtigung über Spam-Filter-Aktualisierung an Systemverwalter senden
Diese Option bewirkt, dass die Systemverwalter per E-Mail benachrichtigt werden, sobald der Spam-Filter aktualisiert wurde. Die Benachrichtigung enthält die Ergebnisse der Aktualisierung. Diese Option entspricht der Option "*Nachricht über die Ergebnisse der Aktualisierung per E-Mail senden*" im Konfigurationsdialog Spam-Filter » Aktualisierungen.

Betreffzeile der Nachricht:
Der hier eingetragene Text erscheint in der Betreffzeile der Benachrichtigungen.

Nachricht
Der Text, der in diesem Textfeld erscheint, wird als Nachrichtentext in die Benachrichtigungen eingefügt. Es erscheint jeweils der Nachrichtentext für die gerade in der Liste ausgewählte Benachrichtigung. Der Nachrichtentext kann in diesem Textfeld unmittelbar bearbeitet werden.

Die eigentlichen Dateien, die diese Nachrichtentexte enthalten, sind im Verzeichnis `MDaemon\app\` abgelegt. Ihre Dateinamen lauten:

`cfattrem[adm].dat` – Gesperrte Dateianlage – Verwalter
`cfattrem[rec].dat` – Gesperrte Dateianlage – Empfänger
`cfattrem[snd].dat` – Gesperrte Dateianlage – Absender
`cfvirfnd[adm].dat` – Virenwarnung – Verwalter
`cfvirfnd[rec].dat` – Virenwarnung – Empfänger
`cfvirfnd[snd].dat` – Virenwarnung – Absender

Die Nachrichtentexte lassen sich leicht in die Voreinstellung zurück versetzen, indem einfach nur die entsprechende Datei gelöscht wird. Beim nächsten Programmstart legt MDaemon die betreffende Datei mit Standardinhalt neu an.

4.5.1.3.1 Makros für Nachrichten

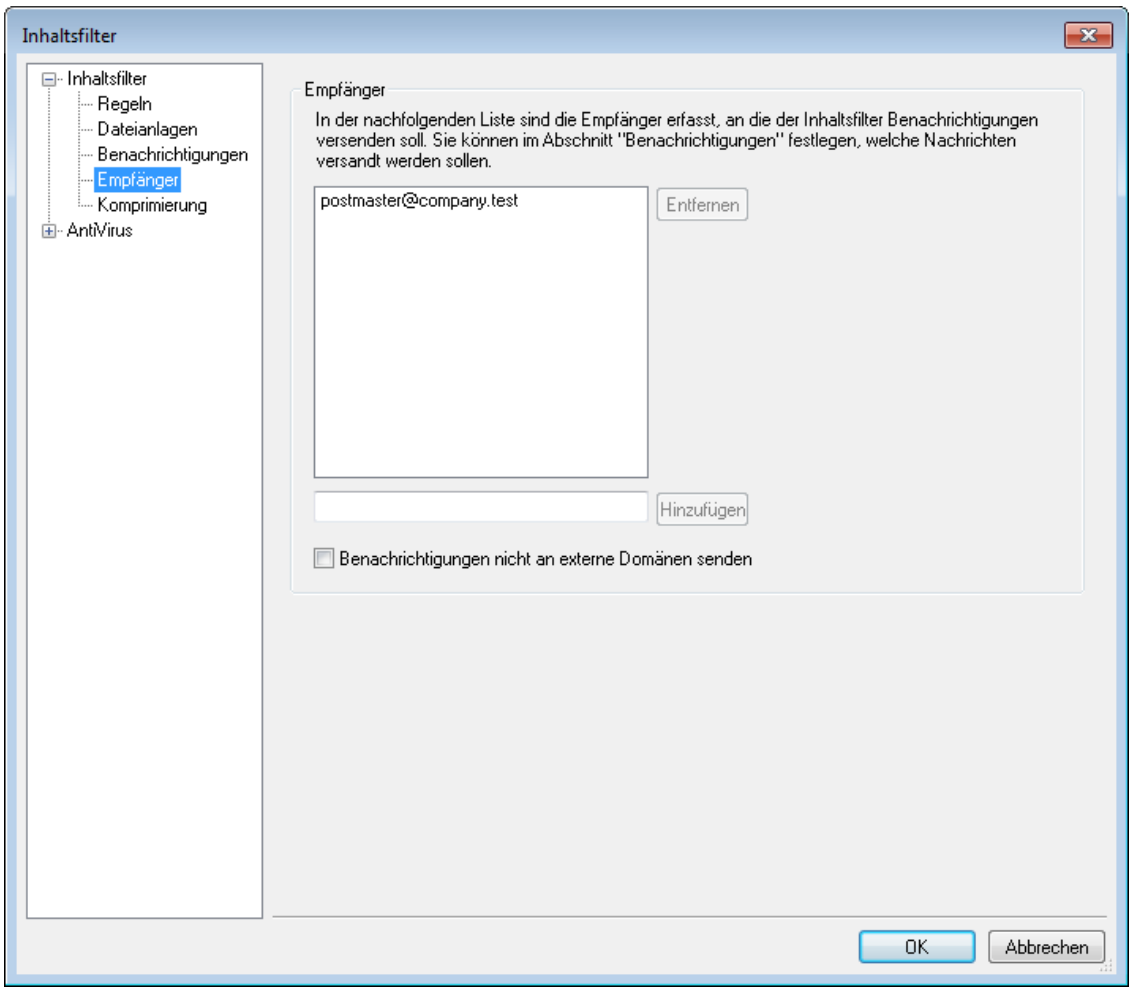
Um den Bedienkomfort zu erhöhen, dürfen bestimmte Makros bei der Abfassung von Warnmeldungen und anderen Nachrichten, die der Inhaltsfilter erzeugt, verwendet werden. Alle nachfolgend aufgeführten Makros sind zulässig.

`$ACTUALTO$` Manche Nachrichten enthalten ein Feld „ActualTo" („Eigentlich an"), in dem die ursprünglich vom Absender eingegebene Zieladresse zu finden ist, wie sie vor

	irgendwelchen Umformungen oder Formatänderungen lautete. Dieses Makro fügt diesen Text ein.
$AV_VERSION$	Gibt die Versionsnummer der auf dem System vorhandenen Version von AntiVirus aus.
$CURRENTTIME$	Dieses Makro wird durch die aktuelle Uhrzeit bei Verarbeitung der Nachricht ersetzt.
$ACTUALFROM$	Manche Nachrichten enthalten ein Feld "ActualFrom" ("Eigentlich von"), in dem die ursprüngliche Absenderadresse zu finden ist, wie sie vor irgendwelchen Umformungen oder Formatänderungen lautete. Dieses Makro fügt diesen Text ein.
$FILTERRULENAME$	Hierdurch wird der Name der Regel eingefügt, deren Kriterien auf die Nachricht zutreffen.
$FROM$	Dieses Makro wird durch die vollständige Adresse aus der Absenderkopfzeile "From:" der Nachricht ersetzt-
$FROMDOMAIN$	Dieses Makro wird durch den Domänennamen aus der E-Mail-Adresse ersetzt, die in der Absenderkopfzeile "From:" der Nachricht gefunden wird (dies ist der Wert rechts vom Zeichen "@" in der E-Mail-Adresse).
$FROMMAILBOX$	Dieses Makro wird durch den Postfachnamen aus der E-Mail-Adresse ersetzt, die in der Absenderkopfzeile "From:" der Nachricht gefunden wird (dies ist der Wert links vom Zeichen "@" in der E-Mail-Adresse).
$LIST_ATTACHMENTS_REMOVED$	Werden Dateianlagen aus der Nachricht gelöscht, so fügt dieses Makro ihre Namen ein.
$LIST_VIRUSES_FOUND$	Werden Viren in der Nachricht entdeckt, fügt dieses Makro eine Liste der Viren ein.
$MESSAGEFILENAME$	Hierdurch wird der Name der gerade verarbeiteten Nachricht eingefügt.
$MESSAGEID$	Wie oben $HEADER:MESSAGE-ID$, dieses Makro entfernt jedoch "<>" aus der Nachrichten-ID.
$PRIMARYDOMAIN$	Gibt den Namen der Standard-Domäne von MDaemon aus, der im Domänen-Manager 181 festgelegt wird.
$PRIMARYIP$	Gibt die IP-Adresse der Standard-Domäne aus (einzustellen im Domänen-Manager 181).
$RECIPIENT$	Dieses Makro gibt die vollständige E-Mail-Adresse des Empfängers aus.
$RECIPIENTDOMAIN$	Dieses Makro wird durch den Domänennamen des Absenders Empfängers ersetzt (dies ist der

	Wert rechts vom Zeichen "@" in der E-Mail-Adresse).
$RECIPIENTMAILBOX$	Dieses Makro wird durch den Postfachnamen des Empfängers ersetzt (dies ist der Wert links vom Zeichen "@" in der E-Mail-Adresse).
$REPLYTO$	Dieses Makro wird durch den Inhalt der Kopfzeile "Reply-To" ("Antwort an") ersetzt.
$SENDER$	Dieses Makro wird durch die vollständige Adresse des Absenders der Nachricht ersetzt
$SENDERDOMAIN$	Dieses Makro wird durch den Domänennamen des Absenders ersetzt (dies ist der Wert rechts vom Zeichen "@" in der E-Mail-Adresse).
$SENDERMAILBOX$	Dieses Makro wird durch den Postfachnamen des Absenders ersetzt (dies ist der Wert links vom Zeichen "@" in der E-Mail-Adresse).
$SUBJECT$	Dieses Makro wird durch den Betreff der Nachricht ersetzt.

4.5.1.4 Empfänger

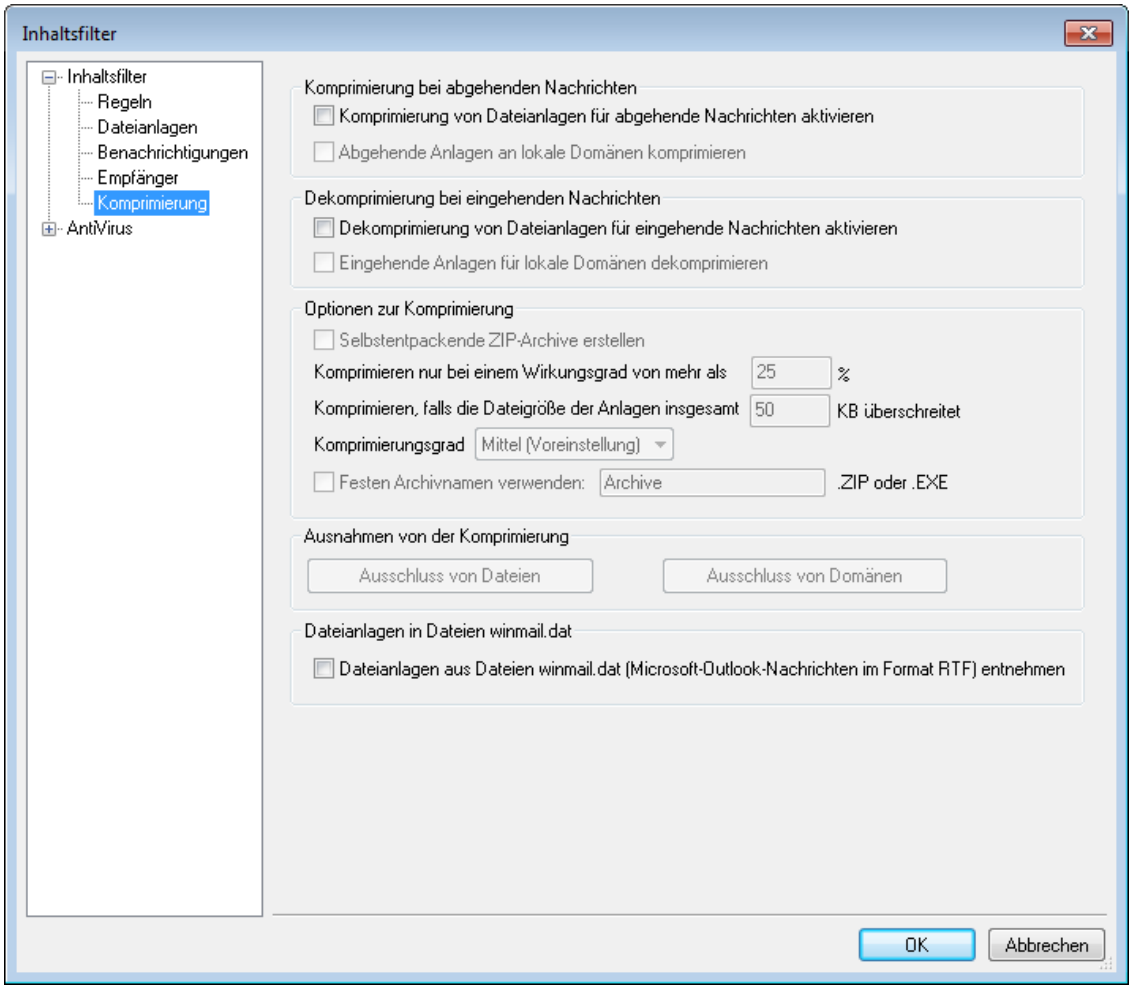


Empfänger

Die hier aufgeführte Liste der Empfänger steht mit den verschiedenen Benachrichtigungs-Einstellungen in Verbindung, die im Konfigurationsdialog Benachrichtigungen zu finden sind. Die hier eingetragenen Adressen erhalten Benachrichtigungen, falls eine der Einstellungen über die *Benachrichtigung von Systemverwaltern* im Konfigurationsdialog Benachrichtigungen aktiv ist. Um dieser Liste eine Adresse hinzuzufügen, wird die Adresse hier eingetragen, danach muss *Hinzufügen* angeklickt werden. Um eine Adresse zu löschen, muss sie ausgewählt werden; danach wird *Entfernen* angeklickt.

Benachrichtigungen nicht an externe Domänen senden
Diese Option bewirkt, dass die Benachrichtigungen des Inhaltsfilters nur an Empfänger in den lokalen Domänen, nicht aber an externe Empfänger versandt werden. Diese Option ist per Voreinstellung aktiv.

4.5.1.5 Komprimierung



Die Einstellungen in diesem Konfigurationsdialog bewirken, dass Dateianlagen automatisch gepackt oder entpackt werden, bevor eine Nachricht zugestellt wird. Der Komprimierungsgrad und verschiedene andere Parameter sowie eine Ausschlussliste lassen sich einstellen. Diese Funktion kann die Bandbreite und das Datenvolumen, das zur Zustellung abgehender Nachrichten nötig ist, bedeutend verringern.

Komprimierung bei abgehenden Nachrichten

Komprimierung von Dateianlagen für abgehende Nachrichten aktivieren
Mit dieser Option werden Dateianlagen in abgehenden externen Nachrichten automatisch komprimiert. Dies bedeutet noch nicht, dass zwingend alle Dateianlagen komprimiert werden. Die Festlegungen für den Einzelfall werden mit den folgenden Einstellungen dieses Konfigurationsdialogs getroffen.

Abgehende Anlagen an lokale Domänen komprimieren
Diese Option bewirkt, dass die Einstellungen zur Komprimierung auf die gesamte abgehende Post angewendet werden – also auch auf Nachrichten, die an eine lokale Adresse gerichtet sind.

Komprimierung bei eingehenden Nachrichten

Dekomprimierung von Dateianlagen für eingehende Nachrichten aktivieren
Mit dieser Option können gepackte Dateianlagen in eingehenden Nachrichten automatisch ausgepackt werden. Kommt eine Nachricht mit einer komprimierten Dateianlage an, so packt MDaemon diese Anlage aus, bevor die Nachricht in das lokale Postfach zugestellt wird.

Eingehende Anlagen für lokale Domänen dekomprimieren
Diese Option muss aktiv sein, wenn sich die automatische Dekomprimierung auch auf Nachrichten an lokale Domänen erstrecken soll.

Optionen zur Komprimierung

Selbstentpackende ZIP-Archive erstellen
Ist diese Option aktiviert, so erstellt MDaemon ZIP-Archive mit der Dateiendung EXE, die sich selbst entpacken können. Dies ist besonders dann hilfreich, wenn zu besorgen ist, dass den Nachrichtenempfänger kein Programm zur Dekomprimierung zur Verfügung steht. Selbstentpackende ZIP-Archive können entpackt werden, indem man sie einfach ausführt.

Komprimieren nur bei Wirkungsgrad von mehr als [xx] %
MDaemon komprimiert eine Dateianlage nur dann, wenn dabei der hier angegebene Wirkungsgrad übertroffen werden kann. Ist hier beispielsweise der Wert 20 angegeben, und kann eine bestimmte Dateianlage nicht wenigstens mit 21 % komprimiert werden, so wird MDaemon die Komprimierung vor dem Versand nicht durchführen.

Um den Wirkungsgrad festzustellen, muss MDaemon die Datei zunächst komprimieren. Diese Funktion unterbindet daher die Komprimierung von Dateianlagen nicht vollständig – sie verhindert nur, dass Dateianlagen in komprimierter Form versandt werden, wenn bei der Komprimierung der angegebene Wirkungsgrad nicht überschritten werden kann. Stellt MDaemon also nach der Komprimierung fest, dass der Wert nicht übertroffen werden konnte, wird die gepackte Datei verworfen. Die Dateianlagen bleiben dann im ursprünglichen Zustand bei der Nachricht.

Komprimieren, falls die Dateigröße der Anlagen insgesamt [xx] KB überschreitet
Bei automatischer Komprimierung packt MDaemon die Dateianlagen nur dann, wenn ihre Gesamtgröße den hier angegebenen Wert übersteigt. Nachrichten, deren Dateianlagen den Wert nicht überschreiten, werden zugestellt, ohne dass die Anlagen komprimiert werden.

Komprimierungsgrad
In diesem Rollmenü kann ausgewählt werden, wie stark die Dateianlagen komprimiert werden sollen. Es stehen drei Stufen zur Verfügung: minimal (schnellste Methode bei geringstem Wirkungsgrad), mittel (Vorgabe), oder maximal (langsamste Methode bei größtem Wirkungsgrad).

Festen Archivnamen verwenden: [Archivname]
Diese Option bewirkt, dass bei allen automatisch komprimierten Dateianlagen nur der hier angegebene Dateiname für das Archiv verwendet wird.

Ausnahmen von der Komprimierung

Ausschluss von Dateien
Diese Option legt fest, welche Dateien von der automatischen Komprimierung ausgenommen sind. Dateianlagen, die auf die hier erfassten Namen passen, werden nicht gepackt – und zwar unabhängig von den sonstigen Einstellungen. Jokerzeichen sind zulässig. Es darf also beispielsweise "*.exe" angegeben werden; damit wären alle Dateien mit der Endung ".exe" von der Komprimierung ausgenommen.

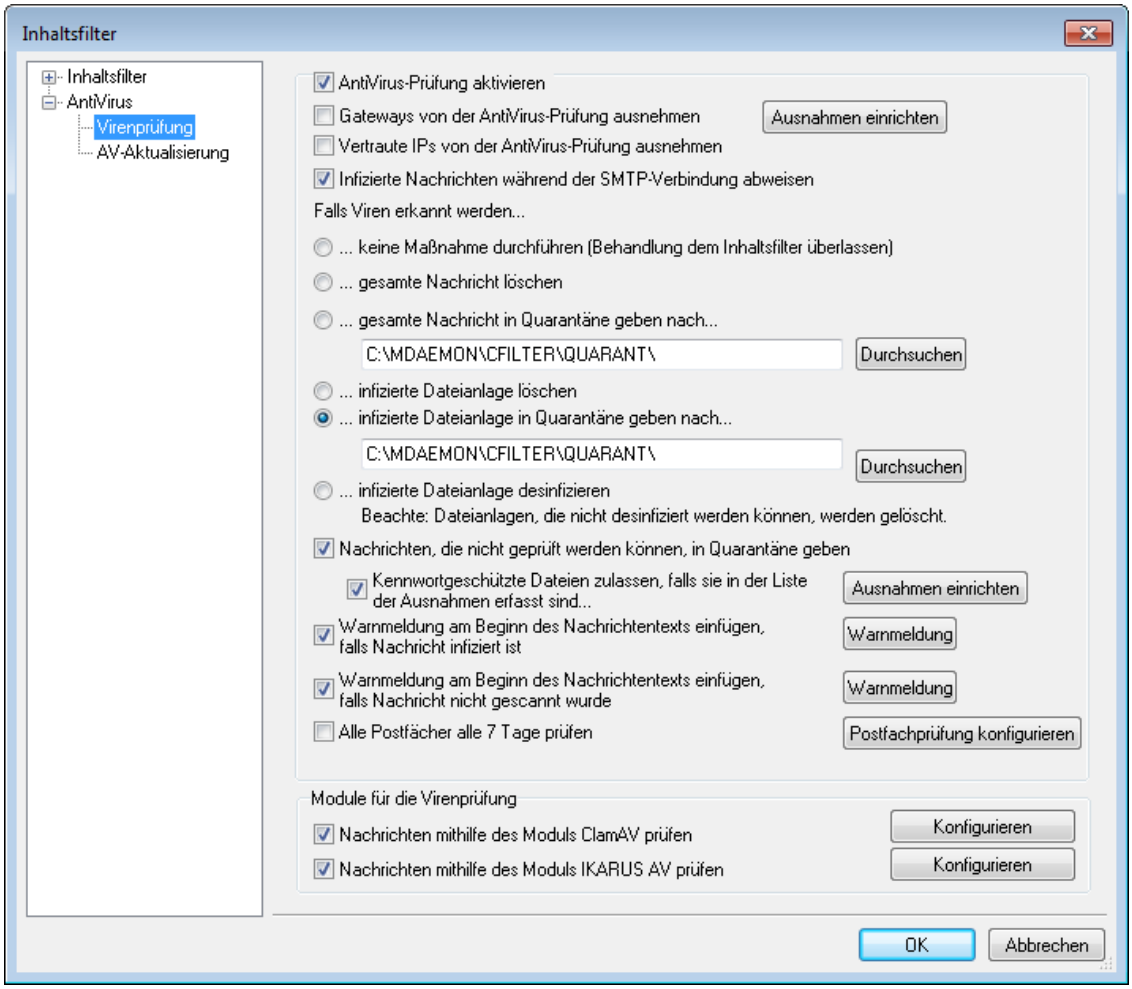
Ausschluss von Domänen
Hier lassen sich Empfängerdomänen angeben, die von der automatischen Komprimierung ausgenommen sind. Nachrichten an diese Domänen werden – unabhängig von den sonstigen Einstellungen – mit unkomprimierten Dateianlagen zugestellt.

Dateianlagen in Dateien Winmail.dat

Dateianlagen aus Dateien winmail.dat (Microsoft-Outlook-Nachrichten im Format RTF) entnehmen
Diese Option bewirkt, dass Dateien aus Dateianlagen winmail.dat entnommen und in Standard-Dateianlagen der Kodierung MIME umgewandelt werden.

4.5.2 AntiVirus

4.5.2.1 Virenprüfung



Die Optionen in diesem Konfigurationsdialog sind nur verfügbar, wenn das optional erhältliche Leistungsmerkmal MDaemon AntiVirus 671 eingesetzt wird. Wenn Sie MDaemon AntiVirus erstmals aktivieren, beginnt hierdurch ein 30 Tage dauernder Testzeitraum. Lizenzen für dieses Leistungsmerkmal können Sie über Ihren autorisierten Reseller für MDaemon oder auf der Website www.mdaemon.com kaufen.

AntiVirus-Prüfung aktivieren

Mithilfe dieser Option aktivieren Sie die Prüfung von Nachrichten auf Viren. Geht bei MDaemon eine Nachricht mit einer Dateianlage oder mehreren Dateianlagen ein, so prüft MDaemon die Nachricht vor der Zustellung auf Viren.

Gateways von der AntiVirus-Prüfung ausnehmen

Sollen Nachrichten an einen Domänen-Gateway von MDaemon von der Virenprüfung ausgenommen werden, ist diese Option zu aktivieren. Diese

Vorgehensweise kann wünschenswert sein, wenn die Virenprüfung dem eigenen Mailserver der Zieldomäne überlassen werden soll. Nähere Informationen über Domänen-Gateways finden Sie im Abschnitt Gateway-Manager 250.

Ausnahmen einrichten
Der Menüpunkt Ausnahmen einrichten erlaubt die Angabe von Empfängeradressen, die von der Virenprüfung ausgenommen sind. Nachrichten an diese Adressen werden nicht auf Viren geprüft. Bei den ausgeschlossenen Adressen sind Jokerzeichen zulässig. Es lassen sich somit auch ganze Domänen oder bestimmte Postfächer in allen Domänen von der Prüfung ausnehmen. Beispiele: "*@example.com" oder "VirenArchiv@*".

Vertraute IPs von der AntiVirus-Prüfung ausnehmen
Diese Option bewirkt, dass Nachrichten dann von der AntiVirus-Prüfung ausgenommen sind, wenn sie durch eine Ihrer Vertrauten IP-Adressen 521 übermittelt wurden.

Infizierte Nachrichten während der SMTP-Verbindung abweisen
Diese Option bewirkt, dass eingehende Nachrichten bereits während der laufenden SMTP-Übertragung schritthaltend, und nicht erst nach Eingang der vollständigen Nachricht, auf Viren geprüft werden. MDaemon weist Nachrichten, in denen Viren entdeckt werden, sofort ab. Da jede eingehende Nachricht auf Viren geprüft wird, noch bevor MDaemon die vollständig übertragene Nachricht zur Zustellung entgegengenommen, dies der Gegenstelle mitgeteilt und die Verbindung beendet hat, bleibt der Mailserver des Absenders weiter für die Nachricht verantwortlich. Die Nachricht kann sofort abgewiesen werden, wenn ein Virus gefunden wird, und in diesem Falle sind keine weiteren AntiVirus-Aktionen erforderlich. Die Optionen für die Behandlung vireninfizierter Nachrichten, die auf diesem Dialog konfiguriert werden, kommen nicht zu Anwendung. Die Nachrichten werden nicht in Quarantäne gegeben, und es werden keine Warnnachrichten versandt. Die Zahl der verseuchten Nachrichten und der Warnmeldungen, die die Benutzer empfangen, kann damit erheblich verringert werden.

Das Protokoll SMTP-(eing.) erfasst die Ergebnisse der Virenprüfung. Dabei können folgende Meldungen angezeigt werden:

- Die Nachricht wurde geprüft, und es wurde ein Virus gefunden.
- Die Nachricht wurde geprüft und war virenfrei.
- Die Nachricht konnte nicht geprüft werden (üblicherweise bei ZIP-Dateien oder wenn die Dateianlage nicht geöffnet werden konnte).
- Die Nachricht konnte nicht schritthaltend geprüft werden, weil sie zu groß war.
- Während der Prüfung ist ein Fehler aufgetreten.

Falls Viren erkannt werden...
Die Optionen in diesem Abschnitt legen fest, welche Maßnahmen MDaemon ergreifen soll, falls AntiVirus einen Virus erkennt.

...keine Maßnahme durchführen (Behandlung dem Inhaltsfilter überlassen)
Diese Option bewirkt, dass keine der genannten Maßnahmen ergriffen wird. Die Bearbeitung erfolgt dann nur noch durch den Inhaltsfilter, in dem entsprechende Regeln vorgesehen sein müssen.

...gesamte Nachricht löschen
Ist diese Option aktiv, so wird die gesamte Nachricht, nicht nur die verseuchte Dateianlage, gelöscht, wenn ein Virus festgestellt wurden. Da hierbei die gesamte Nachricht verloren geht, kann ihr auch kein Hinweistext mehr hinzugefügt werden. Stattdessen kann aber der Empfänger mit Hilfe der Optionen im Konfigurationsdialog "Benachrichtigung" verständigt werden.

...gesamte Nachricht in Quarantäne geben nach...
Diese Option arbeitet ähnlich wie die vorstehende Option "*gesamte Nachricht löschen*", die Nachricht wird aber in dem angegebenen Pfad in Quarantäne gegeben und nicht gelöscht.

...infizierte Dateianlage löschen
Hiermit wird die infizierte Dateianlage gelöscht. Die Nachricht selbst wird dem Empfänger zugestellt, jedoch ohne die fragliche Dateianlagen. Mit der Option "*Warnmeldung...*" kann solchen Nachrichten ein Text hinzugefügt werden, der den Empfänger davon informiert, dass eine vireninfizierte Dateianlage gelöscht wurde.

...infizierte Dateianlage in Quarantäne geben nach...
Soll die verseuchte Dateianlage nicht gelöscht oder gesäubert werden, so kann man hier einen Pfad angeben, in den die Dateianlage statt dessen verschoben wird. Wie bei der Option zur Löschung verseuchter Dateianlagen, so wird auch hier die Nachricht selbst dem Empfänger zugestellt – allerdings ohne die Dateianlage.

...infizierte Dateianlage desinfizieren
Diese Option bewirkt, dass AntiVirus versucht, die infizierte Dateianlage zu desinfizieren. Falls dies nicht gelingt, wird die Dateianlage gelöscht.

Nachrichten, die nicht geprüft werden können, in Quarantäne geben
Diese Option bewirkt, dass MDaemon Nachrichten in Quarantäne gibt, falls die Nachrichten nicht auf Viren geprüft werden konnten, etwa, weil die Nachrichten kennwortgeschützte Dateien enthielten.

Kennwortgeschützte Dateien zulassen, falls sie in der Liste der Ausnahmen erfasst sind...
Diese Option bewirkt, dass Nachrichten mit kennwortgeschützten Dateianlagen, die deswegen nicht auf Viren geprüft werden konnten, den AntiVirus-Scanner durchlaufen dürfen. Diese Option wirkt auf alle Nachrichten mit Dateianlagen, deren Dateinamen in der Liste der Ausnahmen erfasst sind.

Ausnahmen einrichten
Durch Anklicken dieses Steuerelements kann die Liste der Ausnahmen verwaltet werden. Dateien, deren Namen und Endung hier erfasst sind, werden nicht geprüft.

Warnmeldung am Beginn des Nachrichtentexts einfügen, falls Nachricht infiziert ist
Ist eine der oben stehenden Optionen zur Bearbeitung von Dateianlagen aktiv, so kann mithilfe dieser Option dem Nachrichtentext der vormals infizierten Nachricht ein Hinweis vorangestellt werden, bevor die Nachricht dem Empfänger zugestellt wird. Der Empfänger kann beispielsweise darüber informiert werden, dass eine Dateianlage entfernt wurde, und aus welchem Grund dies geschah.

Warnmeldung
Ein Klick auf dieses Steuerelement zeigt den Text der Warnmeldung an, die bei entsprechend gesetzter Option am Beginn des Nachrichtentexts eingefügt wird. Nachdem alle gewünschte Änderungen erledigt sind, schließt ein Klick auf **OK** das Fenster und speichert die Änderungen.

Warnmeldung am Beginn des Nachrichtentexts einfügen, falls Nachricht nicht gescannt wurde
Wurde eine Nachricht nicht auf Viren geprüft, so kann mithilfe dieser Option dem Nachrichtentext der Nachricht ein Hinweis vorangestellt werden, bevor die Nachricht dem Empfänger zugestellt wird. Der Empfänger kann beispielsweise darüber informiert werden, dass die Nachricht nicht auf Viren geprüft wurde.

Warnmeldung
Ein Klick auf dieses Steuerelement zeigt den Text der Warnmeldung an, die bei entsprechend gesetzter Option am Beginn des Nachrichtentexts eingefügt wird. Nachdem alle gewünschte Änderungen erledigt sind, schließt ein Klick auf **OK** das Fenster und speichert die Änderungen.

Alle Postfächer alle *x* Tage prüfen
Diese Option bewirkt, dass alle gespeicherten Nachrichten in regelmäßigen Zeitabständen auf Viren geprüft werden. Mithilfe einer solchen turnusgemäßen Prüfung können auch infizierte Nachrichten entdeckt werden, die zum Zeitpunkt ihrer ursprünglichen Zustellung noch nicht als infiziert erkannt werden konnten, etwa, weil eine die passende Signatur enthaltende Virendefinition erst nach der Zustellung verfügbar wurde. Infizierte Nachrichten werden in Quarantäne gegeben, und ihnen wird die Kopfzeile `X-MDBadQueue-Reason` hinzugefügt. Anhand des Inhalts dieser Kopfzeile können Sie in MDaemon weitere Erklärungen erhalten. Nachrichten, die nicht geprüft werden können, werden auch nicht in Quarantäne gegeben.

Postfachprüfung konfigurieren
Mithilfe dieser Schaltfläche können Sie festlegen, wie oft die Nachrichten geprüft werden sollen, und ob jeweils alle Nachrichten oder nur Nachrichten bis zu einem bestimmten Alter geprüft werden sollen. Sie können auch eine sofortige Prüfung aller Postfächer veranlassen.

Module für die Virenprüfung

MDaemon AntiVirus ist mit zwei Modulen für die Virenprüfung ausgerüstet: ClamAV und Cyren Anti-Virus. Sind beide Module aktiv, so werden die Nachrichten durch beide Module geprüft, und zwar zuerst durch Cyren Anti-Virus und danach durch ClamAV. Hierdurch wird das Schutzniveau erhöht, da ein Virus durch ein Modul möglicherweise bereits erkannt wird, bevor die Signaturen für das andere Modul entsprechend aktualisiert wurden.

Nachrichten mithilfe des Moduls ClamAV prüfen
Um die Nachrichten durch das Modul ClamAV prüfen zu lassen, aktivieren Sie diese Option.

Konfigurieren
Durch Anklicken dieser Schaltfläche rufen Sie einen Konfigurationsdialog für die Protokollierung für ClamAV im Detailgrad Debug auf. Die entsprechende Protokolldatei wird im Verzeichnis log unter dem MDaemon-Hauptverzeichnis gespeichert.

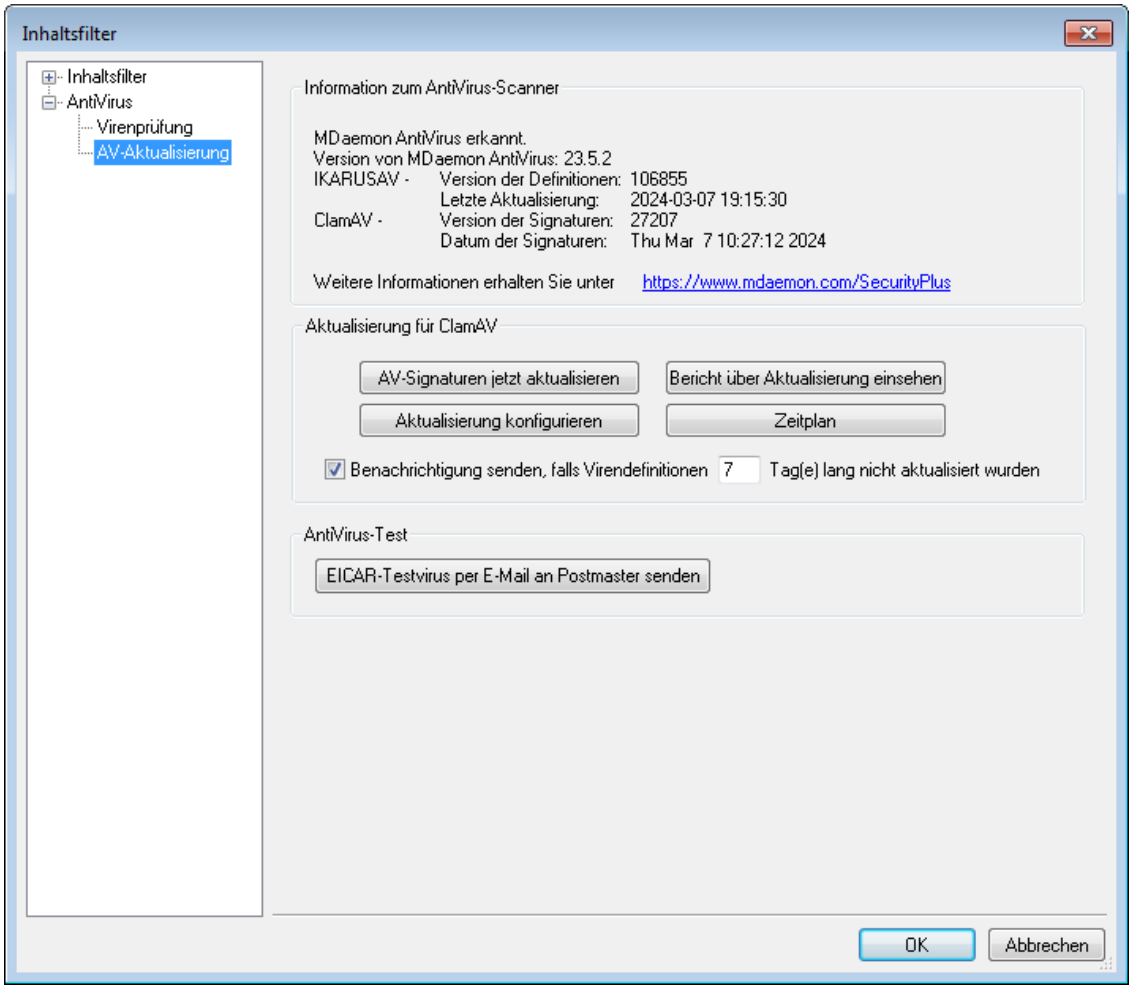
Nachrichten mithilfe des Moduls Cyren Anti-Virus prüfen
Um die Nachrichten durch das Modul Cyren Anti-Virus prüfen zu lassen, aktivieren Sie diese Option.

Konfigurieren
Durch Anklicken dieser Schaltfläche rufen Sie den Konfigurationsdialog für Cyren Anti-Virus auf. Sie können hier die Option "*Dateianlagen als Viren kennzeichnen, falls sie Makros enthalten*" und die gewünschte Heuristik-Stufe konfigurieren. Es stehen Stufen von -1 bis 5 zur Verfügung, wobei "-1" für automatisch, "0" für deaktiviert und 1-5 für die niedrigste bis zur höchsten Heuristik-Stufe stehen.

Siehe auch:

AV-Aktualisierung 675
Inhaltsfilter und AntiVirus 648

4.5.2.2 AV-Aktualisierung



Die Optionen in diesem Konfigurationsdialog sind nur verfügbar, wenn das optional erhältliche Leistungsmerkmal MDaemon AntiVirus 671 eingesetzt wird. Wenn Sie MDaemon

> AntiVirus erstmals aktivieren, beginnt hierdurch ein 30 Tage dauernder Testzeitraum. Lizenzen für dieses Leistungsmerkmal können Sie über Ihren autorisierten Reseller für MDaemon oder auf der Website www.mdaemon.com kaufen.

Mithilfe der Optionen in diesem Konfigurationsdialog können Sie die automatische und manuelle Aktualisierung der Virendefinitionen und Signaturdateien konfigurieren. Für die automatische Aktualisierung steht ein Zeitplan zur Verfügung. Mithilfe eines Protokollbetrachters können Sie prüfen, wann welche Aktualisierungen abgerufen wurden. Mithilfe eines Funktionstests können Sie sich bestätigen lassen, dass die Virenprüfung ordnungsgemäß arbeitet.

Information zum AntiVirus-Scanner

Die Informationen in diesem Abschnitt geben Aufschluss darüber, ob AntiVirus verfügbar ist, und welche Version Sie einsetzen. Sie geben weiter Aufschluss über die Version und den Zeitpunkt der letzten Aktualisierung der Virendefinitionen.

Cyren-Anti-Virus-Aktualisierung

AV-Signaturen jetzt aktualisieren
Durch Anklicken dieser Schaltfläche können Sie die Virendefinitionen manuell aktualisieren. Die Aktualisierung wird sofort nach Anklicken der Schaltfläche durchgeführt.

Aktualisierung konfigurieren
Durch Anklicken dieser Schaltfläche rufen Sie den Konfigurationsdialog Konfiguration der Aktualisierungsroutine 678 auf. Dieser Konfigurationsdialog ist unterteilt in die vier Registerkarten *URLs für die Aktualisierung*, *Verbindung, Proxy* und *Verschiedenes*.

Bericht über Aktualisierung einsehen
Durch Anklicken dieser Schaltfläche öffnen Sie den Protokollbetrachter für die AntiVirus-Aktualisierung. Hier erscheinen für jede Aktualisierung der Zeitpunkt, Informationen über die ausgeführten Aktionen und weitere Informationen.

Zeitplan
Durch Anklicken dieser Schaltfläche rufen Sie den Zeitplan für die AntiVirus-Aktualisierungen 377 auf. Hier können Sie die Zeitpunkte festlegen, zu denen die Aktualisierungen durchgeführt werden, und Sie können Intervalle zwischen den Aktualisierungen konfigurieren.

ClamAV-Aktualisierung

Bericht über Aktualisierung einsehen
Durch Anklicken dieser Schaltfläche öffnen Sie den Protokollbetrachter für die AntiVirus-Aktualisierung. Hier erscheinen für jede Aktualisierung der Zeitpunkt, Informationen über die ausgeführten Aktionen und weitere Informationen.

Benachrichtigung senden, falls Virendefinitionen nicht aktualisiert wurden seit [xx] Tagen
Diese Option bestimmt, nach wie vielen Tagen der Administrator davon verständigt wird, dass die Virendefinitionen für ClamAV nicht aktualisiert wurden und somit veraltet sind.

AntiVirus-Test

EICAR-Testvirus per E-Mail an Postmaster senden
Durch Anklicken dieser Schaltfläche wird eine Testnachricht an den Postmaster gesendet. An dieser Testnachricht befindet sich als Dateianlage eine EICAR-Virendatei. Diese Dateianlage ist völlig ungefährlich und dient nur dazu, die Virenprüfung und die zugehörigen Leistungsmerkmale zu testen. Im Protokollfenster des Inhaltsfilters auf der Benutzeroberfläche können Sie verfolgen, wie MDaemon mit dieser Nachricht verfährt, sobald sie eingegangen ist. In Abhängigkeit von den Einstellungen im Einzelfall ergibt sich ein Protokoll wie etwa das folgende:

```
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 from: postmaster@example.com
Mon 2008-02-25 18:14:49: > Message to: postmaster@example.com
Mon 2008-02-25 18:14:49: > Message subject: EICAR Test Message
Mon 2008-02-25 18:14:49: > Message ID:
<MDAEMON10001200202251814.AA1447619@example.com>
Mon 2008-02-25 18:14:49: Performing viral scan...
Mon 2008-02-25 18:14:50: > eicar.com is infected by EICAR-Test-File
Mon 2008-02-25 18:14:50: > eicar.com was removed from message
Mon 2008-02-25 18:14:50: > eicar.com quarantined to C:
\MDAEMON\CFILTER\QUARANT\
Mon 2008-02-25 18:14:50: > Total attachments scanned    : 1
(including multipart/alternatives)
Mon 2008-02-25 18:14:50: > Total attachments infected   : 1
Mon 2008-02-25 18:14:50: > Total attachments disinfected: 0
Mon 2008-02-25 18:14:50: > Total attachments removed    : 1
Mon 2008-02-25 18:14:50: > Total errors while scanning  : 0
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (sender)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (recipient)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (admin)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (admin)
Mon 2002-02-25 18:14:50: Processing complete (matched 0 of 12 active
rules)
```

Siehe auch:

Konfiguration der Aktualisierungsroutine 678
AntiVirus 671
Inhaltsfilter und AntiVirus 648

4.5.2.2.1 Konfiguration der Aktualisierungsroutine

Klicken Sie im Konfigurationsdialog AV-Aktualisierung 675 auf *Aktualisierung konfigurieren*, um die Aktualisierungsroutine zu konfigurieren. Es öffnet sich ein Fenster, das folgende vier Registerkarten enthält:

URLs für die Aktualisierung
Diese Registerkarte enthält die Liste der Server, die AntiVirus nach Aktualisierungen abfragt. Sie können die Reihenfolge selbst bestimmen, in der die Server abgefragt werden, oder sie können die Server in zufälliger Reihenfolge abfragen lassen.

Verbindung
Auf dieser Registerkarte wird das Verbindungsprofil für die Internetverbindung festgelegt, die AntiVirus bei der Suche nach Aktualisierungen nutzen soll. Es können die Internet-Einstellungen aus der Systemsteuerung oder manuell eingetragene Einstellungen verwendet werden. Sie können dabei den Eintrag im RAS-Telefonbuch sowie Benutzername und Kennwort angeben.

Proxy
Hier können HTTP- und FTP-Proxies konfiguriert werden, falls sie für die Verbindung zu den Sites nötig sind.

Verschiedenes
Diese Registerkarte enthält verschiedene Einstellungen zur Protokollierung. Es können eine Protokolldatei ausgewählt und eine Maximalgröße für das Protokoll festgelegt werden.

Siehe auch:

AV-Aktualisierung 675
AntiVirus 671
Inhaltsfilter und AntiVirus 648

4.6 Spam-Filter

4.6.1 Spam-Filter

Der Spam-Filter ist eine der wichtigsten der umfangreichen Schutzmaßnahmen, die MDaemon gegen Spam bietet. Der Spam-Filter setzt eine Technik ein, mit deren Hilfe eingehende E-Mail-Nachrichten heuristisch untersucht werden können, um dann nach einem umfassenden und differenzierten Regelwerk bewertet zu werden. Anhand der Bewertung stellt das System fest, wie sicher es ist, dass es sich bei einer Nachricht um Spam handelt; das Ergebnis dieser Prüfung wiederum kann bestimmte Aktionen auslösen. So kann die Nachricht unter anderem abgewiesen oder als möglicher Spam gekennzeichnet werden.

Bestimmte Adressen können in die Freigabelisten und die Sperrlisten aufgenommen oder von der Prüfung durch den Spam-Filter vollständig ausgenommen werden. Ein Bericht über Einzelheiten zu der Spam-Prüfung kann in die Nachrichten eingefügt werden. Er gibt Auskunft über die Bewertung einer Nachricht und ihre Grundlage; der Bericht kann auch als gesonderte Nachricht versandt werden, in die das System die Ursprungsnachricht als Anlage einfügt. Weiter kann ein ebenfalls implementiertes

Bayes'sches 683 Lernverfahren dem Spam-Filter sogar helfen, zu lernen, Spam treffsicherer zu erkennen und damit mit der Zeit immer zuverlässiger zu werden.

Die Regeln wurden durch die Auswertung tausender Spam-Nachrichten mit der Zeit immer mehr verfeinert und ermöglichen eine sehr treffsichere Erkennung einer Nachricht als Spam. Die Regeln des Spam-Filters lassen sich jedoch durch Bearbeiten der entsprechenden Konfigurationsdateien an die eigenen Bedürfnisse anpassen, auch das Hinzufügen völlig neuer Regeln ist möglich.

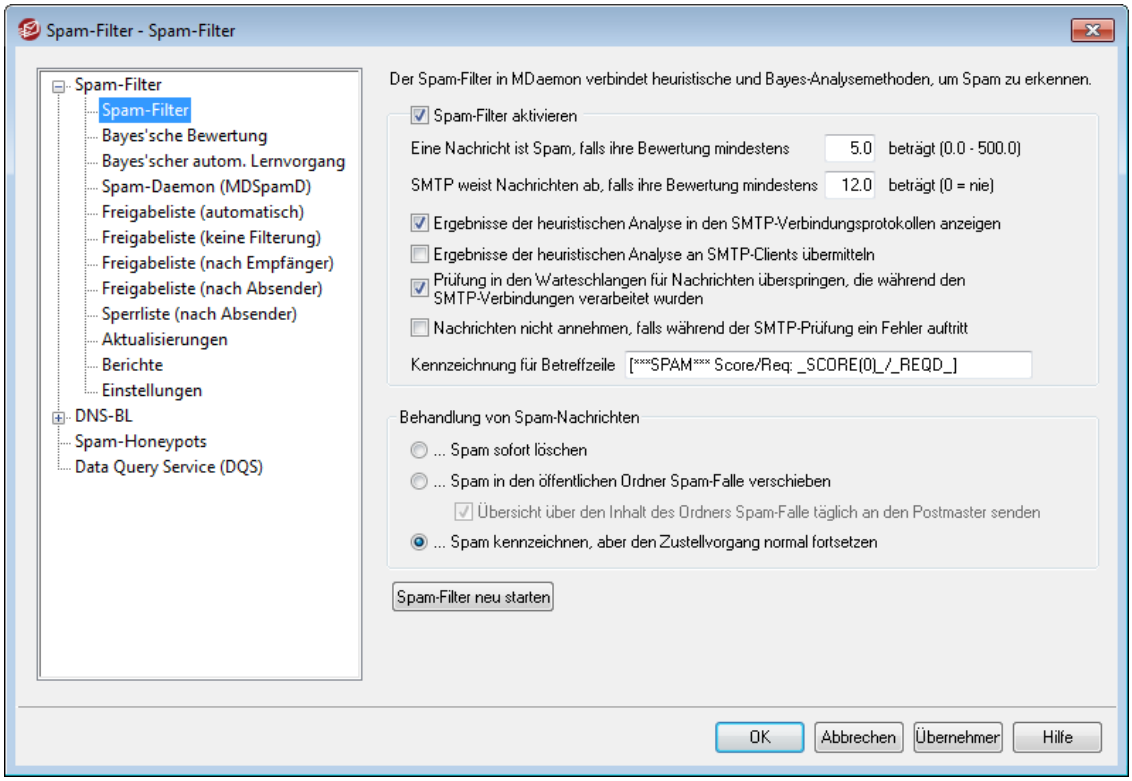
Der Spam-Filter in MDaemon nutzt als Programmkern eine beliebte heuristische Open-Source-Technik. Die Website für das Open-Source-Projekt finden Sie unter:

```
http://www.spamassassin.org
```

Siehe auch:

Spam-Filter 679
Sperrlisten für DNS 704

4.6.1.1 Spam-Filter



Spam-Filter aktivieren

Diese Option aktiviert den Spam-Filter einschließlich der heuristischen Bewertung von Nachrichten. Die weiteren Optionen in diesem Konfigurationsdialog sind nur verfügbar, wenn diese Option aktiv ist.

Eine Nachricht ist Spam, falls ihre Bewertung mindestens [xx] beträgt (0.0 - 500.0)
Der Wert, den Sie hier angeben, ist der Schwellwert, den MDaemon mit der Spam-Bewertung jeder Nachricht vergleicht. Eine Nachricht, deren Spam-Bewertung diesen Wert erreicht oder überschreitet, wird als Spam behandelt, und

es werden, je nach den Einstellungen des Spam-Filters, die nötigen Maßnahmen durchgeführt.

SMTP weist Nachrichten ab, falls ihre Bewertung mindestens [xx] beträgt (0 = nie)
Mithilfe dieser Option können Sie einen Schwellwert bestimmen, ab dem Nachrichten abgewiesen werden. Erreicht oder überschreitet die Spam-Bewertung einer Nachricht diesen Wert, so wird sie nicht weiterverarbeitet und möglicherweise zugestellt, sondern sie wird direkt abgewiesen. Der Wert dieser Option soll immer höher angesetzt sein als der Wert der Option "*Eine Nachricht ist Spam, falls ihre Bewertung...*" weiter oben. Andernfalls können auf eine Nachricht, die einmal als Spam erkannt wurde, die weiteren Optionen des Spam-Filters nicht mehr wirken; sie würde in j4edem Falle während der Zustellung abgewiesen. Der Wert 0 unterbindet die Prüfung während der SMTP-Verbindung; sie müssen diesen Wert setzen, falls MDaemon Nachrichten unabhängig von ihrer Bewertung nie vollständig abweisen soll. Falls die SMTP-Prüfung deaktiviert ist, wird dennoch eine Prüfung in den Warteschlangen durchgeführt, nachdem die Nachricht übermittelt wurde. Die Voreinstellung für diese Option beträgt 12.0.

Ein Beispiel hierzu:

Falls der Schwellwert für die Spam-Bewertung auf 5.0 und der Schwellwert zum Abweisen auf 10.0 gesetzt ist, werden alle Nachrichten mit einer Spam-Bewertung von mindestens 5.0, aber unter 10.0 als Spam bewertet und in Übereinstimmung mit den weiteren Einstellungen des Spam-Filters behandelt. Alle Nachrichten mit einer Spam-Bewertung von mindestens 10.0 weist MDaemon noch während der Zustellung ab.

Sie sollten die Leistung des Spam-Filters überwachen und mit der Zeit die Schwellwerte für die Bewertung als Spam und zum Abweisen von Nachrichten auf Ihre Bedürfnisse anpassen. In den meisten Fällen erfasst ein Schwellwert von 5.0 als Grenze für die Erkennung von Spam die meisten Spam-Nachrichten und lässt nur wenige falsche negative Treffer (Spam-Nachrichten, die unerkannt ins System gelangen) passieren. Es treten auch nur wenige falsche positive Treffer (normale Nachrichten, die als Spam behandelt werden) auf. Ein Schwellwert zum Abweisen von Nachrichten von 10-15 führt dazu, dass nur Nachrichten, die fast ganz sicher Spam sind, abgewiesen werden. Es kommt nur sehr selten vor, dass eine legitime Nachricht eine so hohe Bewertung aufweist. Die Voreinstellung für den Schwellwert zum Abweisen beträgt 12.

Ergebnisse der heuristischen Analyse in den SMTP-Verbindungsprotokollen anzeigen
Diese Option bewirkt, dass die Ergebnisse der heuristischen Prüfung während der SMTP-Verbindung in den SMTP-Verbindungsprotokollen erfasst werden 175.

Ergebnisse der heuristischen Analyse an SMTP-Clients übermitteln
Diese Option bewirkt, dass die Ergebnisse der heuristischen Verarbeitung als Teil der SMTP-Verbindungsmitschnitte übermittelt werden. Falls der Schwellwert zum Abweisen von Spam auf 0 gesetzt ist, kann diese Option nicht genutzt werden, da dann Spam aufgrund der Bewertung keinesfalls während der SMTP-Verbindung abgewiesen wird. Weitere Informationen hierzu finden Sie im Abschnitt "*SMTP weist Nachrichten ab, falls ihre Bewertung mindestens [xx] beträgt (0=nie)*" weiter oben.

Prüfung in den Warteschlangen für Nachrichten überspringen, die während den SMTP-Verbindungen verarbeitet wurden
MDaemon prüft per Voreinstellung die Nachrichten während der SMTP-Verbindung, um festzustellen, ob ihre Spam-Bewertung über dem Schwellwert zum Abweisen liegt und sie daher abgewiesen werden müssen. MDaemon prüft bei der zur Zustellung angenommenen Nachrichten dann die Nachrichten erneut, sobald sie in die Warteschlange eingestellt wurden. MDaemon behandelt dann die Nachrichten in Abhängigkeit von ihrer Spam-Bewertung und der Konfiguration des Spam-Filters. Diese Option bewirkt, dass MDaemon die Prüfung in der Warteschlange unterlässt und die Ergebnisse der Prüfung durch den Spam-Filter während der SMTP-Verbindung als endgültig ansieht. Dies kann die Systemlast erheblich verringern und die Effizienz des AntiSpam-Systems deutlich erhöhen. Es werden dann aber, wenn keine Prüfung in den Warteschlangen stattfindet, nur die Standard-Kopfzeilen des SpamAssassins in die Nachrichten eingefügt. Falls Sie Änderungen an den Standard-Kopfzeilen des SpamAssassins vorgenommen haben oder in der Datei `local.cf` benutzerdefinierte Kopfzeilen hinterlegt haben, werden diese Änderungen und zusätzlichen Kopfzeilen ignoriert.

Nachrichten nicht annehmen, falls während der SMTP-Prüfung ein Fehler auftritt
Diese Option bewirkt, dass Nachrichten abgewiesen werden, falls während der Prüfung während der SMTP-Verbindung ein Fehler auftritt.

Kennzeichnung für Betreffzeile
Die hier definierte Kennzeichnung wird am Beginn der Betreffzeile aller Nachrichten eingefügt, die den Schwellwert für die Spam-Bewertung erreichen oder überschreiten. Sie kann Informationen über die Spam-Bewertung enthalten, und Sie können mithilfe der IMAP-Nachrichtenfilter nach der Bewertung suchen und die Nachricht entsprechend filtern (dies ist aber nur möglich, falls der Spam-Filter so konfiguriert ist, dass er auch als Spam erkannte Nachrichten zustellt). Dies ist eine einfache Methode für die automatische Sortierung von Spam-Nachrichten in einen besonderen "Spam-Ordner". Falls Sie die Spam-Bewertung und den anwendbaren Schwellwert dynamisch in die Kennzeichnung einfügen wollen, können Sie die Makros "`_HITS_`" für die Bewertung der Nachricht und "`_REQD_`" für den erforderlichen Schwellwert nutzen. Anstatt von "`_SCORE(0)_`" können Sie auch "`_HITS_`" einsetzen; hierdurch wird einstelligen Bewertungen eine Ziffer 0 vorangestellt, sodass sich die Nachrichten bei Sortierung nach der Betreffzeile in E-Mail-Clients richtig sortiert darstellen lassen.

Ein Beispiel hierzu:

> Die Kennzeichnung `***SPAM*** Bewertung/Schwelle: _HITS_/_REQD_ -` bewirkt, dass in einer Spam-Nachricht mit einer Bewertung von 6.2 und dem Betreff "Hallo, hier kommt Spam!" die Betreffzeile geändert wird in "***SPAM*** Bewertung/Schwelle: 6.2/5.0 – Hallo, hier kommt Spam!"
>
> Wird "`_SCORE(0)_`" durch "`_HITS_`" ersetzt, so ergibt sich die Betreffzeile "***SPAM*** Bewertung/Schwelle: 06.2/5.0 – Hallo, hier kommt Spam!"

Falls Sie die Betreffzeile nicht ändern wollen, lassen Sie dieses Textfeld leer. Es wird dann keine Kennzeichnung in die Betreffzeile eingefügt.

Diese Option ist nicht verfügbar, falls MDaemon den MDaemon-Spam-Daemon (MDSpamD) eines anderen MDaemon-Servers für den Spam-Filter verwendet. Die

> Konfiguration der Betreffzeile wird dann durch die anderen Einstellungen des Servers bestimmt. Weitere Informationen enthält der Abschnitt Spam-Daemon 689.

Behandlung von Spam-Nachrichten

Falls die Spam-Bewertung einer Nachricht den oben angegebenen Schwellwert erreicht oder überschreitet, führt der Spam-Filter die nachfolgend ausgewählte Aktion durch.

...Spam sofort löschen
Diese Option bewirkt, dass eingehende Nachrichten gelöscht werden, falls ihre Spam-Bewertung den Schwellwert erreicht oder überschreitet.

...Spam in den öffentlichen Ordner Spam-Falle verschieben
Diese Option bewirkt, dass Nachrichten, die als Spam erkannt wurden, gekennzeichnet und dann in den öffentlichen Ordner Spam-Falle verschoben werden. Sie werden nicht an die Empfänger zugestellt.

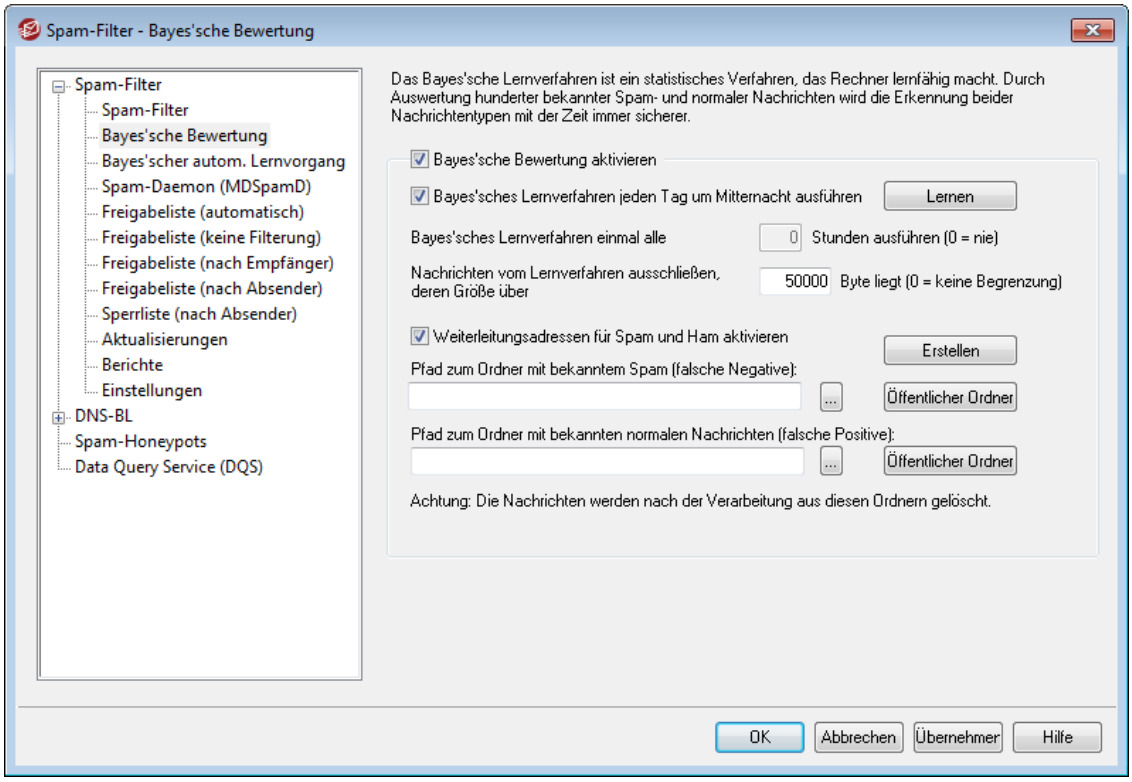
Übersicht über den Inhalt des Ordners Spam-Falle täglich an den Postmaster senden
Bei Nutzung der Option *...Spam in den öffentlichen Ordner Spam-Falle verschieben* weiter oben können Sie diese Option aktivieren; der Postmaster erhält dann einmal täglich eine Übersicht über die Inhalte des Ordners Spam-Falle.

...Spam kennzeichnen, aber den Zustellvorgang normal fortsetzen
Diese Option bewirkt, dass alle Spam-Nachrichten an die beabsichtigten Empfänger zugestellt, zuvor aber durch Einfügen verschiedener Spam-Kopfzeilen und Kennzeichnungen gekennzeichnet werden, die weiter oben und im Abschnitt Berichte 700 konfiguriert werden. Diese Option ist per Voreinstellung aktiv. Sie gestattet den Benutzern, die Nachrichten automatisch in bestimmte Ordner zu sortieren und sie dann selbst durchzusehen, und sie vermeidet damit den Verlust von Nachrichten, die irrtümlich als Spam erkannt wurden (sog. falsche positive Treffer).

Spam-Filter neu starten

Um den Spam-Filter neu zu starten, klicken Sie auf diese Schaltfläche.

4.6.1.2 Bayes'sche Bewertung



Der Konfigurationsdialog Bayes ist nicht verfügbar, falls MDaemon den MDaemon-Spam-Daemon (MDSpamD) eines anderen MDaemon-Servers für den Spam-Filter verwendet. Alle Bayes'schen Lernvorgänge werden dann auf dem anderen Server durchgeführt. Weitere Informationen enthält der Abschnitt Spam-Daemon 689.

Der Spam-Filter unterstützt das Bayes'sche Lernverfahren, ein statistisches Verfahren, das wahlweise zur Analyse von Spam- und normalen Nachrichten eingesetzt werden kann, um die Treffsicherheit des Spam-Filters mit der Zeit zu erhöhen. Der Benutzer kann zwei Verzeichnisse angeben, eines für bekannte Spam- und eines für bekannte normale Nachrichten, die beide jeweils um Mitternacht verarbeitet werden. Alle Nachrichten in den Verzeichnissen werden analysiert und indiziert. Neue Nachrichten können mit den hieraus gewonnenen Erkenntnissen statistisch verglichen werden, um festzustellen, ob es sich um Spam handelt. Anhand der Ergebnisse des Bayes'schen Verfahrens kann der Spam-Filter dann die Bewertungen der Nachrichten anpassen.

Der Spam-Filter wendet die Ergebnisse des Bayes'schen Lernverfahrens erst an, wenn mindestens die Anzahl an Spam- und normalen Nachrichten analysiert wurde, die im Konfigurationsdialog Bayes'scher automatischer Lernvorgang 687 festgelegt sind. Dies ist erforderlich, weil der Spam-Filter sonst keine ausreichende statistische Datenbasis hat, um Vergleiche nach dem Bayes'schen

Verfahren durchzuführen. Hat das System diese Nachrichten analysiert, so hat es eine ausreichende Datenbasis geschaffen, um die gewonnenen Ergebnisse in die Spam-Bewertung eingehender Nachrichten einfließen zu lassen. Das Bayes'sche Lernverfahren kann jedoch auch dann fortgesetzt werden, und durch die fortlaufende Analyse immer neuer Nachrichten wird die Einordnung nach dem Bayes'schen Verfahren mit der Zeit immer zuverlässiger.

Bayes'sche Bewertung

Bayes'sche Bewertung aktivieren
Diese Option bewirkt, dass die Ergebnisse des Bayes'schen Lernverfahrens in die Bewertung der eingehenden Nachrichten eingehen.

Bayes'sches Lernverfahren jeden Tag um Mitternacht ausführen
Ist diese Option aktiv, so analysiert der Spam-Filter jeden Tag um Mitternacht alle Nachrichten in den Ordnern für Spam und normale Nachrichten, die weiter unten beschrieben sind. Nach der Analyse werden die Nachrichten gelöscht. Soll das Bayes'sche Lernverfahren in einem abweichenden Intervall ausgeführt werden, so muss diese Option deaktiviert werden. Das Intervall kann dann über die Option *Bayes'sches Lernverfahren einmal alle [xx] Stunden ausführen* konfiguriert werden. Soll hingegen das Bayes'sche Lernverfahren überhaupt nicht ausgeführt werden, so müssen diese Option abgeschaltet und in der folgenden Option der Wert 0 eingetragen sein.

Bayes'sches Lernverfahren einmal alle [xx] Stunden ausführen (0=nie)
Soll das Bayes'sche Lernverfahren in einem anderen Intervall als jeden Tag um Mitternacht ausgeführt werden, so muss die Option oben deaktiviert werden. Danach muss in dem Eingabefeld zu dieser Option das Intervall in Stunden eingetragen werden. Nach Ablauf der hier in Stunden angegebenen Zeit analysiert der Spam-Filter alle Nachrichten in den Ordnern für Spam und normale Nachrichten, die weiter unten beschrieben sind. Nach der Analyse werden die Nachrichten gelöscht. Soll hingegen das Bayes'sche Lernverfahren überhaupt nicht ausgeführt werden, so müssen die Option oben abgeschaltet und in dieser Option der Wert 0 eingetragen sein.

Falls die Nachrichten nach der Analyse nicht aus den Verzeichnissen gelöscht werden sollen, kann dies durch Kopieren der Datei `LEARN.BAT` nach `MYLEARN.BAT` im Verzeichnis `\MDaemon\App\` und anschließende Bearbeitung der Datei `MYLEARN.BAT` erreicht werden; dabei müssen nur die beiden Zeilen gegen Ende der Datei gelöscht werden, die mit "`if exist`" beginnen. So lange eine Datei `MYLEARN.BAT` vorhanden ist, ignoriert MDaemon die Datei `LEARN.BAT`. Wegen weiterer Informationen hierzu, vgl. die Textdatei `SA-Learn.txt` in dem Verzeichnis `\MDaemon\SpamAssassin\`. Weitere Informationen zur Heuristik bei der Erkennung von Spam und zum Bayes'schen Lernverfahren sind erhältlich unter:

http://www.spamassassin.org/doc/sa-learn.html.

Nachrichten vom Lernverfahren ausschließen, deren Größe über [xx] Byte liegt (0=keine Begrenzung)
Mit dieser Option kann definiert werden, wie groß die Nachrichten höchstens sein dürfen, damit sie vom Bayes'schen Lernverfahren noch umfasst sind. Nachrichten, deren Größe den hier angegebenen Wert überschreitet, werden nicht analysiert. Sollen Nachrichten unabhängig von ihrer Größe analysiert werden, muss hier der Wert 0 eingetragen werden.

Lernen
Ein Klick auf diesen Knopf führt mit den beiden angegebenen Ordnern sofort eine Bayes'sche Analyse durch, die sonst nur in den oben ausgewählten Intervallen stattfinden würde.

Weiterleitungsadressen für Spam und Ham aktivieren
Diese Option stellt den Benutzern Adressen zur Verfügung, an die sie Spam- und normale Nachrichten (letztere werden auch als "Ham" bezeichnet) weiterleiten können. Das Bayes'sche Lernverfahren verarbeitet auch solche weitergeleiteten Nachrichten und bindet sie in den Lernvorgang ein. MDaemon stellt per Vorgabe die Adressen "SpamLearn@<Domäne>" und "HamLearn@<Domäne>" zur Verfügung. Nachrichten an diese Adressen werden nur verarbeitet, wenn sie in einer SMTP-Verbindung übertragen werden, die über den SMTP-Befehl AUTH echtheitsbestätigt wurde. MDaemon setzt außerdem voraus, dass die Nachrichten an die genannten Adressen als Dateianlagen des Typs "message/rfc822" weitergeleitet werden. Andere Nachrichtentypen verarbeitet MDaemon nicht.

Die Zieladressen, die MDaemon verwendet, können durch Einfügen der folgenden Einträge in die Datei CFilter.INI angepasst werden:

```
[SpamFilter]
SpamLearnAddress=MySpamLearnAddress@
HamLearnAddress=MyNonSpamLearnAddress@
```

Beachte: Beide Einträge müssen auf das at-Zeichen "@" enden.

Erstellen
Ein Klick auf dieses Steuerelement bewirkt, dass MDaemon automatisch die öffentlichen IMAP-Ordner 119 für Spam und normale Nachrichten ("Ham") anlegt und sich selbst so konfiguriert, dass diese Ordner genutzt werden. Im Einzelnen werden folgende Ordner angelegt:

\Bayesian Learning.IMAP\	Haupt-IMAP-Ordner.
\Bayesian Learning.IMAP\Spam.IMAP\	Ordner für falsche negative Treffer, also Nachrichten, deren Spam-Bewertung zu niedrig war, und die nicht als Spam erkannt und gekennzeichnet wurden.
\Bayesian Learning.IMAP\Non-Spam.IMAP\	Ordner für falsche positive Treffer, also normale Nachrichten, die

fälschlich zu hoch bewertet und als Spam erkannt und gekennzeichnet wurden.

Die Berechtigungen für diese Ordner werden grundsätzlich so eingerichtet, dass nur lokale Benutzer lokaler Domänen auf sie zugreifen können, und dass ihre Rechte außerdem auf das Durchsuchen und Erstellen ("Lookup" und "Insert") beschränkt sind. Der Postmaster erhält die Rechte Durchsuchen, Lesen, Erstellen und Löschen ("Lookup", "Read", "Insert" und "Delete").

Pfad zum Ordner mit bekanntem Spam (falsche Negative):
Dieses Verzeichnis, das für das Bayes'sche Lernverfahren benutzt wird, muss Nachrichten enthalten, von denen bekannt ist, dass es sich bei ihnen um Spam handelt. Andere Nachrichten dürfen nicht in dieses Verzeichnis kopiert werden. Die Nachrichten sollen auch nicht automatisch in dieses Verzeichnis verschoben werden, es sei denn durch die Funktionen Bayes'scher automatischer Lernvorgang 687 und Spam-Honeypots 709, da in anderen Fällen die Gefahr zu groß ist, dass Nachrichten fälschlich in das Verzeichnis geraten. Würden normale Nachrichten, die nicht Spam sind, in dem Verzeichnis für Spam gefunden und analysiert, so würde dies die Verlässlichkeit des Ergebnisse aus dem Bayes'schen Lernverfahren verringern.

Pfad zum Ordner mit bekannten normalen Nachrichten (falsche Positive):
In dieses Verzeichnis, das ebenfalls für das Bayes'sche Lernverfahren verwendet wird, müssen Nachrichten kopiert werden, von denen es einwandfrei klar ist, dass es sich nicht um Spam handelt. Es sollen keinesfalls Nachrichten in dieses Verzeichnis kopiert werden, von denen nicht sicher feststeht, dass es sich nicht um Spam handelt. Auch diese Nachrichten sollten wegen der Fehleranfälligkeit nicht automatisch in das Verzeichnis kopiert werden, es sei denn durch die Funktion Bayes'scher automatischer Lernvorgang 687, da sonst die Gefahr zu groß ist, dass Nachrichten fälschlich in das Verzeichnis geraten. Würden Spam-Nachrichten in dem Verzeichnis für bekannte normale Nachrichten gefunden und analysiert, so würde dies die Verlässlichkeit des Ergebnisse aus dem Bayes'schen Lernverfahren verringern.

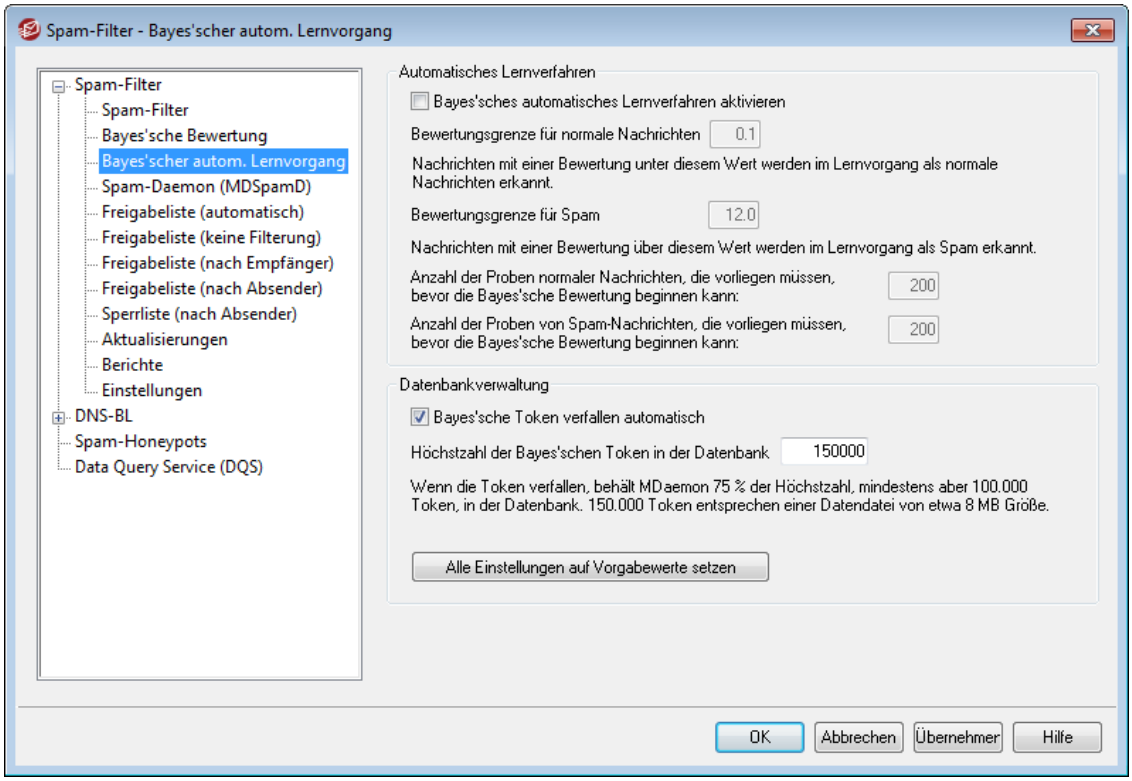
Öffentlicher Ordner
Mithilfe dieser Steuerelemente lassen sich bestehende öffentliche Ordner als Quellverzeichnisse für das Bayes'sche Lernverfahren definieren. Die Benutzer können dann sehr einfach Nachrichten, bei denen sie erkennen, dass sie fälschlich als Spam erkannt oder nicht erkannt wurden, in das zugehörige Verzeichnis kopieren und so dem Lernverfahren zuführen. Je mehr Benutzer Zugriff auf diese Ordner erhalten, desto höher ist aber auch das Risiko, dass eine Nachricht, die aus Versehen in den falschen Ordner kopiert wurde, die Treffsicherheit verringert.

Wird einer dieser öffentlicher Ordner über einen Mailclient, den Windows-Explorer oder auf andere Weise umbenannt, so muss der betroffene Eintrag in diesem Menü von Hand angepasst werden. Der Spam-Filter kann sonst nicht erkennen, dass er einen anderen Ordner verwenden soll, und verwendet weiterhin den alten, nicht mehr gültigen Ordner.

Siehe auch:

[Bayes'scher automatischer Lernvorgang 687]
[Spam-Honeypots 709]

4.6.1.3 Bayes'scher automatischer Lernvorgang



Die Einstellungen für das Automatische Lernverfahren sind nicht verfügbar, falls MDaemon den MDaemon-Spam-Daemon (MDSpamD) eines anderen MDaemon-Servers für den Spam-Filter verwendet. Alle Bayes'schen Lernvorgänge werden dann auf dem anderen Server durchgeführt. Weitere Informationen enthält der Abschnitt Spam-Daemon [689].

Automatisches Lernverfahren

Bayes'sches automatisches Lernverfahren aktivieren
Für das Bayes'sche automatische Lernverfahren können Schwellwerte für Spam- und normale Nachrichten festgelegt werden. Nachrichten, deren Bewertung unter der Bewertungsgrenze für normale Nachrichten liegt, werden durch das Bayes'sche Lernverfahren automatisch wie normale Nachrichten behandelt. Entsprechendes gilt für Nachrichten über der Bewertungsgrenze für Spam, die das Lernverfahren automatisch als Spam behandelt. Dieses automatische Lernverfahren kann in der Praxis zwar durchaus zu Problemen führen; ein sinnvoller Einsatz ist trotzdem möglich, wenn die Bewertungsgrenzen richtig gesetzt werden. Der Vorteil des automatischen Lernverfahrens ist, dass alte und

nicht mehr gültige Token (siehe *Datenbankverwaltung* unten) aus den Datenbankdateien entfernt und automatisch ersetzt werden. Verfallene Token müssen daher nicht mehr durch manuell ausgelöste Lernvorgänge wieder hergestellt werden.

Bewertungsgrenze für normale Nachrichten
Nachrichten, deren Spam-Bewertung unter dem hier angegebenen Wert liegt, werden durch das Bayes'sche Lernverfahren automatisch als normale Nachrichten behandelt, die keinen Spam enthalten.

Bewertungsgrenze für Spam
Nachrichten, deren Spam-Bewertung über dem hier angegebenen Wert liegt, werden durch das Bayes'sche Lernverfahren automatisch als Spam behandelt.

Anzahl der Proben normaler Nachrichten, die vorliegen müssen, bevor die Bayes'sche Bewertung beginnen kann
Der Spam-Filter beginnt erst mit der Bewertung und Kennzeichnung eingehender Nachrichten, wenn diese Anzahl an normalen Nachrichten und die Anzahl Spam-Nachrichten, die mit der folgenden Einstellung festgelegt wird, durch das Bayes'sche Lernverfahren verarbeitet und ausgewertet wurde. Dies ist erforderlich, damit der Spam-Filter eine ausreichend große Datenbasis zur Verfügung hat, die er zur Bewertung von Nachrichten heranziehen kann. Sobald das System mit der hier angegebenen Anzahl von Nachrichten beschickt wurde und diese ausgewertet sind, ist das System bereit, die Ergebnisse des Bayes'schen Bewertungen auf eingehende Nachrichten anzuwenden. Indem die Auswertung von Spam- und normalen Nachrichten fortlaufend weitergeführt wird, steigern sich Zuverlässigkeit und Genauigkeit des Bayes'schen Systems mit der Zeit immer mehr.

Anzahl der Proben von Spam-Nachrichten, die vorliegen müssen, bevor die Bayes'sche Bewertung beginnen kann
Für diese Einstellung gilt die Erläuterung zu der vorherigen Einstellung entsprechend; allerdings legt diese Einstellung fest, wie viele Spam-Nachrichten das System mindestens ausgewertet haben muss, bevor der Spam-Filter beginnt, eingehende Nachrichten zu bewerten.

Datenbankverwaltung

Bayes'sche Token verfallen automatisch
Diese Option bewirkt, das das Bayes'sche System die in der Datenbank eingetragenen Token automatisch verfallen lässt, sobald die unten angegebene *Höchstzahl der Token* erreicht ist. Die Festlegung einer Höchstzahl für die Token in der Datenbank kann verhindern, dass die Bayes'sche Datenbank unverhältnismäßig groß wird.

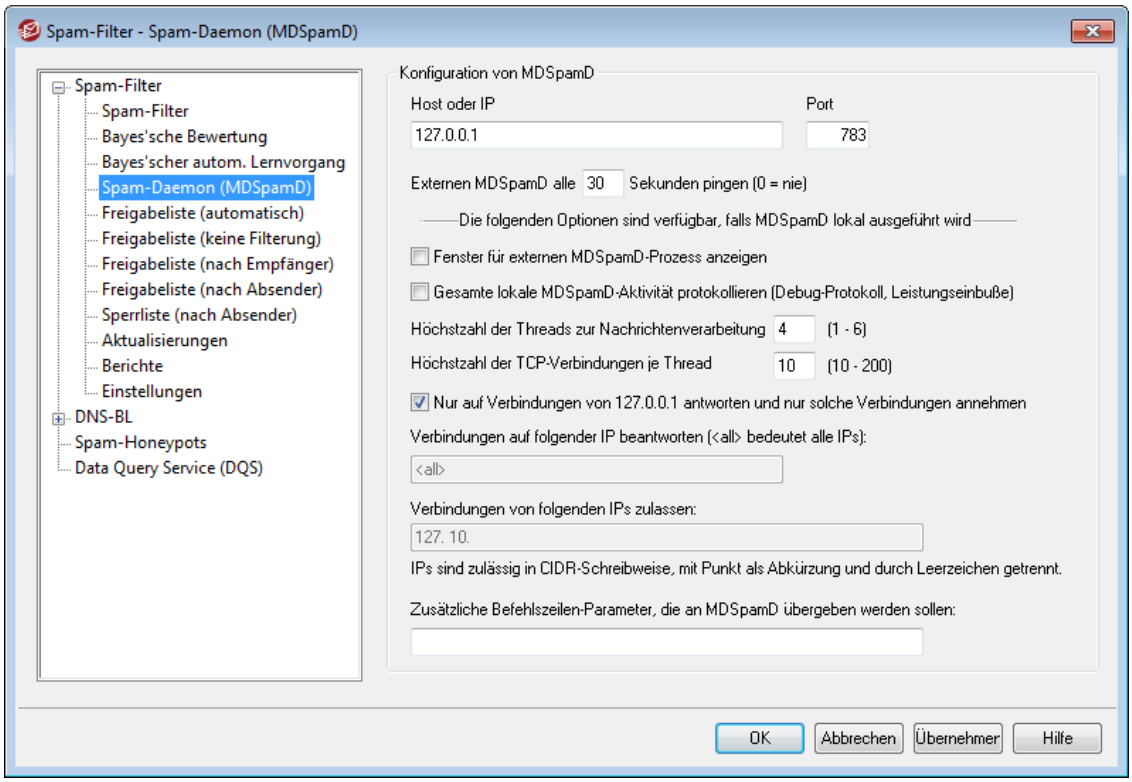
Höchstzahl der Bayes'schen Token in der Datenbank
Hier wird die Höchstzahl der Token festgelegt, die sich in der Datenbank befinden dürfen. Wird diese Zahl erreicht, so löscht das Bayes'sche System die ältesten Token zuerst, bis die Anzahl der Token auf 75 % der hier angegebenen Höchstzahl gefallen ist. Die Zahl von 100.000 Token kann dabei aber keinesfalls unterschritten werden. Beachte: 150.000 Token in der Datenbank belegen etwa 8 MB Speicherplatz.

Alle Einstellungen auf Vorgabewerte setzen
Ein Klick auf diesen Knopf setzt alle erweiterten Bayes-Einstellungen auf die Vorgabewerte zurück.

Siehe auch:

Bayes'sche Bewertung 683
Spam-Honeypots 709

4.6.1.4 Spam-Daemon (MDSpamD)



Das Anti-Spam-System von MDaemon wird als getrenntes Programm (sog. Daemon) ausgeführt und wird als MDaemon Spam Daemon (kurz MDSpamD) bezeichnet. Die Nachrichten werden an den MDSpamD zur Prüfung über TCP/IP geleitet. Die Leistungsfähigkeit des Spam-Filters wird dadurch erheblich gesteigert. Außerdem kann MDSpamD nun wahlweise lokal oder auf einem anderen Rechner ausgeführt werden, und MDaemon kann auch den MDSpamD (oder ein anderes zur SpamD-Technik kompatibles Produkt) einer anderen Installation nutzen. MDSpamD läuft in der Grundeinstellung lokal auf Port 783 an der IP-Adresse 127.0.0.1. Soll der Spam-Daemon einer anderen Installation oder eines anderen Standorts genutzt werden, so können jedoch auch ein anderer Port und eine andere IP-Adresse angegeben werden.

Host oder IP
Hier müssen der Hostname oder die IP-Adresse angegeben werden, an die MDaemon die Nachrichten zwecks Prüfung durch MDSpamD senden soll. Falls MDSpamD auf dem lokalen System läuft, muss 127.0.0.1 angegeben werden.

Port
Hier wird der Port eingetragen, über den die Nachrichten gesendet werden. Die Voreinstellung für MDSpamD lautet 783.

Externen MDSpamD alle [xx] Sekunden pingen (0 = nie)
Werden der MDSpamD oder ein anderes Produkt nach dem SpamD-Standard auf einem anderen System ausgeführt, so kann dieses andere System mithilfe dieser Option durch Ping-Befehle auf Reaktionsfähigkeit überprüft werden. Der Wert 0 bewirkt, dass das System nicht gepingt wird.

Die folgenden Optionen sind verfügbar, falls MDSpamD lokal ausgeführt wird

Fenster für MDSpamD-Prozess anzeigen
Wird MDSpamD auf dem lokalen System ausgeführt, und soll der Prozess sichtbar in einem eigenen Fenster ausgeführt werden, so muss diese Option aktiv sein. Sie bewirkt, dass die Meldungen des MDSpamD in das eigene Fenster umgeleitet und nicht über die Benutzeroberfläche und das Protokoll von MDaemon angezeigt werden. Diese Option kann die Systemleistung erhöhen, da die Daten des MDSpamD nicht an MDaemon übermittelt und dort angezeigt werden müssen. Es wird aber kein Protokoll erstellt, und die Option ist daher nicht zu der Protokoll-Option für Debug-Zwecke weiter unten kompatibel. Die Meldungen des MDSpamD erscheinen dann auch nicht im Hauptfenster von MDaemon auf der Registerkarte MDSpamD unter Sicherheit.

Gesamte lokale MDSpamD-Aktivität protokollieren (Debug-Protokoll, Leistungeinbuße)
Soll die gesamte Aktivität des MDSpamD protokolliert werden, so muss diese Option aktiv sein. Diese Option ist nicht verfügbar, falls die Option Fenster für MDSpamD-Prozess anzeigen aktiv ist, die weiter oben beschrieben wird. Die Option ist nicht wirksam, wenn im Konfigurationsdialog Windows-Dienst 506 für den Zugriff auf Netzwerkressourcen besondere Anmeldedaten angegeben sind und MDaemon daher nicht unter dem Benutzerkonto SYSTEM ausgeführt wird. Die MDSpamD-Aktivität kann dann nicht protokolliert werden.

Wird die MDSpamD-Aktivität protokolliert, so kann sich die Leistung des Mail-Servers verschlechtern. Dies hängt von der Leistungsfähigkeit des Servercomputers und den weiteren dort laufenden Anwendungen ab. Im Allgemeinen empfiehlt es sich, diese Option nur zur Fehlerbehebung (zu Debug-Zwecken) zu aktivieren.

Höchstzahl der Threads zur Nachrichtenverarbeitung (1-6)
Hier wird die Höchstzahl der Threads angegeben, die MDaemon zur internen Verarbeitung von Nachrichten verwendet. Sie können einen Wert von 1 bis 6 eintragen.

Höchstzahl der TCP-Verbindungen je Thread (10-200)
Hier wird die Höchstzahl der TCP-Verbindungen angegeben, die MDSpamD annimmt, bevor ein neuer Thread gestartet wird. Sie können einen Wert von 10 bis 200 eintragen.

Nur auf Verbindungen von 127.0.0.1 antworten und nur solche Verbindungen annehmen
Diese Option bewirkt, dass ein lokal ausgeführter MDSpamD Verbindungen von anderen Systemen nicht annimmt. Verbindungen werden nur angenommen, wenn sie von demselben Rechner ausgehen, auf dem MDSpamD ausgeführt wird.

Verbindungen auf folgender IP beantworten
Ist die vorherige Option deaktiviert, so können mithilfe dieser Option die zulässigen Verbindungen auf solche Verbindungen beschränkt werden, die an eine bestimmte IP-Adresse gebunden sind. Es werden dann nur noch Verbindungen an die angegebene IP-Adresse beantwortet. Der Eintrag "<all>" bewirkt, dass MDSpamD nicht auf eine bestimmte IP-Adresse beschränkt ist.

Verbindungen von folgenden IPs zulassen
Hier werden die IP-Adressen eingetragen, von denen MDSpamD eingehende Verbindungen annimmt. Verbindungen, die von anderen IP-Adresse ausgehen, werden abgewiesen. Dies ist nützlich, falls Verbindungen von anderen Servern zugelassen sein sollen, denn so kann die Verarbeitung durch den Spam-Filter für mehrere Server gemeinsam auf einem Rechner durchgeführt werden.

Zusätzliche Befehlszeilenparameter, die an MDSpamD übergeben werden sollen:

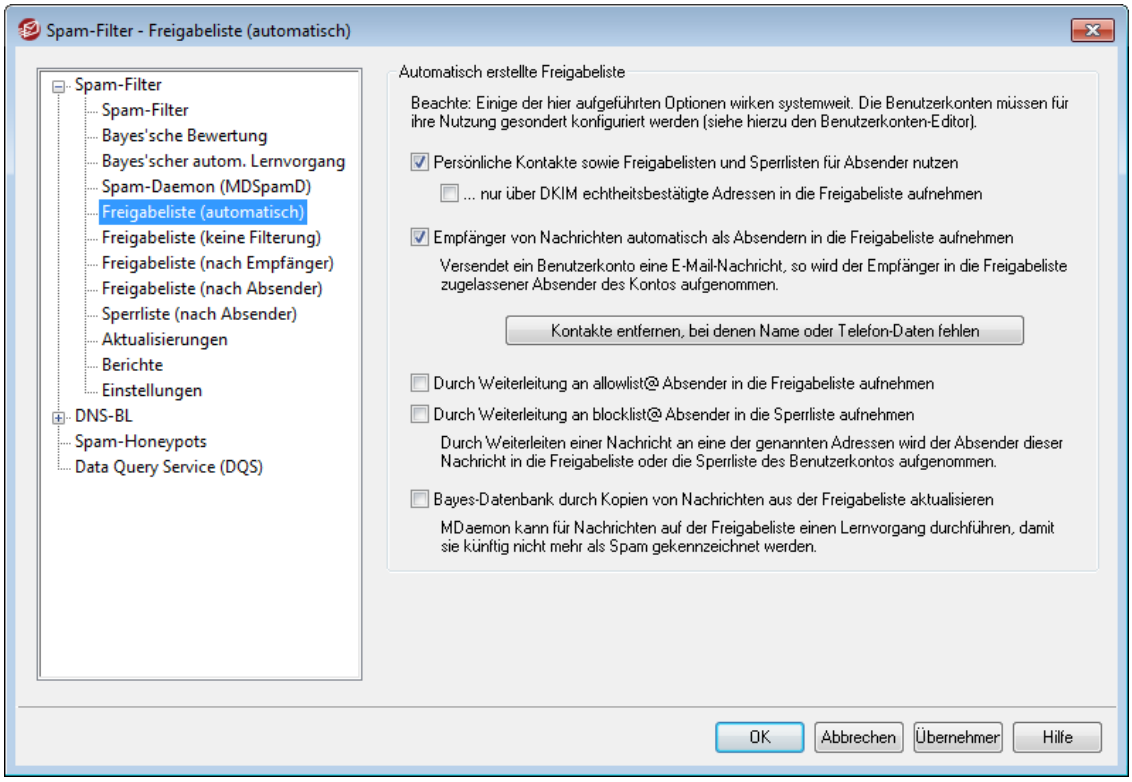
MDSpamD unterstützt zahlreiche Befehlszeilenparameter und Optionen. Sie sind unter folgendem URL dokumentiert:

http://spamassassin.apache.org/

Sollen die Befehlszeilenparameter eingesetzt werden, so müssen die gewünschten Befehle und Optionen zunächst zu einer Zeichenkette zusammengefügt und in dieses Feld eingetragen werden.

Einige dieser Optionen können über den hier dokumentierten Konfigurationsdialog gesteuert werden; sie müssen nicht als Befehlszeilenparameter übergeben werden.

4.6.1.5 Freigabeliste (automatisch)



Automatisch erstellte Freigabeliste

Persönliche Kontakte sowie Freigabelisten und Sperrlisten für Absender nutzen
Mithilfe dieser Option können Sie die persönlichen Kontakte sowie die Freigabelisten und die Sperrlisten der Benutzer für den Spam-Filter auswerten lassen. MDaemon prüft bei allen eingehenden Nachrichten, ob die Absender in den persönlichen Kontakten, den Freigabelisten oder den Sperrlisten der Empfänger enthalten sind. Wird eine Absenderadresse in einer der Listen gefunden, dann wird die Nachricht automatisch zugestellt oder abgewiesen. Falls Sie diese automatische Freigabe und Sperrung nicht auf alle Benutzerkonten in MDaemon gleichermaßen anwenden wollen, können Sie diese Option nach Benutzerkonten getrennt deaktivieren. Bearbeiten Sie hierzu die Option *Spam-Filter nutzt persönliche Kontakte sowie Dateien für Freigabeliste und Sperrlisten* im Abschnitt Freigabeliste 758 des Benutzerkonten-Editors.

... nur über DKIM echtheitsbestätigte Adressen in die Freigabeliste aufnehmen
Diese Option bewirkt, dass MDaemon eine Nachricht mit einem Absender auf der Freigabeliste nur dann als Treffer wertet, wenn die Nachricht über DomainKeys Identified Mail 529 (DKIM) echtheitsbestätigt wurde. Diese Option hilft, zu verhindern, dass Nachrichten mit gefälschten Absendern irrtümlich als Treffer auf der Freigabeliste gewertet werden. Diese Option ist per Voreinstellung abgeschaltet.

Empfänger von Nachrichten automatisch als Absendern in die Freigabeliste aufnehmen
Ist diese Option aktiv, und sendet ein Benutzer eine E-Mail-Nachricht an eine beliebige externe E-Mail-Adresse, dann fügt MDaemon den Empfänger automatisch der Freigabeliste für das Benutzerkonto des Absenders hinzu. Wird diese Option in Verbindung mit der Option "*Persönliche Kontakte sowie*

Freigabelisten und Sperrlisten für Absender nutzen" weiter oben verwendet, so kann die Zahl der falschen positiven Treffer des Spam-Filters erheblich verringert werden.

Falls Sie diese Option nicht auf alle Benutzerkonten in MDaemon gleichermaßen anwenden wollen, können Sie diese Option nach Benutzerkonten getrennt deaktivieren. Bearbeiten Sie hierzu die Option *Empfänger von Nachrichten automatisch als Absendern in die Freigabeliste aufnehmen* im Abschnitt Freigabeliste 758 des Benutzerkonten-Editors.

Für Benutzerkonten, für die ein Autobeantworter aktiv ist, wird diese Funktion automatisch gesperrt.

Kontakte entfernen, bei denen Name oder Telefon-Daten fehlen
Durch Anklicken dieser Schaltfläche können Sie aus den Standard-Kontaktordnern aller Benutzer alle Kontakte löschen, die nur eine E-Mail-Adresse enthalten. Falls für einen Kontakt nicht wenigstens auch ein Name oder eine Telefon-Nummer erfasst ist, wird der Kontakt dabei gelöscht. Diese Option soll vor allem den Benutzern helfen, die die automatische Freigabeliste in MDaemon vor Version 11 (noch unter der Bezeichnung "Weiße Liste") genutzt haben; sie kann die Kontakte löschen, die nur als Ergebnis der Aufnahme in die Freigabeliste gespeichert wurden. In früheren Versionen von MDaemon wurden die Adressen den Standard-Kontaktordnern hinzugefügt, und es stand kein besonderer Ordner für eine Freigabeliste zur Verfügung. Dies konnte dazu führen, dass Benutzer viele Einträge in den Kontaktordnern hatten, die sie eigentlich gar nicht benötigten.

Sie sollten diese Funktion nur sehr umsichtig einsetzen, da es durchaus legitime Gründe geben kann, warum Einträge in den Kontaktordnern nur E-Mail-Adressen enthalten.

Durch Weiterleitung an allowlist@ Absender in die Freigabeliste aufnehmen
Ist für ein Benutzerkonto die Option *Spam-Filter nutzt persönliche Kontakte sowie Dateien für Freigabeliste und Sperrlisten* aktiv, so kann dieses Benutzerkonto Nachrichten an die Adresse `allowlist@<Domäne>` weiterleiten und so MDaemon veranlassen, den Absender der weitergeleiteten Nachricht in die Freigabeliste des Benutzerkontos einzutragen. Die Adresse, die MDaemon in die Freigabeliste einträgt, wird dabei der Kopfzeile `From` der weitergeleiteten Nachricht entnommen.

Nachrichten an die Adresse `allowlist@<Domäne>` werden nur verarbeitet, wenn sie in einer SMTP-Verbindung übertragen werden, die über den ESMTP-Befehl AUTH echtheitsbestätigt wurde. MDaemon setzt außerdem voraus, dass die Nachrichten an die genannten Adressen als Dateianlagen des Typs `message/rfc822` weitergeleitet werden. Andere Nachrichtentypen verarbeitet MDaemon nicht.

Die Zieladresse, die MDaemon für diese Funktion verwendet, kann durch Bearbeiten des folgenden Eintrags in der Datei `CFILTER.INI` angepasst werden:

```
[SpamFilter]
WhiteListAddress=MyAllowListAddress@
```

Beachte: Der Eintrag muss auf das at-Zeichen "@" enden.

Durch Weiterleitung an blocklist@ Absender in die Sperrliste aufnehmen
Ist für ein Benutzerkonto die Option *Spam-Filter nutzt persönliche Kontakte sowie Dateien für Freigabeliste und Sperrlisten* aktiv, so kann dieses Benutzerkonto Nachrichten an die Adresse `blocklist@<Domäne>` weiterleiten und so MDaemon veranlassen, den Absender der weitergeleiteten Nachricht in die persönliche Sperrliste des Benutzerkontos einzutragen. Die Adresse, die MDaemon in die Sperrliste einträgt, wird dabei der Kopfzeile `From` der weitergeleiteten Nachricht entnommen.

Nachrichten an die Adresse `blocklist@<Domäne>` werden nur verarbeitet, wenn sie in einer SMTP-Verbindung übertragen werden, die über den ESMTP-Befehl AUTH echtheitsbestätigt wurde. MDaemon setzt außerdem voraus, dass die Nachrichten an die genannten Adressen als Dateianlagen des Typs `message/rfc822` weitergeleitet werden. Andere Nachrichtentypen verarbeitet MDaemon nicht.

Bayes-Datenbank durch Kopien von Nachrichten aus der Freigabeliste aktualisieren
Diese Option bewirkt, dass Nachrichten automatisch in den Lernordner für normale Nachrichten (dieser wird im Abschnitt Bayes 683 konfiguriert) kopiert und durch das Bayes'sche Lernverfahren ausgewertet werden, wenn sie bestimmte Kriterien erfüllen. Dadurch kann die dauerhafte Beschickung des Bayes'schen Systems mit Mustern normaler Nachrichten, die keinen Spam darstellen ("Ham"), automatisiert werden. Die fortwährende Beschickung des Bayes'schen Lernverfahrens mit immer neuen Mustern normaler Nachrichten steigert die Zuverlässigkeit und Genauigkeit des Bayes'schen Systems mit der Zeit immer mehr und verringert so die Zahl der falschen positiven Treffer, also der Nachrichten, die irrtümlich als Spam bewertet wurden.

Eine eingehende Nachricht erfüllt die Kriterien, wenn sie an einen lokalen Benutzer gerichtet ist und von einem Absender stammt, der im Adressbuch des Empfängers oder in seiner Freigabeliste eingetragen ist. Eine abgehende Nachricht erfüllt die Kriterien, wenn der Empfänger der Nachricht im Adressbuch oder in der Freigabeliste des Absenders eingetragen ist. Falls abgehende Nachrichten in diesen Vorgang überhaupt nicht einbezogen werden sollen, kann dies durch Bearbeiten des folgenden Eintrags in der Datei `CFilter.ini` erreicht werden:

```
[SpamFilter]
UpdateHamFolderOutbound=No (Nein, Voreinstellung ist "Yes", Ja)
```

Erfüllt eine Nachricht die dargestellten Kriterien, so wird sie automatisch in den Lernordner für HAM kopiert, und zwar auch dann, wenn das Bayes'sche automatische Lernverfahren selbst deaktiviert ist. So ist sicher gestellt, dass das Lernverfahren, wenn es aktiviert wird, oder wenn ein Lernvorgang von Hand ausgelöst wird, immer eine ausreichend große Datenbasis normaler Nachrichten zur Verfügung hat. Es wird allerdings nicht jede Nachricht, welche die Kriterien erfüllt, in den Lernordner kopiert. MDaemon kopiert, sobald diese Option aktiv ist, Nachrichten nur, bis eine bestimmte Anzahl erreicht ist; danach kopiert MDaemon Nachrichten nur noch in festgelegten Intervallen. Per Voreinstellung werden, jeweils, sofern sie den Kriterien entsprechen, die ersten 25 Nachrichten und danach jede zehnte Nachricht kopiert. Die Zahl der erstmalig zu kopierenden Nachrichten entspricht der Mindestzahl an Mustern für normale Nachrichten, die im Abschnitt Bayes'scher automatischer Lernvorgang 687 festgelegt wurden. Eine Änderung an dieser Einstellung bewirkt daher auch eine Änderung des hier beschriebenen Werts. Um das Intervall zu ändern, das MDaemon beim Kopieren

der danach folgenden Nachrichten beachtet, muss der folgende Eintrag in der Datei `MDaemon.ini` bearbeitet werden:

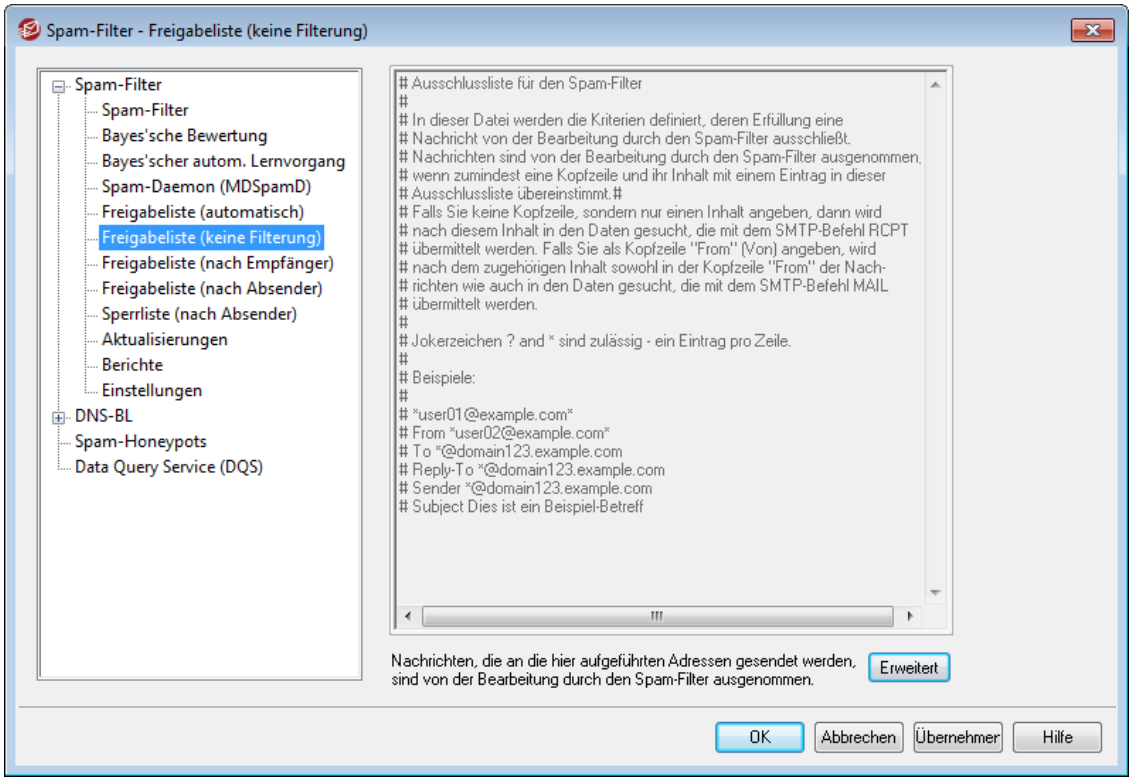
```
[SpamFilter]
HamSkipCount=10 (Voreinstellung = 10)
```

Sobald schließlich eine bestimmte Gesamtzahl Nachrichten kopiert wurden, beginnt MDaemon den gesamten Vorgang erneut. Wieder werden die ersten 25 Nachrichten und dann jede zehnte Nachricht kopiert, die den Kriterien entsprechen. Etwa abweichende Werte, die konfiguriert wurden, wie oben beschrieben, werden dabei ebenfalls berücksichtigt. Per Voreinstellung beginnt der Vorgang erneut, sobald 500 Nachrichten kopiert wurden. Dieser Wert kann durch Bearbeiten des folgenden Eintrags in der Datei `MDaemon.ini` geändert werden:

```
[SpamFilter]
HamMaxCount=500 (Voreinstellung = 500)
```

Diese Option ist nicht verfügbar, wenn MDaemon den MDaemon-Spam-Daemon (MDSpamD) eines anderen MDaemon-Servers für den Spam-Filter verwendet. Alle Bayes'schen Lernvorgänge richten sich dann nach der Einstellung des anderen Servers und werden auch durch den anderen Server ausgeführt. Weitere Informationen enthält der Abschnitt Spam-Daemon 689.

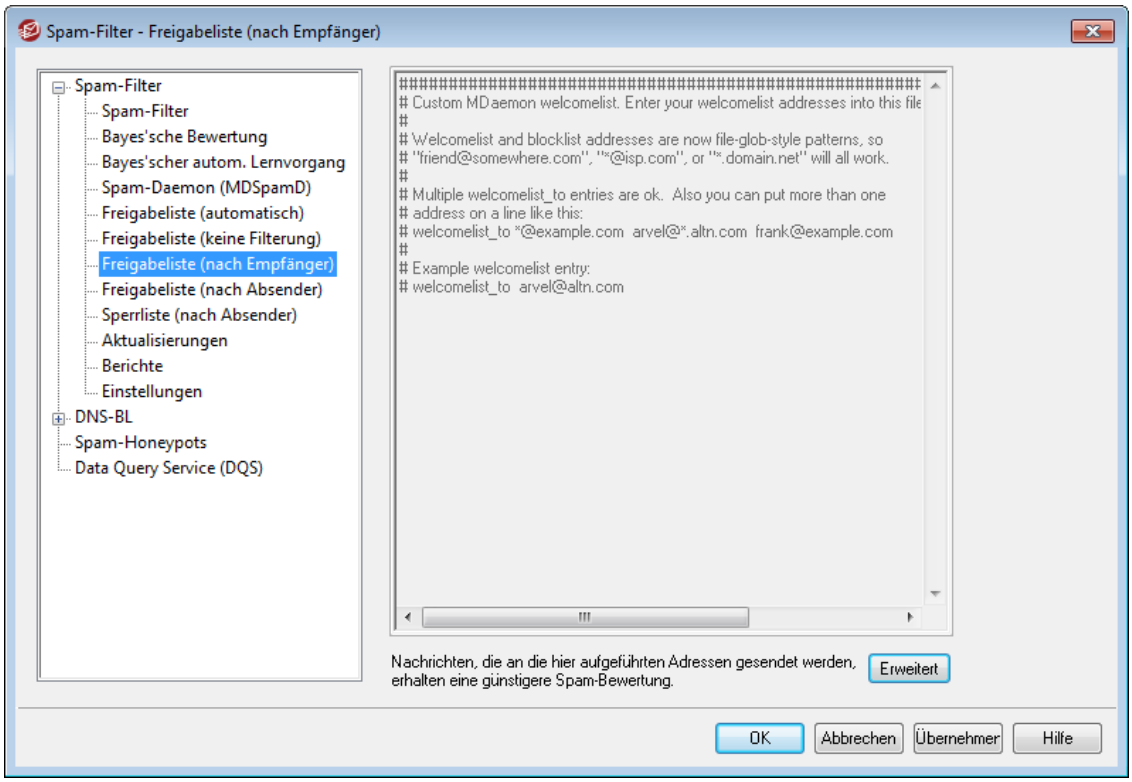
4.6.1.6 Freigabeliste (keine Filterung)



Nachrichten an die folgenden Adressen werden nicht gefiltert
In diesem Konfigurationsdialog können Sie Empfängeradressen erfassen, die von der Bearbeitung durch den Spam-Filter ausgenommen sind. Um die Adressen zu erfassen, klicken Sie auf **Erweitert**. Nachrichten, die an die hier erfassten Adressen gerichtet sind, werden nicht durch den Spam-Filter verarbeitet.

Dieser Konfigurationsdialog ist nicht verfügbar, wenn MDaemon den MDaemon-Spam-Daemon (MDSpamD) eines anderen MDaemon-Servers für den Spam-Filter verwendet. Alle Bayes'schen Lernvorgänge richten sich dann nach der Einstellung des anderen Servers und werden auch durch den anderen Server ausgeführt. Weitere Informationen enthält der Abschnitt Spam-Daemon 689.

4.6.1.7 Freigabeliste (nach Empfänger)

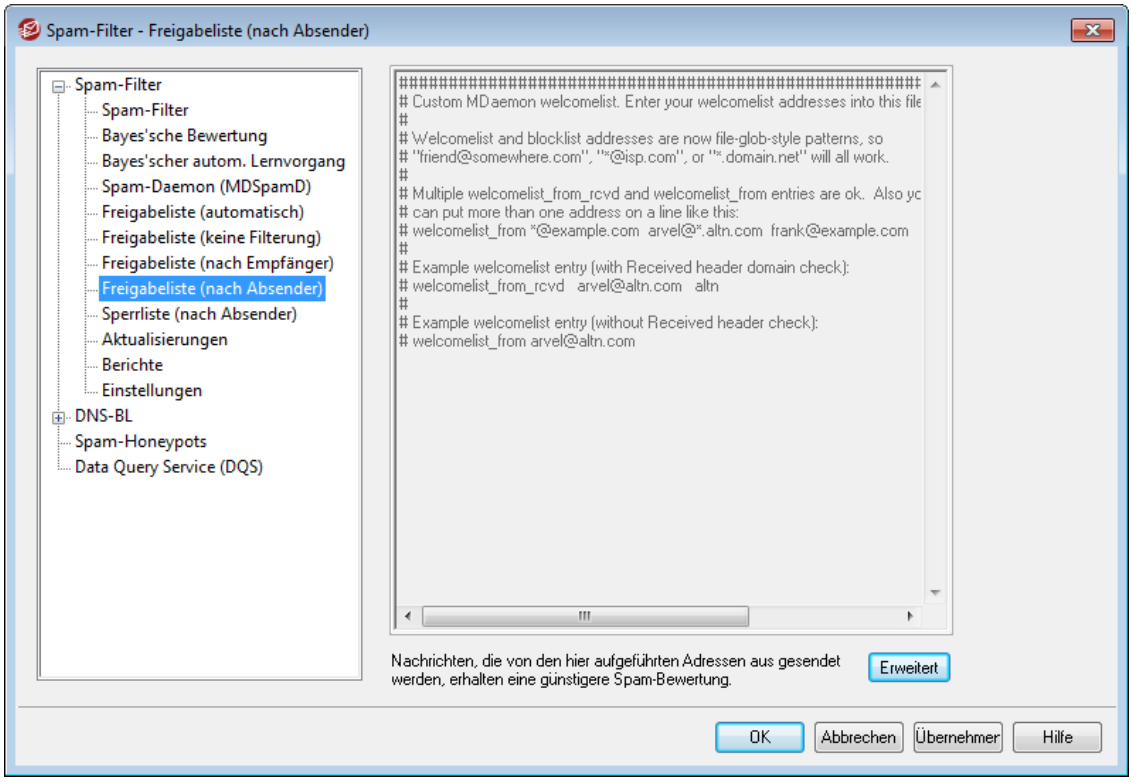


Nachrichten an folgende Adressen werden günstig bewertet
Um die Liste der Adressen in diesem Konfigurationsdialog zu bearbeiten, klicken Sie auf **Erweitert**. Diese Freigabeliste arbeitet ähnlich wie die *Freigabeliste (keine Filterung)* 695; Treffer auf dieser Freigabeliste (nach Empfänger) führen aber nicht dazu, dass die Nachrichten den Spam-Filter nicht durchlaufen. Sie durchlaufen des Spam-Filter, und ihre Spam-Bewertung 679 wird dabei um den Punktwert verringert, der im Konfigurationsdialog Optionen für den Spam-Filter 701 festgelegt ist. Wird in dieser Freigabeliste eine Empfängeradresse erfasst, so gewährleistet dies daher noch nicht, dass Nachrichten an diese Empfängeradresse nicht trotzdem als Spam erkannt und behandelt werden. Ein Beispiel hierzu: Liegt der Schwellwert für Spam bei 5,0, und liegt der Punktwert für Treffer auf der Freigabeliste bei 100, so wird eine Nachricht als Spam erkannt werden, die eine Spam-Bewertung von mindestens 105 erreicht, bevor der

Punktwert für Treffer auf der Freigabeliste abgezogen wird. Solche hohen Punktwerte sind bei Zusammentreffen zahlreicher ungünstiger Spam-Eigenschaften, etwa, wenn die Nachricht Adressen aus einer Sperrliste enthält, zwar selten, aber vorstellbar. Im Beispiel ergibt sich auch nach dem Abzug des Punktwerts für Treffer auf der Freigabeliste noch eine Spam-Bewertung, den Schwellwert für Spam-Nachrichten erreicht.

Dieser Konfigurationsdialog ist nicht verfügbar, wenn MDaemon den MDaemon-Spam-Daemon (MDSpamD) eines anderen MDaemon-Servers für den Spam-Filter verwendet. Die hier dargestellte Liste wird dann auf dem anderen Server gepflegt. Weitere Informationen enthält der Abschnitt Spam-Daemon 689.

4.6.1.8 Freigabeliste (nach Absender)

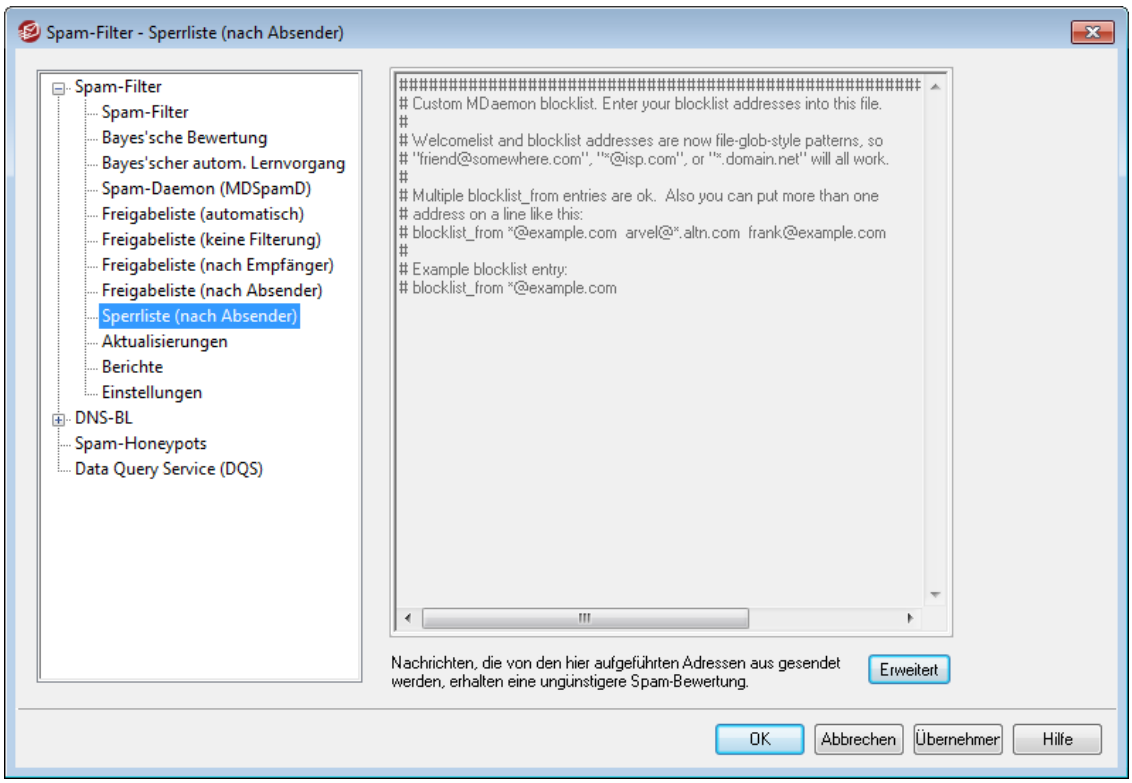


Nachrichten von folgenden Adressen werden günstig bewertet
Um die Liste der Adressen in diesem Konfigurationsdialog zu bearbeiten, klicken Sie auf **Erweitert**. Diese Freigabeliste arbeitet ähnlich wie die *Freigabeliste (nach Empfänger)* 696; Treffer auf dieser Freigabeliste (nach Absender) richten sich jedoch nach dem Absender und führen dazu, dass die Spam-Bewertung 679 der fraglichen Nachricht um den Punktwert verringert wird, der im Konfigurationsdialog Optionen für den Spam-Filter 701 festgelegt ist. Wird in dieser Freigabeliste eine Absenderadresse erfasst, so gewährleistet dies daher noch nicht, dass Nachrichten an von dieser Absenderadresse nicht trotzdem als Spam erkannt und behandelt werden. Ein Beispiel hierzu: Liegt der Schwellwert für Spam bei 5,0, und liegt der Punktwert für Treffer auf der Freigabeliste bei 100, so wird eine Nachricht als Spam erkannt werden, die eine Spam-Bewertung von mindestens 105 erreicht, bevor der Punktwert für Treffer auf der Freigabeliste

abgezogen wird. Solche hohen Punktwerte sind bei Zusammentreffen zahlreicher ungünstiger Spam-Eigenschaften, etwa, wenn die Nachricht Adressen aus einer Sperrliste enthält, zwar selten, aber vorstellbar. Im Beispiel ergibt sich auch nach dem Abzug des Punktwerts für Treffer auf der Freigabeliste noch eine Spam-Bewertung, den Schwellwert für Spam-Nachrichten erreicht.

Dieser Konfigurationsdialog ist nicht verfügbar, wenn MDaemon den MDaemon-Spam-Daemon (MDSpamD) eines anderen MDaemon-Servers für den Spam-Filter verwendet. Die hier dargestellte Liste wird dann auf dem anderen Server gepflegt. Weitere Informationen enthält der Abschnitt Spam-Daemon 689.

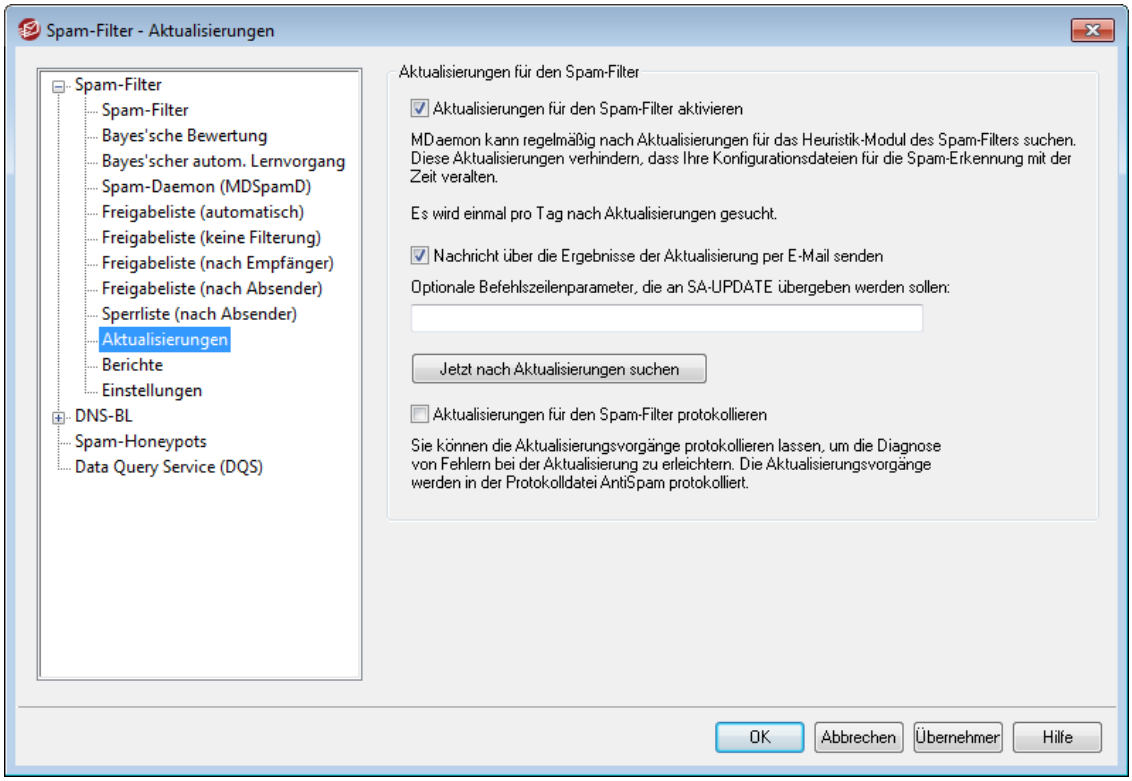
4.6.1.9 Sperrliste (nach Absender)



Nachrichten von folgenden Adressen werden nachteilig bewertet
Um die Liste der Adressen in diesem Konfigurationsdialog zu bearbeiten, klicken Sie auf **Erweitert**. Die Spam-Bewertung 679 für Nachrichten von Adressen auf dieser Sperrliste wird um den Punktwert erhöht, der im Konfigurationsdialog Optionen für den Spam-Filter 701 festgelegt ist. Sie werden üblicherweise als Spam gekennzeichnet werden. Dass eine Absenderadresse auf dieser Sperrliste erfasst ist, gewährleistet aber noch nicht, dass eine Nachricht von dieser Adresse in jedem Fall als Spam behandelt wird. Stammt etwa eine Nachricht von einem Absender auf der Sperrliste, und ist sie aber an einen Empfänger auf einer Freigabeliste gerichtet, so kann der mit der Freigabeliste verbundene günstige Punktwert den ungünstigen Punktwert der Sperrliste wieder aufheben, und die Nachricht kann eine endgültige Bewertung erhalten, die unter dem Schwellwert für Spam-Nachrichten liegt. Diese Wirkung kann auch eintreten, wenn der Punktwert für Treffer auf der Sperrliste sehr gering festgelegt ist.

Dieser Konfigurationsdialog ist nicht verfügbar, wenn MDaemon den MDaemon-Spam-Daemon (MDSpamD) eines anderen MDaemon-Servers für den Spam-Filter verwendet. Die hier dargestellte Liste wird dann auf dem anderen Server gepflegt. Weitere Informationen enthält der Abschnitt Spam-Daemon 689.

4.6.1.10 Aktualisierungen



Aktualisierungen für den Spam-Filter

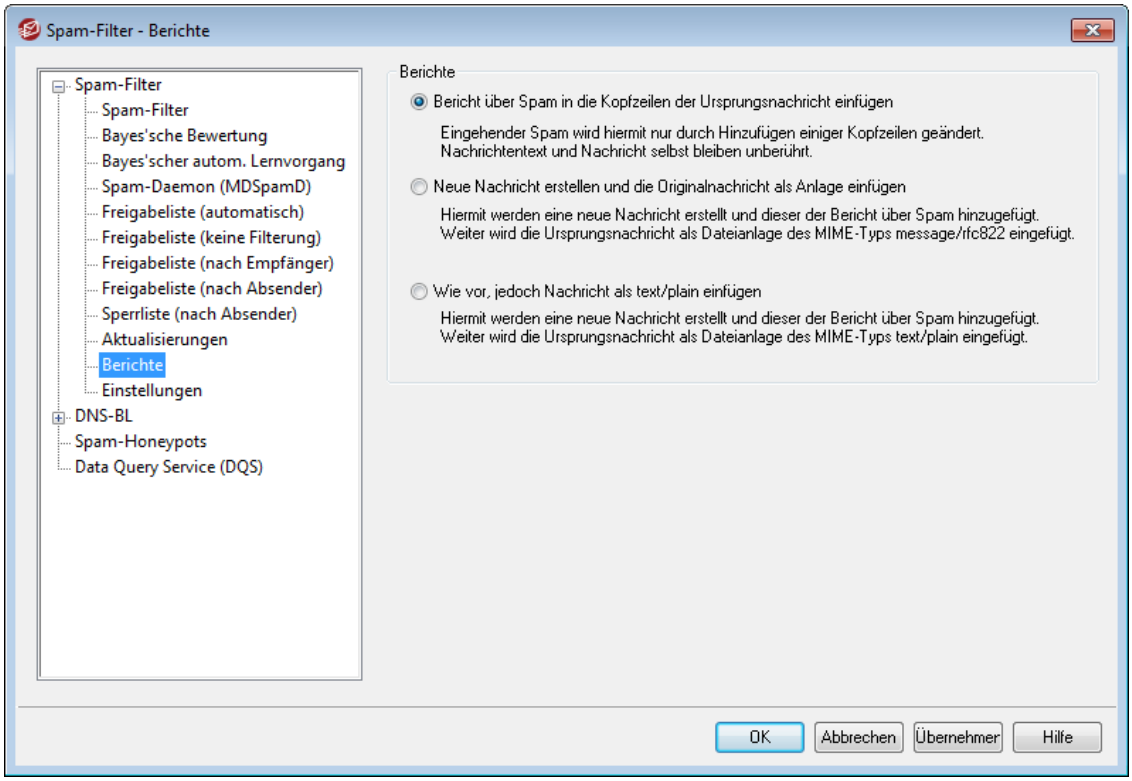
Aktualisierungen für den Spam-Filter aktivieren
Diese Option bewirkt, dass der Spam-Filter automatisch aktualisiert wird. So lange die Option aktiv ist, prüft MDaemon einmal täglich, ob die das Heuristikmodul des Spam-Filters Aktualisierungen verfügbar sind. Solche Aktualisierungen werden automatisch abgerufen und installiert.

Nachricht über die Ergebnisse der Aktualisierung per E-Mail senden
Diese Option bewirkt, dass die Systemverwalter von jeder Aktualisierung des Spam-Filters und den Ergebnissen der Aktualisierung benachrichtigt werden. Diese Option entspricht der Option "*Benachrichtigung über Spam-Filter-Aktualisierung an Systemverwalter senden*" im Konfigurationsdialog Inhaltsfilter » Benachrichtigungen.

Optionale Befehlszeilenparameter, die an SA-UPDATE übergeben werden sollen
Falls Sie Befehlszeilenparameter an SA-UPDATE übergeben wollen, tragen Sie diese Parameter in dieses Textfeld ein.

Jetzt nach Aktualisierungen suchen
Durch Anklicken dieses Steuerelements veranlassen Sie, dass sofort nach aktualisierten Regeln für den Spam-Filter gesucht wird, und dass eine allenfalls mögliche Aktualisierung sofort durchgeführt wird.

4.6.1.11 Berichte



Die Einstellungen zu den Berichten des Spam-Filters sind nicht verfügbar, wenn MDaemon den MDaemon-Spam-Daemon (MDSpamD) eines anderen MDaemon-Servers für den Spam-Filter verwendet. Die Berichte des Spam-Filters richten sich dann nach der Konfiguration des anderen Servers. Weitere Informationen enthält der Abschnitt Spam-Daemon 689.

Berichte

Bericht über Spam in die Kopfzeilen der Ursprungsnachricht einfügen
Diese Option bewirkt, dass der Spam-Filter die Kopfzeilen jeder als Spam erkannten Nachricht um einen Bericht ergänzt. Nachfolgend ist beispielhaft ein solcher Bericht, der in englischer Sprache erscheint, wiedergegeben:

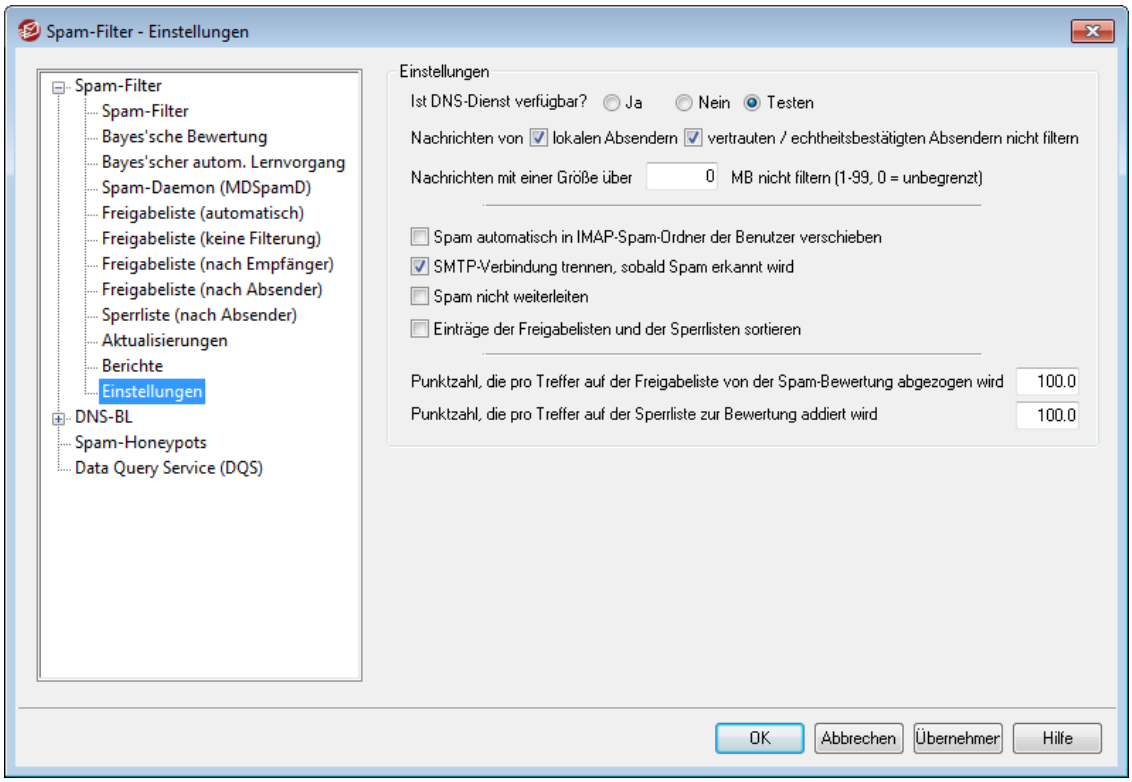
```
X-Spam-Report: ---- Start Spam Filter results
 5.30 points, 5 required;
 * -5.7 -- Message-Id indicates the message was sent from MS
Exchange
 * 2.0 -- Subject contains lots of white space
 * -3.3 -- Has a In-Reply-To header
```

```
 * 3.0 -- Message has been marked by MDaemon's DNS-BL
 * 2.9 -- BODY: Impotence cure
 * 2.2 -- BODY: Talks about exercise with an exclamation!
 * 0.5 -- BODY: Message is 80% to 90% HTML
 * 0.1 -- BODY: HTML included in message
 * 1.6 -- BODY: HTML message is a saved web page
 * 2.0 -- Date: is 96 hours or more before Received: date
---- End of Spam Filter results
```

Neue Nachricht erstellen und die Originalnachricht als Anlage einfügen
Diese Option bewirkt, dass der Spam-Filter eine neue Nachricht erstellt, die den Bericht über die Ergebnisse der Auswertung enthält. Die ursprüngliche Spam-Nachricht wird an diese neue Nachricht als Dateianlage angehängt.

Wie vor, jedoch Nachricht als text/plain einfügen
Wie bereits die letzte beschriebene Option, erstellt der Spam-Filter auch mit dieser Option eine eigene Nachricht, die den Bericht über die Spam-Auswertung sowie als Dateianlage die ursprüngliche Spam-Nachricht enthält. Anders als bei der vorherigen Option wird die ursprüngliche Nachricht hier jedoch als MIME-Dateianlage des Typs text/plain angehängt. Spam-Nachrichten enthalten manchmal besonderen HTML-Kode, der jeder Nachricht eindeutig zuordenbar ist und dem Spammer E-Mail- und IP-Adresse des Benutzers mitteilen kann, der diese Nachricht empfangen und geöffnet hat. Indem die Spam-Nachricht in reinen Text umgewandelt wird, bevor sie der Benutzer betrachten kann, wird auch solcher HTML-Kode deaktiviert.

4.6.1.12 Einstellungen



Einstellungen

Ist DNS-Dienst verfügbar?
Mithilfe dieser Option kann festgelegt werden, ob dem Spam-Filter bei der Verarbeitung von Nachrichten DNS zur Verfügung steht. Die folgenden drei Möglichkeiten stehen zur Auswahl:

Ja - DNS ist verfügbar; SURBL/RBL und andere Regeln, die DNS-Abfragen erfordern, werden daher genutzt.

Nein - DNS ist nicht verfügbar. Die Regeln des Spam-Filters, die DNS-Abfragen erfordern, werden nicht genutzt.

Testen - Die Verfügbarkeit des DNS wird geprüft, und nach positivem Ergebnis wird der DNS genutzt. Dies ist die Voreinstellung.

Nachrichten von...

lokalen Absendern nicht filtern
Diese Option nimmt Nachrichten von lokalen Benutzern und Domänen von der Bearbeitung durch den Spam-Filter aus.

vertrauten / echtheitsbestätigten Absendern nicht filtern
Sollen Nachrichten, die von vertrauten Domänen oder Absendern mit Echtheitsbestätigung aus versandt wurden, von der Bearbeitung durch den Spam-Filter ausgenommen sein, so muss diese Option aktiviert werden.

Nachrichten mit einer Größe über [xx] MB nicht filtern (1-99, 0 = unbegrenzt)
Spam-Nachrichten sind üblicherweise sehr klein, da es das Ziel der Spam-Versender ist, möglichst viele Nachrichten in möglichst kurzer Zeit zu versenden. Sollen Nachrichten über einer bestimmten Größe nicht mehr durch den Spam-Filter bearbeitet werden, so muss der Schwellwert für die Größe hier in MB angegeben werden. Der Wert 0 bewirkt, dass Nachrichten den Spam-Filter ohne Rücksicht auf ihre Größe durchlaufen.

Spam automatisch in IMAP-Spam-Ordner der Benutzer verschieben
Diese Option bewirkt, dass MDaemon automatisch jede als Spam erkannte Nachricht in den IMAP-Ordner "Spam" des betreffenden Benutzers verschiebt, falls dieser Ordner besteht. So lange die Option aktiv ist, wird der Ordner für jedes neue Benutzerkonto automatisch angelegt.

Beim Aktivieren dieser Option bietet MDaemon an, diesen Ordner auch für alle bereits bestehenden Benutzerkonten automatisch anzulegen. Falls Sie hier mit "Ja" antworten, werden die Ordner für alle Benutzer angelegt. Falls Sie hier mit "Nein" antworten, so werden die Spam-Ordner nur beim Erstellen neuer Benutzerkonten angelegt; die bestehenden Benutzerkonten bleiben unberührt. In keinem Falle wirkt sich die Änderung auf andere bereits bestehende IMAP-Ordner der Benutzer aus.

SMTP-Verbindung trennen, sobald Spam erkannt wird
Diese Option ist per Voreinstellung aktiv und trennt die SMTP-Verbindung, sobald im Rahmen der schritthaltenden Prüfung eine Spam-Nachricht erkannt wurde.

Spam nicht weiterleiten
Diese Option bewirkt, dass Nachrichten, die als Spam erkannt und gekennzeichnet wurden, nicht weitergeleitet werden.

Einträge der Freigabelisten und der Sperrlisten sortieren
Diese Option bewirkt, dass die Einträge in den Freigabelisten und den Sperrlisten stets sortiert werden. **Beachte:** Falls Sie in die zugehörigen Datendateien eigene Kommentare eingefügt haben (also Zeilen, die mit dem Zeichen # beginnen), werden diese Zeilen an den Anfang der Datei verschoben, sobald Sie die Option aktivieren. Diese Option ist per Voreinstellung abgeschaltet. Nach dem Einschalten der Option wird die Sortierung bei der nächsten Änderung an der Datendatei einer Freigabeliste oder Sperrliste erstmals durchgeführt.

Die weiteren Einstellungen in diesem Konfigurationsdialog sind nicht verfügbar, wenn MDaemon den MDaemon-Spam-Daemon (MDSpamD) eines anderen MDaemon-Servers für den Spam-Filter verwendet. Weitere Informationen hierzu enthält die Beschreibung des Konfigurationsdialogs Spam-Daemon 689.

Punktzahl, die pro Treffer auf der Freigabeliste von der Spam-Bewertung abgezogen wird
Nachrichten können auch dann als Spam bewertet und erkannt werden, wenn ihre Absender oder Empfänger in den Freigabelisten (nach Empfänger) 696 und den Freigabelisten (nach Absender) 697 geführt werden. Ein Eintrag des Absenders in der Freigabeliste bewirkt lediglich, dass von der Bewertung, die der Spam-Filter für die betreffende Nachricht ermittelt, die hier festgelegte Punktzahl abgezogen wird. Ein Beispiel hierzu. Ist der Schwellwert für die Erkennung als Spam auf 5,0 festgesetzt, und beträgt die abzuziehende Punktzahl 100, so kann theoretisch eine Nachricht, die besonders viele Spam-Kriterien erfüllt und daher mit dem Wert 105 oder höher bewertet wurde, nach Abzug der Punktzahl von 100 für den Eintrag in der Freigabeliste immer noch eine Bewertung von 5,0 oder höher erhalten und damit als Spam erkannt werden. Dies dürfte indessen selten passieren, weil Spam-Nachrichten kaum eine so hohe Punktzahl in der Bewertung erreichen, wenn sie nicht gerade besonders hoch bewertete Kriterien erfüllen, wie etwa eine Adresse, die in der Sperrliste geführt wird. Wird die abzuziehende Punktzahl für einen Eintrag in der Freigabeliste jedoch gegenüber dem Beispiel stark verringert, so dürfte dies deutlich öfter auftreten.

Falls Nachrichten, die an bestimmte Empfänger gerichtet sind, den Spam-Filter vollständig umgehen sollen, und auch eine bloße Änderung ihrer Spam-Bewertung nicht gewünscht ist, müssen die betreffenden Empfängeradressen in die Freigabeliste (keine Filterung) 695 eingetragen werden. Nachrichten können von der Bewertung durch den Spam-Filter auch mithilfe der Optionen im Konfigurationsdialog Freigabeliste (automatisch) 692 ausgenommen werden.

Punktzahl, die pro Treffer auf der Sperrliste zur Bewertung addiert wird
Was oben für den Eintrag in der Freigabeliste gesagt wurde, gilt für die Einträge in der Sperrliste (nach Absender) 698 entsprechend; auch sie bewirken nicht ohne weiteres, dass eine Nachricht als Spam angesehen wird. Stattdessen wird der Wert, der in diesem Feld angegeben ist, der Spam-Bewertung der Nachricht hinzugerechnet; erst der sich hieraus ergebende Wert entscheidet, ob es sich um Spam handelt.

4.6.2 Sperrlisten für DNS (DNS-BL)

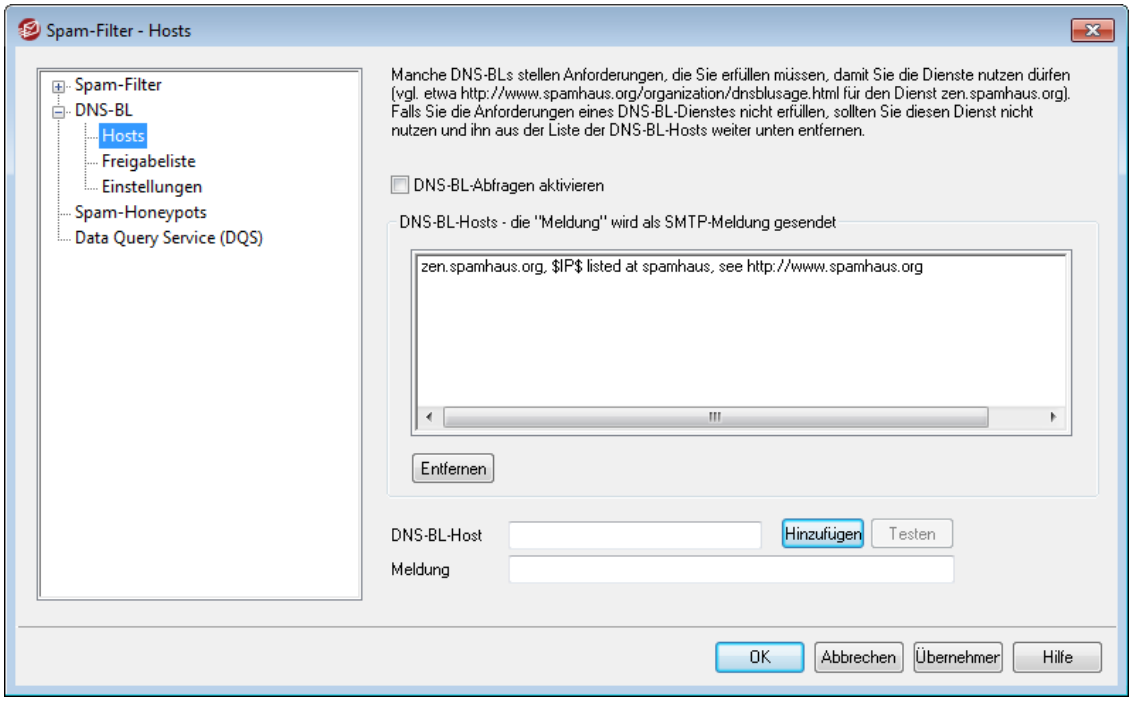
Sperrlisten für DNS, nach dem englischen Begriff DNS Block Lists auch DNS-BL abgekürzt, können helfen, Spam von Ihren Benutzern fernzuhalten. Diese Sicherheitsfunktion gestattet Ihnen die Nutzung verschiedener Sperrlisten für DNS (diese unterhalten Listen von Servern, die für Spam-Versand bekannt sind). Diese Listen werden jedes Mal abgefragt, wenn eine Gegenstelle versucht, eine Nachricht an Ihren Server zuzustellen. Falls die IP der Gegenstelle in einer der Listen erfasst ist, kann die Nachricht wahlweise abgewiesen oder in Übereinstimmung mit den Einstellungen im Abschnitt Optionen 706 gekennzeichnet werden.

Sperrlisten für DNS gestatten auch die Nutzung einer Freigabeliste für solche IP-Adressen, die von den DNS-BL-Abfragen ausgenommen sein sollen. Bevor Sie DNS-BL aktivieren, sollten Sie sicherstellen, dass Ihre lokalen IP-Adressbereiche in der Freigabeliste eingetragen sind, damit für diese Adressbereiche keine Abfragen durchgeführt werden. "127.0.0.1" ist immer ausgenommen und muss nicht eigens in die Liste eingetragen werden.

Siehe auch:

Hosts für DNS-BL 704
Optionen für DNS-BL 706
Freigabeliste für DNS-BL 705

4.6.2.1 Hosts



Hosts für DNS-BL

DNS-BL-Abfragen aktivieren
Soll eingehende Post anhand der Sperrlisten für DNS geprüft werden, so muss diese Option aktiv sein. MDaemon fragt alle hier angegebenen Server ab, um die IP-Adresse einer Gegenstelle mit Hilfe von DNS-BL zu überprüfen. Wenn die Antwort von einem Server positiv ausfällt, kann MDaemon alle Nachrichten von

der fraglichen Gegenstelle abweisen oder kennzeichnen, je nach dem, welche Einstellungen im Abschnitt Optionen für DNS-BL 706 getroffen sind.

Entfernen
Um einen Eintrag aus der Liste der DNS-BL-Dienste zu entfernen, wählen Sie den Eintrag aus der Liste aus, und klicken Sie dann auf dieses Steuerelement.

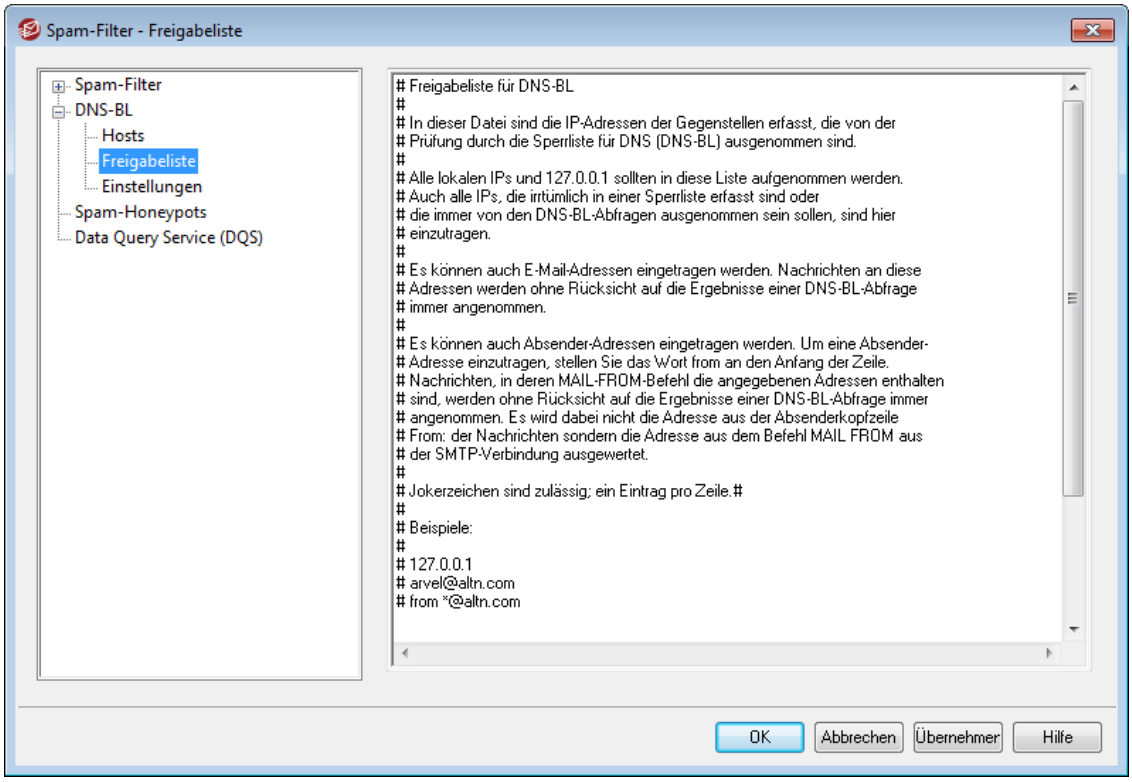
DNS-BL-Host
Um einen neuen Host einzutragen und nach IP-Adressen auf der Sperrliste abzufragen, geben Sie den Host hier ein.

Testen
Um einen Host zu testen, geben Sie den Hostnamen in das Feld *DNS-BL-Host* ein, und klicken Sie danach auf Testen. Hierdurch wird eine Abfrage nach 127.0.0.2 über den Host ausgeführt.

Meldung
Diese Meldung wird während der SMTP-Verbindung übermittelt, falls eine IP-Adresse durch im Feld *DNS-BL-Server* angegebenen Dienst erfasst ist. Dieses Textfeld gehört zu der Option *...und gibt statt "Benutzer unbekannt" die "Meldung" aus* im Abschnitt Optionen für DNS-BL 706.

Hinzufügen
Nachdem Sie Host und Nachricht eingetragen haben, klicken Sie auf dieses Steuerelement, um den Eintrag der Liste der DNS-BL-Hosts hinzuzufügen.

4.6.2.2 Freigabeliste

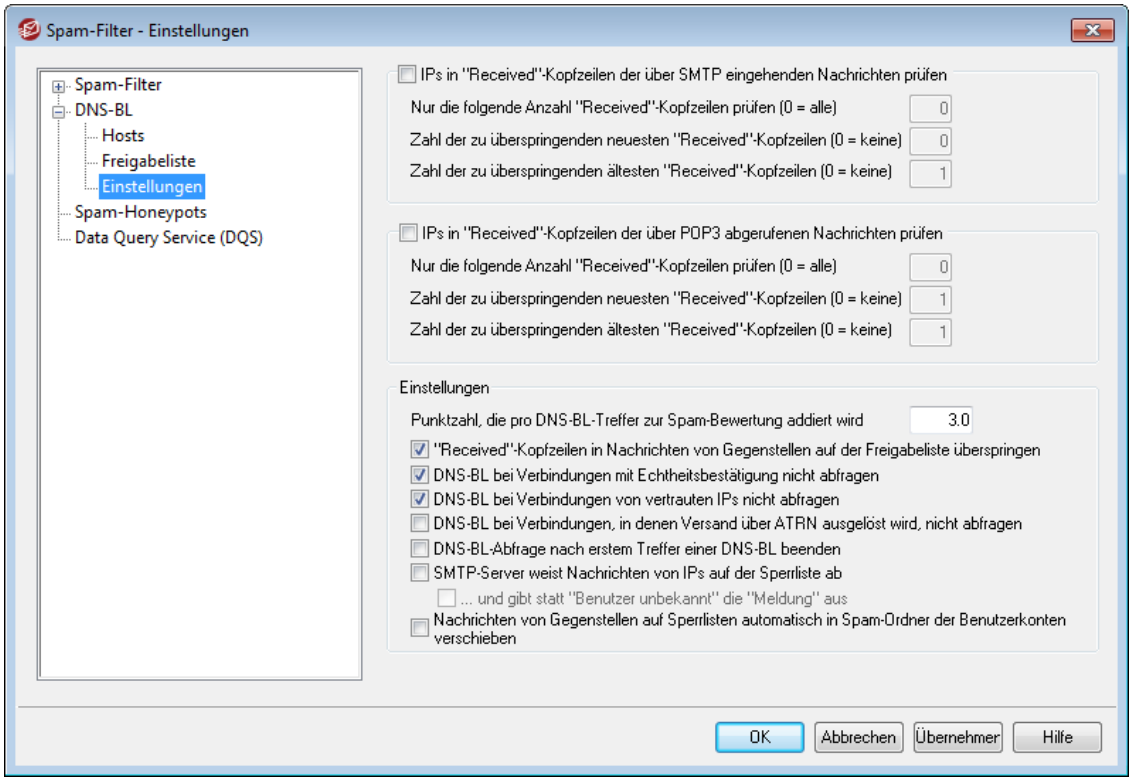


Mithilfe dieses Konfigurationsdialogs können Sie die IP-Adressen erfassen, die von den Abfragen der Sperrlisten für DNS (DNS-BL) ausgenommen sind. Es sollten immer

alle lokalen IP-Adressen erfasst sein, damit DNS-BL-Abfragen für Nachrichten von lokalen Benutzern und Domänen nicht durchgeführt werden. Lokale Adressbereiche sind insbesondere `127.0.0.*`, `192.168.*.*` usw. Sie können in der Liste auch E-Mail-Adressen erfassen. Ist eine Nachricht an eine hier erfasste E-Mail-Adresse gerichtet, so wird die Nachricht ohne Rücksicht auf die Ergebnisse der DNS-BL-Abfragen zur Zustellung angenommen. Sie können auch bestimmte Absender von der DNS-BL-Abfrage ausnehmen, indem Sie die Adressen der Absender nach dem Muster "from *Absender@example.com*" erfassen. Die hier erfassten Adressen werden mit den Daten aus dem SMTP-Befehl "MAIL FROM", nicht jedoch mit dem Inhalt der Absenderkopfzeile "From", abgeglichen.

Sie dürfen nur einen Eintrag je Zeile erfassen. Jokerzeichen sind zulässig.

4.6.2.3 Einstellungen



IPs in "Received"-Kopfzeilen der über SMTP eingehenden Nachrichten prüfen
Diese Option bewirkt, dass die IP-Adressen in den `Received`-Kopfzeilen der über SMTP empfangenen Nachrichten mit den Sperrlisten für DNS (DNS-BL) abgeglichen werden.

Nur die folgende Anzahl "Received"-Kopfzeilen prüfen (0 = alle)
Diese Option begrenzt die Anzahl der `Received` Kopfzeilen, die DNS-BL prüft. Die Prüfung beginnt mit dem neuesten Eintrag. Der Wert 0 bedeutet, dass alle `Received`-Kopfzeilen geprüft werden.

Zahl der zu überspringenden neuesten "Received"-Kopfzeilen (0 =keine)
Diese Option veranlasst DNS-BL, eine oder mehrere der neuesten `Received`-Kopfzeilen der über SMTP empfangenen Nachrichten bei der Prüfung zu überspringen.

Zahl der zu überspringenden ältesten "Received"-Kopfzeilen (0 =keine)
Diese Option veranlasst DNS-BL, eine oder mehrere der ältesten "Received"-Kopfzeilen der über SMTP empfangenen Nachrichten bei der Prüfung zu überspringen.

IPs in "Received"-Kopfzeilen der über POP3 abgerufenen Nachrichten prüfen
Diese Option bewirkt, dass die IP-Adressen in den "Received"-Kopfzeilen der über DomainPOP und MultiPOP empfangenen Nachrichten mit den Sperrlisten für DNS (DNS-BL) abgeglichen werden.

Nur die folgende Anzahl "Received"-Kopfzeilen prüfen (0 = alle)
Diese Option begrenzt die Anzahl der "Received" Kopfzeilen, die DNS-BL prüft. Die Prüfung beginnt mit dem neuesten Eintrag. Der Wert 0 bedeutet, dass alle "Received"-Kopfzeilen geprüft werden.

Zahl der zu überspringenden neuesten "Received"-Kopfzeilen (0 =keine)
Diese Option veranlasst DNS-BL, eine oder mehrere der neuesten "Received"-Kopfzeilen der über POP3 empfangenen Nachrichten bei der Prüfung zu überspringen. Da es beim Abruf von Nachrichten über POP3, wie etwa DomainPOP, oft erforderlich ist, die neueste "Received"-Kopfzeile zu überspringen, beträgt die Voreinstellung hier 1.

Zahl der zu überspringenden ältesten "Received"-Kopfzeilen (0 =keine)
Diese Option veranlasst DNS-BL, eine oder mehrere der ältesten "Received"-Kopfzeilen der über DomainPOP oder MultiPOP empfangenen Nachrichten bei der Prüfung zu überspringen.

Einstellungen

Punktzahl, die pro DNS-BL-Treffer zur Spam-Bewertung addiert wird
Diese Option bestimmt, welche Punktzahl der Spam-Bewertung[679] einer Nachricht hinzugerechnet wird, wenn ein Treffer auf einer Sperrliste für DNS gefunden wird. Die heuristische Bewertung einer Nachricht durch den Spam-Filter ergibt bisweilen einen Punktwert, der nicht hoch genug ist, um die Nachricht als Spam einzustufen. Ein Treffer auf einer Sperrliste für DNS kann dann darauf hinweisen, dass es sich doch um eine Spam-Nachricht handelt. Indem nach solchen Treffern der Nachrichtenbewertung eine bestimmte Punktzahl hinzugerechnet wird, können Nachrichten als Spam erkannt werden, die sonst möglicherweise irrtümlich als normale Nachrichten behandelt werden würden. Per Voreinstellung werden nach einem Treffer auf einer Sperrliste der Spam-Bewertung 3.0 Punkte hinzugerechnet.

DNS-BL nicht abfragen bei...

Verbindungen mit Echtheitsbestätigung
Diese Option bewirkt, dass für Verbindungen, die über den Befehl AUTH echtheitsbestätigt wurden, keine DNS-BL-Abfragen durchgeführt werden.

Verbindungen von vertrauten IPs
Diese Option bewirkt, dass für Adressen, die im Abschnitt Vertraute Hosts[520] erfasst sind, keine DNS-BL-Abfragen durchgeführt werden.

Verbindungen, in denen Versand über ATRN ausgelöst wird
Diese Option bewirkt, dass für Verbindungen, in denen der Versand wartender Nachrichten über ATRN ausgelöst wird, keine DNS-BL-Abfrage erfolgt. Diese

Option ist per Voreinstellung abgeschaltet. Sie können sie beispielsweise dann aktivieren, wenn Ihr Smarthost bereits für die eingehenden Nachrichten DNS-BL-Abfragen durchführt.

"Received"-Kopfzeilen in Nachrichten von Gegenstellen auf der Freigabeliste überspringen
Diese Option bewirkt, dass DNS-BL die "Received"-Kopfzeilen aus Nachrichten nicht prüft, wenn diese Nachrichten von einer in der Freigabeliste für DNS-BL[705] eingetragenen IP-Adresse stammen.

DNS-BL-Abfrage nach erstem Treffer einer DNS-BL beenden
Oft enthalten die Kopfzeilen der Nachrichten, die MDaemon verarbeitet, mehrere verschiedene Hostnamen, und es werden verschiedene DNS-BL-Dienste nach ihnen abgefragt. DNS-BL fragt üblicherweise alle vorhandenen Dienste nach allen in der Nachricht gefundenen Hostnamen ab, und zwar unabhängig von der Anzahl an Treffern, die bereits erzielt wurden. Diese Option bewirkt, dass DNS-BL die Abfragen für eine Nachricht nach dem ersten Treffer beendet.

SMTP-Server weist Nachrichten von IPs auf der Sperrliste ab
Wenn diese Option aktiv ist, weist MDaemon während der SMTP-Verbindung Nachrichten ab, deren DNS-BL-Abfrage ergeben hat, dass der Absender in einer Sperrliste für DNS erfasst ist. Falls diese Option abgeschaltet wird, werden Nachrichten von gesperrten Gegenstellen zur Zustellung angenommen; sie erhalten dann eine Kopfzeile X-MDDNSBL-Result. Mithilfe des Inhaltsfilters kann nach dieser Kopfzeile gesucht werden, die Nachrichten können im Rahmen der Möglichkeiten des Inhaltsfilters weiterverarbeitet werden. Nähere Informationen sind bei der Option *Nachrichten von Gegenstellen auf Sperrlisten automatisch in Spam-Ordner der Benutzerkonten verschieben* weiter unten aufgeführt. Ist diese Option aktiv, so weist MDaemon Nachrichten von erfassten IP-Adressen ab, statt sie zu kennzeichnen.

IP-Adressen können auch irrtümlich in Sperrlisten erfasst werden; Sie sollten daher die Option, Nachrichten von IP-Adressen auf einer Sperrliste für DNS abzuweisen, nur vorsichtig einsetzen. Sie können die Nachrichten nicht nur kennzeichnen, sondern auch ihre Spam-Bewertung auf Grundlage der DNS-BL-Ergebnisse anpassen. Die entsprechenden Optionen finden Sie im Abschnitt Spam-Filter[679].

...und gibt statt "Benutzer unbekannt" unbekannt die "Meldung" aus
Diese Option bewirkt, dass MDaemon während einer SMTP-Verbindung nach Erkennen einer gesperrten IP-Adresse die Nachricht an die Gegenstelle sendet, die mit dem Host für DNS-BL[704] verknüpft ist, auf dem die IP-Adresse erfasst war. Ist die Option nicht aktiv, so meldet MDaemon stattdessen der Gegenstelle "Benutzer unbekannt". Diese Option steht nur zur Verfügung, wenn Sie die Option "*SMTP-Server weist Nachrichten von IPs auf der Sperrliste ab*" weiter oben aktiviert haben.

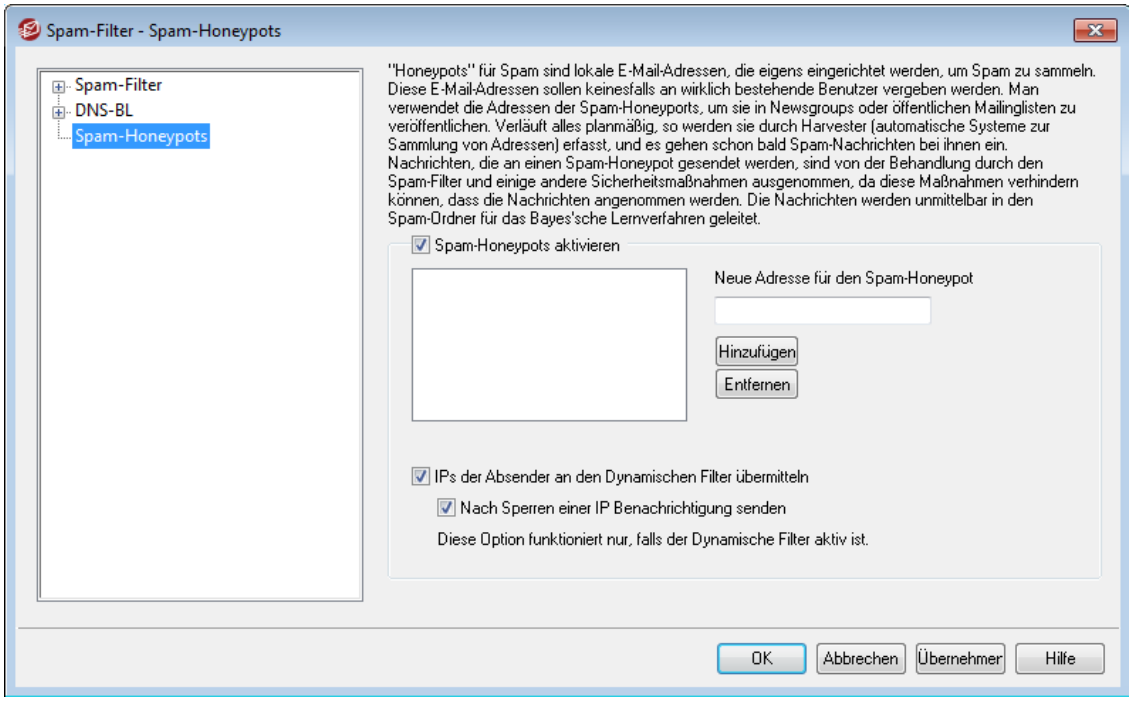
Nachrichten von Gegenstellen auf Sperrlisten automatisch in Spam-Ordner der Benutzerkonten verschieben
Ist diese Option aktiv, so wird für alle später angelegten Benutzerkonten automatisch ein IMAP-Ordner "Junk-E-Mail" unter dem Posteingangsordner erzeugt. MDaemon legt für diese Benutzer außerdem eine Filter-Regel an, die in

den eingehenden Nachrichten nach der Kopfzeile `X-MDDNSBL-Result` sucht und Nachrichten, die sie enthalten, in den Spam-Ordner des Benutzers verschiebt. Bei Auswahl dieser Option bietet MDaemon an, den Ordner und den Filter automatisch auch für alle bestehenden Benutzerkonten anzulegen. Nähere Informationen hierzu finden Sie unter Automatische Erstellung eines Spam-Ordners und -Filters für jedes Benutzerkonto 709.

Automatische Erstellung eines Spam-Ordners und -Filters für jedes Benutzerkonto

MDaemon kann für jedes Benutzerkonto automatisch einen IMAP-Ordner "Junk-E-Mail" unter dem Ordner Posteingang anlegen und einen Filter erzeugen, mit dessen Hilfe alle Nachrichten, die eine Kopfzeile `X-MDDNSBL-Result` enthalten, in den Spam-Ordner verschoben werden. Beim Aktivieren der Option *Nachrichten von Gegenstellen auf Sperrlisten automatisch in Spam-Ordner der Benutzerkonten verschieben* fragt MDaemon, ob der Ordner und der zugehörige Filter für alle Benutzerkonten angelegt werden sollen. Der Vorgang wird nach Auswahl von "Ja" in dem Dialogfenster automatisch abgewickelt. Obwohl sie natürlich keine lückenlose Sicherheit bieten kann, ist diese Methode doch eine einfache und im Allgemeinen zuverlässige Hilfe für die Benutzer, um Spam schnell zu erkennen. So lässt sich auch verhindern, dass Spam mit normalen Nachrichten vermischt wird, und die Benutzer müssen nur gelegentlich den Spam-Ordner durchsehen, um festzustellen, ob (was gelegentlich vorkommen kann), eine wichtige Nachricht unbeabsichtigt dorthin verschoben wurde. Falls MDaemon beim Anlegen der Ordner und Filter für die Benutzerkonten auf ein Benutzerkonto trifft, für das bereits ein Filter zur Auswertung der Kopfzeile `X-MDDNSBL-Result` besteht, wird dieses Benutzerkonto übersprungen, Ordner und Filter werden nicht angelegt. Soll der IMAP-Ordner einen anderen Namen erhalten als "Junk-E-Mail", so kann die entsprechende Voreinstellung mithilfe der Option *Voreinstellung für Namen des Spam-Ordners* im Abschnitt System 495 unter `Einstellungen » Voreinstellungen` angepasst werden.

4.6.3 Spam-Honeypots



Mithilfe des Leistungsmerkmals Spam-Honeypots (erreichbar über Sicherheit » Spam-Filter » Spam-Honeypots) können Sie lokale E-Mail-Adressen bestimmen, die eigens zum Sammeln von Spam vorgesehen sind. Die Spam-Honeypots sind keine gültigen MDaemon-Benutzerkonten und Aliasnamen für gültige Benutzerkonten. Sie sollen keinesfalls zum Empfang und Versand normaler Nachrichten verwendet werden. Sie werden stattdessen gezielt in Newsgroups, öffentlichen Mailinglisten und an anderen Stellen veröffentlicht, von denen bekannt ist, dass Spammer dort E-Mail-Adressen sammeln. Alsbald nach einer solchen Veröffentlichung werden Spam-Nachrichten in den Spam-Honeypots auflaufen. Zusätzlich können Spam-Honeypots aus nicht existierenden lokalen E-Mail-Adressen geschaffen werden, für die versucht wurde, Spam-Nachrichten zuzustellen. Da Spam-Honeypots keine normalen Nachrichten empfangen, werden alle unter ihren Adressen eingehenden Nachrichten direkt in den Spam-Ordner für das Bayes'sche Lernverfahren 683 geleitet und dort weiter verarbeitet. Wahlweise können auch die IP-Adressen der Server, die solche Nachrichten anliefern, in den Dynamischen Filter 567 übernommen werden. Verbindungen mit diesen Gegenstellen sind dann für die festgelegte Zeit gesperrt. Die Spam-Fallen helfen, die Treffergenauigkeit für die Spam-Erkennung zu erhöhen und das Blockieren von Spam-Nachrichten mit der Zeit immer zuverlässiger werden zu lassen.

Spam-Honeypots

In dieser Liste sind alle Adressen aufgeführt, die als Spam-Honeypots definiert wurden.

Spam-Honeypots aktivieren
Diese Option ist per Voreinstellung aktiv. Um die Leistungsmerkmale der Spam-Honeypots abzuschalten, deaktivieren Sie diese Option.

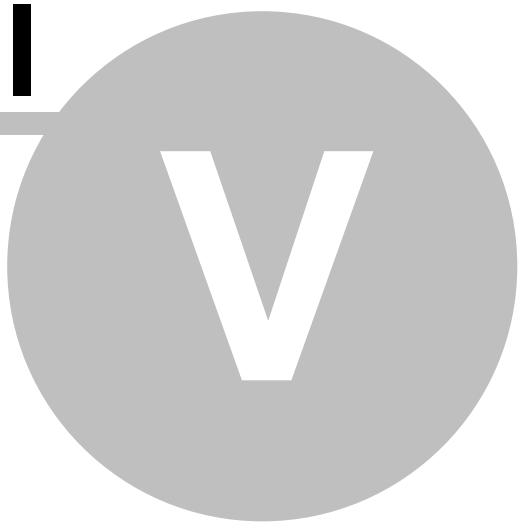
Neue Adresse für den Spam-Honeypot
Um einen Spam-Honeypot hinzuzufügen, muss seine Adresse hier eingetragen, danach muss *Hinzufügen* angeklickt werden.

Entfernen
Um einen Spam-Honeypot zu löschen, muss die zu löschende Adresse ausgewählt, danach muss *Entfernen* angeklickt werden.

IPs der Absender an den Dynamischen Filter übermitteln
Diese Option bewirkt, dass alle IP-Adressen, von denen aus Nachrichten an einen Spam-Honeypot übermittelt wurden, in den Dynamischen Filter 567 eingetragen werden. Diese Funktion ist jedoch nur verfügbar, wenn der Dynamische Filter (erreichbar über Sicherheit » Sicherheits-Einstellungen » Filter » Dynamischer Filter) auf dem Server aktiv ist.

Nach Sperren einer IP Benachrichtigung senden
Wird eine IP-Adresse durch den Dynamischen Filter gesperrt, so werden die im Konfigurationsdialog für die *Berichte über gesperrte IP-Adressen* 621 konfigurierten Empfänger von dieser Sperre unterrichtet. Falls Sie solche Benachrichtigungen nach einer Sperre, die durch einen Treffer auf einem Spam-Honeypot veranlasst wurde, nicht wünschen, deaktivieren Sie diese Option. Diese Option ist per Voreinstellung aktiv.

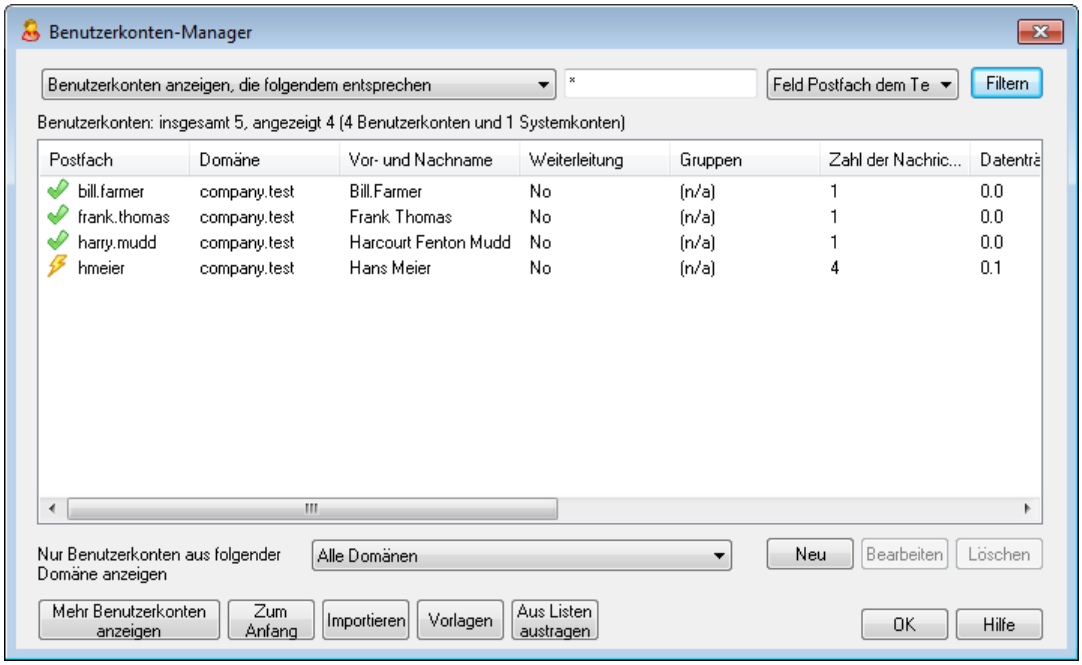
Kapitel



5 Das Menü Benutzerkonten

5.1 Der Benutzerkonten-Manager

Um die Auswahl, das Hinzufügen, Löschen und Ändern der Benutzerkonten zu erleichtern, verfügt MDaemon über einen Benutzer-Manager. Er ermöglicht den Zugriff auf Benutzerdaten und umfangreiche Auswahlfunktionen, unter anderem die Sortierung nach Postfach, Vor- und Nachname, Domäne und Nachrichten-Verzeichnis. Sie erreichen den Benutzerkonten-Manager im Menü Benutzerkonten über Benutzerkonten » Benutzerkonten-Manager...



Verwaltung der Benutzerkonten

Über der Liste der Benutzerkonten finden Sie zwei Statistiken zu den Benutzerkonten. Die erste Zahl gibt an, wie viele Benutzerkonten in MDaemon derzeit bestehen, die zweite Zahl gibt an, wie viele davon gerade im Listenfenster angezeigt werden. Welche Konten angezeigt werden, hängt davon ab, was bei der Option *Nur Benutzerkonten aus folgender Domäne anzeigen* ausgewählt ist. Nur bei der Auswahl "Alle Domänen" werden alle in MDaemon bestehenden Benutzerkonten aufgeführt. Sie finden oberhalb der Liste außerdem eine Suchfunktion, mit deren Hilfe Sie genau bestimmen können, welche Benutzerkonten angezeigt werden sollen. Sie sind dabei nicht auf die Auswahl einer ganzen Domäne beschränkt.

In jedem Listeneintrag erscheinen ein Symbol für den Zustand des Benutzerkontos (siehe unten), weiter der Postfachname, die Domäne, zu der das Konto gehört, der Vor- und Nachname des Benutzers, die Gruppen, denen das Benutzerkonto angehört, der Zeitpunkt des letzten Zugriffs auf das Benutzerkonto, das Nachrichten-Verzeichnis, in dem die Nachrichten abgelegt werden, sowie die Zahl der Nachrichten und der belegte Speicherplatz (in MB). Die Liste kann wahlweise auf- oder absteigend nach jeder gewünschten Spalte sortiert werden. Ein Klick auf eine Spaltenüberschrift sortiert die Liste nach dieser Spalte aufsteigend, ein erneuter Klick sortiert nach der Spalte absteigend.

Per Voreinstellung erscheinen in der Liste nur höchstens 500 Benutzerkonten gleichzeitig. Sollen mehr Benutzerkonten der gewählten Domäne oder aller Domänen angezeigt werden, muss zur Anzeige der nächsten 500 Einträge das Steuerelement *Mehr Benutzerkonten anzeigen* angeklickt werden. Sollen mehr als 500 Konten gleichzeitig angezeigt werden, müssen Sie in der Datei `MDaemon.ini` den Eintrag `MaxAccountManagerEntries=500` auf den gewünschten Wert setzen.

Symbole für den Zustand der Benutzerkonten

 Benutzerkonto ist ein globaler oder Domänen-Administrator.

 Benutzerkonto mit uneingeschränktem Zugriff. Zugriff über POP und IMAP ist zugelassen.

 Benutzerkonto mit eingeschränktem Zugriff. Zugriff entweder über POP oder IMAP ist gesperrt.

 Eingefrorenes Benutzerkonto. Das Benutzerkonto nimmt Nachrichten entgegen, der Benutzer kann Nachrichten aber weder abrufen noch versenden.

 Gesperrtes Benutzerkonto. Jeder Zugriff auf das Benutzerkonto ist gesperrt.

Neu
Dieses Steuerelement öffnet den Benutzerkonten-Editor 714, um ein neues Benutzerkonto anzulegen.

Bearbeiten
Dieses Steuerelement lädt den jeweils ausgewählte Eintrag der Kontenliste in den Benutzerkonten-Editor 714. Sie können Benutzerkonten auch durch Doppelklick zum Bearbeiten öffnen.

Löschen
Dieses Steuerelement löscht das gewählte Benutzerkonto; vorher wird eine Bestätigungsabfrage eingeblendet.

Mehr Benutzerkonten anzeigen
In der Kontenliste erscheinen nur höchstens 500 Einträge gleichzeitig. Bestehen in der ausgewählten Domäne mehr als 500 Benutzerkonten, so zeigt ein Klick auf diesen Knopf die jeweils nächsten 500 Konten an. Um die Zahl der gleichzeitig angezeigten Konten zu erhöhen, vgl. den oben stehenden Hinweis.

Zum Anfang
Mit diesem Knopf können Sie direkt zum Anfang der Liste springen.

Nur Benutzerkonten aus folgender Domäne anzeigen
Um alle bestehenden Benutzerkonten anzuzeigen, wählen Sie den Eintrag "Alle Domänen". Um nur die Konten einer bestimmten Domäne anzuzeigen, wählen Sie die Domäne aus.

Vorlagen
Durch Anklicken dieses Steuerelements rufen Sie den Konfigurationsdialog Gruppen & Vorlagen 782 auf. Von dort aus können Sie die Voreinstellungen für neue Benutzerkonten 788 und die Mitgliedschaften von Benutzerkonten in Benutzergruppen steuern.

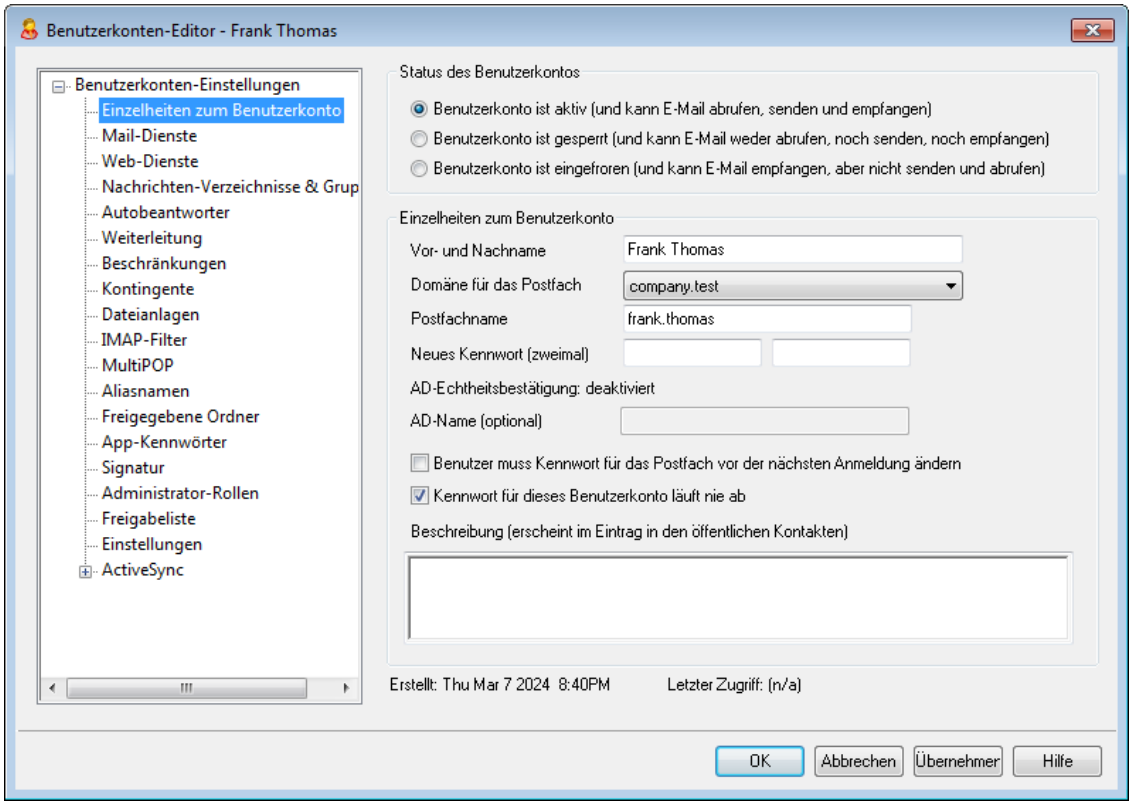
Aus Listen austragen
Mithilfe dieses Steuerelements können Sie ein Benutzerkonto oder mehrere Benutzerkonten aus allen Mailinglisten 275 austragen, die auf dem Server verwaltet werden. Wählen Sie dazu die gewünschten Benutzerkonten aus, und klicken Sie auf dieses Steuerelement. Es erscheint eine Sicherheitsabfrage, ob Sie die Adressen wirklich aus den Listen austragen wollen.

Siehe auch:

Benutzerkonten-Editor 714
Vorlage "Neue Benutzerkonten" 788

5.1.1 Der Benutzerkonten-Editor

5.1.1.1 Einzelheiten zum Benutzerkonto



Status des Benutzerkontos

Benutzerkonto ist aktiv (und kann E-Mail abrufen, senden und empfangen)
Diese Option ist per Voreinstellung aktiv. Sie bewirkt, dass das Benutzerkonto E-Mail-Nachrichten abrufen, versenden und empfangen kann.

Benutzerkonto ist gesperrt (und kann E-Mail weder abrufen, noch senden, noch empfangen)
Diese Option bewirkt, dass der Zugriff auf das Benutzerkonto vollständig unterbunden wird. Der Benutzer, dem das gesperrte Benutzerkonto gehört, kann keinen Zugriff auf das Konto erlangen, und MDaemon nimmt keine Nachrichten an, die an das Konto gerichtet sind. Das Konto wird nicht gelöscht, und es zählt auch zu den Benutzerkonten, die in der verwendeten Lizenz als belegt gerechnet werden. Ansonsten verhält sich MDaemon so, wie wenn das Benutzerkonto nicht besteht, wobei jedoch eine Ausnahme besteht: Ordner in dem Benutzerkonto, die zur gemeinsamen Nutzung mit anderen Benutzern freigegeben waren, bleiben für diese anderen Benutzer weiterhin zugänglich, und es gelten weiterhin die Berechtigungen, die in den Zugriffskontrolllisten (ACL) 311 eingerichtet sind.

Benutzerkonto ist eingefroren (und kann E-Mail empfangen, aber nicht senden und abrufen)
Diese Option bewirkt, dass das Benutzerkonto eingehende Nachrichten empfangen kann, dass aber aus dem Benutzerkonto keine Nachrichten abgerufen oder versendet werden können. Diese Option ist hilfreich, wenn etwa der Verdacht besteht, dass das Benutzerkonto durch Hijacking kompromittiert sein könnte. Das Einfrieren des Benutzerkontos verhindert, dass ein Angreifer auf die Nachrichten des Benutzerkontos zugreifen oder über das Benutzerkonto Nachrichten versenden kann; dennoch gehen eingehende Nachrichten nicht verloren.

Einzelheiten zum Benutzerkonto

Vor- und Nachname
Hier werden Vor- und Nachname des Kontoinhabers eingetragen. Während ein neues Benutzerkonto angelegt wird, werden in die meisten Felder im Benutzerkonten-Editor Daten aufgrund des Vor- und Nachnamens des Benutzers eingetragen; dies geschieht bereits während der Eingabe. Diese Daten werden anhand der Vorlagen und Einstellungen in den Voreinstellungen für neue Benutzerkonten erstellt. Vor- und Nachname dürfen die Zeichen "!" und "|" nicht enthalten.

Domäne für das Postfach
Aus diesem Auswahlmenü wählen Sie die Domäne aus, der das Benutzerkonto angehören, und die in der E-Mail-Adresse genutzt werden soll. Per Voreinstellung erscheint die Standard-Domäne 181 von MDaemon.

Postfachname
In dieses Feld muss der Postfachname eingetragen werden; dies ist der Teil der E-Mail-Adresse, der das Benutzerkonto von anderen Benutzerkonten derselben Domäne unterscheidet. Die vollständige E-Mail-Adresse (sie besteht aus den Elementen [*Postfachname*]@[*Domäne für das Postfach*]) dient als eindeutiges Identifikationsmerkmal des Benutzerkontos und zugleich als der Anmeldename für Dienste wie POP3, IMAP und Webmail. E-Mail-Adressen dürfen weder Leerzeichen noch die Zeichen "!" und "|" enthalten. In dieses Feld dürfen Sie auch das

Zeichen "@" nicht eintragen. Ein Eintrag darf also beispielsweise nur "frank.thomas" lauten, nicht jedoch "frank.thomas@".

Neues Kennwort (zweimal)
Falls Sie das Kennwort für das gerade bearbeitete Benutzerkonto ändern wollen, tragen Sie das neue Kennwort gleichlautend in beide Felder ein. Dies ist das Kennwort, mit dessen Hilfe sich das Benutzerkonto beim Zugriff über POP3, IMAP, Webmail und der Remoteverwaltung, bei Nutzung des Outlook Connectors sowie bei der Echtheitsbestätigung während des SMTP-Versandes anmelden muss. Die beiden Eingabefelder erscheinen rot hinterlegt, falls das Kennwort nicht zweimal gleich eingegeben wurde, oder falls es nicht alle Anforderungen an die Kennwörter 847 erfüllt.

Falls Sie für das gerade bearbeitete Benutzerkonto die Echtheitsbestätigung über das Active Directory 859 nutzen wollen, müssen Sie als Kennwort zwei Backslashes und danach den Namen der Windows-Domäne angeben, zu der der Benutzer gehört. Es ergibt sich beispielsweise der Eintrag `\\ALTN` statt `123Kennwort`. Unter den Eingabefeldern erscheint ein Hinweistext, der mitteilt, ob die dynamische Echtheitsbestätigung für das Benutzerkonto aktiv ist.

Jedes Benutzerkonto sollte mit einem Kennwort versehen sein, und zwar auch dann, wenn der Zugriff auf das Benutzerkonto über POP oder IMAP nicht zugelassen werden soll. Zusätzlich zur Echtheitsbestätigung für den Abruf von Nachrichten dienen E-Mail-Adresse und Kennwort auch der Fernwartung des Benutzerkontos und dem Abruf von Dateien. Falls der Zugriff auf das Benutzerkonto über POP oder IMAP verhindert werden soll, so sollen dazu die entsprechenden Optionen im Konfigurationsdialog Mail-Dienste 718 verwendet werden. Soll der Zugriff auf das Benutzerkonto vollständig unterbunden werden, so sollen dazu die Optionen *Benutzerkonto ist gesperrt* oder *Benutzerkonto ist eingefroren* weiter oben aktiviert werden.

AD-Name (optional)
Mithilfe dieser Einstellung können Sie, falls gewünscht, einen Benutzernamen im Active Directory angeben, über den der Zugriff auf dieses Benutzerkonto erfolgt.

Benutzer muss Kennwort für das Postfach vor der nächsten Anmeldung ändern
Diese Option bewirkt, dass das *Kennwort* für das gerade bearbeitete Benutzerkonto geändert werden muss, bevor ein Zugriff auf die Dienste POP, IMAP, SMTP, Webmail und die Remoteverwaltung wieder möglich ist. Der Benutzer kann sich zwar bei Webmail und der Remoteverwaltung noch anmelden, bevor er jedoch die entsprechenden Dienste nutzen kann, wird er aufgefordert, das Kennwort zu ändern. Damit die Benutzer ihre Kennwörter auch tatsächlich über Webmail oder die Remoteverwaltung ändern können, muss ihnen die Berechtigung zum Bearbeiten ihrer Kennwörter im Abschnitt Web-Dienste 720 erteilt sein. Nachdem der Benutzer das Kennwort geändert hat, wird diese Option wieder deaktiviert.

Für manche Benutzer kann es nur schwer oder gar nicht möglich sein, das Kennwort zu ändern. Sie sollten daher diese Funktion nur vorsichtig einsetzen.

Kennwort für dieses Benutzerkonto läuft nie ab
Diese Option bewirkt, dass das Kennwort für dieses Benutzerkonto nicht nach der Zeitspanne abläuft, die im Konfigurationsdialog Kennwörter[847] definiert ist.

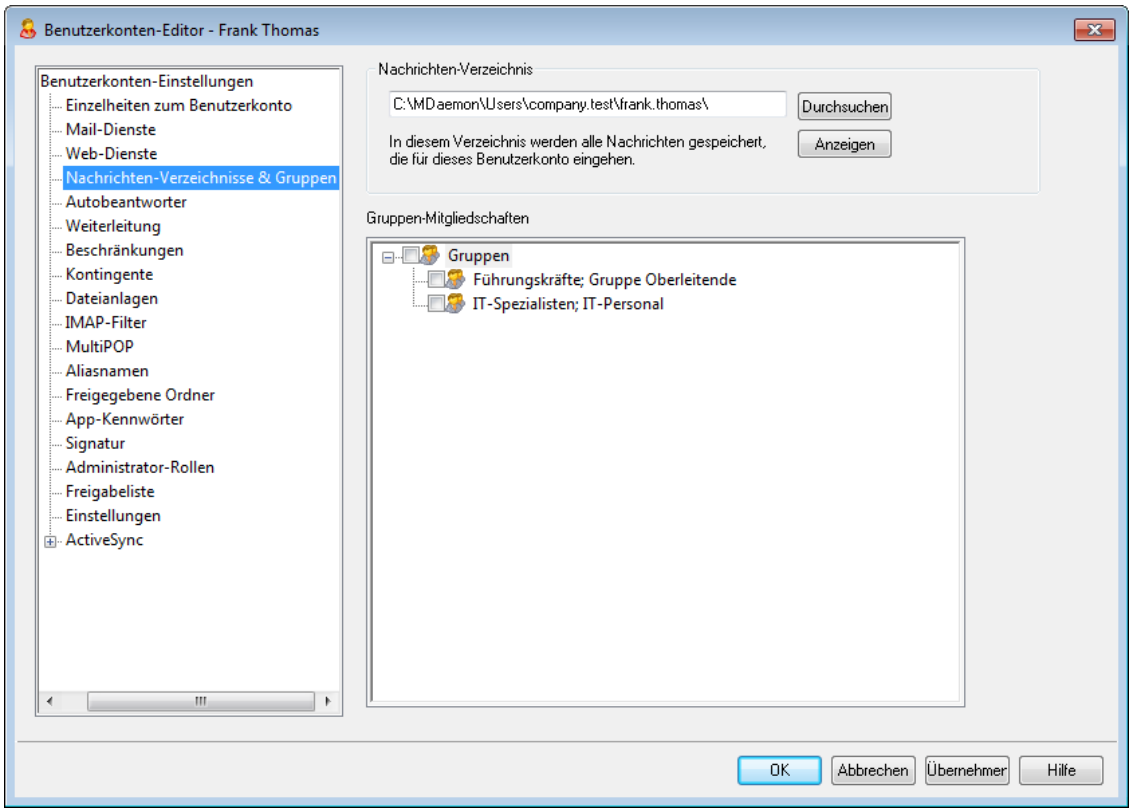
Beschreibung
In dieses Textfeld können Sie eine öffentlich sichtbare Beschreibung für dieses Benutzerkonto eintragen.

> Die Beschreibung, die Sie hier eintragen, wird in den Eintrag für dieses Benutzerkonto in den öffentlichen Kontakten übertragen. Sie ist für andere Benutzer sichtbar. Tragen Sie daher keine geheimhaltungsbedürftigen oder sonst vertraulichen Informationen in dieses Feld ein. Vertrauliche Anmerkungen zu diesem und Kommentare über dieses Benutzerkonto können Sie im Abschnitt Administrator-Rollen[757] erfassen.

Siehe auch:

AD-Echtheitsbestätigung[859]
Kennwörter[847]
Benutzerkonten-Editor » Web-Dienste[720]

5.1.1.2 Nachrichten-Verzeichnisse & Gruppen



Nachrichten-Verzeichnis

Hier können Sie das Verzeichnis eintragen, in dem Sie die E-Mail-Nachrichten des gerade bearbeiteten Benutzerkontos speichern wollen. Beim Anlegen eines neuen Benutzerkontos wird die Voreinstellung hierfür auf Grundlage der Einstellung *Nachrichten-Verzeichnis* in der Vorlage "Neue Benutzerkonten" 789 gebildet.

Anzeigen
Ein Klick auf dieses Steuerelement ruft den Warteschlangen- und Statistikmanager 876 auf und lädt das *Nachrichten-Verzeichnis* des gerade bearbeiteten Benutzers.

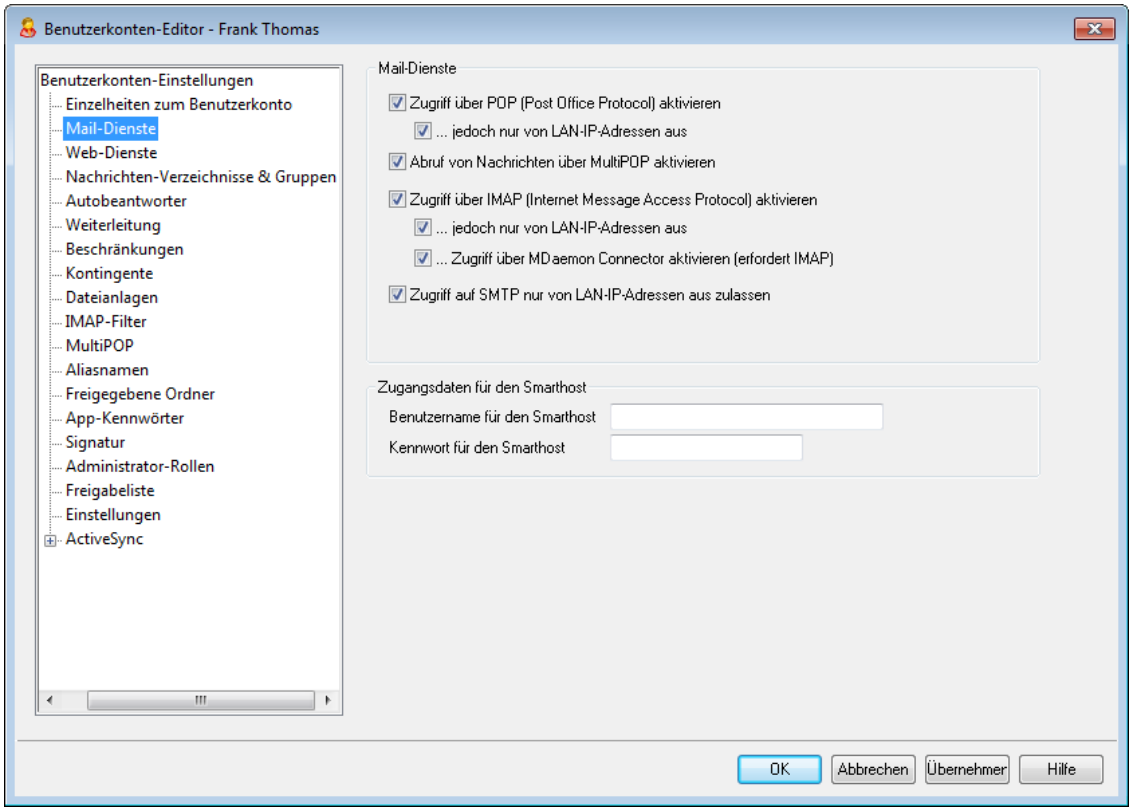
Gruppenmitgliedschaften

In diesem Abschnitt können Sie das Benutzerkonto in eine oder mehrere Gruppen 782 aufnehmen. Klicken Sie hierzu das Kontrollkästchen neben jeder Gruppe an, in die Sie das Benutzerkonto aufnehmen wollen.

Siehe auch:

Vorlage "Neue Benutzerkonten" 789
Gruppen 782

5.1.1.3 Mail-Dienste



Die Optionen in diesem Konfigurationsdialog steuern, auf welche Mail-Dienste das Benutzerkonto Zugriff erhält. Es stehen zur Auswahl POP, IMAP, MultiPOP und der MDaemon Connector. Es können auch besondere Zugangsdaten für den Zugang zum Smarthost festgelegt werden. Der Zugriff über Webmail wird mithilfe des Konfigurationsdialogs Web-Dienste 720 gesteuert.

Mail-Dienste

Zugriff über POP (Post Office Protocol) aktivieren
Diese Option ermöglicht den Zugriff auf die Nachrichten des Benutzerkontos über das Post Office Protocol (POP). Dieses Protokoll wird von nahezu allen E-Mail-Clients unterstützt.

...jedoch nur von LAN-IP-Adressen aus
Mithilfe dieser Option können Sie den Zugriff auf das Benutzerkonto über POP beschränken, sodass der Benutzer über dieses Protokoll nur von einer LAN-IP-Adresse 610 aus zugreifen kann.

Abruf von Nachrichten über MultiPOP aktivieren
Diese Option ermöglicht die Nutzung des Leistungsmerkmals MultiPOP 739 für dieses Benutzerkonto. MultiPOP erlaubt es dem Benutzer, Nachrichten von anderen E-Mail-Konten abzurufen, die auf anderen Mail-Servern unterhalten werden.

Zugriff über IMAP (Internet Message Access Protocol) aktivieren
Diese Option ermöglicht den Zugriff auf die Nachrichten des Benutzerkontos über das Internet Message Access Protocol (IMAP). IMAP ist vielseitiger als POP und gestattet die Verwaltung der Nachrichten auf dem Server sowie den Zugriff über mehrere verschiedene E-Mail-Clients. Dieses Protokoll wird von den meisten E-Mail-Clients unterstützt.

...jedoch nur von LAN-IP-Adressen aus
Mithilfe dieser Option können Sie den Zugriff auf das Benutzerkonto über IMAP beschränken, sodass der Benutzer über dieses Protokoll nur von einer LAN-IP-Adresse 610 aus zugreifen kann.

...Zugriff über MDaemon Connector aktivieren (erfordert IMAP)
Diese Option ermöglicht dem Benutzerkonto die Nutzung des MDaemon Connectors 385. **Beachte:** Diese Option ist nur verfügbar, wenn der MDaemon Connector auf dem Server aktiv ist.

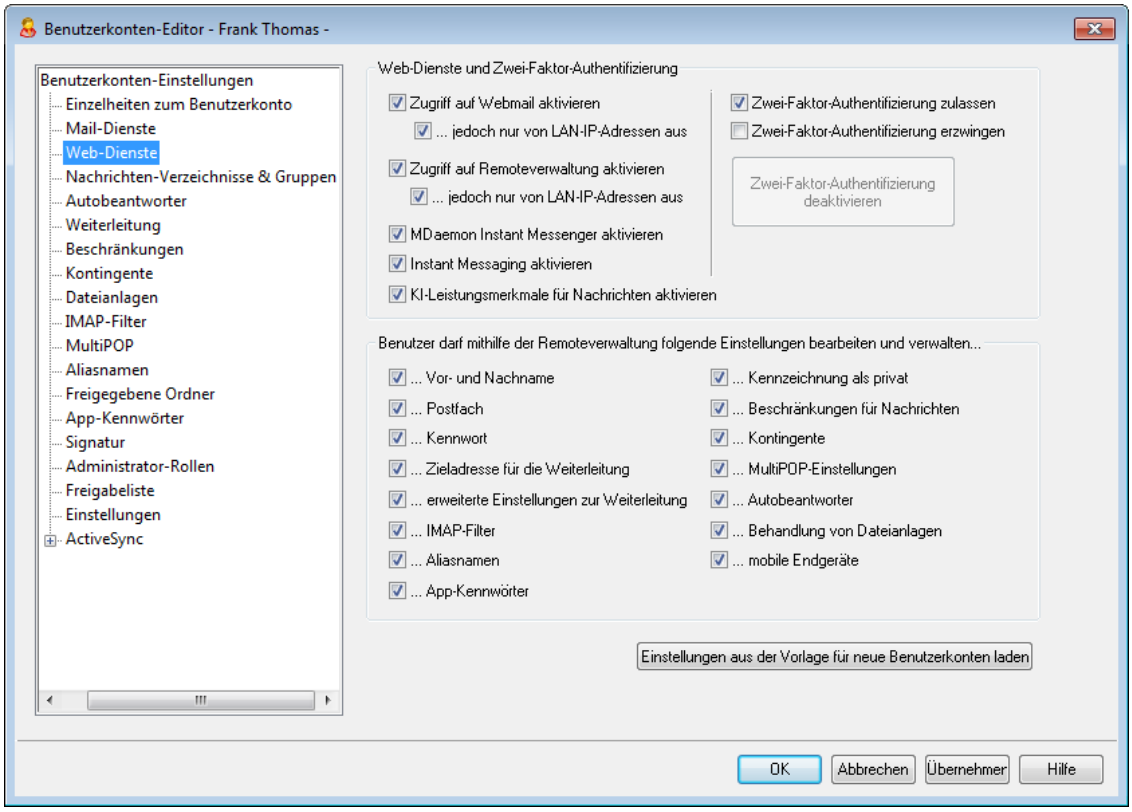
Zugriff auf SMTP nur von LAN-IP-Adressen aus zulassen
Diese Option beschränkt den Zugriff auf SMTP und lässt den Zugriff durch das Benutzerkonto nur von LAN-IP-Adressen aus. Hierdurch wird verhindert, dass Benutzerkonten E-Mail-Nachrichten über den Server versenden, solange sie nicht mit dem lokalen Netzwerk verbunden sind. Versucht ein Benutzerkonto, Nachrichten von externen IP-Adressen aus zu versenden, so wird der Verbindungsversuch abgewiesen.

Zugangsdaten für den Smarthost

Benutzername/Kennwort für Smarthost
Ist im Abschnitt Postausgang 97 des Menüs Einstellungen » Server-Einstellungen die Option *Nach Benutzerkonten getrennte Echtheitsbestätigung* aktiv, und soll MDaemon für die Echtheitsbestätigung bei abgehendem Nachrichtenversand über den Smarthost nicht den Benutzernamen und das Kennwort aus dem Konfigurationsdialog Postausgang übermitteln, so muss hier ein Kennwort für den Smarthost eingetragen sein. MDaemon übermittelt dann beim Versand abgehender Nachrichten dieses Benutzerkontos die E-Mail-Adresse und das Kennwort für den Smarthost für das Benutzerkonto. Soll die nach Benutzerkonten

getrennte Echtheitsbestätigung für dieses Benutzerkonto nicht genutzt werden, so muss diese Option leer bleiben.

5.1.1.4 Web-Dienste



Web-Dienste

Zugriff auf Webmail aktivieren
Diese Option bewirkt, dass das Benutzerkonto Zugriff auf den Dienst Webmail[317] erhält, der die Abfrage von E-Mail, die Verwaltung der Kalender und die Nutzung weiterer Leistungsmerkmale per Web-Browser zulässt.

...jedoch nur von LAN-IP-Adressen aus
Mithilfe dieser Option können Sie den Zugriff auf das Benutzerkonto über Webmail beschränken, sodass der Benutzer über diesen Dienst nur von einer LAN-IP-Adresse[610] aus zugreifen kann.

Zugriff auf Remoteverwaltung aktivieren
Diese Option bewirkt, dass der Benutzer die Einstellungen seines Benutzerkontos über die Remoteverwaltung[350] bearbeiten kann. Die Benutzer dürfen dort nur jene Einstellungen bearbeiten, die Sie im Folgenden freigeben.

Ist dieses Leistungsmerkmal aktiv, und wird der Remoteverwaltungs-Server ausgeführt, so kann sich der Benutzer bei der Remoteverwaltung anmelden. Er muss dazu in einem Browser die gewünschte MDaemon-Domäne und den Port, der der Remoteverwaltung zugewiesen ist[352], angeben (z.B. `http://example.com:1000`). Es erscheint zunächst ein Anmeldedialog und dann eine Übersicht aller Einstellungen, die der Benutzer bearbeiten darf. Nachdem er die Einstellungen bearbeitet und durch Anklicken des entsprechenden Steuerelements die Änderungen gespeichert hat, kann er sich wieder abmelden

und den Browser schließen. Falls der Benutzer auch Zugriff auf Webmail hat, kann er über die erweiterten Einstellungen aus Webmail heraus die Remoteverwaltung ebenfalls aufrufen.

Falls der Benutzer ein globaler oder Domänen-Administrator ist (beides wird im Abschnitt Administrator-Rollen 757 des Benutzerkonten-Editors festgelegt), wird ihm nach der Anmeldung an der Remoteverwaltung ein anderer Konfigurationsdialog angezeigt.

...jedoch nur von LAN-IP-Adressen aus
Mithilfe dieser Option können Sie den Zugriff auf das Benutzerkonto über die Remoteverwaltung beschränken, sodass der Benutzer über diesen Dienst nur von einer LAN-IP-Adresse 610 aus zugreifen kann.

MDaemon Instant Messenger aktivieren
Diese Option bewirkt, dass das gerade bearbeitete Benutzerkonto den MDIM 318 nutzen darf.

Instant Messaging aktivieren
Diese Option bewirkt, dass das gerade bearbeitete Benutzerkonto auch die Instant-Messaging-Funktionen des MDIM nutzen darf. Diese Option ist nur wirksam, wenn die Option *MDaemon Instant Messenger aktivieren* ebenfalls aktiv ist. Falls Sie diese Option deaktivieren, wird dem Benutzer der Zugriff auf MDIM ermöglicht, gleichzeitig aber die Nutzung der Instant-Messaging-Funktionen unterbunden.

Zwei-Faktor-Authentifizierung

MDaemon unterstützt die Zwei-Faktor-Authentifizierung (2FA) für alle Benutzer, die sich an den Webschnittstellen von Webmail und der Remoteverwaltung anmelden. Benutzerkonten, die sich an Webmail über HTTPS anmelden, können die Zwei-Faktor-Authentifizierung über den Konfigurationsdialog **Optionen » Sicherheit** aktivieren. Ab diesem Zeitpunkt muss der Benutzer bei jeder Anmeldung an Webmail oder der Remoteverwaltung einen Bestätigungkode eingeben. Der Benutzer erhält den Bestätigungskode während der Anmeldung über eine Authentifizierungs-App, die er auf seinem Mobiltelefon oder Tablet installiert. Dieses Leistungsmerkmal arbeitet mit allen Clients, die den Google Authenticator unterstützen. Die Hilfe für Webmail enthält nähere Informationen über die Einrichtung der Zwei-Faktor-Authentifizierung für die Benutzerkonten.

Zwei-Faktor-Authentifizierung zulassen
Neue Benutzerkonten 795 dürfen per Voreinstellung die Zwei-Faktor-Authentifizierung in Webmail aktivieren und nutzen. Um die Zwei-Faktor-Authentifizierung für das gerade bearbeitete Benutzerkonto zu sperren, deaktivieren Sie diese Option.

Zwei-Faktor-Authentifizierung erzwingen
Diese Option bewirkt, dass das Benutzerkonto die Zwei-Faktor-Authentifizierung für die Anmeldung an Webmail nutzen muss. Falls sie für das Benutzerkonto noch nicht eingerichtet ist, wird der Benutzer bei der nächsten Anmeldung an Webmail auf eine Konfigurationsseite umgeleitet, auf der er die Zwei-Faktor-Authentifizierung einrichten muss. Die Hilfe für Webmail enthält nähere Informationen über die Einrichtung der Zwei-Faktor-Authentifizierung für die Benutzerkonten.

Zwei-Faktor-Authentifizierung deaktivieren
Durch Anklicken dieses Steuerelements können Sie die Zwei-Faktor-Authentifizierung für das Benutzerkonto deaktivieren. Dies kann beispielsweise erforderlich sein, wenn das für die Zwei-Faktor-Authentifizierung genutzte Endgerät verloren gegangen ist oder der Benutzer auf die Daten für die Zwei-Faktor-Authentifizierung nicht mehr zugreifen kann.

Benutzer darf mithilfe der Remoteverwaltung folgende Einstellungen bearbeiten und verwalten...

Vor- und Nachname
Diese Option berechtigt den Benutzer, seinen *Vor- und Nachnamen* 714 zu bearbeiten.

Postfach
Diese Option berechtigt den Benutzer, den *Postfachnamen* 714 als Teil der E-Mail-Adresse zu bearbeiten.

Der Postfachname ist Teil der E-Mail-Adresse des Benutzerkontos, und diese dient zugleich als eindeutiges Identifizierungsmerkmal für das Benutzerkonto und als Benutzer- oder Anmeldename. Ändert der Benutzer den Postfachnamen, so ändert sich daher auch die E-Mail-Adresse. Nachrichten an die alte E-Mail-Adresse könnten dann abgewiesen oder gelöscht werden, oder sonst verloren gehen.

Kennwort
Diese Option berechtigt den Benutzer, sein Kennwort für sein Postfach zu bearbeiten. Weitere Informationen über die Kennwörter finden Sie im Abschnitt Kennwörter 847.

Zieladresse für die Weiterleitung
Diese Option berechtigt den Benutzer, die Zieladresse für die Weiterleitung 727 zu bearbeiten.

erweiterte Einstellungen zur Weiterleitung
Diese Option berechtigt den Benutzer, die erweiterten Einstellungen zur Weiterleitung 727 zu bearbeiten.

IMAP-Filter
Diese Option berechtigt den Benutzer, eigene IMAP-Filter 736 zu erstellen und zu bearbeiten.

Aliasnamen
Diese Option berechtigt den Benutzer, die Konfiguration seiner Aliasnamen 741 über die Remoteverwaltung zu bearbeiten.

App-Kennwörter
Per Voreinstellung dürfen die Benutzer ihre App-Kennwörter[750] bearbeiten. Falls Sie Ihren Benutzern das Bearbeiten der App-Kennwörter nicht gestatten wollen, deaktivieren Sie diese Option.

Kennzeichnung als privat
Diese Option berechtigt den Benutzer, die Option *Benutzerkonto aus Listen "Everyone" und Ordner Öffentliche Kontakte der Domäne ausblenden* im Abschnitt Optionen[760] des Benutzerkonten-Editors zu bearbeiten.

Beschränkungen für Nachrichten
Diese Option berechtigt den Benutzer, die Beschränkungen für eingehende und abgehende Nachrichten zu bearbeiten, die über den Konfigurationsdialog Beschränkungen[729] erreichbar sind.

Kontingente
Diese Option berechtigt den Benutzer, seine Kontingenteinstellungen[731] zu bearbeiten.

MultiPOP-Einstellungen
Diese Option berechtigt die Benutzer, mithilfe der MDaemon-Remoteverwaltung[350] neue MultiPOP-Einträge[739] hinzuzufügen und den Abruf von Nachrichten für diese Einträge über MultiPOP zu aktivieren und zu deaktivieren. Ist diese Option aktiv, und ist für das betreffende Benutzerkonto auch die Option *MultiPOP aktivieren*[739] aktiv, so steht den Benutzern in Webmail[317] die Seite Postfächer zur Verfügung. Dort können die Benutzer die MultiPOP-Einstellungen verwalten. Die systemweit gültige Option zum Aktivieren und Deaktivieren des MultiPOP-Servers finden Sie unter Einstellungen » Server-Einstellungen » MultiPOP[145].

Autobeantworter
Diese Option berechtigt den Benutzer, eigene Autobeantworter[724] zu erstellen, zu bearbeiten und zu löschen.

Behandlung von Dateianlagen
Diese Option berechtigt den Benutzer, die Optionen zur Behandlung von Dateianlagen zu bearbeiten, die im Abschnitt Dateianlagen[734] erreichbar sind.

mobile Endgeräte
Diese Option berechtigt den Benutzer zur Nutzung der Remoteverwaltung von MDaemon zur Verwaltung der Einstellungen für ihre mobilen Endgeräte, etwa für ActiveSync-Endgeräte.

Voreinstellung setzen
Durch Anklicken dieses Steuerelements werden alle Einstellungen in diesem Konfigurationsdialog auf die Standard-Einstellungen zurückgesetzt, die im Abschnitt Web-Dienste im Menü Benutzerkonten » Gruppen & Vorlagen » Vorlage "Neue Benutzerkonten" festgelegt werden.

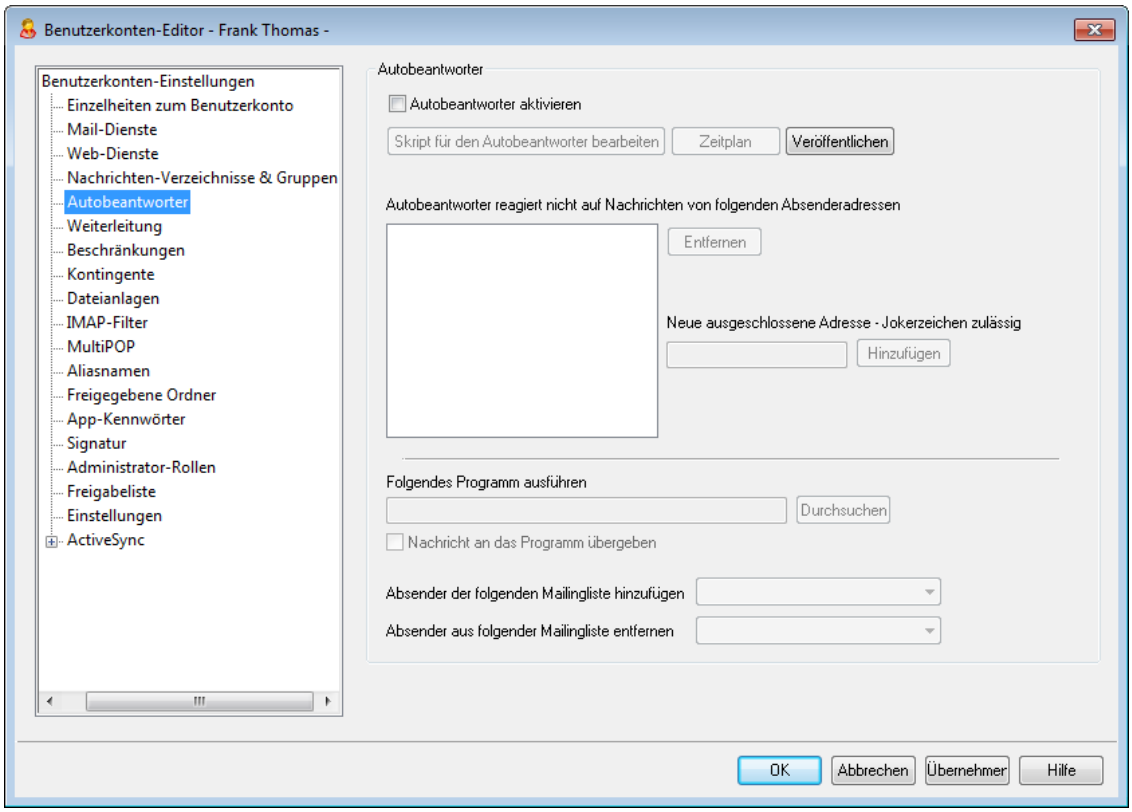
Einstellungen aus der Vorlage für neue Benutzerkonten laden

Durch Anklicken dieses Steuerelements können Sie die Einstellungen in diesem Konfigurationsdialog auf die Voreinstellungen zurücksetzen. Diese Voreinstellungen werden im Abschnitt Web-Dienste[795] der Vorlage "Neue Benutzerkonten" festgelegt.

Siehe auch:

Webmail 317
Remoteverwaltung 350
Vorlagen-Manager » Web-Dienste 795

5.1.1.5 Autobeantworter



Autobeantworter sind nützliche Werkzeuge, mit denen Aktionen durch eingehende E-Mail-Nachrichten ausgelöst werden können. Eine weit verbreitete Einsatzmöglichkeit für Autobeantworter ist es, eine benutzerdefinierte Nachricht als "Anrufbeantworter" für abwesende oder anderweit an der Beantwortung eingehender Nachrichten verhinderte Benutzer zu verwenden. Eingehende Nachrichten können mit ihrer Hilfe automatische benutzerdefinierte Antwortnachrichten oder eine Programmausführung auf dem Server auslösen, wobei die Nachricht selbst über die Kommandozeile an das externe Programm übergeben wird. MDaemon-Benutzer mit Web-Zugriff 720 auf Webmail 317 oder die Remoteverwaltung 350 können diese Verwaltungswerkzeuge verwenden, um Nachrichten und Zeitpläne für den Autobeantworter selbst zu erstellen. Nachrichten der Autobeantworter stützen sich auf die Inhalte der Dateien `OOF.mrk`, die in den Verzeichnissen `\data\` unter den jeweiligen Hauptverzeichnissen der Benutzerkonten abgelegt sind. Diese Dateien unterstützen zahlreiche Makros, und die Inhalte der Nachrichten der Autobeantworter lassen sich hierdurch weitgehend dynamisch gestalten. Autobeantworter sind hierdurch sehr vielseitig einsetzbar.

Nachrichten von externen Absendern lösen Autobeantworter immer aus. Auf Nachrichten von Benutzern derselben Domäne reagieren Autobeantworter nur, falls die

> Einstellung *Autobeantworter reagieren auf Nachrichten aus eigenen Domänen* im Konfigurationsdialog Autobeantworter » Einstellungen 835 aktiv ist. Dort steht auch eine weitere Option zur Verfügung, die die Anzahl der automatisch erzeugten Antwortnachrichten auf eine Antwort pro Empfänger und Tag begrenzt.

Autobeantworter

Autobeantworter aktivieren

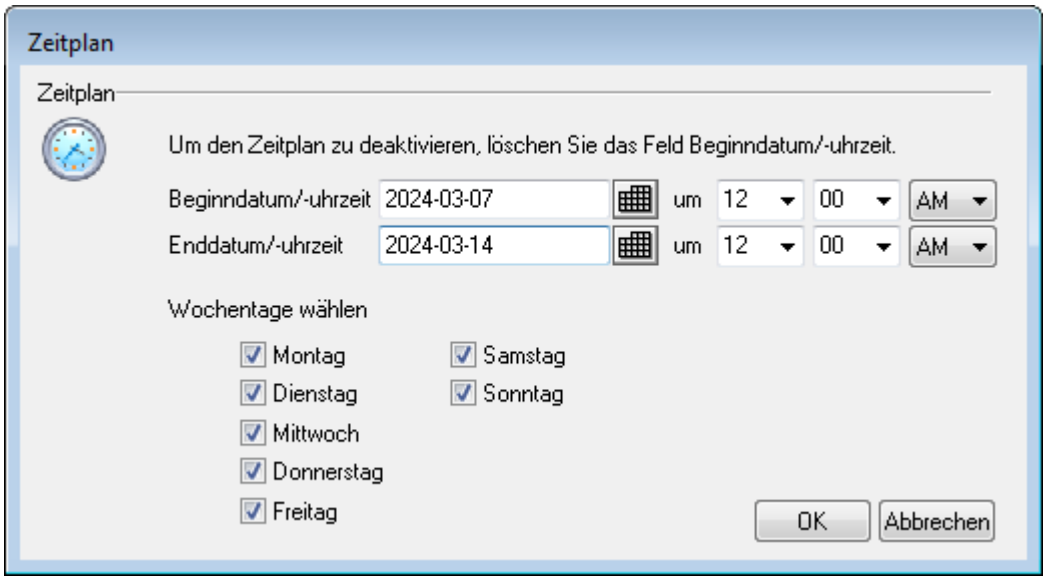
Mit dieser Option wird ein Autobeantworter für das gegenwärtige Benutzerkonto aktiviert. Nähere Informationen über Autobeantworter erhalten Sie im Abschnitt Autobeantworter 831.

Skript für den Autobeantworter bearbeiten

Durch Anklicken dieses Steuerelements können Sie die Datei des Autobeantworters für das Benutzerkonto bearbeiten. Der Name dieser Datei lautet `OOF.mrk`, und sie ist im Verzeichnis `\data\` unter dem Hauptverzeichnis des Benutzerkontos gespeichert.

Zeitplan

Ein Klick auf dieses Steuerelement öffnet den Konfigurationsdialog für die Zeitsteuerung der Autobeantworter. Dort können Daten und Uhrzeiten für Beginn und Ende der Autobeantworter festgelegt werden, sowie die Wochentage, an denen der Autobeantworter aktiv sein soll. Die Uhrzeit muss dabei nach US-amerikanischem Standard im 12-Stunden-Format unter Verwendung von AM und PM eingetragen werden. Soll der Autobeantworter immer aktiv sein, dann darf in diesem Konfigurationsdialog nichts eingetragen werden.



Veröffentlichen

Mithilfe dieses Steuerelements können Sie Datei und Einstellungen des Autobeantworters aus diesem Benutzerkonto auf ein anderes Benutzerkonto oder mehrere andere Benutzerkonten übertragen. Wählen Sie dazu die Benutzerkonten, auf die Sie die Datei und die Einstellungen übertragen wollen, und klicken Sie anschließend auf **OK**.

Autobeantworter reagiert nicht auf Nachrichten von folgenden Absenderadressen
Absender-Adressen, die hier eingetragen sind, lösen den Autobeantworter nicht aus.

Manchmal werden Nachrichten von Autobeantwortern an Adressen gesandt, die ihrerseits automatisch antworten. Dies kann einen "Ping-Pong-Effekt" auslösen; die Nachrichten werden immer wieder zwischen beiden Servern hin- und hergeschickt. Mit der oben stehenden Funktion lässt sich verhindern, dass MDaemon automatische Antwortnachrichten an solche Adressen schickt. Im Konfigurationsdialog Autobeantworter » Einstellungen 835 steht auch eine weitere Option zur Verfügung, die die Anzahl der automatisch erzeugten Antwortnachrichten auf eine Antwort pro Empfänger und Tag begrenzt.

Entfernen
Durch Anklicken dieses Steuerelements werden die gewählten Einträge aus der Liste ausgeschlossener Adressen entfernt.

Neue ausgeschlossene Adresse - Jokerzeichen zulässig
Soll eine neue Adresse ausgeschlossen werden, wird sie hier eingetragen und durch einen Klick auf *Hinzufügen* der Liste angefügt.

Bearbeiten
Durch Anklicken dieses Steuerelements können Sie das ausgewählte Skript für den Autobeantworter bearbeiten.

Ausführen eines Programms

Folgendes Programm ausführen
Hier sind Pfad und Dateiname eines Programms anzugeben, das nach dem Empfang neuer Nachrichten in dem entsprechenden Postfach ausgeführt werden soll. Das Programm muss unbeaufsichtigt laufen können und muss sich jedenfalls selbst beenden. Zusätzliche Befehlszeilenparameter können nach dem Dateinamen angegeben werden.

Nachricht an das Programm übergeben
Mit dieser Option wird dem oben angegebenen Programm der Name der empfangenen Nachrichtendatei als erster verfügbarer Befehlszeilenparameter übergeben. Diese Funktion ist gesperrt und wirkungslos, wenn der Autobeantworter für ein Benutzerkonto mit Nachrichten-Weiterleitung eingerichtet ist und keine Kopien der weitergeleiteten Post aufbewahrt werden (siehe Weiterleitung 727).

MDaemon übergibt den Dateinamen grundsätzlich als letzten Parameter an die Befehlszeile. Dieses Verhalten kann mit dem Makro `$MESSAGE$` geändert werden. Dieses Makro muss auf der Kommandozeile dort eingesetzt werden, wo der Dateiname stehen soll. Damit lässt sich auch eine komplex aufgebaute Kommandozeile wie die folgende herstellen: `logmail /e /j /message=$MESSAGE$ /q`.

Mailinglisten

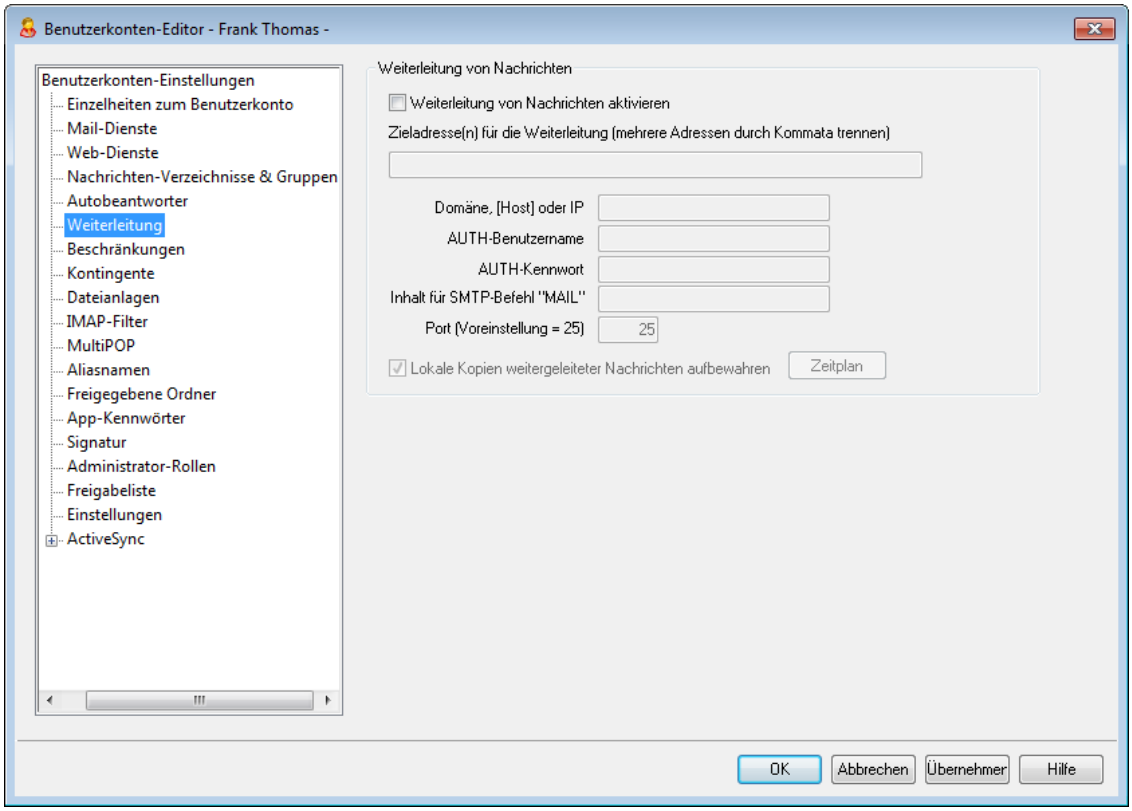
Absender der folgenden Mailingliste hinzufügen
Wird in diesem Feld eine Mailingliste eingetragen, so wird der Absender einer Nachricht durch den Autobeantworter dieser Mailingliste automatisch hinzugefügt. Automatisch arbeitende Mailingliste können so einfach erstellt werden.

Absender aus folgender Mailingliste entfernen
Wird hier eine Mailingliste eingetragen, so wird der Absender einer Nachricht durch den Autobeantworter automatisch von dieser Liste gelöscht.

Siehe auch:

Autobeantworter » Benutzerkonten 831
Autobeantworter » Ausnahmeliste 834
Autobeantworter » Einstellungen 835
Erstellen von Skripten für den Autobeantworter 836

5.1.1.6 Weiterleitung



Weiterleitung von Nachrichten

Weiterleitung von Nachrichten aktivieren
Mit dieser Option wird bestimmt, ob die eingehende Nachrichten dieses Benutzerkontos an die Adresse im Feld *Zieladresse(n) für die Weiterleitung* weitergeleitet werden. Benutzer von MDaemon mit Web-Zugriff 720 auf Webmail 317 oder die Remoteverwaltung 350 können die Einstellungen zur Weiterleitung selbst ändern; sie müssen damit nicht einen Systemverwalter beauftragen.

Zieladresse(n) für die Weiterleitung (mehrere Adressen durch Kommata trennen)
Hier ist die Adresse anzugeben, an die eine Kopie jeder eingehenden Nachricht für dieses Benutzerkonto automatisch weitergeleitet wird, sobald die Nachricht im Postfach des Benutzers ankommt. Die Weiterleitung selbst wird mit der oben stehenden Option *Weiterleitung von Nachrichten aktivieren* ein- und ausgeschaltet. Mehrere Adressen müssen durch Kommata getrennt werden.

Domäne, [Host] oder IP
Falls Sie die weitergeleiteten Nachrichten an einen bestimmten Server leiten wollen, etwa an die MX-Hosts einer bestimmten Domäne, dann geben Sie die Domäne oder die IP-Adresse hier an. Falls Sie die Nachrichten an einen bestimmten Host leiten wollen, setzen Sie den Hostnamen in eckige Klammern (z.B. `[host1.example.com]`).

AUTH-Benutzername/Kennwort
Falls der Server, an den Sie die Nachrichten leiten, eine Echtheitsbestätigung über Benutzername und Kennwort verlangt, tragen Sie die Zugangsdaten in diese Felder ein.

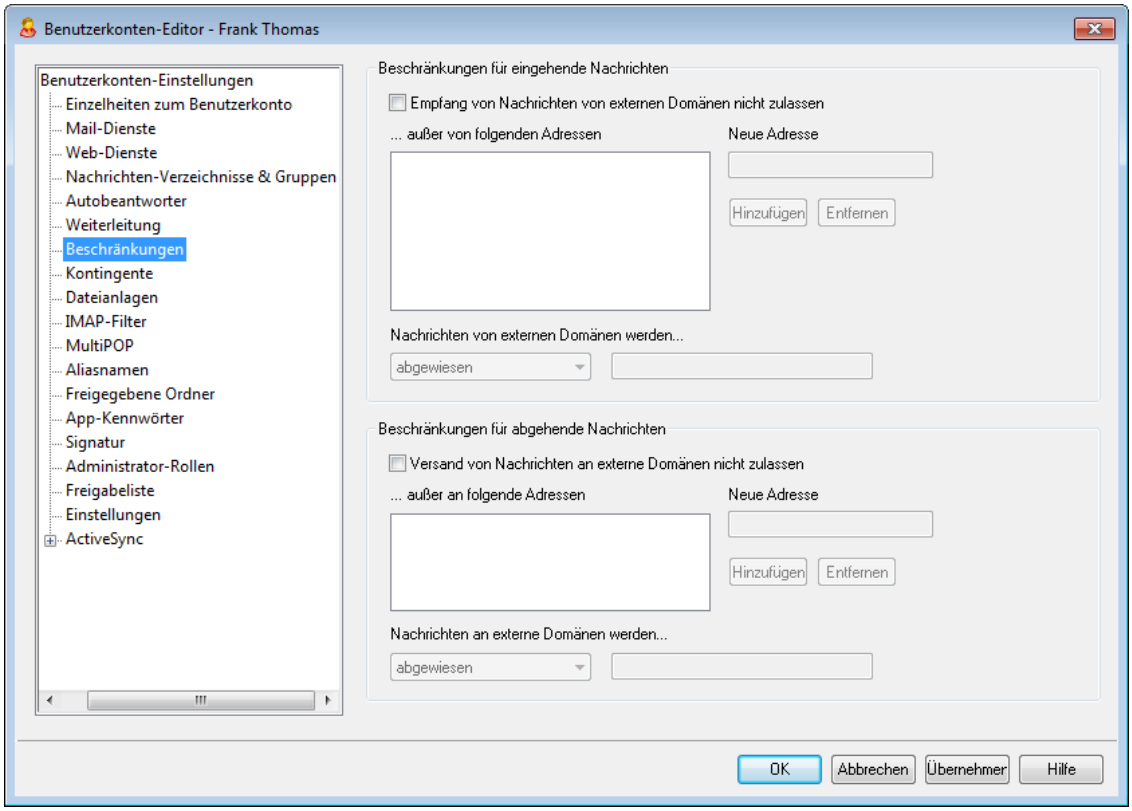
Inhalt für SMTP-Befehl 'MAIL'
Falls hier eine E-Mail-Adresse angegeben wird, verwendet MDaemon diese für den SMTP-Befehl "`MAIL From`" "Nachricht von:") während des Protokolldialogs mit der Gegenstelle. Normalerweise wird für diesen Befehl die Absenderadresse verwendet. Soll der SMTP-Befehl eine leere Adresse übermitteln ("`MAIL FROM <>`"), so ist hier "[trash]" einzugeben.

Port (Voreinstellung = 25)
MDaemon übermittelt die weitergeleiteten Nachrichten über den hier angegebenen TCP-Port. Die Voreinstellung beträgt 25.

Lokale Kopien weitergeleiteter Nachrichten aufbewahren
Mit dieser Option wird festgelegt, ob MDaemon eine Kopie jeder weitergeleiteten Nachricht im Postfach des Benutzers für den späteren Abruf behalten soll.

Zeitplan
Durch Anklicken dieses Steuerelements können Sie einen Zeitplan für die Weiterleitung der Nachrichten aus diesem Benutzerkonto erstellen. Sie können Beginn und Ende der Weiterleitung mit Datum und Uhrzeit bestimmen, und Sie können die Wochentage auswählen, an denen die Weiterleitung aktiv ist.

5.1.1.7 Beschränkungen



Die Einstellungen in diesem Dialog legen fest, ob das jeweilige Benutzerkonto Nachrichten an externe Domänen versenden oder von ihnen empfangen darf.

Beschränkungen für eingehende Nachrichten

Empfang von Nachrichten von externen Domänen nicht zulassen
Diese Option verhindert, dass das Benutzerkonto Nachrichten von externen Domänen empfängt.

...außer von folgenden Adressen
Die hier angegebenen Adressen sind von der Beschränkung für eingehende Nachrichten ausgenommen. Jokerzeichen sind zulässig. Wird also beispielsweise "*@altn.com" als Ausnahme definiert, so werden alle eingehenden Nachrichten von jeder beliebigen Adresse bei altn.com angenommen und dem Benutzerkonto zugestellt.

Neue Adresse
Um der Ausschlussliste eine neue Adresse anzufügen, muss diese Adresse hier eingegeben werden. Ein Klick auf *Hinzufügen* übernimmt die neue Adresse in die Liste.

Hinzufügen
Nachdem eine neue Adresse im Feld *Neue Adresse* eingegeben wurde, übernimmt ein Klick auf dieses Steuerelement die Adresse in die Ausschlussliste.

Entfernen
Soll eine Adresse von der Ausschlussliste gelöscht werden, so wird diese zunächst ausgewählt; ein Klick auf diesen Knopf löscht die Adresse.

Nachrichten von externen Domänen werden...
Die Optionen in diesem Rollmenü bestimmen, wie MDaemon mit Nachrichten an dieses Benutzerkonto verfahren soll, wenn sie von einer externen Domäne stammen. Zur Auswahl stehen folgende Möglichkeiten:

abgewiesen – Die Nachrichten werden durch MDaemon abgewiesen.

an den Absender zurückgeleitet – Nachrichten von nicht zugelassenen Domänen gehen zurück an den Absender.

an den Postmaster geleitet – Nachrichten von nicht zugelassenen Domänen werden angenommen, jedoch nicht dem beabsichtigten Empfänger sondern dem Postmaster zugestellt.

an folgenden Empfänger gesendet... – Nachrichten von nicht zugelassenen Domänen werden angenommen, aber nicht dem beabsichtigten Empfänger sondern der hierfür angegebenen Empfängeradresse zugeleitet.

Beschränkungen für abgehende Nachrichten

Versand von Nachrichten an externe Domänen nicht zulassen
Diese Option verhindert, dass das Benutzerkonto Nachrichten an externe Domänen versendet.

...außer an folgende Adressen
Die hier angegebenen Adressen sind von der Beschränkung für abgehende Nachrichten ausgenommen. Jokerzeichen sind zulässig. Wird also beispielsweise "*@altn.com" als Ausnahme definiert, so werden alle Nachrichten an jede beliebige Adresse bei altn.com angenommen und weitergeleitet.

Neue Adresse
Um der Ausschlussliste eine neue Adresse anzufügen, muss diese Adresse hier eingegeben werden. Ein Klick auf

Hinzufügen
Nachdem eine neue Adresse im Feld *Neue Adresse* eingegeben wurde, übernimmt ein Klick auf diesen Kopf die Adresse in die Ausschlussliste.

Entfernen
Soll eine Adresse von der Ausschlussliste gelöscht werden, so wird diese zunächst ausgewählt; ein Klick auf diesen Knopf löscht die Adresse.

Nachrichten an externe Domänen werden...
Die Optionen in diesem Rollmenü bestimmen, wie MDaemon mit Nachrichten von diesem Benutzerkonto verfahren soll, wenn sie an eine externe Domäne gerichtet sind. Zur Auswahl stehen folgende Möglichkeiten:

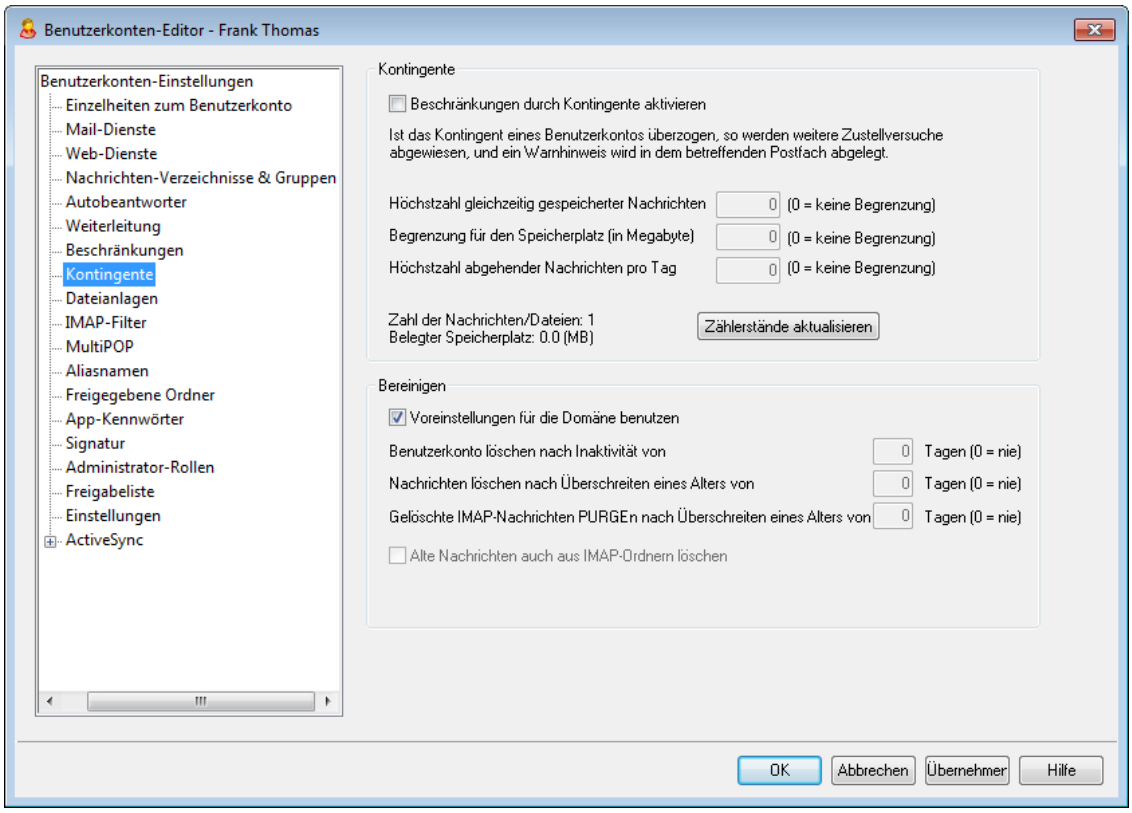
abgewiesen – Die Nachrichten werden durch MDaemon abgewiesen.

an den Absender zurückgeleitet – Nachrichten an nicht zugelassene Domänen gehen zurück an den Absender.

an den Postmaster geleitet – Nachrichten an nicht zugelassene Domänen werden angenommen, jedoch nicht dem beabsichtigten Empfänger sondern dem Postmaster zugestellt.

an folgenden Empfänger gesendet... – Nachrichten an nicht zugelassene Domänen werden angenommen, aber nicht dem beabsichtigten Empfänger sondern der hierfür angegebenen Empfängeradresse zugeleitet.

5.1.1.8 Kontingente



Kontingente

Beschränkungen durch Kontingente aktivieren
Hier werden die Voreinstellungen für die Höchstzahl der Nachrichten, die in einem Postfach abgelegt sein dürfen, den höchstzulässigen Speicherplatz, den ein Benutzerkonto belegen darf (dieser Wert schließt alle entpackten und dekodierten Dateianlagen im Dokumentenverzeichnis des Benutzerkontos ein) und die Höchstzahl der Nachrichten getroffen, die ein Benutzerkonto pro Tag über SMTP versenden darf. Würde die Zustellung einer Nachricht das Kontingent für ein Benutzerkonto überschreiten, so werden die Nachricht abgewiesen und eine entsprechende Warnnachricht im Posteingang des Benutzers abgelegt. Würde der Abruf von Nachrichten über MultiPOP 739 das Kontingent überschreiten, so erhält der Benutzer eine entsprechende Warnnachricht; gleichzeitig werden die MultiPOP-Einträge für das Benutzerkonto abgeschaltet. Sie bleiben aber in der Datenbank erhalten.

Mithilfe der *Option Benutzer warnen, sobald ihr Kontingent zu folgendem Prozentsatz ausgeschöpft ist* im Menü Benutzerkonten » Benutzerkonten-Optionen »

Kontingente[805] erhalten Benutzer eine Warnnachricht, wenn sie sich der Grenze ihres Kontingents nähern. Wird das Kontingent für Höchstzahl der Nachrichten oder höchstzulässigen Speicherplatz zu mehr als dem dort festgelegten Prozentsatz ausgeschöpft, so erhält das betroffene Benutzerkonto um Mitternacht eine Warnnachricht. In ihr sind die Zahl der gespeicherten Nachrichten sowie der belegte Speicherplatz und die Prozentzahl, zu der das Kontingent ausgeschöpft ist, enthalten. Wird im Posteingang des Benutzers bereits eine Warnnachricht gefunden, so wird sie aktualisiert.

Höchstzahl gleichzeitig gespeicherter Nachrichten
Diese Option bestimmt, wie viele Nachrichten höchstens gleichzeitig für das Benutzerkonto gespeichert werden dürfen. Der Wert 0 bewirkt, dass die Zahl der Nachrichten nicht begrenzt wird.

Begrenzung für den Speicherplatz (in Megabyte)
Diese Option bestimmt, wieviel Speicherplatz das Benutzerkonto höchstens belegen darf, wobei auch alle Dateianlagen im Dokumentenverzeichnis des Benutzerkontos einbezogen werden. Der Wert 0 bewirkt, dass der Speicherplatz für das Benutzerkonto nicht beschränkt wird.

Höchstzahl abgehender Nachrichten pro Tag
Diese Option bestimmt, wie viele Nachrichten das Benutzerkonto täglich höchstens über SMTP versenden darf. Ist die Höchstzahl für dieses Benutzerkonto erreicht, so werden alle weiteren Nachrichten abgewiesen, bis der Zähler um Mitternacht zurückgesetzt wird. Der Wert 0 bewirkt, dass das Benutzerkonto in der Zahl der Nachrichten, die es täglich versenden darf, nicht begrenzt ist.

Zählerstände aktualisieren
Durch Anklicken dieses Steuerelements können Sie die Zähler für die *Zahl der Nachrichten/Dateien*, die links von diesem Steuerelement angezeigt werden, aktualisieren.

Bereinigen

Die Einstellungen in diesem Abschnitt legen fest, ob und wann dieses Benutzerkonto durch MDaemon gelöscht wird, falls es inaktiv wird. Es kann außerdem angegeben werden, ob alte Nachrichten, die zu diesem Benutzerkonto gehören, nach einer gewissen Zeit gelöscht werden. Jeden Tag um Mitternacht löscht MDaemon alle Nachrichten, die die gesetzte Altersgrenze überschritten haben. Falls das Benutzerkonto die Inaktivitätsgrenze erreicht hat, wird es durch MDaemon vollständig gelöscht.

Voreinstellungen für die Domäne benutzen
Sollen zum Aufräumen von Benutzerkonten und alter Post jene Vorgaben verwendet werden, die für die Domäne des Benutzerkontos festgelegt wurden, ist diese Option zu aktivieren. Diese Vorgaben können im Abschnitt Optionen[211] des Domänen-Managers[181] festgelegt werden, je nachdem, zu welcher Domäne das Benutzerkonto gehört. Falls Sie für dieses Benutzerkonto die Voreinstellungen nicht nutzen wollen, deaktivieren Sie diese Option und nehmen Sie die folgenden Einstellungen vor.

Benutzerkonto automatisch löschen nach Inaktivität von [xx] Tagen (0 = nie)
Hier ist anzugeben, wie lange ein Benutzerkonto in dieser Domäne inaktiv sein darf, bevor es gelöscht wird. Der Wert 0 bewirkt, dass Benutzerkonten nicht wegen Inaktivität gelöscht werden.

Nachrichten löschen nach Überschreiten eines Alters von [xx] Tagen (0 = nie)
Dieser Wert bestimmt, wie viele Tage lang eine Nachricht im Postfach eines Benutzers liegen darf, bevor sie gelöscht wird. Der Wert 0 bewirkt, dass die Nachrichten nicht wegen ihres Alters gelöscht werden. **Beachte:** Diese Option wirkt auf die Nachrichten in IMAP-Ordnern nur dann, wenn Sie auch die Option "*Alte Nachrichten auch aus IMAP-Ordnern löschen*" weiter unten aktivieren.

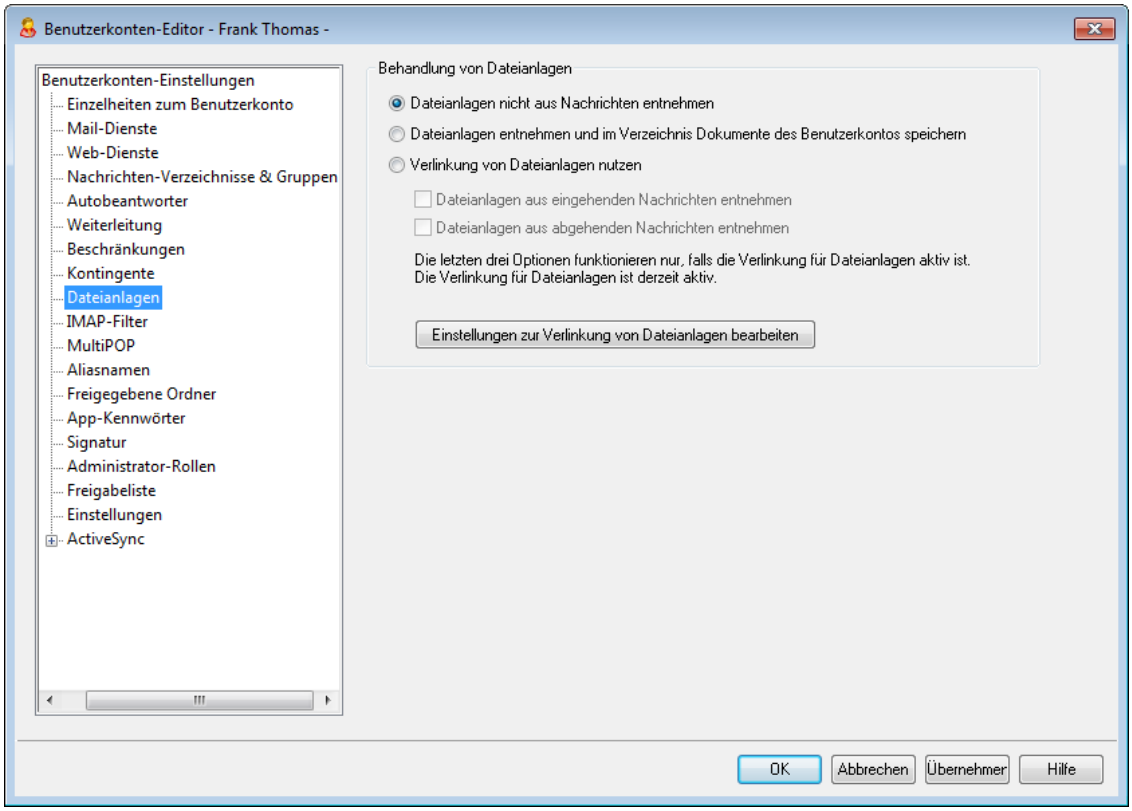
Gelöschte IMAP-Nachrichten entfernen nach Überschreiten eines Alters von [xx] Tagen (0 = nie)
Diese Option legt fest, wie lange IMAP-Nachrichten noch in den Benutzerverzeichnissen verbleiben dürfen, nachdem sie zur Löschung vorgemerkt wurden. Nachrichten, bei denen die hier angegebene Grenze überschritten ist, werden aus den Postfächern gelöscht. Der Wert 0 bedeutet, dass zur Löschung vorgemerkte Nachrichten nicht wegen ihres Alters gelöscht werden.

Alte Nachrichten auch aus IMAP-Ordnern löschen
Diese Option bewirkt, dass die Option "*Nachrichten löschen nach Überschreiten eines Alters von [xx] Tagen*" weiter oben auch auf Nachrichten in IMAP-Ordnern wirkt. Ist diese Option abgeschaltet, dann werden normale Nachrichten in IMAP-Ordnern nicht wegen Überschreitens eines Höchstalters gelöscht.

Siehe auch:

Vorlagen-Manager » Kontingente 805
Benutzerkonten-Optionen » Kontingente 852

5.1.1.9 Dateianlagen



Behandlung von Dateianlagen

Dieser Konfigurationsdialog bestimmt, ob MDaemon Dateianlagen aus den E-Mail-Nachrichten des gerade bearbeiteten Benutzerkontos entnimmt. Sie können mithilfe des Vorlagen-Managers 808 die Voreinstellungen für die folgenden Optionen festlegen.

Dateianlagen nicht aus Nachrichten entnehmen
Diese Option bewirkt, dass Dateianlagen nicht aus den Nachrichten des Benutzerkontos entnommen werden. Nachrichten, die Dateianlagen enthalten, werden normal verarbeitet, und an den Dateianlagen werden keine Änderungen vorgenommen.

Dateianlagen entnehmen und im Verzeichnis Dokumente des Benutzerkontos speichern
Diese Option bewirkt, dass MDaemon automatisch alle Dateianlagen, die als Base64 in MIME-Nachrichten eingebunden sind, aus den eingehenden Nachrichten für das gerade bearbeitete Benutzerkonto entnimmt. Die entnommenen Dateianlagen werden aus der eingehenden Nachricht entfernt, dekodiert und im Dokumentenordner des Benutzerkontos abgelegt. In den Nachrichtentext wird dann ein Hinweis eingefügt, der über die Namen der entnommenen Dateien Auskunft gibt. Eine Verknüpfung mit der gespeicherten Dateianlage wird nicht eingefügt; die Benutzer können aber auf ihre Dokumentenordner mithilfe von Webmail 317 zugreifen.

Verlinkung von Dateianlagen nutzen
Um die Leistungsmerkmale zur Verlinkung von Dateianlagen in eingehenden und abgehenden Nachrichten zu nutzen, aktivieren Sie diese Option.

Falls diese Option aktiv ist, das Leistungsmerkmal Verlinkung von Dateianlagen im Konfigurationsdialog Verlinkung von Dateianlagen[364] aber abgeschaltet ist, werden keine Dateianlagen entnommen.

Dateianlagen aus eingehenden Nachrichten entnehmen
Ist diese Option aktiv, so werden Dateianlagen aus eingehenden Nachrichten solcher Benutzerkonten entnommen, deren Einstellungen diese Vorlage steuert. Die entnommenen Dateianlagen werden an dem Speicherort abgelegt, der im Konfigurationsdialog Verlinkung von Dateianlagen[364] festgelegt ist. In den Nachrichtentext werden URL-Verknüpfungen eingefügt; der Benutzer kann durch Anklicken dieser Verknüpfungen die entnommenen Dateianlagen abrufen. Aus Sicherheitsgründen enthalten diese Verknüpfungen keine direkt zugänglichen Dateipfade. Stattdessen enthalten sie eindeutige Kennzeichnungen (GUID), mit deren Hilfe der Server die Verknüpfung der jeweiligen Datei zuordnen kann. Die Zuordnungstabelle für die GUID wird in der Datei `AttachmentLinking.dat` gespeichert.

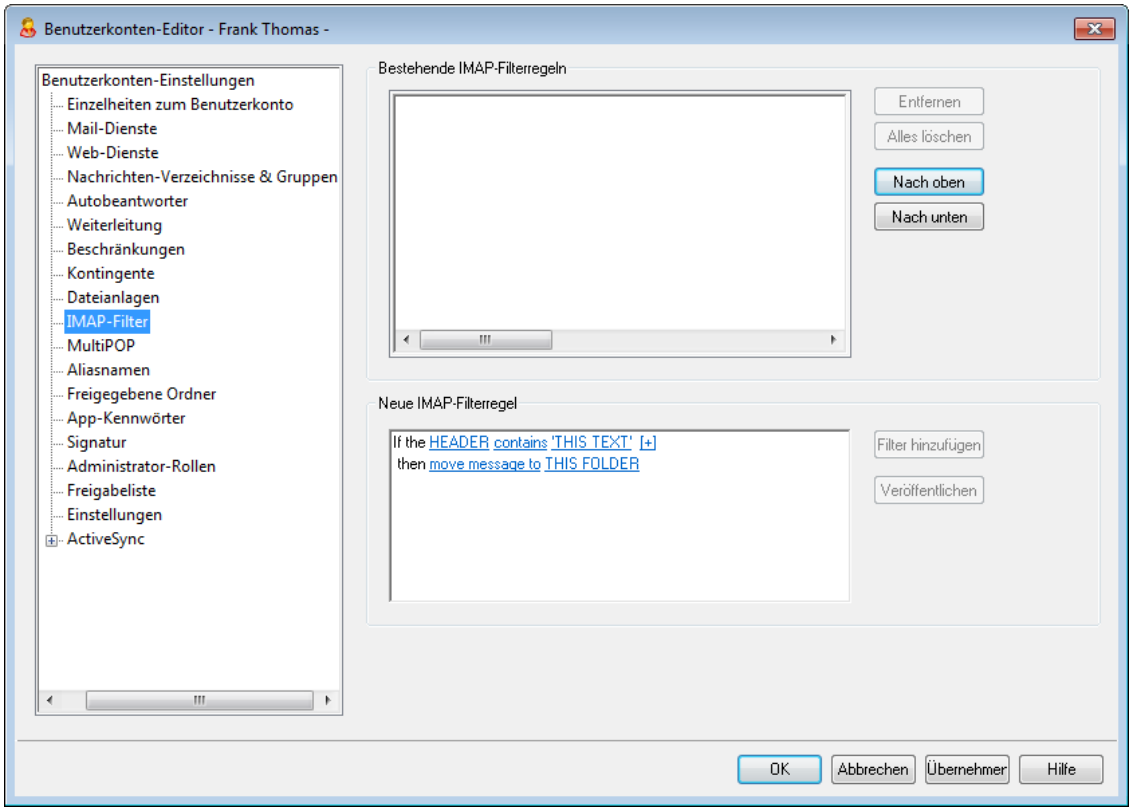
Dateianlagen aus abgehenden Nachrichten entnehmen
Ist diese Option aktiv, so werden Dateianlagen aus abgehenden Nachrichten solcher Benutzerkonten entnommen, deren Einstellungen diese Vorlage steuert. Versendet ein solches Benutzerkonto eine Nachricht mit Dateianlage, so wird die Dateianlage aus der Nachricht entnommen und gespeichert. In den Nachrichtentext wird eine URL-Verknüpfung eingefügt, mit deren Hilfe die Datei abgerufen werden kann.

Einstellungen zur Verlinkung von Dateianlagen bearbeiten
Durch Anklicken dieses Steuerelements können Sie den Konfigurationsdialog Verlinkung von Dateianlagen[364] aufrufen.

Siehe auch:

Verlinkung von Dateianlagen[364]
Vorlagen-Manager » Dateianlagen[808]

5.1.1.10 IMAP-Filter



MDaemon ermöglicht es den Benutzern von IMAP und Webmail[317], ihre Nachrichten auf dem Server durch Filter automatisch in bestimmte Ordner verteilen zu lassen. Dieses Verfahren funktioniert ganz ähnlich wie der Inhaltsfilter[649]: MDaemon untersucht die Kopfzeilen der für die Benutzerkonten eingehenden Nachrichten und vergleicht sie mit den Filtern der Benutzerkonten. Erfüllt eine Nachricht die Bedingungen eines Filters, so verschiebt MDaemon diese Nachricht in den Ordner, der in dem Filter bezeichnet ist, löscht die Nachricht oder leitet sie an die gewünschten E-Mail-Adressen weiter oder um. Dieses Verfahren ist für Client und Server deutlich effizienter als das Filtern der Nachrichten auf dem Client selbst. Benutzern solcher Clients, die keine Leistungsmerkmale zum Filtern von Nachrichten bieten, bietet der IMAP-Filter die ihnen fehlenden Funktionen.

Administratoren können Filter im Abschnitt IMAP-Filter des Benutzerkonten-Editors oder mithilfe der Remoteverwaltung[350] erstellen. Sie können den Benutzern auch die Berechtigung erteilen, ihre Filter mithilfe von Webmail oder der Remoteverwaltung selbst zu erstellen und zu verwalten. Sie können die entsprechenden Berechtigungen im Konfigurationsdialog Web-Dienste[720] zuweisen.

Bestehende IMAP-Filterregeln

In dieser Liste erscheinen alle Filter, die für das betreffende Benutzerkonto bestehen. Die Filter werden in der angegebenen Reihenfolge abgearbeitet, bis eine passender Filter gefunden ist. In diesem Fall wird die Nachricht in den im Filter bezeichneten Ordner verschoben, und die Abarbeitung der Filter für diese Nachricht beendet. Mit den Schaltflächen *Nach oben* und *Nach unten* lässt sich die Reihenfolge der Filter ändern.

Entfernen
Hiermit wird der gewählte Filter aus der Liste gelöscht.

Alle löschen
Hiermit werden sämtliche definierten Filter des Benutzers gelöscht.

Nach oben
Diese Funktion bewegt den gewählten Filter in der Liste nach oben.

Nach unten
Diese Funktion bewegt den gewählten Filter in der Liste nach unten.

Neue IMAP-Filterregel

Mithilfe der Verknüpfungen in diesem Bereich können Sie neue Filterregeln erstellen. Sobald Sie eine Regel erstellt haben, klicken Sie auf **Filter hinzufügen**, um die Regel der Liste *Bestehende IMAP-Filterregeln* hinzuzufügen. Der Inhalt der Filterregeln erscheint hierbei aus technischen Gründen in englischer Sprache.

Bedingung für den Filter

Die Verknüpfungen im ersten Abschnitt der Filterregel bestimmen die Bedingungen für den Filter. Erfüllt eine Nachricht die Bedingungen des Filters, die hier festgelegt sind, so wird die **Aktion für den Filter** ausgeführt. Zum Bearbeiten der Bedingung klicken Sie auf die einzelnen Elemente, die als Verknüpfungen dargestellt werden.

HEADER (Kopfzeile)
Durch Anklicken der Verknüpfung "**HEADER"** können Sie die Kopfzeile oder den sonstigen Bestandteil der Nachricht auswählen, die für diesen Filter ausgewertet wird. Es stehen folgende Kopfzeilen zur Verfügung: **TO (An)**, **CC (CC)**, **FROM (Von)**, **SUBJECT (Betreff)**, **SENDER (Absender)**, **LIST-ID (Listen-ID)**, **X-MDMAILING-LIST**, **X-MDRCPT-TO**, **X-MDDNSBL-RESULT**, **X-SPAM-FLAG**, **MESSAGE SIZE (Nachrichtengröße), MESSAGE BODY (Nachrichtentext)** sowie **Other... (Andere)**. Falls Sie "Other..." auswählen, öffnet sich ein Eingabefenster, indem Sie den Namen der Kopfzeile angeben können, die nicht in der Auswahlliste enthalten ist. Falls Sie auf MESSAGE SIZE klicken, werden die Bedingung "contains" (enthält) und "THIS TEXT" (folgenden Text) ersetzt durch "is greater than" (ist größer als) und "0KB".

contains (enthält) / is greater than (ist größer als)
Durch Anklicken der Verknüpfungen "**contains**" oder "**is greater than"** können Sie die Art Bedingung festlegen, die bei Auswertung der Kopfzeile erfüllt sein muss. Kriterien sind beispielsweise, ob die Kopfzeile überhaupt besteht, dass sie bestimmten Text enthält oder nicht enthält, dass sie mit bestimmtem Text beginnt oder nicht beginnt und anderes. Es stehen folgende Bedingungen zur Verfügung: **starts with (beginnt mit(**, **ends with (endet mit)**, **is equal to (entspricht)**, **is not equal to (entspricht nicht)**, **contains (enthält)**, **does not contain (enthält nicht)**, **exists (besteht)**, **does not exist (besteht nicht)**, **is greater than (ist größer als)** und **is less than (ist kleiner als)**. Die Bedingungen "is greater than" und "is less than" sind nur verfügbar, wenn die Verknüpfung HEADER auf "MESSAGE SIZE" gesetzt ist.

THIS TEXT (folgender Text) / 0 KB
Nach Anklicken dieser Verknüpfung können Sie den Text angeben, nachdem MDaemon die für den Filter ausgewählte Kopfzeile durchsuchen soll. Ist die Option HEADER auf MESSAGE SIZE gesetzt, so zeigt die Verknüpfung auf "0

KB", und es steht ein Eingabefeld zur Verfügung, in dem die Nachrichtengröße in KB angegeben werden kann.

[+] [x] and (und)
Um mehr als eine Bedingung für die Filterregel zu definieren, klicken Sie auf **[+]**. Es wird hierdurch eine weitere Zeile mit den Elementen "HEADER", "contains" und "THIS TEXT" hinzugefügt und so der Filter um zusätzliche Bedingungen erweitert. Per Voreinstellung muss eine Nachricht alle diese Bedingungen erfüllen, damit die Filterregel wirksam wird. Falls die Filterregel wirksam werden soll, wenn auch nur eine der Bedingungen erfüllt ist, klicken Sie auf "**and**" (und), und wählen Sie dann "**or**" (oder) aus. Enthält ein Filter mehrere Zeilen, so können Sie einzelne Zeilen durch Anklicken der Verknüpfung **[x]** in der betreffenden Zeile löschen.

Aktion für den Filter

Die Verknüpfungen im unteren Abschnitt der Filterregel bestimmen die Aktion, die der Filter ausführt, falls eine Nachricht die Bedingungen des Filters erfüllt. Zum Bearbeiten der Aktion klicken Sie auf die einzelnen Elemente, die als Verknüpfungen dargestellt werden.

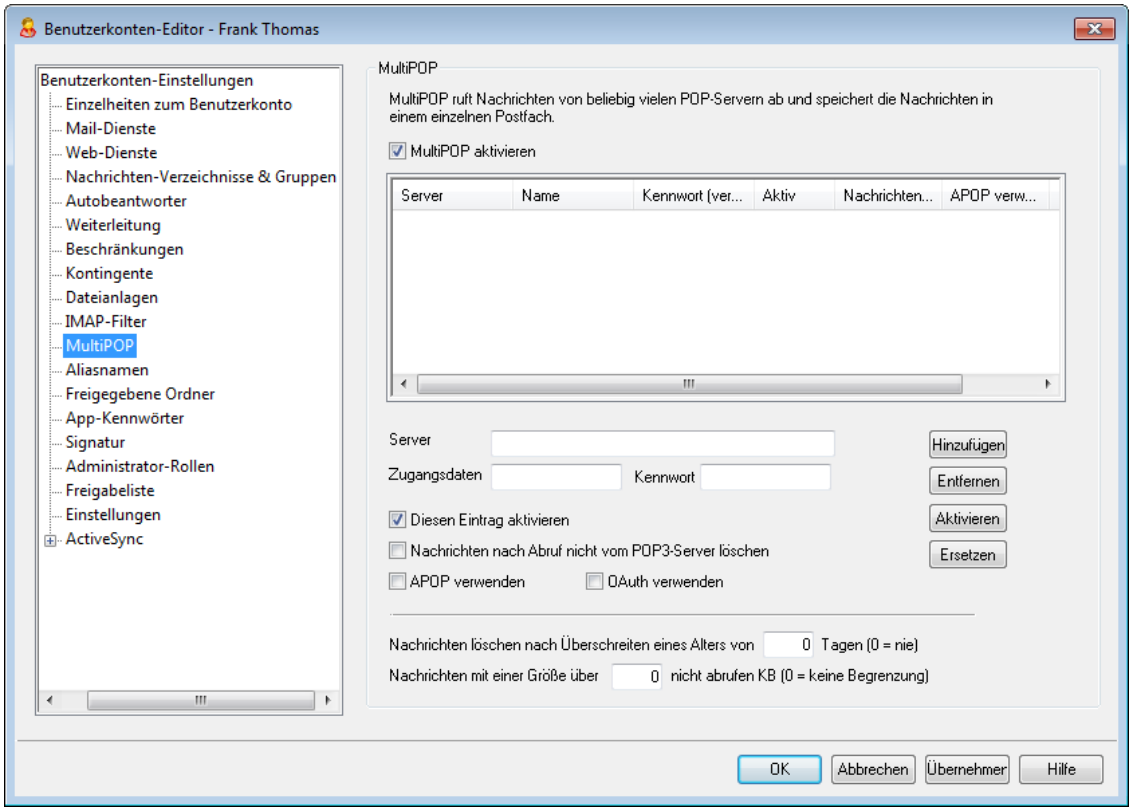
move message to (Nachricht verschieben nach)
Durch Anklicken der Verknüpfung "**move message to**" bestimmen Sie die Aktion, die der Filter ausführt. Es stehen folgende Aktionen zur Verfügung: **move message to (Nachricht verschieben nach)**, **delete message (Nachricht löschen)**, **redirect message to (Nachricht umleiten an)** und **forward message to (Nachricht weiterleiten an)**.

THIS FOLDER / EMAIL (folgenden Ordner/folgende E-Mail-Adresse)
Falls Sie die Option "**move message to**" ausgewählt haben, können Sie durch Anklicken der Verknüpfung **THIS FOLDER** den Ordner bestimmen, in den die Nachricht verschoben werden soll. Falls Sie die Nachricht umleiten oder weiterleiten lassen wollen, klicken Sie auf die Verknüpfung **EMAIL**, und geben Sie die E-Mail-Adresse des Empfängers an. Bei der Umleitung von Nachrichten bleiben die Kopfzeilen und der Nachrichtentext unverändert; geändert wird nur der Empfänger im SMTP-Umschlag. Bei der Weiterleitung von Nachrichten wird eine neue Nachricht erstellt und versandt, wobei die Betreffzeile und der Nachrichtentext der Ursprungsnachricht entnommen werden.

Filter hinzufügen
Nachdem Sie die einzelnen Bestandteile des Filters bearbeitet haben, klicken Sie auf diese Schaltfläche, um den Filter der Liste *Bestehende IMAP-Filterregeln* hinzuzufügen.

Veröffentlichen
Mithilfe dieses Steuerelements können Sie die Regel für alle anderen Benutzerkonten derselben Domäne übernehmen. Es erscheint eine Sicherheitsabfrage, bevor die Regel übernommen wird.

5.1.1.11 MultiPOP



Das Leistungsmerkmal MultiPOP gestattet die Erstellung einer unbegrenzten Zahl von externen POP3-Postfächern, jeweils bestehend aus Servername, Benutzername und Kennwort, von denen jeweils Nachrichten abgerufen werden sollen. Dies ist für Benutzer mit mehreren E-Mail-Konten auf verschiedenen Servern hilfreich, wenn sie es vorziehen, alle E-Mail gesammelt von nur noch einem Server abzurufen. Bevor die Nachrichten im Postfach des jeweiligen Benutzers abgelegt werden, gelangen sie in die lokale Nachrichten-Warteschlange, sodass sie genau wie alle sonstigen Nachrichten verarbeitet werden können. Autobeantworter und der Inhaltsfilter werden auf diese Nachrichten folglich ebenfalls angewandt. Sie erreichen den Zeitplan für MultiPOP über Einstellungen » Zeitplan » Abruf über MultiPOP 382.

MultiPOP aktivieren
Mithilfe dieser Option aktivieren Sie das Leistungsmerkmal MultiPOP für das gerade bearbeitete Benutzerkonto. Sie können dem Benutzer wahlweise das Bearbeiten der eigenen MultiPOP-Einstellungen in der MDaemon-Remoteverwaltung 350 gestatten. Die entsprechende Berechtigung können Sie auf der Seite Web-Dienste 720 des Benutzerkontos erteilen. Sind beide genannte Optionen aktiv, so steht den Benutzern in Webmail 317 die Seite Postfächer zur Verfügung. Dort können die Benutzer die MultiPOP-Einstellungen verwalten. Die systemweit gültige Option zum Aktivieren und Deaktivieren des MultiPOP-Servers finden Sie unter Einstellungen » Server-Einstellungen » MultiPOP 145. Ist diese systemweite Option deaktiviert, dann ist MultiPOP insgesamt nicht nutzbar, und zwar auch dann nicht, wenn MultiPOP für das Benutzerkonto aktiv ist.

Liste der MultiPOP-Gegenstellen für dieses Benutzerkonto
Diese Liste enthält alle MultiPOP-Servereinträge, die für dieses Benutzerkonto angelegt wurden.

Erstellen und Bearbeiten eines MultiPOP-Eintrags

Server
Hier muss der POP3-Server angegeben werden, von dem die Nachrichten abgerufen werden sollen. Falls für Verbindungen mit diesem Server bestimmte Portnummern verwendet werden müssen, die von den Standard-Ports für POP3 abweichen, so fügen Sie dem Servernamen die einen Doppelpunkt und die Portnummer nach dem Schema ":`[Port]`" hinzu. Ein Beispiel hierzu: "`mail.example.com:1000`". Für den Abruf von Gmail und Microsoft (Office) 365 tragen Sie "`pop.gmail.com:995`" und "`outlook.office365.com:995`" ein.

Benutzername
Der Anmeldename oder Benutzername (Befehl USER oder LOGON) für das POP3-Postfach auf dem angegebenen Server wird hier eingetragen.

Kennwort
Hier wird das POP3- oder APOP-Kennwort zu dem vorher eingegebenen Benutzernamen eingetragen.

APOP verwenden
Diese Option schaltet die Anmeldung über die Echtheitsbestätigungsmethode APOP für diesen MultiPOP-Eintrag ein.

OAuth verwenden
Beim Abruf von Nachrichten aus Gmail und Microsoft (Office) 365 nutzen Sie dieses Verfahren zur Echtheitsbestätigung. Nähere Informationen hierzu finden Sie auf der Seite Server-Einstellungen » MultiPOP unter MultiPOP OAuth 2.0 145.
Beachte: Damit Benutzer OAuth mit Gmail oder Microsoft (Office) 365 verwenden können, muss den betreffenden Benutzerkonten auf der Seite Web-Dienste 720 die Berechtigung zum Bearbeiten der "*MultiPOP-Einstellungen*" erteilt sein. Dies ist erforderlich, weil sich die Benutzer an Webmail anmelden und auf der Seite **Postfächer** die Anmeldung für Gmail und Microsoft (Office) 365 durchführen müssen, und die Seite Postfächer nur den Benutzern zur Verfügung steht, die zum Bearbeiten der MultiPOP-Einstellungen berechtigt sind.

Nachrichten nach Abruf nicht vom POP3-Server löschen
Diese Option bewirkt, dass die Nachrichten nach dem Abruf auf dem Server verbleiben und nicht gelöscht werden. Dies ist sinnvoll, wenn die Nachrichten später noch von einem anderen Rechner aus abgerufen werden sollen. Falls Sie diese Option für alle Benutzer übergehen und festlegen wollen, dass die Nachrichten nach dem Abruf durch MDaemon immer vom POP-Server gelöscht werden, aktivieren Sie unter Einstellungen » Server-Einstellungen » MultiPOP 145 die Option "*MultiPOP löscht Nachrichten nach dem Abruf immer von allen Servern*".

Hinzufügen
Mit diesem Knopf werden die eingegebenen Daten der Liste als neuer Eintrag angefügt.

Entfernen
Mit diesem Knopf werden die jeweils ausgewählten MultiPOP-Einträge aus der Liste gelöscht.

Aktivieren/Deaktivieren
Mit dieser Option wird für den gewählten Eintrag festgelegt, ob der Eintrag aktiv oder nicht aktiv ist. Hiermit bestimmen Sie, ob MDaemon von dem Server Nachrichten durch MultiPOP abrufen oder den Server bei der MultiPOP-Verarbeitung unberücksichtigt lassen soll.

Ersetzen
Um einen Eintrag zu bearbeiten, wählen Sie den Eintrag in der Liste durch Anklicken aus, nehmen Sie die gewünschten Änderungen vor, und klicken Sie dann auf dieses Steuerelement, um die Änderungen zu speichern.

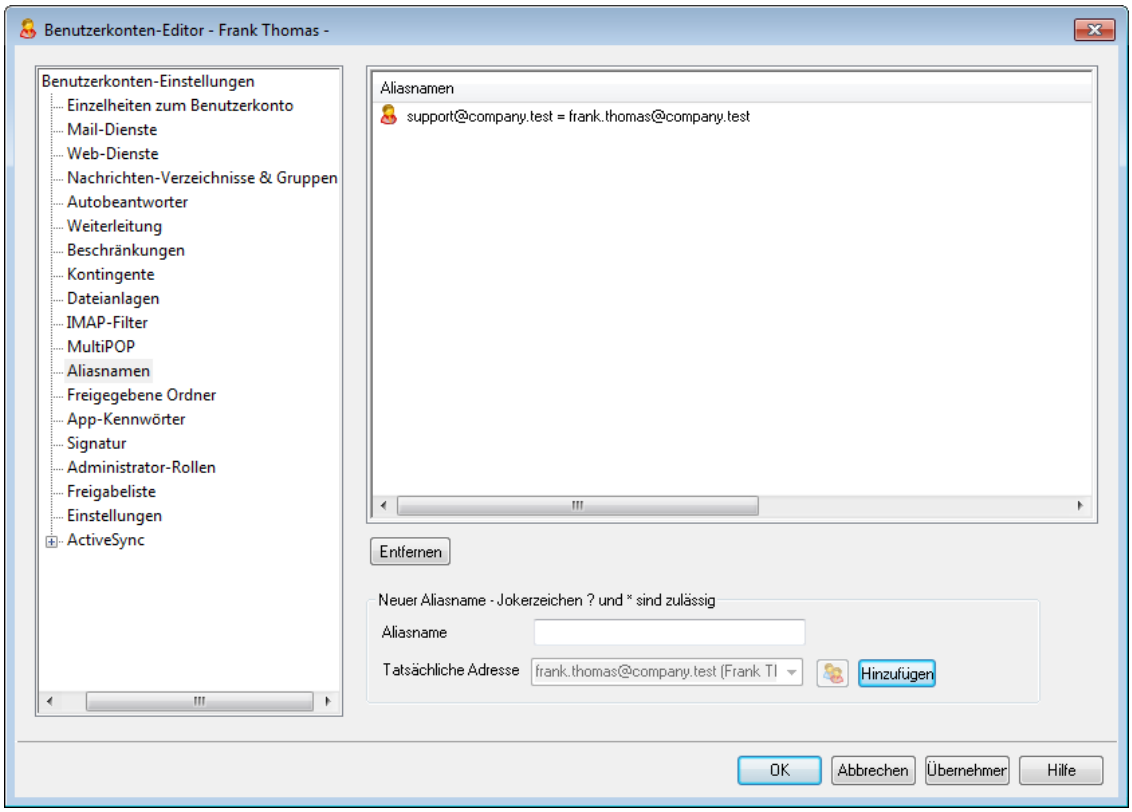
Nachrichten löschen nach Überschreiten eines Alters von [xx} Tagen (0 = nie)
Hier wird die Zeit in Tagen angegeben, für die eine Nachricht auf dem MultiPOP-Host verbleiben darf, bevor sie gelöscht wird. Der Wert 0 bewirkt, dass Nachrichten nicht aufgrund ihres Alters gelöscht werden.

Nachrichten mit einer Größe über [xx] KB nicht abrufen (0 = keine Begrenzung)
Soll für die zu empfangenden Nachrichten eine Größenbegrenzung gelten, muss die maximale Größe hier eingetragen werden.

Siehe auch:

Server-Einstellungen » MultiPOP 145
Zeitplan » Abruf über MultiPOP 382

5.1.1.12 Aliasnamen



In diesem Abschnitt sind alle Adress-Aliasnamen[827] aufgeführt, die mit dem Benutzerkonto verknüpft sind. Aliasnamen können über diesen Konfigurationsdialog auch hinzugefügt und entfernt werden.

Entfernen eines Aliasnamens

Um einen Aliasnamen aus dem Benutzerkonto zu entfernen, wählen Sie den Aliasnamen aus, und klicken Sie dann auf **Entfernen**.

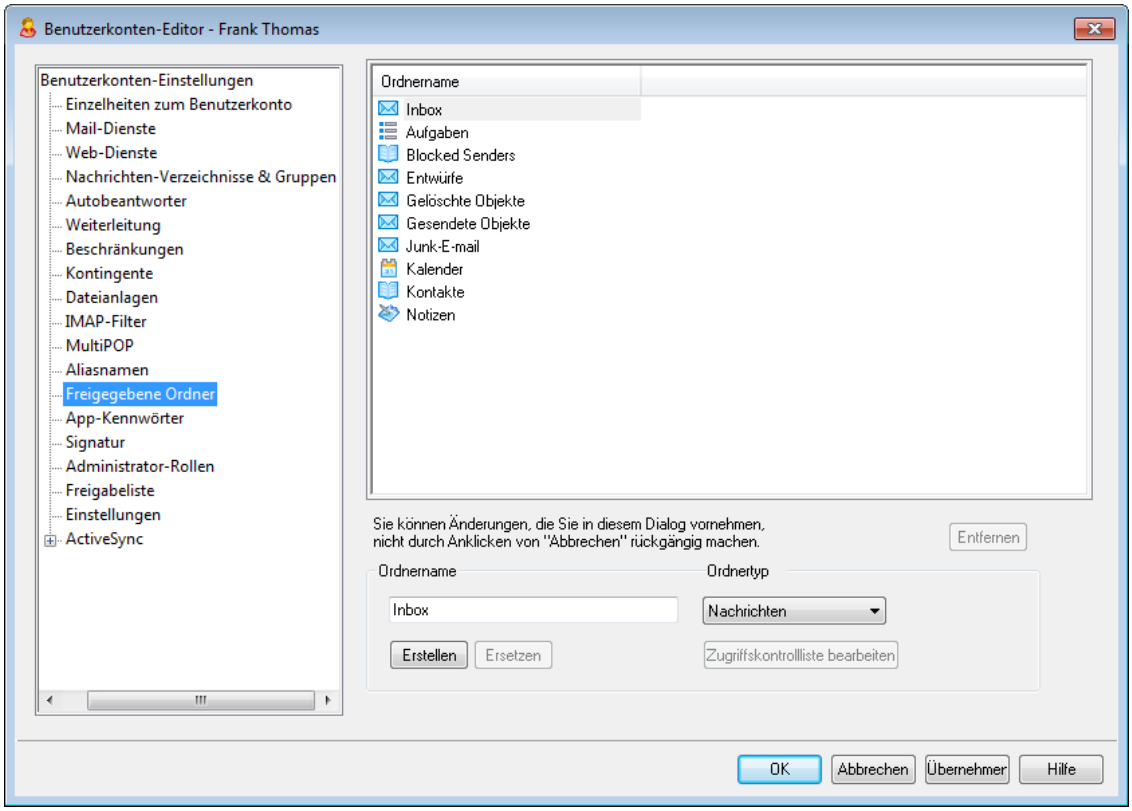
Hinzufügen eines Aliasnamens

Um dem Benutzerkonto einen neuen Aliasnamen hinzuzufügen, tragen Sie in das Textfeld *Aliasname* die Adresse ein, die Sie mit dem Benutzerkonto verknüpfen wollen, und klicken Sie dann auf **Hinzufügen**. Die Jokerzeichen "?" und "*" sind dabei zugelassen; sie ersetzen einzelne Zeichen und einzelne Wörter.

Siehe auch:

Benutzerkonten-Optionen » Aliasnamen[827]

5.1.1.13 Freigegebene Ordner



Dieser Konfigurationsdialog ist nur verfügbar, falls die Option *Ordnerfreigaben aktivieren* im Konfigurationsdialog Öffentliche & Freigegebene Ordner[122] aktiv ist (erreichbar über Einstellungen » Server-Einstellungen » Öffentliche & Freigegebene Ordner). Öffentliche Ordner können über die Verwaltung für öffentliche Ordner[309] verwaltet werden.

In diesem obersten Abschnitt sind alle bestehenden IMAP-Ordner des Benutzers aufgeführt; von hier aus wird auch die Freigabe für andere MDaemon-Benutzer und Benutzergruppen[782] gesteuert. Nachdem das Benutzerkonto angelegt wurde, erscheint hier nur der Posteingang. Sie können mithilfe der Optionen *Ordnername* und *Erstellen* (und der Optionen im Abschnitt IMAP-Filter[736]) weitere Ordner hinzufügen. Unterordner sind von den Namen der übergeordneten Ordner durch einen Schrägstrich getrennt.

Entfernen
Um einen öffentlichen IMAP-Ordner aus der Liste zu löschen, wählen Sie den Ordner aus, und klicken Sie dann auf *Entfernen*.

Neuer IMAP-Ordner

Ordnername
Um der Liste einen Ordner hinzuzufügen, tragen Sie den gewünschten Name in dieses Feld ein, und klicken Sie dann auf *Erstellen*. Soll der neue Ordner als Unterordner unter einem in der Liste aufgeführten Ordner angelegt werden, so müssen dem eigentlichen Namen des Unterordners der Name des übergeordneten Ordners und ein Schrägstrich als Trennzeichen voran gestellt werden. Heißen beispielsweise der übergeordnete Ordner "`Mein Ordner`" und der neue Ordner "`Mein neuer Ordner`", so ergibt sich als Name des Unterordners "`Mein Ordner/Mein neuer Ordner`". Soll der Ordner kein Unterordner sein, so lautet im Beispiel sein Name nur "`Mein neuer Ordner`".

Ordnertyp
Wählen Sie aus diesem Auswahlmenü den Typ für diesen Ordner: Nachrichten, Kontakte, Kalender usw.

Erstellen
Nachdem Sie den Namen und die Einstellungen für einen Ordner festgelegt haben, klicken Sie auf dieses Steuerelement, um den Ordner der Liste hinzuzufügen.

Ersetzen
Um den Namen oder die anderen Einstellungen eines Eintrags in der Liste zu ändern, wählen Sie den Eintrag durch Anklicken aus, nehmen Sie die Änderungen vor, und klicken Sie dann auf *Ersetzen.*

Zugriffskontrollliste bearbeiten
Nach Auswahl eines Ordners können Sie die Zugriffskontrollliste (ACL)[311] für diesen Ordner durch Anklicken dieses Steuerelements öffnen. In der Zugriffsliste legen Sie fest, welche Benutzer oder Benutzergruppen Zugriff auf den Ordner erhalten und welche Rechte die einzelnen Benutzer oder Benutzergruppen dabei haben sollen.

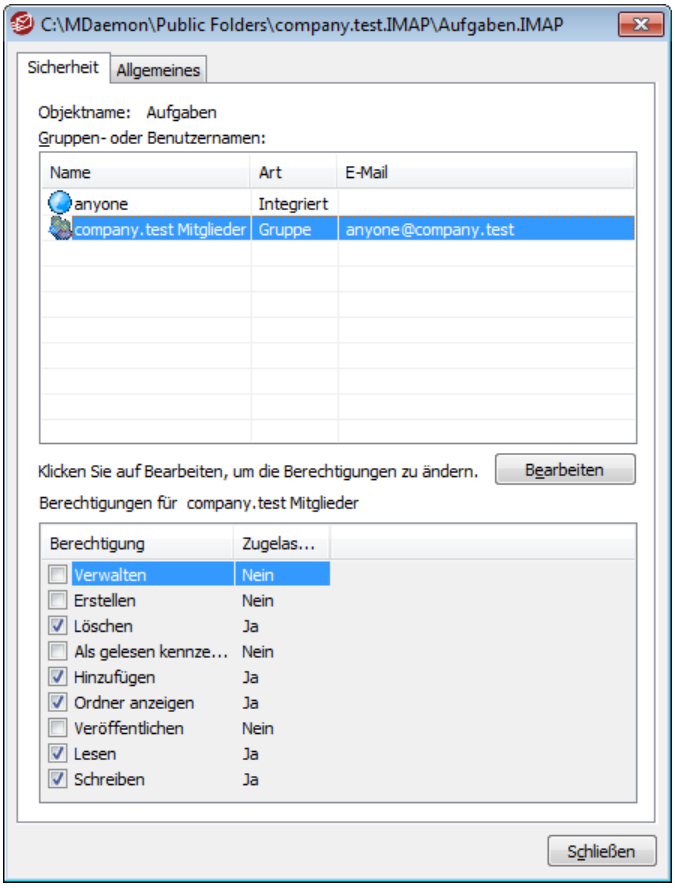
Siehe auch:

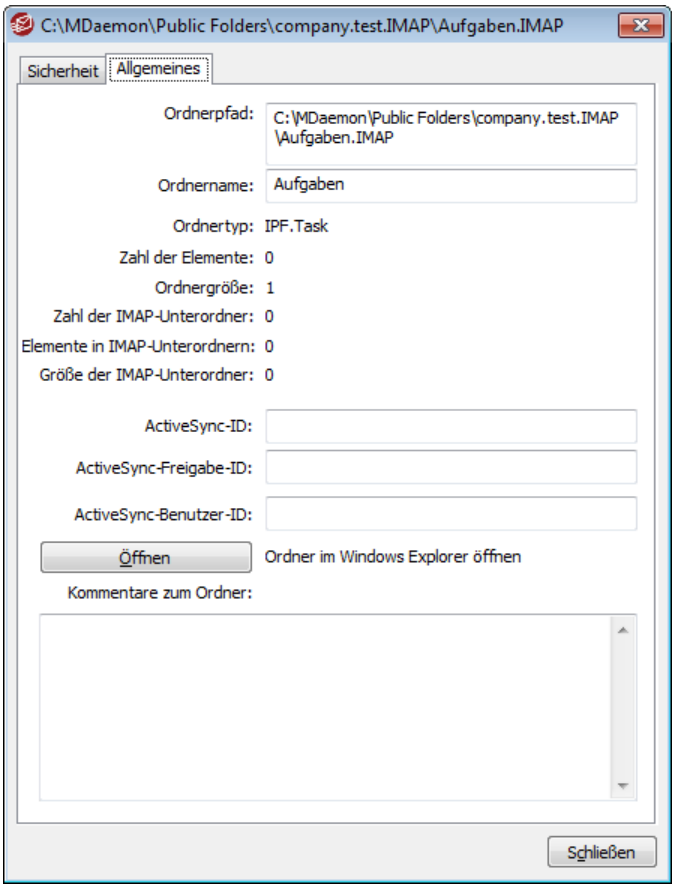
Zugriffskontrollliste (ACL)[311]
Verwaltung für öffentliche Ordner[309]

5.1.1.13.1 Zugriffskontrollliste (ACL)

Die Zugriffskontrollliste (nach der englischen Bezeichnung Access Control List auch als ACL abgekürzt) bestimmt, welche Benutzer und Gruppen welche Zugriffsrechte für öffentliche und freigegebene Ordner[119] haben. Die Zugriffskontrollliste ist

erreichbar über das Steuerelement *ACL bearbeiten* im Konfigurationsdialog für die Verwaltung öffentlicher Ordner[309] sowie über das Steuerelement *Zugriffskontrollliste bearbeiten* im Abschnitt Freigegebene Ordner[742] des Benutzerkonten-Editors.





Sicherheit

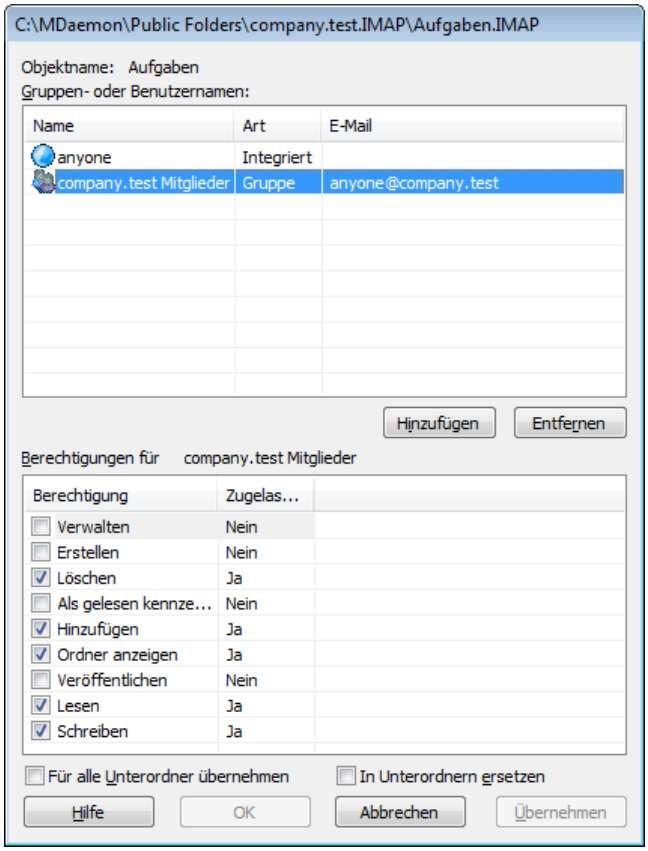
Diese Registerkarte zeigt die Gruppen und Benutzer mit Zugriffsrechten für den Ordner und die Berechtigungen, die ihnen eingeräumt sind. Um die Berechtigungen 314 eines Benutzers oder einer Gruppe einzusehen, klicken Sie auf den Benutzer oder die Gruppe. Um die Berechtigungen zu bearbeiten, klicken Sie auf **Bearbeiten** 313.

Allgemeines

Diese Registerkarte zeigt die Eigenschaften des Ordners, insbesondere Ordnerpfad, Ordnernamen, Ordnertyp und weitere Daten zum Ordner.

Bearbeiten der Zugriffskontrolllisten

Um die Berechtigungen zu bearbeiten, klicken Sie auf der Registerkarte Sicherheit auf **Bearbeiten**. Es öffnet sich der Editor für Zugriffskontrolllisten, in dem Sie die Berechtigungen bearbeiten können.



Objektname
Hier erscheint der Name des Objekts oder Ordners, auf den sich die Berechtigungen beziehen.

Gruppen- oder Benutzernamen
Hier erscheinen die Gruppen und Benutzer, denen Berechtigungen eingeräumt sind. Um die Berechtigungen für eine Gruppe oder einen Benutzer einzusehen, klicken Sie auf den Benutzer oder die Gruppe. Die Berechtigungen erscheinen dann im Abschnitt *Berechtigungen für <Gruppe oder Benutzer>* weiter unten.

Wollen Sie einer Gruppe oder einem Benutzer Berechtigungen einräumen, so aktivieren Sie die Kontrollkästchen für alle gewünschten Berechtigungen.

Hinzufügen
Um einer Gruppe oder einem Benutzer Berechtigungen einzuräumen, der in der Liste noch nicht aufgeführt ist, klicken Sie auf **Hinzufügen** 315.

Entfernen
Um eine Gruppe oder einen Benutzer zu entfernen, wählen Sie den betreffenden Eintrag in der Liste aus, und klicken Sie auf **Entfernen**.

Berechtigungen für <Gruppe oder Benutzer>
Um der oben ausgewählten Gruppe oder dem oben ausgewählten Benutzer Berechtigungen einzuräumen, aktivieren Sie das Kontrollkästchen neben jeder gewünschten Berechtigung.

Sie können die folgenden Berechtigungen einräumen:

Verwalten – Der Benutzer darf die Zugriffskontrollliste des Ordners bearbeiten.

Erstellen – Der Benutzer darf in dem Ordner Unterordner anlegen.

Löschen – Der Benutzer darf Elemente aus dem Ordner löschen.

Als gelesen kennzeichnen – Der Benutzer darf den Status der Nachrichten in dem Ordner zwischen gelesen und ungelesen wechseln.

Hinzufügen – Der Benutzer darf Elemente in dem Ordner erweitern und in den Ordner kopieren.

Ordner anzeigen – Der Benutzer sieht den Ordner in seiner persönlichen Liste der IMAP-Ordner.

Veröffentlichen – Der Benutzer darf Nachrichten direkt an den Ordner senden, falls der Ordner so konfiguriert ist, dass er dies zulässt.

Lesen – Der Benutzer darf den Ordner öffnen und seinen Inhalt einsehen.

Schreiben – Der Benutzer darf Kennzeichnungen (Flags) für die Nachrichten in dem Ordner bearbeiten.

Für alle Unterordner übernehmen
Diese Option überträgt die für den gerade bearbeiteten Ordner festgelegten Berechtigungen auch auf alle Unterordner, die der Ordner zum Zeitpunkt der Bearbeitung enthält. Die Berechtigungen für alle Gruppen und Benutzer des gerade bearbeiteten Benutzers werden den Zugriffskontrolllisten der Unterordner hinzugefügt. Bestehen im Unterordner bereits Berechtigungen für die Gruppen und Benutzer, die auch für den gerade bearbeiteten Ordner Berechtigungen haben, dann werden diese bestehenden Berechtigungen im Unterordner ersetzt. Berechtigungen anderer Gruppen und Benutzer, die für die Unterordner etwa bereits bestehen, werden nicht gelöscht.

Ein Beispiel hierzu:

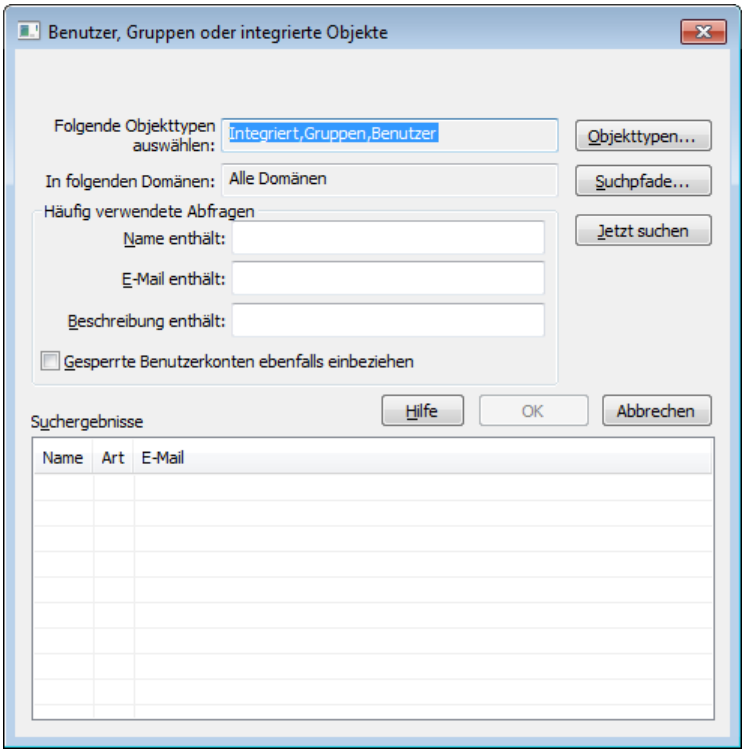
Für den gerade bearbeiteten Ordner bestehen bestimmte Berechtigungen für `Benutzer_A` und `Benutzer_B`. In einem Unterordner des gerade bearbeiteten Ordners bestehen Berechtigungen für `Benutzer_B` und `Benutzer_C`. Diese

Option fügt die Berechtigungen für `Benutzer_A` auch dem Unterordner hinzu und ersetzt die Berechtigungen für den `Benutzer_B` für den Unterordner durch die Berechtigungen des gerade bearbeiteten Ordners. Sie lässt die Berechtigungen für `Benutzer_C` unverändert. Für den Unterordner bestehen danach Berechtigungen für `Benutzer_A`, `Benutzer_B` und `Benutzer_C`.

In Unterordnern ersetzen
Diese Option bewirkt, dass die Berechtigungen aller Unterordner durch die Berechtigungen des gerade bearbeiteten Ordners ersetzt werden. Die Berechtigungen der Unterordner entsprechen dann dem gerade bearbeiteten Ordner.

Hinzufügen einer Gruppe oder eines Benutzers

Um der Zugriffskontrollliste Gruppen und Benutzer hinzuzufügen, klicken Sie im Editor für Zugriffskontrolllisten auf **Hinzufügen**. Es öffnet sich der Konfigurationsdialog zum Hinzufügen von Gruppen und Benutzern, in dem Sie nach Gruppen und Benutzern suchen und sie hinzufügen können.



Folgende Objekttypen auswählen
Um die Objekttypen auszuwählen, die Sie nach Gruppen und Benutzern durchsuchen wollen, klicken Sie auf **Objekttypen...**. Sie können wählen zwischen Integriert, Gruppen und Benutzern.

In folgenden Suchpfaden auswählen
Um die Domänen auszuwählen, die Sie durchsuchen wollen, klicken Sie auf **Suchpfade...**.Sie können alle oder einzelne MDaemon-Domänen auswählen.

Häufig verwendete Abfragen
Sie können die Felder in diesem Abschnitt verwenden, um den Umfang der Suche zu beschränken. Sie können nach Inhalten aus dem Namen des Benutzers, der E-Mail-Adresse und der Beschreibung[714] des Benutzerkontos suchen. Wenn Sie diese Felder leer lassen, ergibt die Suche alle Gruppen und Benutzer, die in den oben ausgewählten Objekttypen und Suchpfaden enthalten sind.

Gesperrte Benutzerkonten ebenfalls einbeziehen
Diese Option bewirkt, dass auch gesperrte Benutzerkonten[714] in die Suche einbezogen werden.

Jetzt suchen
Um die Suche auszuführen, geben Sie alle gewünschten Suchkriterien an, und klicken Sie danach auf **Jetzt suchen**.

Suchergebnisse
Nachdem die Suche abgeschlossen ist, können Sie in diesem Abschnitt alle gewünschten Gruppen und Benutzer auswählen. Um die ausgewählten Gruppen und Benutzer der Zugriffskontrollliste hinzuzufügen, klicken Sie danach auf **OK**.

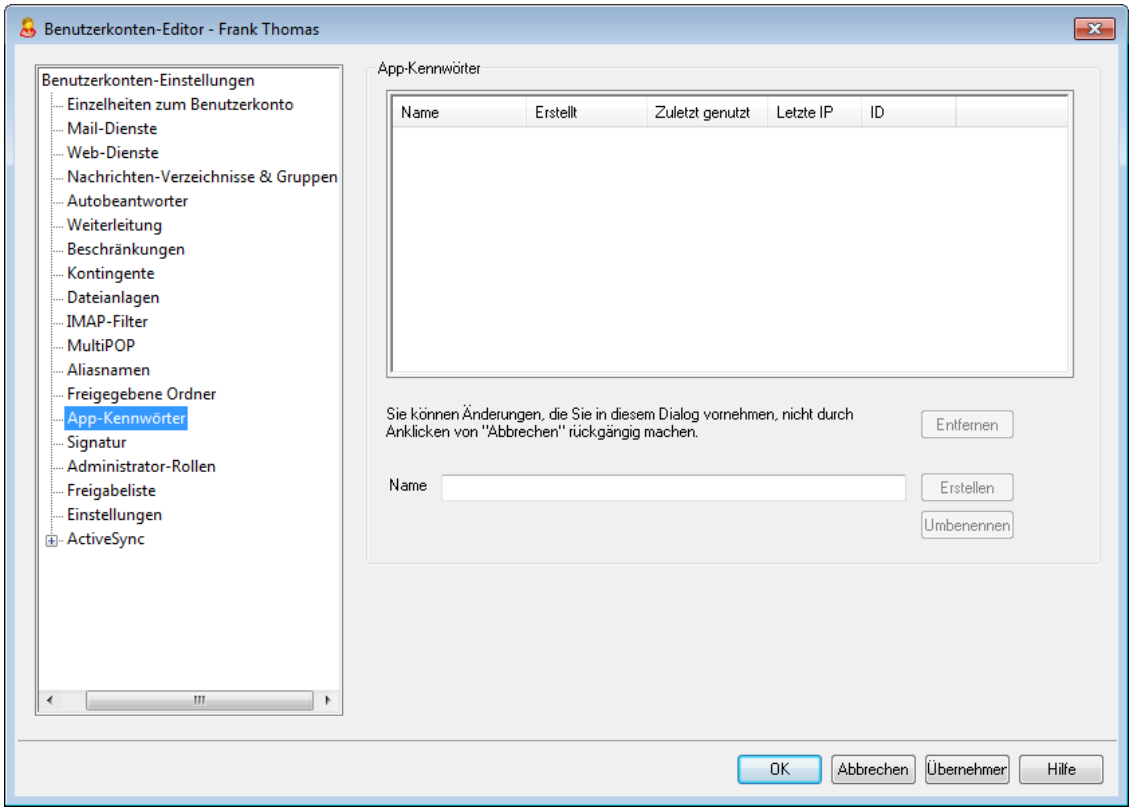
Die Berechtigungen werden mithilfe der in MDaemon enthaltenen Leistungsmerkmale für Zugriffskontrolllisten (ACL) gesteuert. ACL ist eine Erweiterung des Internet Message Access Protocols (IMAP4), die das Erstellen eigener Zugriffskontrolllisten für alle IMAP-Nachrichtenordner gestattet. Sie können damit anderen Benutzern, die über Benutzerkonten auf demselben Server verfügen, Zugriff auf Ihre Ordner gestatten. Falls Ihr E-Mail-Client keine Zugriffskontrolllisten unterstützt, können Sie die Berechtigungen mithilfe dieses Konfigurationsdialogs bearbeiten.

ACL wird ausführlich in RFC 2086 beschrieben. Sie erhalten dieses Dokument in englischer Sprache unter http://www.rfc-editor.org/rfc/rfc2086.txt.

Siehe auch:

Verwaltung für öffentliche Ordner[309]
Übersicht über die öffentlichen Ordner[119]
Öffentliche & Freigegebene Ordner[122]
Benutzerkonten-Editor » Freigegebene Ordner[742]
Mailinglisten » Öffentlicher Ordner[298]

5.1.1.14 App-Kennwörter



App-Kennwörter

App-Kennwörter sind sehr starke, zufällig erzeugte Kennwörter, die in E-Mail-Clients und E-Mail-Apps eingesetzt werden können. Sie erhöhen die Sicherheit Ihrer E-Mail-Apps, da diese Apps nicht durch die Zwei-Faktor-Authentifizierung 720 (2FA) geschützt werden können. Die 2FA ist ein sicheres Anmeldeverfahren, das die Benutzer für Webmail und die MDaemon-Remoteverwaltung (MDRA) nutzen können. Dieses Verfahren ist aber für E-Mail-Apps nicht einsetzbar, da diese Apps im Hintergrund auf Ihre E-Mail-Nachrichten zugreifen müssen, ohne dass Sie dazu einen Kode aus Ihrer Authentifizierungs-App eingeben. Das Leistungsmerkmal App-Kennwörter gestattet Ihnen die Erstellung starker, sicherer Kennwörter, die Sie in Ihren Apps einsetzen können, während Ihr eigentliches Kennwort für das Benutzerkonto durch die Zwei-Faktor-Authentifizierung geschützt ist. App-Kennwörter können nur in E-Mail-Apps eingesetzt werden. Für die Anmeldung an Webmail oder der MDaemon-Remoteverwaltung sind sie dagegen nicht nutzbar. Selbst wenn ein App-Kennwort daher kompromittiert werden würde, könnte eine unberechtigte Person sich damit nicht an Ihrem Benutzerkonto anmelden, um etwa Ihr Kennwort oder andere Einstellungen zu ändern. Sie selbst können sich aber mit dem Kennwort für Ihr Benutzerkonto und der Zwei-Faktor-Authentifizierung an Ihrem Benutzerkonto anmelden, das kompromittierte App-Kennwort löschen und nötigenfalls ein neues App-Kennwort erstellen.

Falls Sie einzelnen Benutzern die Erstellung und Nutzung von App-Kennwörtern nicht gestatten wollen, können Sie diesen Benutzern auf der Seite Web-Dienste die Berechtigung zum Bearbeiten der *App-Kennwörter* 720 entziehen. Falls Sie die Unterstützung für die App-Kennwörter für alle Benutzer deaktivieren wollen, können Sie die Option *App-Kennwörter aktivieren* 847 auf der Seite Kennwörter deaktivieren.

Anforderungen an und Empfehlungen für App-Kennwörter

- App-Kennwörter können nur erstellt werden, wenn für das betreffende Benutzerkonto die Zwei-Faktor-Authentifizierung aktiv ist (diese Anforderung können Sie aber deaktivieren 847, falls gewünscht).
- App-Kennwörter können nur in E-Mail-Apps verwendet werden. Sie sind für die Anmeldung an Webmail oder der MDaemon-Remoteverwaltung nicht nutzbar.
- Jedes App-Kennwort wird nur einmal angezeigt, und zwar unmittelbar nach der Erstellung. Später kann das App-Kennwort nicht mehr angezeigt oder abgerufen werden. Die Benutzer müssen daher darauf vorbereitet sein, das App-Kennwort unmittelbar nach der Erstellung in die App einzugeben.
- Die Benutzer sollen für jede E-Mail-App ein eigenes App-Kennwort verwenden. Sie sollen App-Kennwörter, widerrufen (löschen), falls sie die zugehörige App nicht mehr verwenden, oder falls ein Gerät verlorengeht oder gestohlen wird.
- Für jedes App-Kennwort wird aufgeführt, wann es erstellt wurde, wann es zuletzt verwendet wurde, und von welcher IP-Adresse aus die Verbindung mit dem Benutzerkonto hergestellt wurde. Falls ein Benutzer Unregelmäßigkeiten beim Zeitpunkt der letzten Nutzung oder der protokollierten IP-Adresse bemerkt, sollen das betroffene App-Kennwort widerrufen und ein neues App-Kennwort erstellt werden.
- Bei Änderungen am Kennwort des Benutzerkontos werden alle App-Kennwörter des Benutzerkontos automatisch gelöscht. Die Benutzer können die zuvor gültigen App-Kennwörter dann nicht mehr verwenden.

Erstellen und Verwenden von App-Kennwörtern

Die Benutzer erstellen und verwalten üblicherweise ihre eigenen App-Kennwörter mithilfe von Webmail. Sie müssen dazu die nachfolgend aufgeführten Schritte ausführen (diese Informationen sind auch in der Hilfe für Webmail enthalten). Bevor der Benutzer ein App-Kennwort erstellt, sollte die E-Mail-App oder der E-Mail-Client zur Eingabe des App-Kennworts bereit sein. Das App-Kennwort wird nur unmittelbar nach der Erstellung einmal angezeigt und kann danach nicht mehr gelesen oder abgerufen werden.

1. Bereiten Sie Ihre E-Mail-Anwendung oder Ihren E-Mail-Client darauf vor, das App-Kennwort einzugeben.
2. Melden Sie sich an Webmail an und klicken Sie auf **Optionen** » **Sicherheit**.
3. Tragen Sie das Kennwort für Ihr Benutzerkonto in das Feld **Aktuelles Kennwort** ein.
4. Klicken Sie auf **Neues App-Kennwort**.
5. Geben Sie den Namen der E-Mail-Anwendung ein, in der das App-Kennwort genutzt werden wird (z.B. "E-Mail-App auf Mobiltelefon"), und klicken Sie danach auf OK.
6. Das App-Kennwort wird nun angezeigt. Kopieren Sie das App-Kennwort manuell in Ihre E-Mail-Anwendung, oder tragen Sie es dort ein. Falls nötig, kopieren Sie es in eine Textdatei, oder schreiben Sie es auf. Falls Sie das App-Kennwort für spätere Verwendung in eine Textdatei kopieren oder aufschreiben, sollten Sie diese Kopie vernichten, sobald Sie es in Ihre E-Mail-Anwendung eingetragen haben. Wenn Sie den Vorgang abgeschlossen haben, klicken Sie auf OK.

Falls Sie für einen Benutzer ein App-Kennwort erstellen oder löschen müssen, können Sie dies mithilfe der Optionen auf dieser Seite erledigen. Wie auch bei der Erstellung über Webmail, so wird auch hier das App-Kennwort nur unmittelbar nach der Erstellung einmal angezeigt. Es soll daher sofort in die App eingegeben oder zwischengespeichert und dem Benutzer später mitgeteilt werden.

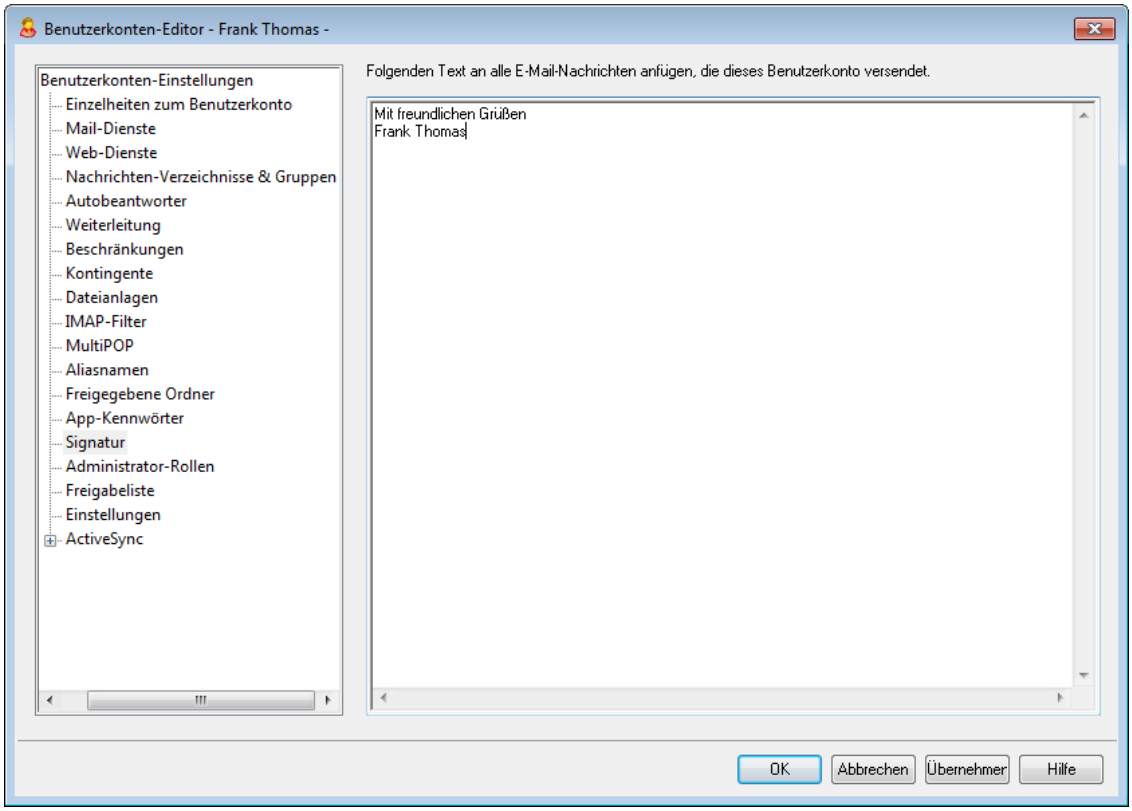
Im Abschnitt Einstellungen des Benutzerkonten-Editors 760 steht die Option "*Anmeldung an SMTP, IMAP, ActiveSync usw. nur über App-Kennwörter zulassen*" zur Verfügung. Sie bewirkt, dass die Anmeldung an den genannten Diensten nur mithilfe von App-Kennwörtern möglich ist.

Wenn Sie die Nutzung von App-Kennwörtern für die genannten Anwendungsfälle erzwingen, so kann dies helfen, das Kennwort für ein Benutzerkonto gegen Brute-Force-Angriffe über SMTP, IMAP und andere Dienste zu schützen. Die Sicherheit ist in diesem Fall erhöht, da selbst bei Bekanntwerden des Kennworts für das Benutzerkonto ein Angriff über die genannten Dienste nicht möglich wäre. Ein Angreifer würde dabei nicht einmal erkennen, dass das Kennwort für das Benutzerkonto entdeckt wurde, da MDaemon für die Anmeldung an den genannten Diensten nicht das Kennwort des Benutzerkontos sondern nur ein gültiges App-Kennwort akzeptiert. Ein weiterer Vorteil ergibt sich bei der Echtheitsbestätigung mithilfe des Active Directory 815. Benutzerkonten im Active Directory werden nach einer bestimmten Anzahl fehlerhafter Anmeldeversuche automatisch gesperrt. Die Nutzung der App-Kennwörter kann solche Sperren verhindern, da MDaemon bei aktivierter Option nur die App-Kennwörter prüft, aber keine Echtheitsbestätigung über das Active Directory versucht.

Siehe auch:

Kennwörter 847
Benutzerkonten-Editor » Einstellungen 760

5.1.1.15 Signatur



Signatur für das Benutzerkonto

In diesem Konfigurationsdialog können Sie eine Signatur hinterlegen, die an das Ende aller Nachrichten angefügt wird, die von diesem Benutzerkonto versandt werden. Die Signatur wird zusätzlich zu den anderen Signaturen und Schlusstexten angefügt, etwa zu den Signaturen von Webmail und anderen verwendeten Mailclients, den Standard-Signaturen[135] und den Domänen-Signaturen[202], den Schlusstexten von Mailinglisten[296]. Standard- und Domänen-Signaturen sowie Schlusstexte von Mailinglisten werden immer nach den Signaturen der Benutzerkonten eingefügt.

Benutzer mit Zugriffsrechten für Webmail oder die Remoteverwaltung[350] können ihre Signaturen über diese Web-Dienste selbst bearbeiten.

Makros für Signaturen

MDaemon unterstützt in den Signaturen Makros, mit deren Hilfe Kontaktdaten des Absenders automatisch in die Signaturen eingefügt werden können. Diese Daten werden den Kontaktdaten des Absenders entnommen, die im Ordner für öffentliche Kontakte seiner Domäne gespeichert sind. Standard- und Domänen-Signaturen können hierdurch mithilfe der Daten des Absenders automatisch individuell gestaltet werden. Zwei Beispiele hierzu: `$CONTACTFULLNAME$` wird umgesetzt in den vollständigen Namen des Absenders, und `$CONTACTEMAILADDRESS$` wird umgesetzt in die E-Mail-Adresse des Absenders. Die Kontaktdaten für die öffentlichen Kontakte können mithilfe von Webmail, des MDaemon Connectors oder über ActiveSync bearbeitet werden. Falls für einen Absender keine Kontaktdaten bestehen, werden Leerstellen eingesetzt. Die verfügbaren Makros sind unten aufgeführt.

Die Benutzer können steuern, welche MDaemon-Signaturen wie in ihre Nachrichten

eingefügt werden. Hierzu fügen sie zwei bestimmte Makros in die Nachrichten ein: Das Makro `$SYSTEMSIGNATURE$` wird ersetzt durch die Standard- oder Domänen-Signatur, und das Makro `$ACCOUNTSIGNATURE$` wird ersetzt durch die Signatur des Benutzerkontos.

Namen und IDs	
Vollständiger Name	**$CONTACTFULLNAME$**
Vorname	**$CONTACTFIRSTNAME$**
Zweiter Vorname	**$CONTACTMIDDLENAME$**
Nachname	**$CONTACTLASTNAME$**
Titel	**$CONTACTTITLE$**
Namenszusatz	**$CONTACTSUFFIX$**
Spitzname	**$CONTACTNICKNAME$**
Vorname (Yomi)	**$CONTACTYOMIFIRSTNAME$**
Nachname (Yomi)	**$CONTACTYOMILASTNAME$**
Name des Benutzerkontos	**$CONTACTACCOUNTNAME$**
Kunden-ID	**$CONTACTCUSTOMERID$**
Verwaltungs-ID	**$CONTACTGOVERNMENTID$**
Speichern unter	**$CONTACTFILEAS$**
E-Mail-Adressen	
E-Mail-Adresse	**$CONTACTEMAILADDRESS$**
E-Mail-Adresse 2	**$CONTACTEMAILADDRESS2$**
E-Mail-Adresse 3	**$CONTACTEMAILADDRESS3$**
Telefon- und Faxnummern	
Mobiltelefon	**$CONTACTHOMEMOBILE$**
Mobiltelefon 2	**$CONTACTMOBILE2$**
Autotelefon	**$CONTACTCARPHONENUMBER$**
Telefon privat	**$CONTACTHOMEPHONE$**
Telefon privat 2	**$CONTACTHOMEPHONE2$**
Telefax privat	**$CONTACTHOMEFAX$**
Anderes Telefon	**$CONTACTOTHERPHONE$**
Instant Messaging und Web	
IM-Adresse	**$CONTACTIMADDRESS$**
IM-Adresse 2	**$CONTACTIMADDRESS2$**

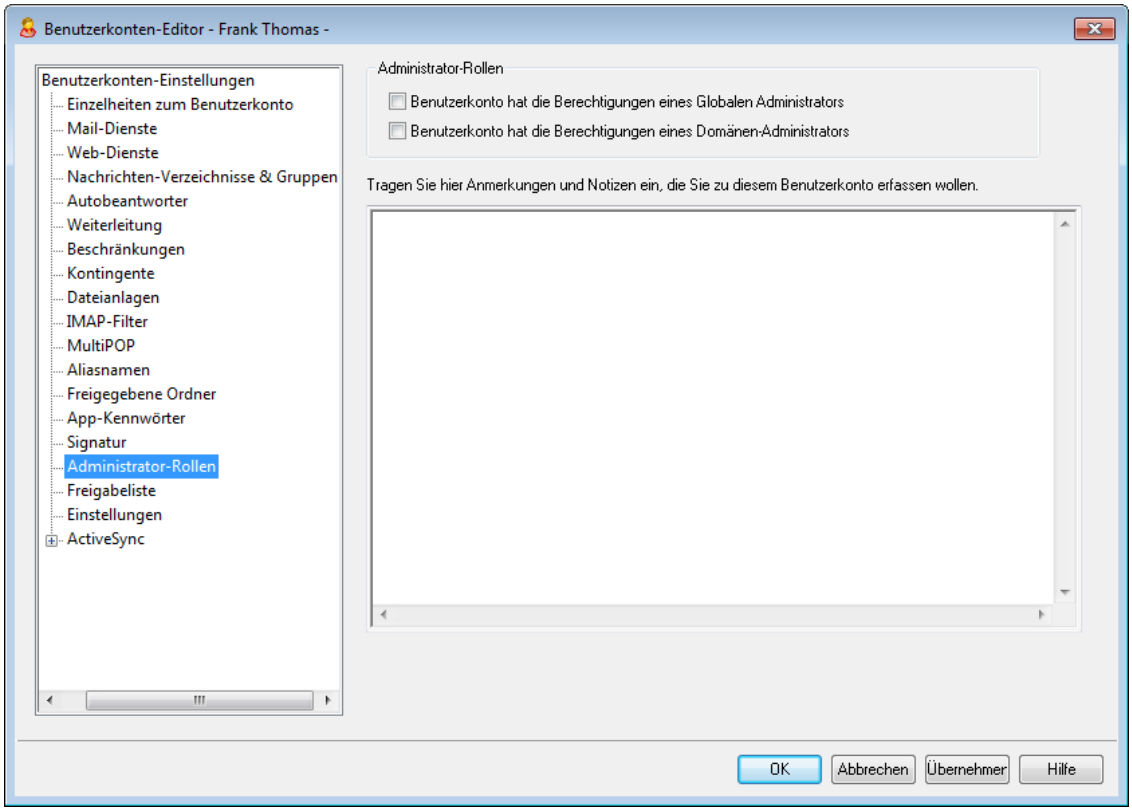
IM-Adresse 3	**$CONTACTIMADDRESS3$**
MMS-Adresse	**$CONTACTMMSADDRESS$**
Web-Adresse privat	**$CONTACTHOMEWEBADDRESS$**
Adresse	
Adresse privat	**$CONTACTHOMEADDRESS$**
Stadt privat	**$CONTACTHOMECITY$**
Bundesland/Kanton privat	**$CONTACTHOMESTATE$**
PLZ privat	**$CONTACTHOMEZIPCODE$**
Land privat	**$CONTACTHOMECOUNTRY$**
Andere Adresse	**$CONTACTOTHERADDRESS$**
Andere Stadt	**$CONTACTOTHERCITY$**
Anderes Bundesland/ anderer Kanton	**$CONTACTOTHERSTATE$**
Andere PLZ	**$CONTACTOTHERZIPCODE$**
Anderes Land	**$CONTACTOTHERCOUNTRY$**
Geschäftsbezogene Daten	
Firma	**$CONTACTBUSINESSCOMPANY$**
Firma (Yomi)	**$CONTACTYOMICOMPANYNAME$**
Titel/Berufsbezeichnung	**$CONTACTBUSINESSTITLE$**
Büro geschäftlich	**$CONTACTBUSINESSOFFICE$**
Abteilung geschäftlich	**$CONTACTBUSINESSDEPARTMENT$**
Manager geschäftlich	**$CONTACTBUSINESSMANAGER$**
Assistenz geschäftlich	**$CONTACTBUSINESSASSISTANT$**
Telefon Assistenz geschäftlich	**$CONTACTBUSINESSASSISTANTPHONE$**
Telefon zentral geschäftlich	**$CONTACTBUSINESSMAINPHONE$**
Telefon geschäftlich	**$CONTACTBUSINESSPHONE$**
Telefon geschäftlich 2	**$CONTACTBUSINESSPHONE2$**
IP-Telefon geschäftlich	**$CONTACTBUSINESSIPPHONE$**
Fax geschäftlich	**$CONTACTBUSINESSFAX$**
Pager geschäftlich	**$CONTACTBUSINESSPAGER$**

Funkdienst geschäftlich	**$CONTACTBUSINESSRADIO$**
Adresse geschäftlich	**$CONTACTBUSINESSADDRESS$**
Stadt geschäftlich	**$CONTACTBUSINESSCITY$**
Bundesland/Kanton geschäftlich	**$CONTACTBUSINESSSTATE$**
PLZ geschäftlich	**$CONTACTBUSINESSZIPCODE$**
Land geschäftlich	**$CONTACTBUSINESSCOUNTRY$**
Web-Adresse geschäftlich	**$CONTACTBUSINESSWEBADDRESS$**
Weitere Daten	
Ehegatte	**$CONTACTSPOUSE$**
Kinder	**$CONTACTCHILDREN$**
Kategorien	**$CONTACTCATEGORIES$**
Kommentar	**$CONTACTCOMMENT$**

Siehe auch:

Standard-Signaturen 135
Domänen-Signaturen 202
Schlusstexte für Mailinglisten 296

5.1.1.16 Administrator-Rollen



Administrator-Rollen

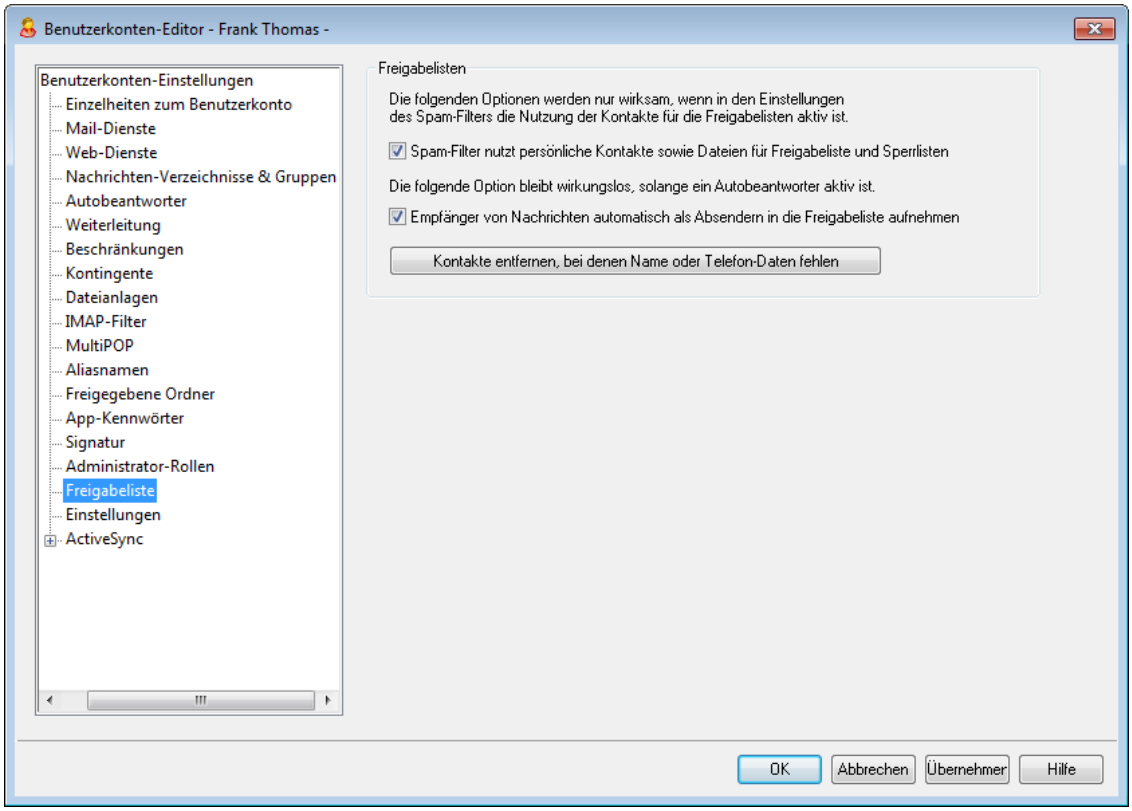
Benutzerkonto hat die Berechtigungen eines Globalen Administrators
Diese Option gibt den Benutzern Zugriffsrechte und Berechtigungen als Administratoren für das gesamte System. Ein so berechtigter Benutzer hat uneingeschränkten Zugriff auf alle Dateien und Einstellungen von MDaemon. Der Abschnitt Remoteverwaltung 350 enthält eine genaue Beschreibung der einzelnen Berechtigungsstufen für Administratoren.

Benutzerkonto hat die Berechtigungen eines Domänen-Administrators
Diese Option gibt den Benutzern die Zugriffsrechte und Berechtigungen eines Domänen-Administrators. Diese Rechte ähneln denen der globalen Administratoren, sind aber auf die Domänen beschränkt, für die dem Administrator die Administratorrechte eingeräumt sind, sowie auf die im Abschnitt Web-Dienste 720 zugewiesenen Rechte.

Falls Sie dem Benutzerkonto Administratorrechte für eine andere Domäne einräumen wollen, können Sie die Rechte im Abschnitt Domänen-Manager » Administratoren der Remoteverwaltung 350 zuweisen.

Tragen Sie hier Anmerkungen und Notizen ein, die Sie zu diesem Benutzerkonto erfassen wollen
In diesem Textfeld können Sie Notizen und andere Informationen eintragen, die Sie in Bezug auf dieses Benutzerkonto für eigene Zwecke nutzen wollen. Anders, als es bei dem Textfeld *Beschreibung* im Konfigurationsdialog Einzelheiten zum Benutzerkonto 714 der Fall ist, werden die Anmerkungen und Notizen hier nicht mit den öffentlichen Kontakten synchronisiert und keinen Feldern im Active Directory zugeordnet.

5.1.1.17 Freigabeliste



Freigabelisten

Spam-Filter nutzt persönliche Kontakte sowie Dateien für Freigabeliste und Sperrlisten
Im Abschnitt Freigabeliste (automatisch) 692 des Konfigurationsdialogs für den Spam-Filter ist eine Option enthalten, die systemweit wirkt, und die bestimmt, ob der Spam-Filter eine Nachricht automatisch als Treffer auf der Freigabeliste behandelt, falls der Absender der Nachricht in den persönlichen Kontakten oder der persönlichen Freigabeliste des lokalen Empfängers enthalten ist. Die Option bewirkt auch, dass eine Nachricht automatisch als Treffer auf der Sperrliste behandelt wird, falls ihr Absender in der Sperrliste des Benutzers gefunden wird. Die hier vorliegende Option steuert dieses Verhalten für das gerade bearbeitete Benutzerkonto. Falls die systemweite Option in der Konfiguration des Spam-Filters aktiv ist, aber nicht auf dieses Benutzerkonto wirken soll, müssen Sie diese Option hier deaktivieren. Falls die systemweite Option abgeschaltet ist, ist die vorliegende Option nicht verfügbar.

Empfänger von Nachrichten automatisch als Absendern in die Freigabeliste aufnehmen
Diese Option bewirkt, dass der Ordner Freigegebene Absender dieses Benutzerkontos immer dann aktualisiert wird, wenn das Benutzerkonto eine abgehende Nachricht an eine externe Empfängeradresse sendet. Zusammen mit der Option *Spam-Filter nutzt persönliche Kontakte sowie Dateien für Freigabeliste und Sperrlisten* weiter oben kann diese Option die Anzahl der falschen positiven Treffer des Spam-Filters erheblich verringern. Diese Option steht aber nur zur Verfügung, falls die Option *Empfänger von Nachrichten automatisch als Absendern in die Freigabeliste aufnehmen* im Abschnitt Freigabeliste (automatisch) 692 ebenfalls aktiv ist.

So lange für das Benutzerkonto ein Autobeantworter aktiv ist, ist diese Funktion automatisch gesperrt.

Kontakte entfernen, bei denen Namen oder Telefon-Daten fehlen
Durch Anklicken dieses Steuerelements können Sie aus den Standard-Kontaktordnern aller Benutzer alle Kontakte löschen, die nur eine E-Mail-Adresse enthalten. Falls für einen Kontakt nicht wenigstens auch ein Name oder eine Telefon-Nummer erfasst ist, wird der Kontakt dabei gelöscht. Diese Option soll vor allem den Benutzern helfen, die die automatische Freigabeliste in MDaemon vor Version 11 (noch unter der Bezeichnung "Weiße Liste") genutzt haben; sie kann die Kontakte löschen, die nur als Ergebnis der Aufnahme in die Freigabeliste gespeichert wurden. In früheren Versionen von MDaemon wurden die Adressen den Standard-Kontaktordnern hinzugefügt, und es stand kein besonderer Ordner für die Freigabeliste zur Verfügung. Dies konnte dazu führen, dass Benutzer viele Einträge in den Kontaktordnern hatten, die sie eigentlich gar nicht benötigten.

Sie sollten diese Funktion nur sehr umsichtig einsetzen, da es durchaus legitime Gründe geben kann, warum Einträge in den Kontaktordnern nur E-Mail-Adressen enthalten.

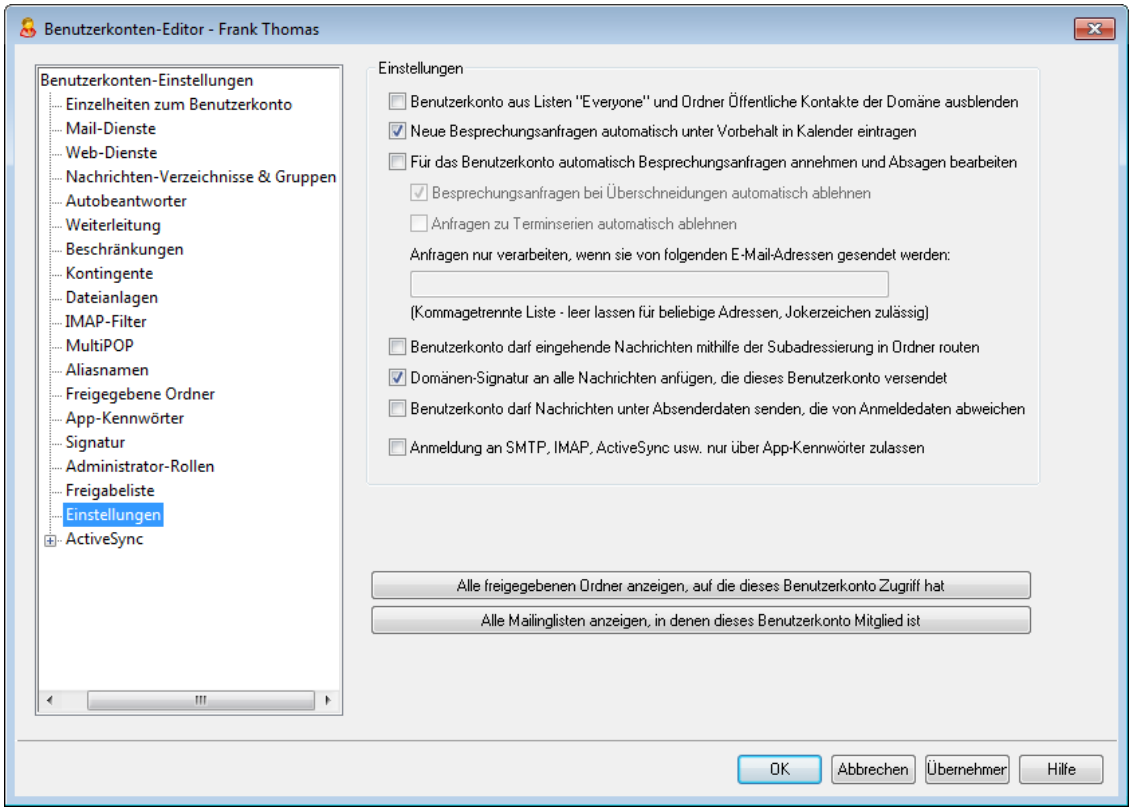
Voreinstellungen für neue Benutzerkonten und Gruppen festlegen

Die Optionen in diesem Konfigurationsdialog entsprechen den Optionen im Konfigurationsdialog Vorlagen-Eigenschaften » Freigabeliste 811, mit deren Hilfe Sie die Voreinstellungen für neue Benutzerkonten 788 und die Einstellungen für Benutzerkonten in bestimmten Gruppen 782 festlegen können.

Siehe auch:

Freigabeliste (automatisch) 692
Vorlagen-Manager 787
Vorlagen-Eigenschaften » Freigabeliste 811

5.1.1.18 Einstellungen



Optionen

Benutzerkonto aus Listen "Everyone" und Ordner Öffentliche Kontakte der Domäne ausblenden
MDaemon erstellt automatisch die Mailinglisten "Everyone@" und "MasterEveryone@"[272]; sie können benutzt werden, um alle Benutzer der jeweiligen Domäne anzusprechen. MDaemon nimmt grundsätzlich alle Benutzerkonten in die Liste auf. Diese Einstellung bewirkt, dass das gerade bearbeitete Benutzerkonto aus den genannten Mailinglisten ausgeblendet wird, und dass das Benutzerkonto über die genannten Mailinglisten keine Nachrichten erhält. Das Benutzerkonto erscheint dann auch nicht im Ordner Öffentliche Kontakte der Domäne.

Neue Besprechungsanfragen automatisch unter Vorbehalt in Kalender eintragen
Diese Option bewirkt, dass Termine aus Besprechungsanfragen nach dem Eingang bei den Empfängern automatisch unter Vorbehalt in die Kalender der Empfänger der Besprechungsanfragen eingetragen werden. Diese Option ist per Voreinstellung aktiv.

Für das Benutzerkonto automatisch Besprechungsanfragen annehmen und Absagen bearbeiten
Diese Option bewirkt, dass Besprechungsanfragen, Aktualisierungen für Termine, sowie Absagen durch dieses Benutzerkonto automatisch verarbeitet werden. Erhält das Benutzerkonto eine Besprechungsanfrage, so wird der Kalender automatisch aktualisiert. Diese Option ist per Voreinstellung für alle Benutzerkonten abgeschaltet.

Besprechungsanfragen bei Überschneidungen automatisch ablehnen
Ist die Option zum Automatischen Bearbeiten von Besprechungsanfragen aktiv, so bewirkt diese Option, dass Besprechungsanfragen immer dann automatisch abgelehnt werden, wenn sie eine Überschneidung oder einen Konflikt mit einem bereits bestehenden Termin verursachen würde. Ist die Option nicht aktiv, so wird auch eine Besprechungsanfrage angenommen, wenn dies einen Terminkonflikt hervorruft.

Anfragen zu Terminserien automatisch ablehnen
Diese Option bewirkt, dass Besprechungsanfragen, die Terminserien zum Gegenstand haben, automatisch abgelehnt werden. Andere Besprechungsanfragen werden so behandelt, wie es die vorstehenden Optionen vorsehen.

Anfragen nur verarbeiten, wenn sie von folgenden E-Mail-Adressen gesendet werden
Sie können die automatische Verarbeitung von Besprechungsanfragen auf bestimmte Absender beschränken. Tragen Sie hierzu die E-Mail-Adressen dieser Absender in das folgende Textfeld ein. Trennen Sie mehrere Adressen durch Kommata. Jokerzeichen in den Adressen sind zulässig (etwa *@example.com). Falls Sie dieses Textfeld leer lassen, werden, sofern die entsprechenden Optionen aktiv sind, Besprechungsanfragen aller Absender automatisch verarbeitet.

Benutzerkonto darf eingehende Nachrichten mithilfe der Subadressierung in Ordner routen
Diese Option gestattet dem gerade bearbeiteten Benutzerkonto die Nutzung der Subadressierung 762.

Domänen-Signatur an alle Nachrichten anfügen, die dieses Benutzerkonto versendet
Ist für die Benutzerkonten einer Domäne eine Domänen-Signature 202 definiert, dann bewirkt diese Option, dass die Domänen-Signatur abgehenden Nachrichten solcher Benutzerkonten hinzugefügt wird, deren Einstellungen durch diese Vorlage gesteuert werden.

Benutzerkonto darf Nachrichten unter Absenderdaten senden, die von Anmeldedaten abweichen
Diese Option bewirkt, dass Benutzerkonten, deren Einstellungen durch diese Vorlage gesteuert werden, von der Anwendung der systemweiten Option "*Anmeldedaten für Echtheitsbestätigung müssen mit Benutzerkonto des Absenders übereinstimmen*" ausgenommen sind. Die systemweite Option ist über den Konfigurationsdialog SMTP-Echtheitsbestätigung 524 zugänglich.

Anmeldung an SMTP, IMAP, ActiveSync usw. nur über App-Kennwörter zulassen
Diese Option bewirkt, dass die Benutzerkonten in E-Mail-Clients, für die Anmeldung an SMTP, IMAP, ActiveSync und anderen E-Mail-Diensten App-Kennwörter 750 verwenden müssen. Die normalen Kennwörter 847 der Benutzerkonten müssen für die Anmeldung an Webmail oder der MDaemon-Remoteverwaltung weiterhin genutzt werden.

Wenn Sie die Nutzung von App-Kennwörtern für die genannten Anwendungsfälle erzwingen, so kann dies helfen, das Kennwort für ein Benutzerkonto gegen Brute-Force-Angriffe über SMTP, IMAP und andere Dienste zu schützen. Die Sicherheit ist in diesem Fall erhöht, da selbst bei Bekanntwerden des Kennworts für das Benutzerkonto ein Angriff über die genannten Dienste nicht möglich wäre. Ein

Angreifer würde dabei nicht einmal erkennen, dass das Kennwort für das Benutzerkonto entdeckt wurde, da MDaemon für die Anmeldung an den genannten Diensten nicht das Kennwort des Benutzerkontos sondern nur ein gültiges App-Kennwort akzeptiert. Ein weiterer Vorteil ergibt sich bei der Echtheitsbestätigung mithilfe des Active Directory. Benutzerkonten im Active Directory 815 werden nach einer bestimmten Anzahl fehlerhafter Anmeldeversuche automatisch gesperrt. Die Nutzung der App-Kennwörter kann solche Sperren verhindern, da MDaemon bei aktivierter Option nur die App-Kennwörter prüft, aber keine Echtheitsbestätigung über das Active Directory versucht.

All freigegebenen Ordner anzeigen, auf die dieses Benutzerkonto Zugriff hat
Um eine Liste aller freigegebenen Ordner einzusehen, auf die das gerade bearbeitete Benutzerkonto Zugriff hat, klicken Sie auf dieses Steuerelement.

Alle Mailinglisten anzeigen, in denen dieses Benutzerkonto Mitglied ist
Um eine Liste aller Mailinglisten 269 einzusehen, in denen das gerade bearbeitete Benutzerkonto Mitglied ist, klicken Sie auf dieses Steuerelement.

Subadressierung

Die Subadressierung gestattet das Einbinden von Ordnernamen in den Postfachnamen, der Teil einer E-Mail-Adresse ist. Mithilfe dieser Funktion können Nachrichten, die an eine Kombination aus Postfach+Ordnername adressiert sind automatisch in dem Ordner abgelegt werden, der in der Adresse bezeichnet ist, falls dieser Ordner existiert. Nachrichten können damit automatisch in Ordner einsortiert werden, ohne dass es eines Filters bedürfte.

Hat beispielsweise "bill.farmer@example.com" einen IMAP-Ordner namens "Verschiedenes", so werden Nachrichten, die an "bill.farmer+Verschiedenes@example.com" gerichtet sind, automatisch in diesen Ordner geleitet. Auch Unterordner können angegeben werden, hierzu müssen die Namen von Ordner und Unterordner durch ein zusätzliches Zeichen + getrennt sein. Leerzeichen in Ordnernamen werden durch Unterstriche dargestellt. Existierte beispielsweise unter Bills Ordner "Verschiedenes" ein Unterordner namens "Alte Nachrichten", so würden Nachrichten, die an "bill.farmer+Verschiedenes.Alte_Nachrichten@example.com" gerichtet wären, automatisch in Bills Ordner "\Verschiedenes\Alte Nachrichten\" geleitet.

Da die Subadressierung das Zeichen + als Steuerzeichen nutzt, können Postfachnamen, die selbst das Zeichen + enthalten, die Subadressierung nicht nutzen. Lautete in dem Beispiel oben die E-Mail-Adresse etwa "bill+farmer@example.com" statt "bill.farmer@example.com"", so wäre die Subadressierung nicht möglich. Auch kann ein Adress-Aliasname nicht als Subadresse genutzt werden. Ein Aliasname, der auf eine E-Mail-Adresse einschließlich der Subadresse verweist, ist aber zulässig. Obwohl also "Alias+Verschiedenes@example.com"" nicht zulässig wäre, könnte ein Aliasname "Alias@example.com"", der auf "bill.farmer+Verschiedenes@example.com"" verweist, problemlos genutzt werden.

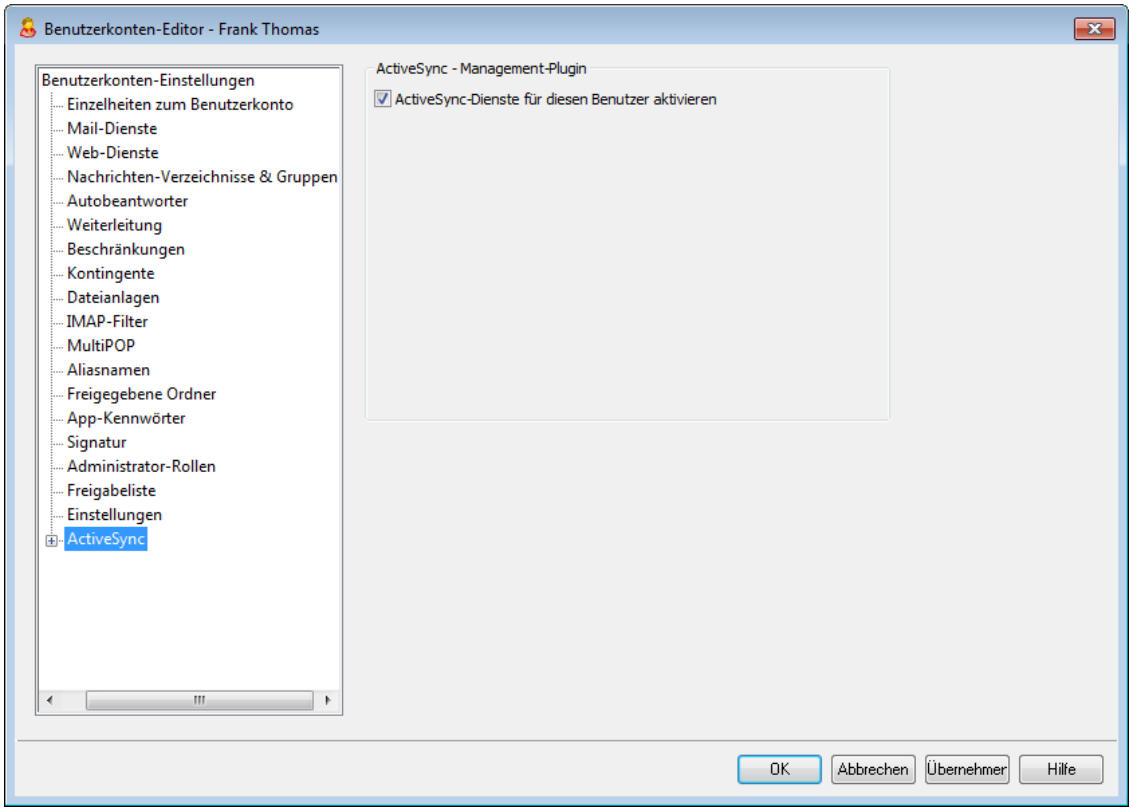
Um Missbrauch und Sicherheitslücken vorzubeugen, **muss** der IMAP-Ordner, der in der Subadresse bezeichnet wird, zwingend vorhanden sein. Ist eine Nachricht mit Subadressierung an ein Benutzerkonto gerichtet, bei dem der angegebene Ordner nicht besteht, so wird die Subadresse wie eine unbekannte E-Mail-Adresse behandelt und nach Maßgabe der allgemeinen Optionen über die

Behandlung unbekannter Empfänger weiterverarbeitet. Hätte im Beispiel `bill.farmer@example.com` keinen Ordner namens "`Verschiedenes`"", und würde dennoch eine Nachricht für "`bill.farmer+Verschiedenes@example.com`" eingehen, so würde die Nachricht behandelt, wie wenn sie an einen unbekannten Benutzer gerichtet wäre. Üblicherweise würde die Nachricht zurückgewiesen werden.

Siehe auch:

Freigabeliste (automatisch) 692
Remoteverwaltung 350
Vorlagen-Manager 787
Kennwörter 847

5.1.1.19 ActiveSync für MDaemon



Die Konfigurationsdialoge im Abschnitt ActiveSync für MDaemon des Benutzerkonten-Editors werden verwendet, um für das gerade bearbeitete Benutzerkonto ActiveSync zu aktivieren und zu deaktivieren, benutzerindividuelle Einstellungen 764 festzulegen, eine Standard-Richtlinie zuzuweisen 770, und die ActiveSync-Clients 772 des Benutzerkontos zu verwalten.

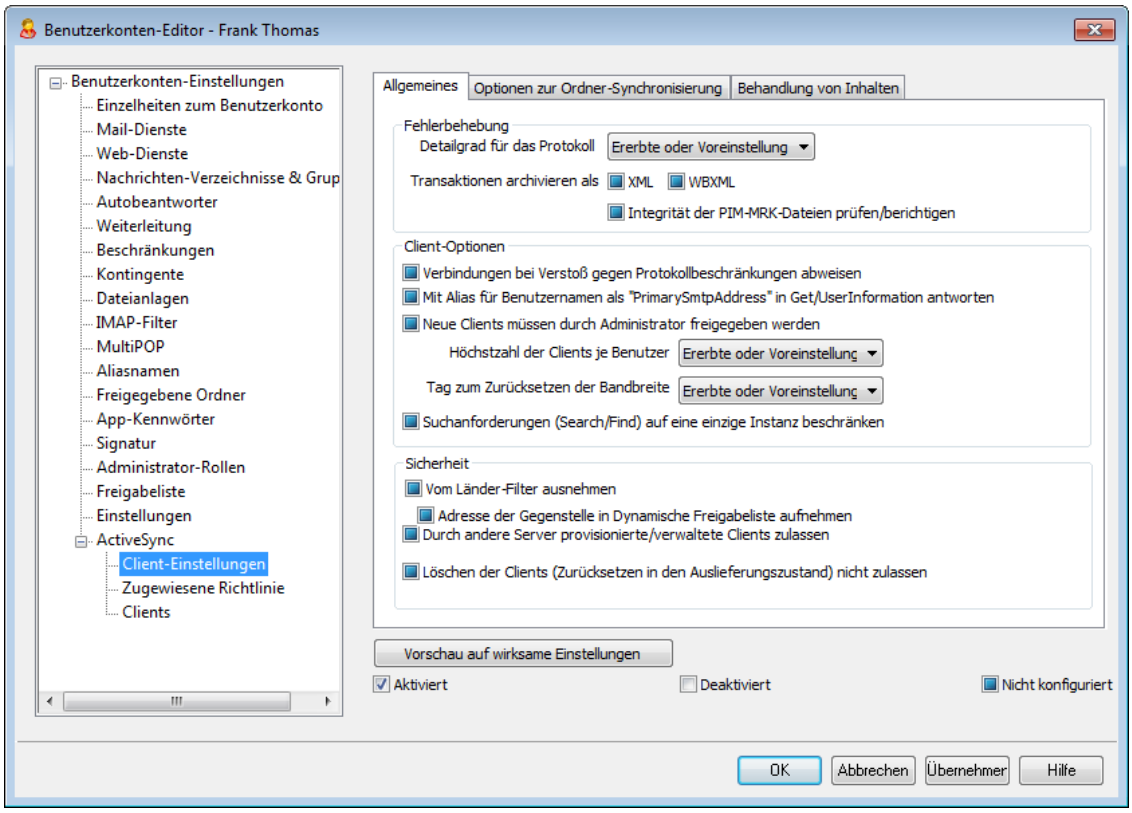
ActiveSync-Dienste für diesen Benutzer aktivieren

Um dem gerade bearbeiteten Benutzerkonto die Nutzung von ActiveSync für den Zugriff auf E-Mail-Nachrichten und PIM-Daten zu gestatten, aktivieren Sie diese Option.

Siehe auch:

Benutzerkonten-Editor » ActiveSync » Client-Einstellungen 764
Benutzerkonten-Editor » ActiveSync » Zugewiesene Richtlinie 770
Benutzerkonten-Editor » ActiveSync » Clients 772

5.1.1.19.1 Client-Einstellungen



Die Optionen in diesem Konfigurationsdialog steuern die Client-Einstellungen für ActiveSync für solche Clients, die mit dem gerade bearbeiteten Benutzerkonto verknüpft sind. Per Voreinstellung erbt jede Option die Einstellung der Domäne, zu der das Benutzerkonto gehört. Durch Anpassen einzelner Optionen in diesem Konfigurationsdialog werden die entsprechenden Domänen-Einstellungen 437 für dieses Benutzerkonto übergangen. Sie können mithilfe der Option *Einstellungen* im Abschnitt Clients 772 auch die für das Benutzerkonto geltenden Einstellungen für einzelne Clients übergehen und ändern.

Allgemeines

Fehlerbehebung

Detailgrad für das Protokoll
ActiveSync für MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur

Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Einstellung erben Per Voreinstellung wird die Einstellung für den Detailgrad aus der Hierarchie der Client-Einstellungen vom jeweils übergeordneten Knoten ererbt. Clients übernehmen dabei die Einstellung aus dem jeweiligen Client-Typ, Client-Typen übernehmen die Einstellung von den Benutzerkonten, Benutzerkonten übernehmen die Einstellung von den Gruppen, und so weiter. Die globale Einstellung für alle Clients wird durch die Einstellung für den Detailgrad im Konfigurationsdialog Diagnose 432 bestimmt.

Transaktionen archivieren als [XML | WBXML]
Mithilfe der Optionen *XML...* und *WBXML...* können Sie die zugehörigen Daten speichern; diese Daten können die Fehlersuche erleichtern. Die systemweit wirksamen Optionen sind per Voreinstellung abgeschaltet.

Integrität der PIM-MRK-Dateien prüfen/berichtigen
Diese Option führt für die PIM-Daten der betroffenen Clients Prüf- und Korrekturvorgänge durch. Sie sollen bekannte Probleme erkennen, die eine ordnungsgemäße Synchronisierung verhindern können. Zu diesen Problemen zählen insbesondere doppelte iCal-UIDs und leere Datenfelder, die eigentlich verpflichtend Daten enthalten müssen. Die systemweit wirksame Option ist per Voreinstellung abgeschaltet.

Client-Optionen

Verbindungen bei Verstoß gegen Protokollbeschränkungen abweisen
Diese Option bewirkt, dass Verbindungen von Clients abgewiesen werden, falls sie versuchen eine nicht für die Clients *Zugelassene Protokollversion* zu verwenden. Per Voreinstellung ist diese Option abgeschaltet; dies bedeutet, dass die Protokollbeschränkung keine Verbindungen solcher Clients verhindern, die andere als die zugelassenen Protokollversionen verwenden. Solange die Option abgeschaltet ist, weist MDaemon die Clients zwar an, nur die zugelassenen Protokollversionen zu verwenden, lässt aber bei Nutzung anderer Protokollversionen die Verbindung trotzdem zu. Nähere Informationen finden Sie unter Protokollbeschränkungen 434.

Mit Alias für Benutzernamen als "PrimarySmtpAddress" in Get/UserInformation antworten
Diese Option gestattet es dem Dienst, als Antwort auf eine Anforderung Settings/Get/UserInformation eine etwa vorhandene Alias-Adresse oder eine sekundäre Adresse des betroffenen Benutzerkontos als primäre Adresse zu übermitteln. Hierdurch wird ein Problem umgangen, das mit einer iOS-Aktualisierung nach Version 9.x verursacht wird, und das verhinderte, dass Clients unter einer etwa vorhandenen Alias-Adresse Nachrichten versenden konnten. Die Nutzung dieser Option bewirkt eine nicht standardkonforme Antwort auf die Anforderung Settings/GetUserInformation.

Neue Clients müssen durch Administrator freigegeben werden
Diese Option bewirkt, dass neue Clients sich erst dann mit Benutzerkonten synchronisieren können, wenn sie zunächst durch einen Administrator freigegeben wurden. In der Liste der Clients[464] sind alle Clients aufgeführt, die noch die Freigabe erwarten, und die Administratoren können sie über diese Liste freigeben. Diese Option ist per Voreinstellung abgeschaltet.

Höchstzahl der Clients je Benutzer
Mithilfe dieser Option können Sie die Anzahl der ActiveSync-Clients und -Endgeräte begrenzen, die mit jedem MDaemon-Benutzerkonto verknüpft sein können. Der hier angegebene Wert ist die Höchstzahl zulässiger Clients. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt. Diese Option steht nur in den Client-Einstellungen auf globaler, Domänen- und Benutzerebene zur Verfügung, nicht jedoch in den Client-Einstellungen für die einzelnen Clients.

Tag zum Zurücksetzen der Bandbreite
Mithilfe dieser Option können Sie Tag bestimmen, an dem in jedem Monat die Bandbreiten-Nutzungsstatistik für die ActiveSync-Endgeräte zurückgesetzt wird. Dieser Vorgang wird während der normalen Bereinigungsvorgänge um Mitternacht aufgeführt und, wie auch andere Bereinigungsvorgänge, in das Protokoll System eingetragen. Der globale Wert lautet per Voreinstellung 0 (nicht zurücksetzen), sodass per Voreinstellung die Nutzungsstatistik nicht zurückgesetzt wird. Für untergeordnete Knoten können Sie abweichende Einstellungen treffen, etwa, um die Einstellung an den Tag anzugleichen, an dem für das betroffene Endgeräte ein neuer Abrechnungszeitraum des Netzbetreibers beginnt.

Sicherheit

Vom Länder-Filter ausnehmen
Wenn Sie diese Option in den Einstellungen eines ActiveSync-Clients aktivieren, kann das Endgerät den Länder-Filter[574] umgehen. Hierdurch kann ein berechtigter Benutzer auf sein Benutzerkonto über ActiveSync beispielsweise auch dann zugreifen, wenn er sich in einem Land befindet, für das Versuche zur Echtheitsbestätigung ansonsten durch den Länder-Filter unterbunden werden. Ein Endgerät kann nur dann vom Länder-Filter ausgenommen sein, wenn es innerhalb des durch die Option Inaktive Clients entfernen nach [x] Tagen[418] im Abschnitt Anpassung bestimmten Zeitraums eine echtheitsbestätigte Verbindung über ActiveSync erfolgreich hergestellt hat.

Adresse der Gegenstelle in Dynamische Freigabeliste aufnehmen
Wenn Sie ein Endgerät vom Länder-Filter ausnehmen, können Sie durch Aktivieren dieser Option die IP-Adresse, von der aus das Endgerät die Verbindung herstellt, in die Freigabeliste eintragen lassen. Hierdurch können

beispielsweise andere Clients, die von der selben IP-Adresse aus eine Verbindung herstellen, ebenfalls zugelassen werden.

Durch andere Server provisionierte/verwaltete Clients zulassen
Per Voreinstellung dürfen Clients auch dann Verbindungen zu MDaemon aufbauen, wenn sie auf die Übermittlung der Provisionierungs- und Richtliniendaten durch den ActiveSync-Server hin melden, dass sie auch durch einen oder mehrere andere ActiveSync-Server verwaltet werden. Bei einer solchen Mehrfachverwaltung kann es nicht sichergestellt werden, dass alle auf Ihrem System bestehenden Richtlinien durch den Client auch umgesetzt werden; dies gilt insbesondere dann, wenn sie Richtlinien des anderen ActiveSync-Servers widersprechen. In vielen Fällen setzen die Clients die am stärksten einschränkende Richtlinie um, falls mehrere einander widersprechende Richtlinien vorhanden sind. Um Verbindungen von Clients zu unterbinden, die durch andere ActiveSync-Server verwaltet werden, deaktivieren Sie diese Option.

Löschen der Clients (Zurücksetzen in den Auslieferungszustand) nicht zulassen
Wenn diese Option aktiv ist, dann können ActiveSync-Clients nicht in den **Auslieferungszustand zurückgesetzt** und damit vollständig gelöscht werden. Wenn Sie Clients ferngesteuert in den Auslieferungszustand zurücksetzen wollen, müssen Sie diese Option deaktivieren. Diese Option ist per Voreinstellung deaktiviert. Nähere Informationen finden Sie auf der Seite Clients im Abschnitt **Vollständiges Löschen eines ActiveSync-Clients** 464.

Optionen zur Ordner-Synchronisierung

Optionen zur Ordner-Synchronisierung

Folgende Ordner ausnehmen

Freigegebene Absender/Gesperrte Absender
Per Voreinstellung werden die Kontaktordner mit Freigabelisten und Sperrlisten der Benutzer nicht mit den Geräten synchronisiert. Diese Ordner dienen üblicherweise nur in MDaemon zum Erkennen und Filtern von Spam. Ihre Inhalte brauchen daher nicht auf den Geräten als Kontakte angezeigt zu werden.

Benutzerdefinierte Nachrichten-Ordner
Per Voreinstellung können alle Standard- und benutzerdefinierten Nachrichten-Ordner mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-Nachrichtenordner synchronisiert werden können. Die Standard-Nachrichtenordner sind insbesondere Posteingang, Gesendete Objekte, Gelöschte Objekte und Entwürfe. Ordner, die die Benutzer selbst anlegen, werden dann nicht mehr synchronisiert. Diese Option ist per Voreinstellung abgeschaltet.

Benutzerdefinierte PIM-Ordner
Per Voreinstellung können alle PIM-Ordner (insbesondere Kontakte, Kalender, Notizen und Aufgaben) mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-PIM-Ordner synchronisiert werden können. Ist diese Option aktiv, so wird beispielsweise für jeden Benutzer nur der Standard-Kalender synchronisiert, auch wenn er über mehrere Kalender-Ordner verfügt. Diese Option ist per Voreinstellung abgeschaltet.

Folgende Ordner einschließen

Hierarchie der öffentlichen Ordner
Diese Option bewirkt, dass die öffentlichen Ordner[309], auf die die Benutzer Zugriff haben, in den Ordnerlisten der Benutzer auf ihren ActiveSync-Geräten erscheinen. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der öffentlichen Ordner[309], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Traversieren öffentlicher Ordner zulassen (legt Ordnernamen offen)
Benutzerkonten, die auf Unterordner in öffentlichen Ordnern zugreifen oder diese synchronisieren wollen, müssen per Voreinstellung sowohl für den betroffenen Unterordner als auch für alle ihm übergeordneten öffentlichen Ordner[309] über die Berechtigung Ordner anzeigen[311] verfügen. Fehlt einem Benutzerkonto diese Berechtigung für einen übergeordneten öffentlichen Ordner, so kann er auch den gewünschten Unterordner nicht synchronisieren und nicht auf ihn zugreifen, und zwar auch dann nicht, wenn das Benutzerkonto für diesen Unterordner selbst die erforderliche Berechtigung hat. Mithilfe dieser Option können Sie den Clients Zugriff auf und Synchronisierung von Unterordnern ermöglichen, ohne dass die Clients Berechtigungen für die übergeordneten öffentlichen Ordner haben. **Beachte:** Ist diese Option aktiv, so erlangt der Client zwangsläufig Kenntnis von den Namen der übergeordneten Ordner, auch wenn er für ihre Inhalte keine Zugriffsrechte hat. Hieraus kann sich ein Sicherheitsrisiko ergeben. Die Option ist per Voreinstellung abgeschaltet.

Höchstzahl zulässiger öffentlicher Ordner
Diese Option begrenzt die Zahl der öffentlichen Ordner, die auf den betroffenen Geräten dargestellt werden können. Ist eine solche Höchstzahl angegeben, dann übermittelt der Server so lange Einträge in der Ordnerliste, bis die Höchstzahl erreicht ist. Danach übermittelt der Server keine Ordner mehr an die Geräte. Die Reihenfolge, in der die Ordner dabei verarbeitet werden, kann weder festgelegt noch vorher bestimmt werden. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt.

Freigegebene Ordner
Diese Option nimmt auch die gemeinsam genutzten Ordner[122], auf die die Benutzer Zugriff haben, in die Ordnerlisten auf ihren ActiveSync-Geräten auf. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der freigegebenen Ordner[742], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Behandlung von Inhalten

Optionen zur Behandlung von Inhalten

Aufgaben/Erinnerungen für durch Clients gekennzeichnete Nachrichtenelemente erstellen
Diese Option ermöglicht es MDaemon, die Benutzer an gekennzeichnete Elemente zu erinnern. Hierzu wird für jede gekennzeichnete E-Mail-Nachricht eine Aufgabe

erstellt, wenn der Client dies anfordert. Die globale Option für dieses Leistungsmerkmal ist per Voreinstellung aktiv.

Aktualisierung nach jeder Änderung der Besprechung senden
Manche Clients versenden aktualisierte Besprechungseinladungen nicht richtig, nachdem eine Besprechung geändert wurde. Diese Option bewirkt, dass der ActiveSync-Dienst immer dann aktualisierte Besprechungseinladungen sendet, wenn der Besprechungsorganisator eine Besprechung aktualisiert hat. Diese Option sollte nur für Clients 464 und Client-Typen 481 aktiviert werden, die die aktualisierten Besprechungseinladungen nicht richtig versenden, da sonst aktualisierte Besprechungseinladungen doppelt versandt werden. Aus diesem Grund ist diese Einstellung nur auf den Seiten Clients und Client-Typen verfügbar.

Lesebestätigung für alle versandten Nachrichten anfordern
Diese Option bewirkt, dass der Server für alle durch einen Client versandten E-Mail-Nachrichten Lesebestätigungen anfordert. Diese Option ist per Voreinstellung abgeschaltet.

Vom Absender angeforderte Lesebestätigung senden, sobald Nachricht als gelesen gekennzeichnet ist
Diese Option bewirkt, dass der Server Anforderungen von Lesebestätigungen beachtet und die Lesebestätigungen dann versendet, wenn eine Nachricht durch den Client als gelesen gekennzeichnet wird. Diese Option ist per Voreinstellung abgeschaltet.

Unter dem in der Antwortadresse (ReplyTo) angegebenen Alias senden
Manche Clients gestatten den Absendern nicht den Versand von E-Mail-Nachrichten unter einem Alias. Dieses Leistungsmerkmal wurde im der Version 16.x des Protokolls Exchange ActiveSync (EAS) 434 erstmals unterstützt, aber manche Clients unterstützen die Version 16.x nicht. So nutzt beispielsweise Microsoft Outlook für Windows nur EAS 14.0 und gestattet zwar den Benutzern die Angabe einer anderen Adresse, unter der eine Nachricht versandt werden soll, aber die dann erstellte Nachricht gibt die Auswahl des Benutzers nicht richtig wieder. Diese Option gestattet die Nutzung des Feldes für die Antwortadresse (ReplyTo) zum Versand von Nachrichten dann, wenn als Antwortadresse ein gültiger Alias 827 des Benutzers eingetragen ist. Die globale Option ist per Voreinstellung aktiv.

Öffentliche Kontakte virtuell mit den Standard-Kontakten zusammenführen
Diese Option bewirkt, dass die öffentlichen Kontakte und die Standard-Kontakte der Benutzer auf ihren Geräten als zusammengeführt dargestellt werden. Die Datenbestände der Kontakte bleiben hierbei getrennt; es werden also keine Kontakte zwischen den Kontaktordnern der Benutzer kopiert. Diese Option kann insbesondere für solche Clients hilfreich sein, die das Durchsuchen der Globalen Adressliste (GAL) nicht unterstützen. Diese Option ist per Voreinstellung abgeschaltet.

Absender sperren, wenn Nachricht in Ordner Junk-Email verschoben wird
Ist diese Option aktiv, so wird die Absender-Adresse (Felder Sender und From) einer E-Mail-Adresse in den Kontaktordner für gesperrte Absender eingetragen, sobald ein Client die zugehörige E-Mail-Nachricht in den Ordner für Spam-Nachrichten verschiebt.

Antworten auf Besprechungsanfragen nach Zusage, Ablehnung usw. zwingend senden
Ist diese Option aktiv, so versendet der ActiveSync-Dienst eine Antwort an den Besprechungsorganisator immer dann, wenn ein Client auf eine Besprechungseinladung zusagt, sie ablehnt oder eine sonstige Aktion für die Einladung ausführt. Diese Option ist für solche Clients nützlich, die solche Antworten nicht selbst richtig senden.

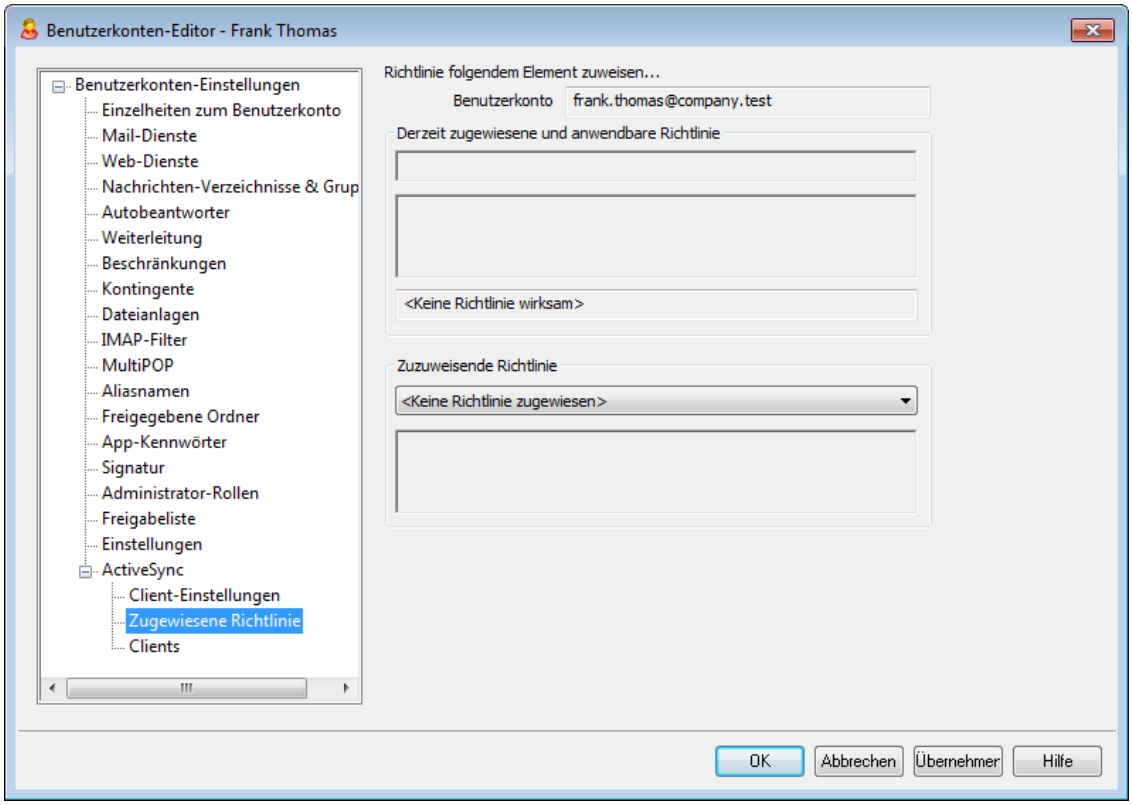
Vorschau auf tatsächlich wirksame Einstellungen

Dieses Steuerelement ist auf allen untergeordneten Konfigurationsdialogen für die Client-Einstellungen (Domänen 437, Benutzerkonten 454 und Clients 464) verfügbar. Per Voreinstellung werden die Optionen auf diesen Konfigurationsdialogen nicht von den übergeordneten Konfigurationsdialogen geerbt. Sie können sich daher mithilfe dieses Steuerelements die Einstellungen anzeigen lassen, die auf den jeweils gerade dargestellten Konfigurationsdialog wirken.

Siehe:

ActiveSync » Domänen 437
Benutzerkonten-Editor » ActiveSync » Clients 772

5.1.1.19.2 Zugewiesene Richtlinie



Mithilfe dieses Konfigurationsdialogs können Sie die ActiveSync-Standardrichtlinie 222 bestimmen, die dem gerade bearbeiteten Benutzerkonto zugewiesen wird. Stellt ein ActiveSync-Client eine Verbindung mit diesem Benutzerkonto her, dann wird dem Client diese Standard-Richtlinie zugewiesen.Per Voreinstellung wird die Richtlinie übernommen, die im als Richtlinie der Domäne 231 bestimmt ist. Sie können hier

jedoch eine abweichende Richtlinie für da sgerade bearbeitete Benutzerkonto bestimmen. Sie können mithilfe der Option *Einstellungen* im Abschnitt Clients 772 auch die für das Benutzerkonto bestimmte Richtlinie für einzelne Clients übergehen und ändern.

Zuweisen einer ActiveSync-Richtlinie

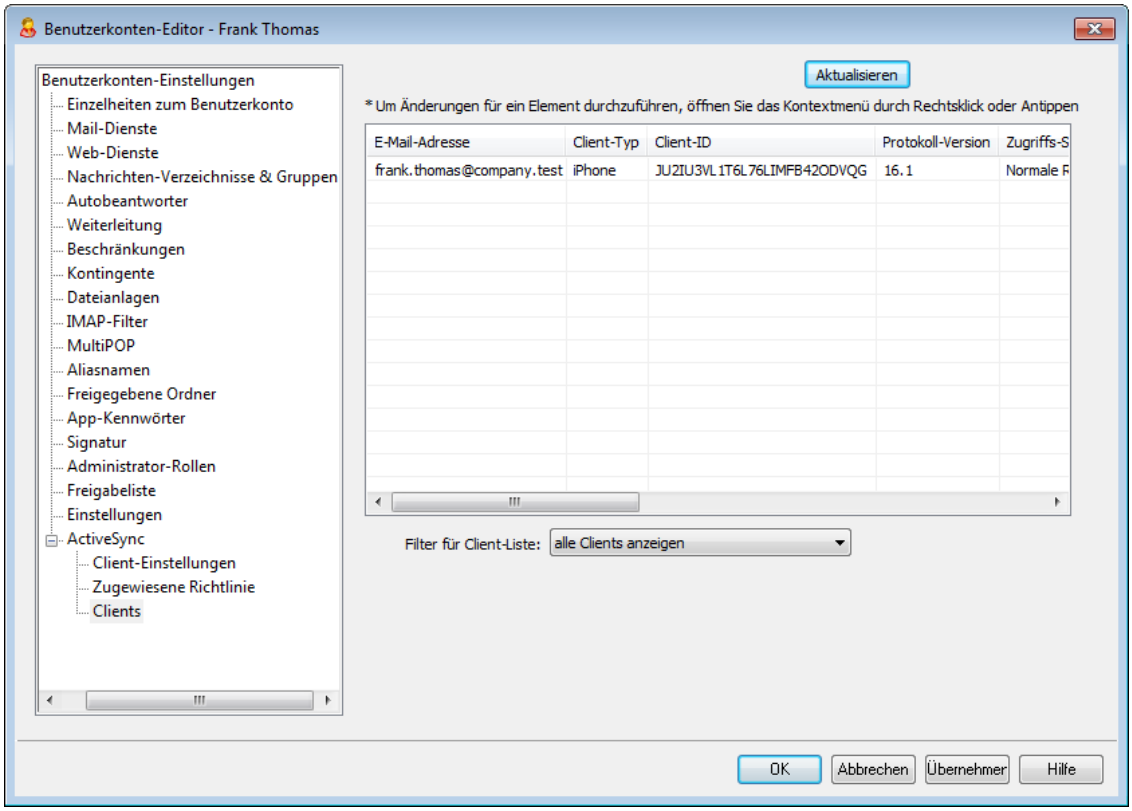
Um dem gerade bearbeiteten Benutzerkonto eine ActiveSync-Richtlinie zuzuweisen, wählen Sie aus dem Dropdown-Menü im Abschnitt **Zuzuweisende Richtlinie** die gewünschte Richtlinie aus, und klicken Sie danach auf **OK** oder **Übernehmen**.

Bitte beachten Sie, dass nicht alle ActiveSync-Endgeräte alle Richtlinien erkennen. Auch können in der Art der Umsetzung Unterschiede auftreten. Manche Geräte ignorieren bestimmte Elemente und Einstellungen der Richtlinien insgesamt; andere erfordern einen Neustart des Geräts, damit Änderungen wirksam werden. Eine Richtlinie kann jedenfalls frühestens dann wirksam werden, wenn das betroffene Gerät selbst eine Verbindung zum ActiveSync-Server herstellt. Eine "Push-Übermittlung" der Richtlinien an die Geräte, ohne dass diese eine Verbindung zum Server herstellen, ist nicht möglich.

Siehe auch:

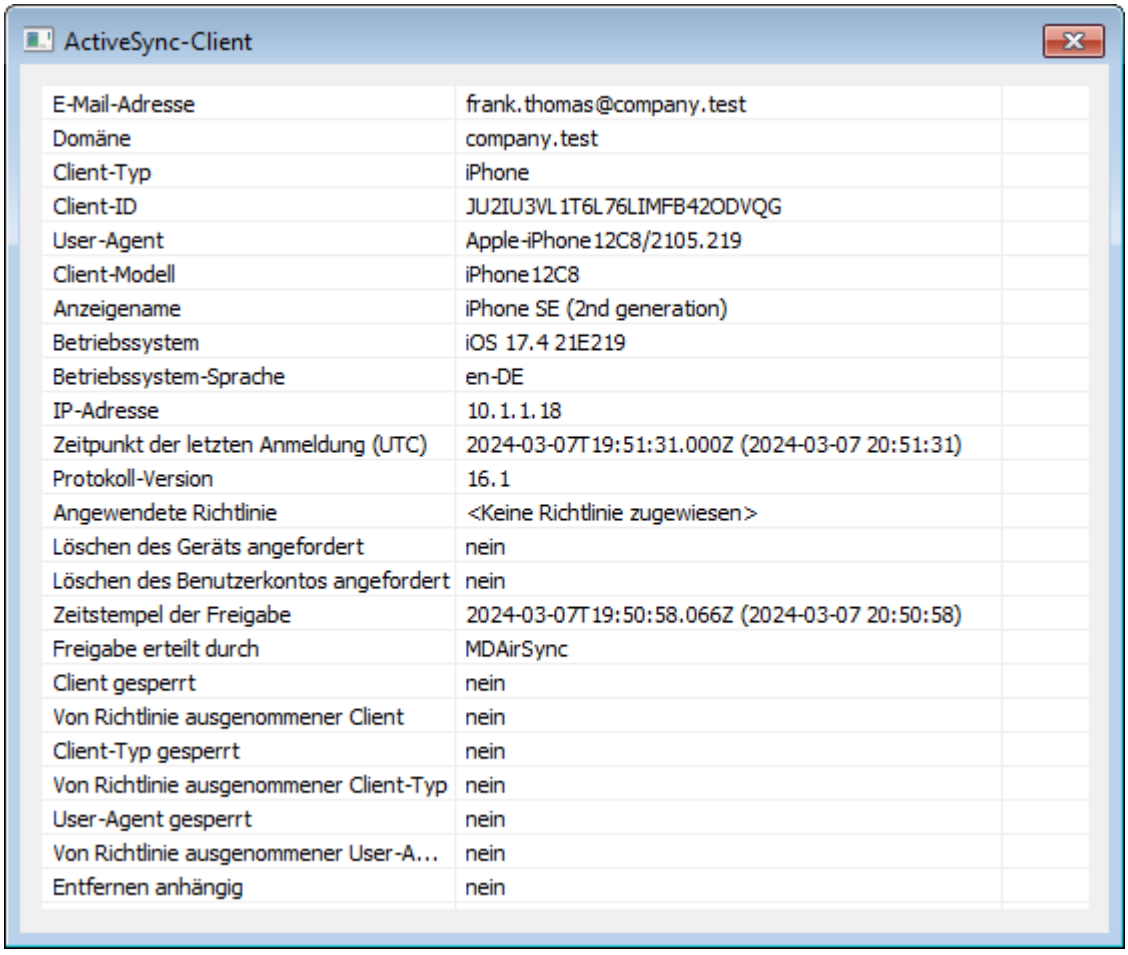
ActiveSync » Richtlinien-Manager 445
ActiveSync » Domänen 437
Benutzerkonten-Editor » ActiveSync - Clients 772

5.1.1.19.3 Clients



In diesem Konfigurationsdialog erscheinen Informationen über alle ActiveSync-Clients, die mit dem gerade bearbeiteten Benutzerkonto verknüpft sind. Von hier aus können Sie jedem Client ActiveSync-Richtlinien 770 zuweisen, verschiedene Client-Einstellungen konfigurieren, Clients entfernen, Clients fernlöschen und die Client-Statistiken zurücksetzen, die MDaemon führt.

Details zu ActiveSync-Clients



Um Detailinformationen über Endgeräte einzusehen, wählen Sie den Eintrag für das Endgerät aus, und klicken Sie dann auf **Details**, oder klicken Sie doppelt auf den Eintrag des Endgeräts. In dem Konfigurationsdialog Details können Sie Informationen über das Gerät einsehen, dem Gerät Richtlinien zuweisen, seine Client-Einstellungen bearbeiten und das Gerät in den Sperrlisten und Freigabelisten[429] erfassen.

Geräte-Einstellungen

Um die Einstellungen für ein Gerät zu bearbeiten, wählen Sie das Gerät aus, und klicken Sie auf **Einstellungen**. Per Voreinstellung werden diese Einstellungen aus den Client-Einstellungen des zugehörigen Benutzerkontos[454] geerbt. Nähere Informationen finden Sie weiter unten unter Verwalten der Client-Einstellungen eines Geräts.

Zuweisen einer ActiveSync-Richtlinie

Um einem Gerät eine Richtlinie[445] zuzuweisen, gehen Sie folgendermaßen vor:

1. Führen Sie auf dem Eintrag des gewünschten Geräts in der Übersicht einen Rechtsklick aus.
2. Klicken Sie auf **Richtlinie anwenden**. Hierdurch wird der Konfigurationsdialog Richtlinie zuweisen aufgerufen.
1. Wählen Sie aus dem Auswahlmenü der **zuzuweisenden Richtlinien** die gewünschte Richtlinie aus.

3. Klicken Sie auf **OK**.

Statistik

Um Statistikdaten für ein Gerät einzusehen, führen Sie einen Rechtsklick auf dem Eintrag des gewünschten Geräts aus, und klicken Sie danach auf **Statistiken anzeigen**. Es öffnet sich die Übersicht Client-Statistik, auf der verschiedene Daten zur Nutzungsstatistik des Geräts einsehbar sind.

Statistik zurücksetzen

Um die Statistikdaten für ein Gerät zurückzusetzen, führen Sie auf dem Eintrag des gewünschten Geräts einen Rechtsklick aus, und klicken Sie danach auf **Statistiken zurücksetzen.** Bestätigen Sie die anschließenden Sicherheitsabfrage durch Anklicken von **OK**.

Entfernen eines ActiveSync-Clients

Um einen ActiveSync-Clients zu entfernen, führen Sie einen Rechtsklick auf dem Eintrag des gewünschten Clients aus, und klicken Sie danach auf **Löschen**. Beantworten Sie die anschließende Sicherheitsabfrage mit **Ja**. Hierdurch werden der Client aus der Liste entfernt und alle Informationen zur Synchronisierung aus MDaemon gelöscht. Führt der entfernte Client später noch einmal eine Synchronisierung über ActiveSync auf dem Server durch, dann behandelt MDaemon den Client so, wie wenn er auf dem Server noch nie verwendet worden wäre. Alle Gerätedaten müssen dann mit MDaemon neu synchronisiert werden.

Vollständiges Löschen eines ActiveSync-Clients

Ist dem ausgewählten ActiveSync-Client eine Richtlinie 445 zugewiesen, und hat der Client die Richtlinie übernommen und entsprechend geantwortet, dann kann dieser Client ferngesteuert vollständig gelöscht werden. Um den Client vollständig zu löschen, führen Sie auf dem Client einen Rechtsklick aus (bei Nutzung der MDaemon-Remoteverwaltung wählen Sie den Client aus), und klicken Sie danach auf **Gerät löschen**. Sobald der Client das nächste Mal eine Verbindung zu MDaemon herstellt, übermittelt MDaemon den Löschbefehl an den Client und fordert ihn auf, sich in den Auslieferungszustand zurückzusetzen. Je nach Client kann dies zur Löschung aller Inhalte, auch etwa installierter Apps, führen. Solange der ActiveSync-Eintrag für den Client besteht, übermittelt MDaemon den Löschbefehl auch bei jedem späteren Verbindungsaufbau erneut. Falls Sie den Client löschen wollen, tragen Sie ihn zunächst in die Sperrliste 429 ein, damit er künftig keine Verbindungen mehr zu MDaemon herstellen kann. Wird ein gelöschtes Endgerät beispielsweise wiedergefunden, und soll er wieder Verbindungen zum Server herstellen können, dann wählen Sie das Gerät aus, und klicken Sie auf **Löschvorgänge abbrechen**. Entfernen Sie das Gerät außerdem aus der Sperrliste.

Daten aus dem Benutzerkonto eines ActiveSync-Clients löschen

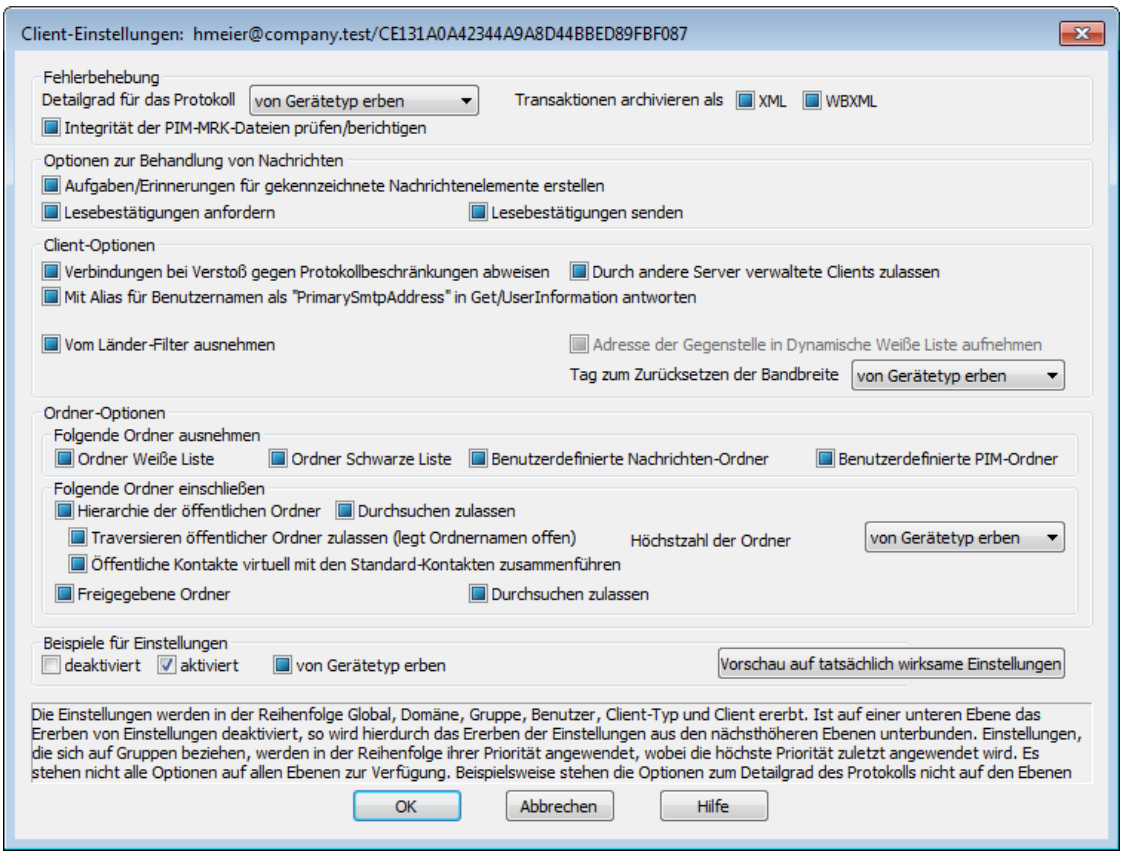
Um die Nachrichten und PIM-Daten von einem Client oder Endgerät zu löschen, führen Sie auf dem Eintrag des gewünschten Geräts einen Rechtsklick aus, und klicken Sie danach auf **Nachrichten des Benutzerkontos und PIM-Elemente vom Client löschen**. Dieser Löschvorgang ist dem vollständigen Löschen eines ActiveSync-Clients ähnlich, das weiter oben beschrieben ist. Es werden aber nicht alle Daten des Clients gelöscht, sondern es werden nur die Daten des Benutzerkontos entfernt, wie etwa E-Mail-Nachrichten, Kalendereinträge, Kontakte und ähnliche Daten. Alle anderen Daten, wie Apps, Fotos und Musik, bleiben unverändert.

Client freigeben

Ist im Konfigurationsdialog ActiveSync - Client-Einstellungen 422 die Option "*Neue Clients müssen durch Administrator freigegeben werden*" aktiv, so können Sie mit diesem Steuerelement Clients freigeben, Wählen Sie dazu den gewünschten Client aus, und klicken Sie danach auf **Client zur Synchronisierung berechtigen**. Nach der Freigabe kann sich der Client mit dem Server synchronisieren.

Verwalten der Client-Einstellungen eines Geräts

Die Client-Einstellungen für einzelne Geräte gestatten Ihnen die Verwaltung der Client-Einstellungen für bestimmte einzelne Endgeräte.



Per Voreinstellung werden alle Optionen in diesem Konfigurationsdialog vom übergeordneten Knoten geerbt, oder es werden die Standardeinstellungen verwendet. Im Falle der Client-Einstellungen ist der übergeordnete Knoten das Benutzerkonto, dem das Gerät zugeordnet ist. Seine Client-Einstellungen werden im Konfigurationsdialog Client-Einstellungen 454 des Benutzerkontos konfiguriert, dem das Gerät zugeordnet ist. Änderungen, die Sie in diesem Konfigurationsdialog vornehmen, übergehen die auf Client-Ebene festgelegten Einstellungen für dieses Gerät.

Allgemeines

Fehlerbehebung

Detailgrad für das Protokoll

ActiveSync für MDaemon unterstützt sechs Detailgrade für die Protokollierung. In der nachfolgenden Übersicht erscheinen sie nach Umfang der protokollierten

Daten absteigend:

Debug Dies ist der höchste Detailgrad. Es werden alle verfügbaren Einträge protokolliert, und er wird üblicherweise nur zur Fehlersuche eingesetzt.

Info Dies ist ein Detailgrad mit üblichem Umfang. Es werden allgemeine Vorgänge ohne Details protokolliert. Dieser Detailgrad ist per Voreinstellung aktiv.

Warnung Es werden Warnungen, Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Fehler Es werden Fehler, schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

kritisch Es werden schwer wiegende Fehler und das Starten und Beenden des Dienstes protokolliert.

Keine Es werden nur Starten und Beenden des Dienstes protokolliert.

Einstellung erben Per Voreinstellung wird die Einstellung für den Detailgrad aus der Hierarchie der Client-Einstellungen vom jeweils übergeordneten Knoten ererbt. Clients übernehmen dabei die Einstellung aus dem jeweiligen Client-Typ, Client-Typen übernehmen die Einstellung von den Benutzerkonten, Benutzerkonten übernehmen die Einstellung von den Gruppen, und so weiter. Die globale Einstellung für alle Clients wird durch die Einstellung für den Detailgrad im Konfigurationsdialog Diagnose 432 bestimmt.

Transaktionen archivieren als [XML | WBXML]
Mithilfe der Optionen *XML...* und *WBXML...* können Sie die zugehörigen Daten speichern; diese Daten können die Fehlersuche erleichtern. Die systemweit wirksamen Optionen sind per Voreinstellung abgeschaltet.

Integrität der PIM-MRK-Dateien prüfen/berichtigen
Diese Option führt für die PIM-Daten der betroffenen Clients Prüf- und Korrekturvorgänge durch. Sie sollen bekannte Probleme erkennen, die eine ordnungsgemäße Synchronisierung verhindern können. Zu diesen Problemen zählen insbesondere doppelte iCal-UIDs und leere Datenfelder, die eigentlich verpflichtend Daten enthalten müssen. Die systemweit wirksame Option ist per Voreinstellung abgeschaltet.

Client-Optionen

Verbindungen bei Verstoß gegen Protokollbeschränkungen abweisen
Diese Option bewirkt, dass Verbindungen von Clients abgewiesen werden, falls sie versuchen eine nicht für die Clients *Zugelassene Protokollversion* zu verwenden. Per Voreinstellung ist diese Option abgeschaltet; dies bedeutet, dass die Protokollbeschränkung keine Verbindungen solcher Clients verhindern, die andere als die zugelassenen Protokollversionen verwenden. Solange die Option abgeschaltet ist, weist MDaemon die Clients zwar an, nur die zugelassenen Protokollversionen zu verwenden, lässt aber bei Nutzung anderer Protokollversionen die Verbindung trotzdem zu. Nähere Informationen finden Sie

unter Protokollbeschränkungen 434.

Mit Alias für Benutzernamen als "PrimarySmtpAddress" in Get/UserInformation antworten
Diese Option gestattet es dem Dienst, als Antwort auf eine Anforderung Settings/Get/UserInformation eine etwa vorhandene Alias-Adresse oder eine sekundäre Adresse des betroffenen Benutzerkontos als primäre Adresse zu übermitteln. Hierdurch wird ein Problem umgangen, das mit einer iOS-Aktualisierung nach Version 9.x verursacht wird, und das verhinderte, dass Clients unter einer etwa vorhandenen Alias-Adresse Nachrichten versenden konnten. Die Nutzung dieser Option bewirkt eine nicht standardkonforme Antwort auf die Anforderung Settings/GetUserInformation.

Neue Clients müssen durch Administrator freigegeben werden
Diese Option bewirkt, dass neue Clients sich erst dann mit Benutzerkonten synchronisieren können, wenn sie zunächst durch einen Administrator freigegeben wurden. In der Liste der Clients 464 sind alle Clients aufgeführt, die noch die Freigabe erwarten, und die Administratoren können sie über diese Liste freigeben. Diese Option ist per Voreinstellung abgeschaltet.

Höchstzahl der Clients je Benutzer
Mithilfe dieser Option können Sie die Anzahl der ActiveSync-Clients und -Endgeräte begrenzen, die mit jedem MDaemon-Benutzerkonto verknüpft sein können. Der hier angegebene Wert ist die Höchstzahl zulässiger Clients. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt. Diese Option steht nur in den Client-Einstellungen auf globaler, Domänen- und Benutzerebene zur Verfügung, nicht jedoch in den Client-Einstellungen für die einzelnen Clients.

Tag zum Zurücksetzen der Bandbreite
Mithilfe dieser Option können Sie Tag bestimmen, an dem in jedem Monat die Bandbreiten-Nutzungsstatistik für die ActiveSync-Endgeräte zurückgesetzt wird. Dieser Vorgang wird während der normalen Bereinigungsvorgänge um Mitternacht aufgeführt und, wie auch andere Bereinigungsvorgänge, in das Protokoll System eingetragen. Der globale Wert lautet per Voreinstellung 0 (nicht zurücksetzen), sodass per Voreinstellung die Nutzungsstatistik nicht zurückgesetzt wird. Für untergeordnete Knoten können Sie abweichende Einstellungen treffen, etwa, um die Einstellung an den Tag anzugleichen, an dem für das betroffene Endgeräte ein neuer Abrechnungszeitraum des Netzbetreibers beginnt.

Sicherheit

Vom Länder-Filter ausnehmen
Wenn Sie diese Option in den Einstellungen eines ActiveSync-Clients aktivieren, kann das Endgerät den Länder-Filter 574 umgehen. Hierdurch kann ein berechtigter Benutzer auf sein Benutzerkonto über ActiveSync beispielsweise auch dann zugreifen, wenn er sich in einem Land befindet, für das Versuche zur Echtheitsbestätigung ansonsten durch den Länder-Filter unterbunden werden. Ein Endgerät kann nur dann vom Länder-Filter ausgenommen sein, wenn es innerhalb des durch die Option Inaktive Clients entfernen nach [x] Tagen 418 im Abschnitt Anpassung bestimmten Zeitraums eine echtheitsbestätigte Verbindung über ActiveSync erfolgreich hergestellt hat.

Adresse der Gegenstelle in Dynamische Freigabeliste aufnehmen
Wenn Sie ein Endgerät vom Länder-Filter ausnehmen, können Sie durch

Aktivieren dieser Option die IP-Adresse, von der aus das Endgerät die Verbindung herstellt, in die Freigabeliste eintragen lassen. Hierdurch können beispielsweise andere Clients, die von der selben IP-Adresse aus eine Verbindung herstellen, ebenfalls zugelassen werden.

Durch andere Server provisionierte/verwaltete Clients zulassen
Per Voreinstellung dürfen Clients auch dann Verbindungen zu MDaemon aufbauen, wenn sie auf die Übermittlung der Provisionierungs- und Richtliniendaten durch den ActiveSync-Server hin melden, dass sie auch durch einen oder mehrere andere ActiveSync-Server verwaltet werden. Bei einer solchen Mehrfachverwaltung kann es nicht sichergestellt werden, dass alle auf Ihrem System bestehenden Richtlinien durch den Client auch umgesetzt werden; dies gilt insbesondere dann, wenn sie Richtlinien des anderen ActiveSync-Servers widersprechen. In vielen Fällen setzen die Clients die am stärksten einschränkende Richtlinie um, falls mehrere einander widersprechende Richtlinien vorhanden sind. Um Verbindungen von Clients zu unterbinden, die durch andere ActiveSync-Server verwaltet werden, deaktivieren Sie diese Option.

Löschen der Clients (Zurücksetzen in den Auslieferungszustand) nicht zulassen
Wenn diese Option aktiv ist, dann können ActiveSync-Clients nicht in den **Auslieferungszustand zurückgesetzt** und damit vollständig gelöscht werden. Wenn Sie Clients ferngesteuert in den Auslieferungszustand zurücksetzen wollen, müssen Sie diese Option deaktivieren. Diese Option ist per Voreinstellung deaktiviert. Nähere Informationen finden Sie auf der Seite Clients im Abschnitt **Vollständiges Löschen eines ActiveSync-Clients** 464.

Optionen zur Ordner-Synchronisierung

Optionen zur Ordner-Synchronisierung

Folgende Ordner ausnehmen

Freigegebene Absender/Gesperrte Absender
Per Voreinstellung werden die Kontaktordner mit Freigabelisten und Sperrlisten der Benutzer nicht mit den Geräten synchronisiert. Diese Ordner dienen üblicherweise nur in MDaemon zum Erkennen und Filtern von Spam. Ihre Inhalte brauchen daher nicht auf den Geräten als Kontakte angezeigt zu werden.

Benutzerdefinierte Nachrichten-Ordner
Per Voreinstellung können alle Standard- und benutzerdefinierten Nachrichten-Ordner mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-Nachrichtenordner synchronisiert werden können. Die Standard-Nachrichtenordner sind insbesondere Posteingang, Gesendete Objekte, Gelöschte Objekte und Entwürfe. Ordner, die die Benutzer selbst anlegen, werden dann nicht mehr synchronisiert. Diese Option ist per Voreinstellung abgeschaltet.

Benutzerdefinierte PIM-Ordner
Per Voreinstellung können alle PIM-Ordner (insbesondere Kontakte, Kalender, Notizen und Aufgaben) mit den Geräten synchronisiert werden. Diese Option bewirkt, dass nur die Standard-PIM-Ordner synchronisiert werden können. Ist diese Option aktiv, so wird beispielsweise für jeden Benutzer nur der Standard-Kalender synchronisiert, auch wenn er über mehrere Kalender-

Ordner verfügt. Diese Option ist per Voreinstellung abgeschaltet.

Folgende Ordner einschließen

Hierarchie der öffentlichen Ordner
Diese Option bewirkt, dass die öffentlichen Ordner[309], auf die die Benutzer Zugriff haben, in den Ordnerlisten der Benutzer auf ihren ActiveSync-Geräten erscheinen. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der öffentlichen Ordner[309], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Traversieren öffentlicher Ordner zulassen (legt Ordnernamen offen)
Benutzerkonten, die auf Unterordner in öffentlichen Ordnern zugreifen oder diese synchronisieren wollen, müssen per Voreinstellung sowohl für den betroffenen Unterordner als auch für alle ihm übergeordneten öffentlichen Ordner[309] über die Berechtigung Ordner anzeigen[311] verfügen. Fehlt einem Benutzerkonto diese Berechtigung für einen übergeordneten öffentlichen Ordner, so kann er auch den gewünschten Unterordner nicht synchronisieren und nicht auf ihn zugreifen, und zwar auch dann nicht, wenn das Benutzerkonto für diesen Unterordner selbst die erforderliche Berechtigung hat. Mithilfe dieser Option können Sie den Clients Zugriff auf und Synchronisierung von Unterordnern ermöglichen, ohne dass die Clients Berechtigungen für die übergeordneten öffentlichen Ordner haben. **Beachte:** Ist diese Option aktiv, so erlangt der Client zwangsläufig Kenntnis von den Namen der übergeordneten Ordner, auch wenn er für ihre Inhalte keine Zugriffsrechte hat. Hieraus kann sich ein Sicherheitsrisiko ergeben. Die Option ist per Voreinstellung abgeschaltet.

Höchstzahl zulässiger öffentlicher Ordner
Diese Option begrenzt die Zahl der öffentlichen Ordner, die auf den betroffenen Geräten dargestellt werden können. Ist eine solche Höchstzahl angegeben, dann übermittelt der Server so lange Einträge in der Ordnerliste, bis die Höchstzahl erreicht ist. Danach übermittelt der Server keine Ordner mehr an die Geräte. Die Reihenfolge, in der die Ordner dabei verarbeitet werden, kann weder festgelegt noch vorher bestimmt werden. Die systemweit wirksame Option ist per Voreinstellung auf unbegrenzt eingestellt.

Freigegebene Ordner
Diese Option nimmt auch die gemeinsam genutzten Ordner[122], auf die die Benutzer Zugriff haben, in die Ordnerlisten auf ihren ActiveSync-Geräten auf. Diese Option ist per Voreinstellung aktiv.

Durchsuchen zulassen
Diese Option ermöglicht den Clients das Durchsuchen der freigegebenen Ordner[742], auf die sie Zugriff haben. Diese Option ist per Voreinstellung aktiv.

Behandlung von Inhalten

Optionen zur Behandlung von Inhalten

Aufgaben/Erinnerungen für durch Clients gekennzeichnete Nachrichtenelemente erstellen
Diese Option ermöglicht es MDaemon, die Benutzer an gekennzeichnete Elemente zu erinnern. Hierzu wird für jede gekennzeichnete E-Mail-Nachricht eine Aufgabe erstellt, wenn der Client dies anfordert. Die globale Option für dieses Leistungsmerkmal ist per Voreinstellung aktiv.

Aktualisierung nach jeder Änderung der Besprechung senden
Manche Clients versenden aktualisierte Besprechungseinladungen nicht richtig, nachdem eine Besprechung geändert wurde. Diese Option bewirkt, dass der ActiveSync-Dienst immer dann aktualisierte Besprechungseinladungen sendet, wenn der Besprechungsorganisator eine Besprechung aktualisiert hat. Diese Option sollte nur für Clients 464 und Client-Typen 481 aktiviert werden, die die aktualisierten Besprechungseinladungen nicht richtig versenden, da sonst aktualisierte Besprechungseinladungen doppelt versandt werden. Aus diesem Grund ist diese Einstellung nur auf den Seiten Clients und Client-Typen verfügbar.

Lesebestätigung für alle versandten Nachrichten anfordern
Diese Option bewirkt, dass der Server für alle durch einen Client versandten E-Mail-Nachrichten Lesebestätigungen anfordert. Diese Option ist per Voreinstellung abgeschaltet.

Vom Absender angeforderte Lesebestätigung senden, sobald Nachricht als gelesen gekennzeichnet ist
Diese Option bewirkt, dass der Server Anforderungen von Lesebestätigungen beachtet und die Lesebestätigungen dann versendet, wenn eine Nachricht durch den Client als gelesen gekennzeichnet wird. Diese Option ist per Voreinstellung abgeschaltet.

Unter dem in der Antwortadresse (ReplyTo) angegebenen Alias senden
Manche Clients gestatten den Absendern nicht den Versand von E-Mail-Nachrichten unter einem Alias. Dieses Leistungsmerkmal wurde im der Version 16.x des Protokolls Exchange ActiveSync (EAS) 434 erstmals unterstützt, aber manche Clients unterstützen die Version 16.x nicht. So nutzt beispielsweise Microsoft Outlook für Windows nur EAS 14.0 und gestattet zwar den Benutzern die Angabe einer anderen Adresse, unter der eine Nachricht versandt werden soll, aber die dann erstellte Nachricht gibt die Auswahl des Benutzers nicht richtig wieder. Diese Option gestattet die Nutzung des Feldes für die Antwortadresse (ReplyTo) zum Versand von Nachrichten dann, wenn als Antwortadresse ein gültiger Alias 827 des Benutzers eingetragen ist. Die globale Option ist per Voreinstellung aktiv.

Öffentliche Kontakte virtuell mit den Standard-Kontakten zusammenführen
Diese Option bewirkt, dass die öffentlichen Kontakte und die Standard-Kontakte der Benutzer auf ihren Geräten als zusammengeführt dargestellt werden. Die Datenbestände der Kontakte bleiben hierbei getrennt; es werden also keine Kontakte zwischen den Kontaktordnern der Benutzer kopiert. Diese Option kann insbesondere für solche Clients hilfreich sein, die das Durchsuchen der Globalen Adressliste (GAL) nicht unterstützen. Diese Option ist per Voreinstellung abgeschaltet.

Absender sperren, wenn Nachricht in Ordner Junk-Email verschoben wird
Ist diese Option aktiv, so wird die Absender-Adresse (Felder Sender und From) einer E-Mail-Adresse in den Kontaktordner für gesperrte Absender eingetragen, sobald ein Client die zugehörige E-Mail-Nachricht in den Ordner für Spam-Nachrichten verschiebt.

Antworten auf Besprechungsanfragen nach Zusage, Ablehnung usw. zwingend senden
Ist diese Option aktiv, so versendet der ActiveSync-Dienst eine Antwort an den Besprechungsorganisator immer dann, wenn ein Client auf eine Besprechungseinladung zusagt, sie ablehnt oder eine sonstige Aktion für die Einladung ausführt. Diese Option ist für solche Clients nützlich, die solche Antworten nicht selbst richtig senden.

Vorschau auf tatsächlich wirksame Einstellungen

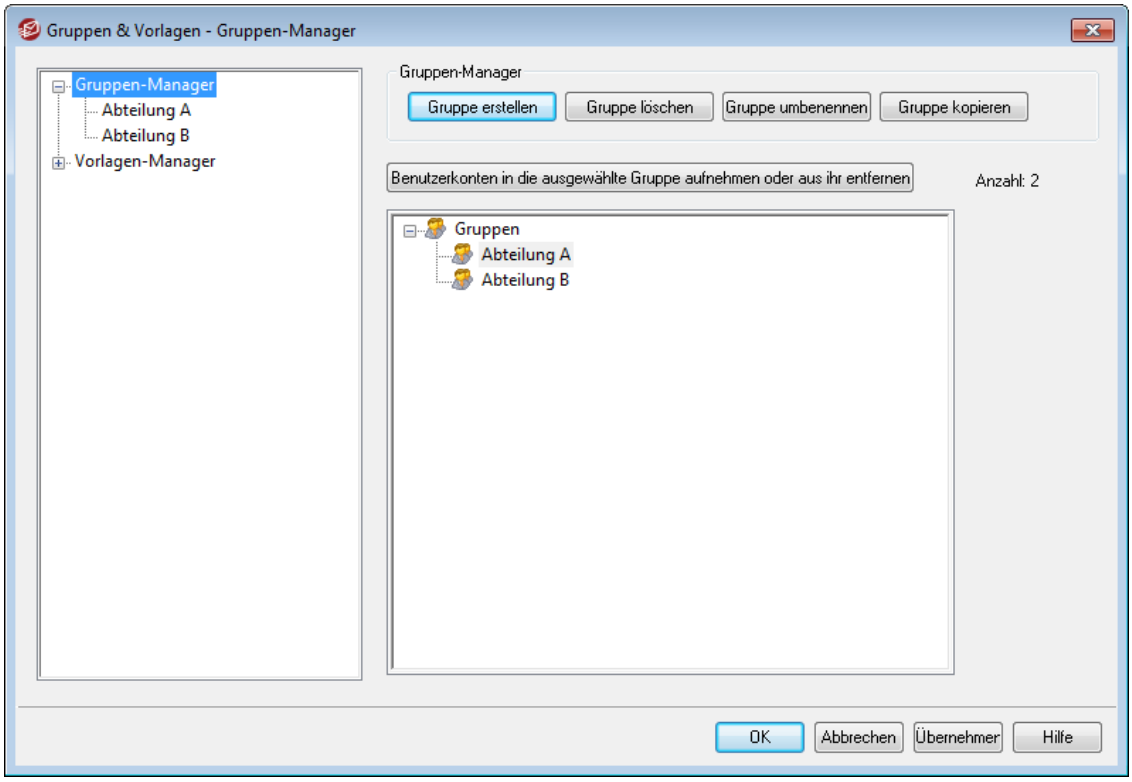
Dieses Steuerelement ist auf allen untergeordneten Konfigurationsdialogen für die Client-Einstellungen (Domänen 437, Benutzerkonten 454 und Clients 464) verfügbar. Per Voreinstellung werden die Optionen auf diesen Konfigurationsdialogen nicht von den übergeordneten Konfigurationsdialogen geerbt. Sie können sich daher mithilfe dieses Steuerelements die Einstellungen anzeigen lassen, die auf den jeweils gerade dargestellten Konfigurationsdialog wirken.

Siehe auch:

ActiveSync » Client-Einstellungen 422
ActiveSync » Domänen 437
ActiveSync » Benutzerkonten 454

5.2 Gruppen & Vorlagen

5.2.1 Gruppen-Manager



Der Gruppen-Manager (erreichbar über Benutzerkonten » Gruppen & Vorlagen... » Gruppen-Manager) ermöglicht es Ihnen, Benutzergruppen zu erstellen und zu bestimmen, welche Benutzerkonten welchen Gruppen angehören. Gruppen erfüllen eine Reihe verschiedener Funktionen. Mithilfe des Konfigurationsdialogs Gruppen-Eigenschaften 784 können Sie beispielsweise einer Gruppe eine Vorlage 787 für Benutzerkonten zuordnen und hierdurch für die Gruppenmitglieder zahlreiche Benutzerkonten-Einstellungen steuern. Weiter können Sie bestimmen, ob die Mitglieder einer Gruppe Zugriff auf den MDaemon Instant Messenger 318 und die Instant-Messaging-Funktionen erhalten. Auch der Inhaltsfilter unterstützt Gruppen; Sie können Bedingungen für Regeln 651 davon abhängig machen, ob Absender oder Empfänger einer Nachricht Mitglieder einer bestimmten Gruppe sind. Schließlich können Sie Zugriffskontrolllisten (ACL) 311 für freigegebene Ordner 119 mit bestimmten Gruppen verknüpfen; alle Mitglieder der betroffenen Gruppe erhalten dann gleichermaßen die Zugriffsrechte aus der Zugriffskontrollliste.

Um Benutzerkonten einer Gruppe hinzuzufügen, können Sie die betroffenen Gruppen aus der Liste in diesem Konfigurationsdialog auswählen und dann das Steuerelement "*Benutzerkonten in die ausgewählte Gruppe aufnehmen oder aus ihr entfernen*" anklicken. Sie können Benutzer auch mithilfe der Optionen im Abschnitt Nachrichten-Verzeichnisse & Gruppen 717 im Benutzerkonten-Editor den Gruppen hinzufügen.

Gruppen-Manager

Gruppe erstellen
Um eine neue Gruppe von Benutzerkonten zu erstellen, klicken Sie auf *Gruppe erstellen*, geben Sie einen Namen und eine Beschreibung für die Gruppe an, und klicken Sie danach auf *OK*. Die neue Gruppe erscheint dann sowohl in der

Übersicht über die Gruppen im unteren Teil dieses Konfigurationsdialogs wie auch in der Baumansicht im linken Bereich.

Gruppe löschen
Um eine Gruppe zu löschen, wählen Sie die Gruppe in der Übersicht über die Gruppen im unteren Teil dieses Konfigurationsdialogs aus, und klicken Sie danach auf *Gruppe löschen*. Bestätigen Sie anschließend die Sicherheitsabfrage mit *Ja*.

Gruppe umbenennen
Um eine Gruppe umzubenennen, wählen Sie die Gruppe in der Übersicht über die Gruppen im unteren Teil dieses Konfigurationsdialogs aus, und klicken Sie danach auf *Gruppe umbenennen*. Geben Sie den neuen Namen für die Gruppe ein, und klicken Sie danach auf *OK*.

Gruppe kopieren
Um eine neue Gruppe anzulegen und dabei die Einstellungen aus einer anderen Gruppe zu übernehmen, wählen Sie die gewünschte Ursprungsgruppe in der Liste aus, und klicken Sie auf *Gruppe kopieren*. Geben Sie dann den Namen und die Beschreibung für die neue Gruppe an.

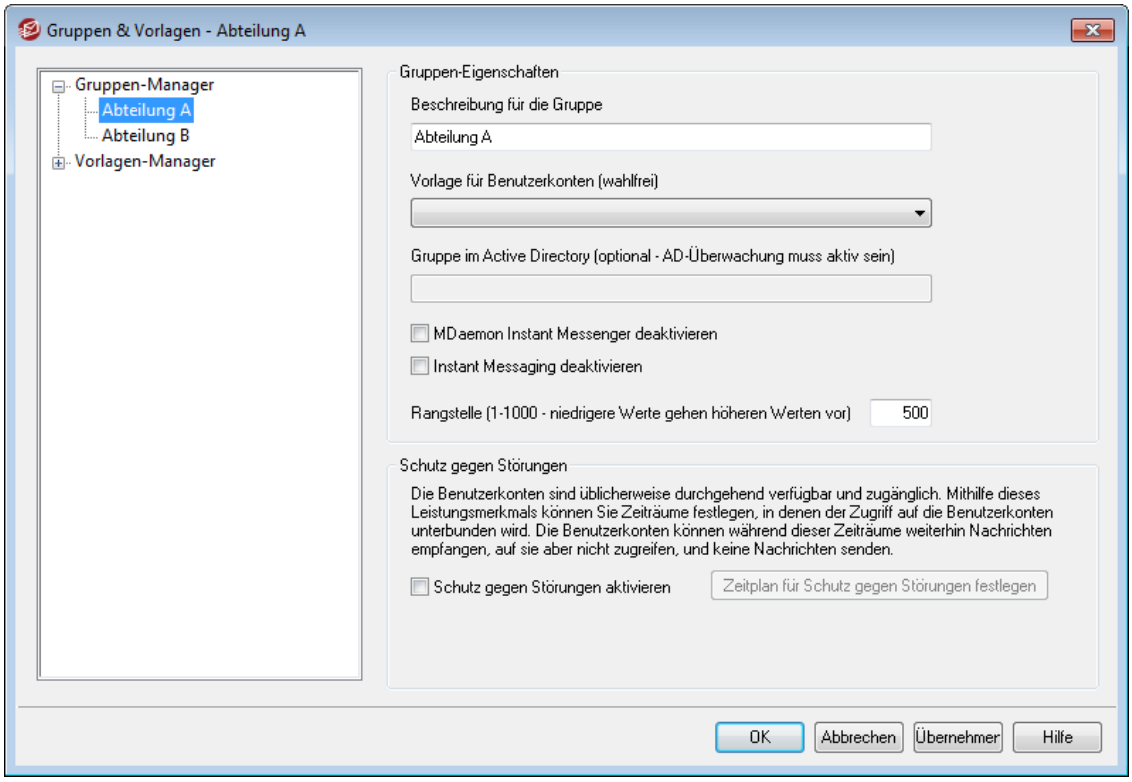
Benutzerkonto in die ausgewählte Gruppe aufnehmen oder aus ihr entfernen

Um die Mitgliedschaften für eine Gruppe zu verwalten, wählen Sie die Gruppe in der Übersicht über die Gruppen im unteren Teil dieses Konfigurationsdialogs aus, und klicken Sie danach auf dieses Steuerelement. Bei Benutzerkonten, die Sie in die Gruppe aufnehmen wollen, aktivieren Sie das Kontrollkästchen neben dem Benutzerkonto. Bei Benutzerkonten, die Sie aus der Gruppe entfernen wollen, deaktivieren Sie das Kontrollkästchen neben dem Benutzerkonto. Klicken Sie danach auf *OK*.

Siehe auch:

Nachrichten-Verzeichnisse & Gruppen 717
Erstellen einer neuen Regel für den Inhaltsfilter 651
Freigegebene Ordner 119

5.2.1.1 Gruppen-Eigenschaften



Im Konfigurationsdialog Gruppen-Eigenschaften (erreichbar über Benutzerkonten » Gruppen & Vorlagen... » [Name der Gruppe]) können Sie die Einstellungen für alle Gruppen konfigurieren, die Sie mithilfe des Gruppen-Managers[782] erstellt haben. Um diesen Konfigurationsdialog aufzurufen, klicken Sie im Gruppen-Manager doppelt auf die Gruppe, die Sie bearbeiten wollen, oder klicken Sie in der Baumansicht im linken Bereich auf die Gruppe. In diesem Konfigurationsdialog können Sie eine Vorlage für Benutzerkonten[787] mit einer Gruppe verknüpfen und so zahlreiche Benutzerkonten-Einstellungen für die Gruppenmitglieder steuern. Sie können die Gruppe auch mit einer Gruppe im Active Directory verknüpfen, festlegen, ob die Gruppenmitglieder auf den MDaemon Instant Messenger (MDIM)[318] und die Instant-Messaging-Funktionen Zugriff erhalten, und eine Rangstelle für die Gruppe festlegen. Die Gruppenmitgliedschaften können Sie über den Gruppen-Manager und über den Abschnitt Nachrichten-Verzeichnisse & Gruppen[717] des Benutzerkonten-Editors bearbeiten.

Gruppen-Eigenschaften

Beschreibung für die Gruppe
Geben Sie hier eine Beschreibung für die Gruppe ein. Diese Beschreibung dient Ihren internen Zwecken. Diese Beschreibung wird üblicherweise bereits beim Erstellen der Gruppe angegeben; Sie können ihren Inhalt aber jederzeit von hier aus bearbeiten.

Vorlage für Benutzerkonten (wahlfrei)
Sie können mithilfe einer Vorlage für Benutzerkonten[787] bestimmte Einstellungen der Benutzerkonten für die Gruppenmitglieder steuern. Hierzu wählen Sie die gewünschte Vorlage aus diesem Auswahlmenü aus. Ist eine Vorlage für Benutzerkonten mit einer Gruppe verknüpft, so werden alle Gruppen von Benutzerkonten-Einstellungen, die Sie in den Vorlagen-Eigenschaften[789]

festgelegt haben, auf alle Benutzerkonten angewendet, die Mitglieder der Gruppe sind. Die Einstellungen aus der Vorlage treten dann an die Stelle der einzeln über den Benutzerkonten-Editor vorzunehmenden Einstellungen. Wird ein Benutzerkonto aus einer Gruppe entfernt, mit der eine Vorlage verknüpft war, und hatte diese Vorlage die Einstellungen des Benutzerkontos gesteuert, so werden die Einstellungen auf die Voreinstellungen zurückgesetzt, die in der Vorlage "Neue Benutzerkonten" 788 festgelegt sind.

Falls ein Benutzerkonto zu mehreren Gruppen gehört, und diese Gruppen mit mehreren Vorlagen verknüpft sind, so werden alle Einstellungen aus diesen Vorlagen angewendet, soweit die betreffenden Eigenschaften der Vorlagen 789 einander nicht widersprechen. Falls mehrere Vorlagen dieselben Einstellungen regeln, dann finden die Einstellungen aus der ersten aufgeführten Vorlage Anwendung.

Gruppe im Active Directory (optional - AD-Überwachung muss aktiv sein)
Mithilfe dieser Option können Sie eine Gruppe von MDaemon-Benutzerkonten mit einer bestimmten Gruppe im Active Directory verknüpfen. Die Mitglieder der Gruppe im Active Directory werden dann der Gruppe der MDaemon-Benutzerkonten automatisch hinzugefügt. Um diese Funktion zu nutzen, müssen die Leistungsmerkmale zur Überwachung des Active Directory 821 aktiv sein.

Sie können jedes beliebige Attribut aus dem Active Directory als Kriterium und Merkmal für das Hinzufügen von Benutzerkonten zu der Gruppe verwenden; üblicherweise wird aber das Attribut "`memberOf`" verwendet. Sie können Änderungen an dem Attribut durch Bearbeiten der Datei `ActiveDS.dat` in einem Texteditor vornehmen. Die Option ist per Voreinstellung abgeschaltet. Um sie zu aktivieren, bearbeiten Sie die Datei `ActiveDS.dat`, und geben Sie an, welches Attribut Sie als Kennzeichen für die Gruppenmitgliedschaft nutzen wollen, oder aktivieren Sie die Zeile "`Groups=%memberOf%`" `ActiveDS.dat` durch Entfernen des Kommentarzeichens.

MDaemon Instant Messenger deaktivieren
Diese Option bewirkt, dass die Mitglieder der Gruppe den MDaemon Instant Messenger nicht nutzen können.

> **Instant Messaging deaktivieren**
> Diese Option bewirkt, dass alle Mitglieder der Gruppe zwar den MDaemon Instant Messenger, nicht jedoch seine Instant-Messaging-Funktionen nutzen können.

Rangstelle (1-1000 - niedrigere Werte gehen höheren Werten vor)
Mithilfe dieser Option können Sie der Gruppe eine Rangstelle (1-1000) zuweisen. Hierdurch wird es möglich, dass dieselben Benutzerkonten Mitglieder mehrerer Gruppen sind, ohne dass deswegen ein Konflikt zwischen den Einstellungen der verschiedenen Gruppen auftritt. Ist beispielsweise ein Benutzerkonto Mitglied mehrerer Gruppen, und sind mit allen diesen Gruppen Vorlagen für Benutzerkonten verknüpft, die alle dieselben Einstellungen steuern, so werden die Einstellungen der Gruppe mit der niedrigsten Rangstelle genutzt. So gehen etwa die Einstellungen einer Gruppe mit der Rangstelle "1" denen einer Gruppe mit der Rangstelle "10" vor. Besteht zwischen den Einstellungen der einzelnen Gruppen kein Konflikt, so werden alle Einstellungen kumulativ angewendet. Bestehen Konflikte zwischen Einstellungen von Gruppen gleicher Rangstufe, geht die Gruppe vor, die zuerst gefunden wurde. Wird ein Benutzerkonto aus einer Gruppe entfernt, und war diese Gruppe mit einer Vorlage für Benutzerkonten verknüpft, so werden die Einstellungen, die bislang durch die Vorlage gesteuert wurden, in

die Einstellungen der Vorlage mit der nächst höheren Rangstelle geändert. Steuern die Einstellungen der anderen Gruppen die weggefallenen Einstellungen nicht, so werden diese Einstellungen auf die Voreinstellungen zurückgesetzt, die in der Vorlage "Neue Benutzerkonten"[788] festgelegt sind.

Schutz gegen Störungen

Mithilfe des Leistungsmerkmals Schutz gegen Störungen können Sie Zeiträume festlegen, während derer Benutzerkonten keine Nachrichten versenden können, und während derer die Benutzer keinen Zugriff auf die Benutzerkonten haben. Zugriffsversuche über IMAP, POP, SMTP, ActiveSync und WorldClient während der festgelegten Zeiträume werden mit entsprechenden Fehlermeldungen abgewiesen. MDaemon nimmt eingehende Nachrichten für die Benutzerkonten auch während dieser Zeiträume an. Der Versand von Nachrichten über die Benutzerkonten und der Zugriff auf die Benutzerkonten mithilfe von Mailclients sind aber nicht möglich.

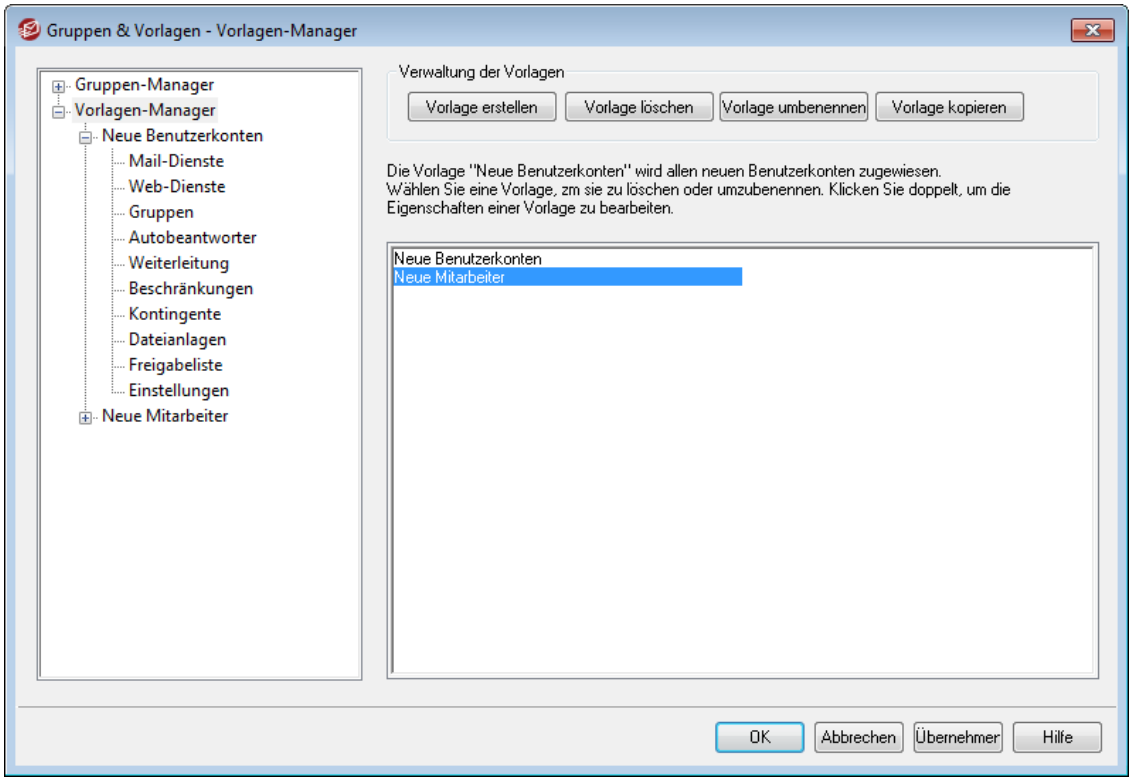
Um den Schutz gegen Störungen auf ein Benutzerkonto oder mehrere Benutzerkonten anzuwenden, gehen Sie folgendermaßen vor:

1. Aktivieren Sie den **Schutz gegen Störungen**.
2. Klicken Sie auf **Zeitplan für Schutz gegen Störungen festlegen**.
3. Wählen Sie Beginn- und Enddatum, Beginn- und Endzeitpunkt, sowie die Wochentage, an denen der Schutz gegen Störungen wirksam sein soll.
4. Klicken Sie auf **OK**.
5. Weisen Sie mithilfe des Gruppen-Managers[782] dieser Gruppe alle Benutzerkonten zu, für die der Schutz gegen Störungen wirksam sein soll.

Siehe auch:

Gruppen-Manager[782]
Nachrichten-Verzeichnisse & Gruppen[717]
Vorlagen-Manager[787]
Vorlagen-Eigenschaften[789]

5.2.2 Vorlagen-Manager



Mithilfe des Vorlagen-Managers (erreichbar über `Benutzerkonten » Gruppen & Vorlagen... » Vorlagen-Manager`) können Sie Vorlagen für Benutzerkonten erstellen und verwalten. Diese Vorlagen sind mit Namen bezeichnete Sammlungen von Einstellungen für Benutzerkonten, die mit bestimmten Gruppen[782] verknüpft werden können. In Benutzerkonten, die zu einer solche Gruppe gehören, sind die durch die Vorlage festgelegten Einstellungen gesperrt und können nicht mithilfe des Benutzerkonten-Editors bearbeitet werden. Sie werden stattdessen nur durch die jeweils verknüpfte Vorlage festgelegt. Die Kategorien der Benutzerkonten-Einstellungen, die eine Vorlage steuert, werden mithilfe des Konfigurationsdialogs Gruppen-Eigenschaften[789] festgelegt. Sie erreichen diesen Konfigurationsdialog durch einen Doppelklick auf die gewünschte Vorlage in der Liste weiter unten, oder durch Anklicken der Vorlage in der Baumansicht im linken Bereich.

Verwaltung der Vorlagen

Vorlage erstellen

Um eine neue Vorlage für Benutzerkonten zu erstellen, klicken Sie auf *Vorlage erstellen*, geben Sie einen Namen für die Vorlage an, und klicken Sie danach auf *OK*. Die neue Vorlage erscheint dann sowohl in der Übersicht über die Vorlagen im unteren Teil dieses Konfigurationsdialogs wie auch in der Baumansicht im linken Bereich.

Vorlage löschen

Um eine Vorlage zu löschen, wählen Sie die Vorlage in der Übersicht über die Vorlagen im unteren Teil dieses Konfigurationsdialogs aus, und klicken Sie danach auf *Vorlage löschen*. Bestätigen Sie anschließend die Sicherheitsabfrage mit *Ja*.

Vorlage umbenennen
Um eine Vorlage umzubenennen, wählen Sie die Vorlage in der Übersicht über die Vorlagen im unteren Teil dieses Konfigurationsdialogs aus, und klicken Sie danach auf *Vorlage umbenennen*. Geben Sie den neuen Namen für die Vorlage ein, und klicken Sie danach auf *OK*.

Vorlage kopieren
Um eine neue Vorlage anzulegen und dabei die Einstellungen aus einer anderen Vorlage zu übernehmen, wählen Sie die gewünschte Ursprungsvorlage in der Liste aus, und klicken Sie auf *Vorlage kopieren*. Geben Sie dann den Namen für die neue Vorlage an.

Liste der Vorlagen

Die Liste der Vorlagen im unteren Bereich des Vorlagen-Managers enthält alle Vorlagen. Klicken Sie hier eine Vorlage an, und verwenden Sie dann die Steuerelemente oberhalb der Liste, um die Vorlage zu löschen oder umzubenennen. Klicken Sie doppelt auf eine Vorlage, um den Konfigurationsdialog für die Eigenschaften 789 zu öffnen. Dort können Sie die Kategorien von Benutzerkonten-Einstellungen festlegen, die diese Vorlage steuert. Sie können mithilfe der Baumansicht im linken Bereich jede Vorlage und ihre Benutzerkonten-Einstellungen direkt aufrufen. Die Vorlage *Neue Benutzerkonten* ist eine besondere Vorlage, die in der Baumansicht immer an oberster Stelle erscheint.

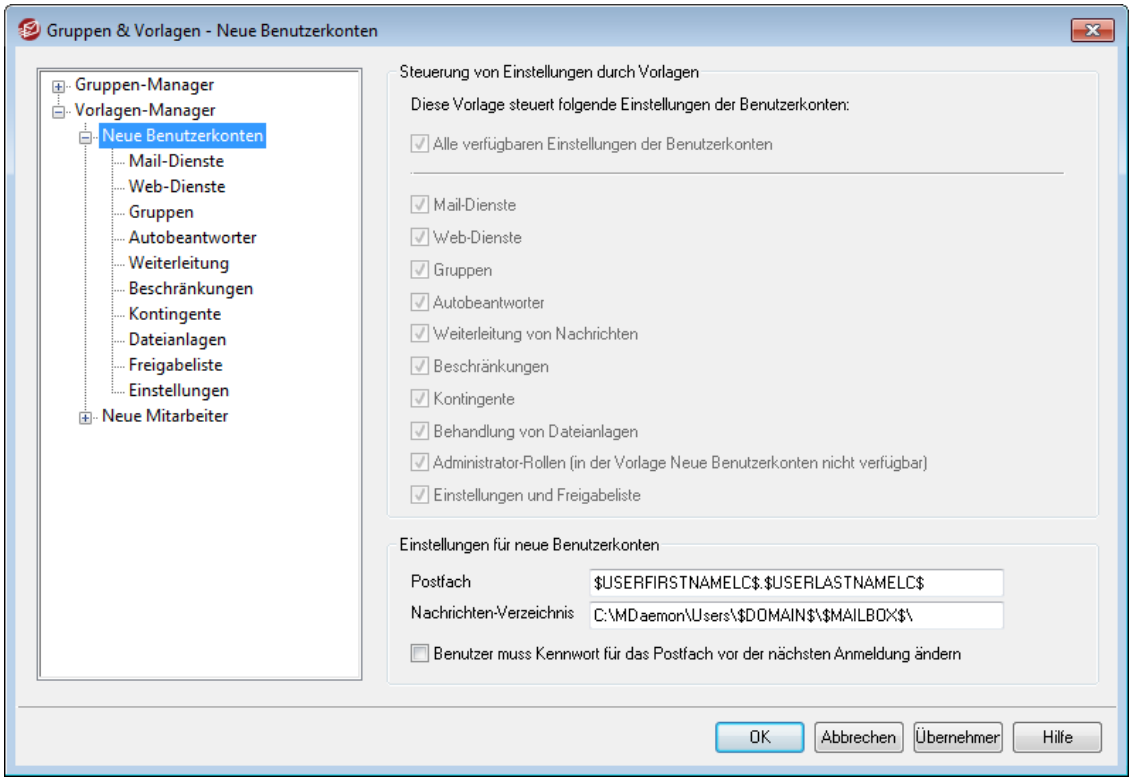
Die Vorlage "Neue Benutzerkonten"

Die Vorlage *Neue Benutzerkonten* ist eine besondere Vorlage, die auf alle neuen Benutzerkonten zu dem Zeitpunkt angewendet wird, zu dem diese erstellt werden. Im Unterschied zu anderen Vorlagen sperrt sie jedoch nicht die Einstellungen der Benutzerkonten gegen Bearbeitung und gibt sie fest vor. Statt dessen legt sie nur einmalig die Einstellungen des jeweils gerade erstellten Benutzerkontos fest, und diese Einstellungen können sofort über den Benutzerkonten-Editor einzeln geändert werden. Manche in Vorlagen verfügbaren Einstellungen, wie etwa die Einstellungen im Abschnitt Administrator-Rollen 810, stehen in der Vorlage Neue Benutzerkonten nicht zur Verfügung.

Siehe auch:

Vorlagen-Eigenschaften 789
Vorlagen-Manager 782

5.2.2.1 Vorlagen-Eigenschaften



Um den Konfigurationsdialog für die Eigenschaften einer Vorlage aufzurufen, öffnen Sie den Vorlagen-Manager[787], und klicken Sie im linken Bereich auf den Namen der Vorlage. Mithilfe dieses Konfigurationsdialogs können Sie für jede Vorlage die Kategorien der Benutzerkonten-Einstellungen festlegen, die diese Vorlage steuern soll. Sind Benutzerkonten Mitglieder einer Gruppe[782], mit der eine Vorlage für Benutzerkonten verknüpft ist, so sind für diese Benutzerkonten die durch die Vorlage festgelegten Einstellungen gesperrt und können nicht mithilfe des Benutzerkonten-Editors bearbeitet werden. Diese Einstellungen werden nur durch die Vorlage gesteuert. Falls ein Benutzerkonto zu mehreren Gruppen gehört, und diese Gruppen mit mehreren Vorlagen verknüpft sind, so werden alle Einstellungen aus diesen Vorlagen angewendet, soweit die betreffenden Eigenschaften der Vorlagen[789] einander nicht widersprechen. Falls mehrere Vorlagen dieselben Einstellungen regeln, dann finden die Einstellungen aus der ersten aufgeführten Vorlage Anwendung.

Steuerung von Einstellungen durch Vorlagen

Alle verfügbaren Einstellungen der Benutzerkonten
Diese Option bewirkt, dass die Vorlage für die Benutzerkonten der Gruppen, die diese Vorlage nutzen, alle verfügbaren Einstellungen steuert. Alle Konfigurationsdialoge für diese Vorlage werden dann für die Benutzerkonten-Einstellungen jedes Gruppenmitglieds benutzt, und die gleichnamigen Konfigurationsdialoge im Benutzerkonten-Editor sind gesperrt. Um nur einzelne Kategorien der *Einstellungen der Benutzerkonten* in der nachfolgenden Liste durch diese Vorlage steuern zu lassen, deaktivieren Sie diese Option, und wählen Sie aus der nachfolgenden Liste die gewünschten Kategorien von Benutzerkonten-Einstellungen aus.

Einstellungen der Benutzerkonten
In diesem Abschnitt sind die Kategorien der Einstellungen für Benutzerkonten aufgeführt, die diese Vorlage für Mitglieder solcher Gruppen steuern kann, die mit

der Vorlage verknüpft sind. Jede Kategorie entspricht einem Abschnitt des Konfigurationsdialogs desselben Namens. Ist eine Kategorie ausgewählt, so werden die Einstellungen des gleichnamigen Konfigurationsdialogs anstatt der Einstellungen im entsprechenden Konfigurationsdialog des Benutzerkonten-Editors für die Gruppenmitglieder übernommen.

Einstellungen für neue Benutzerkonten

Diese Optionen stehen nur in der Vorlage für neue Benutzerkonten 788 zur Verfügung. Sie nutzen eine Vielzahl besonderer Makros 791, um das Nachrichten-Verzeichnis und den Postfachnamen für die E-Mail-Adresse für neue Benutzerkonten automatisch zu erstellen.

Postfach
Mithilfe dieser Option können Sie das Schema vorgeben, nach dem der *Postfachname* 714 für die E-Mail-Adresse für alle neuen Benutzerkonten per Voreinstellung erzeugt wird. Im Abschnitt Makros für Vorlagen 791 weiter unten finden Sie eine Übersicht über die Makros, die Sie in dieser Vorlagen-Option verwenden können. Die Voreinstellung für diese Option lautet "`$USERFIRSTNAMELC$.$USERLASTNAMELC$`". Wird beispielsweise in der Domäne example.com ein Benutzerkonto für "Michael Mason" erstellt, so ergibt sich in der Voreinstellung hieraus die Adresse "`michael.mason@example.com`".

Nachrichten-Verzeichnis
Mithilfe dieser Option können Sie das Schema vorgeben, nach dem das *Nachrichten-Verzeichnis* 717 für alle neuen Benutzerkonten per Voreinstellung festgelegt wird. Das *Nachrichten-Verzeichnis* eines Benutzerkontos ist der Verzeichnispfad, in dem die E-Mail-Nachrichten des Benutzerkontos auf dem Server gespeichert werden. Der Eintrag "`...\$DOMAIN$\$MAILBOX$\`" in dieser Option würde beispielsweise für den Benutzer "michael.mason@example.com" den Pfad "`...\example.com\michael.mason\`" ergeben.

MDaemon unterstützt grundlegende Leistungsmerkmale, um Verzeichnisse mithilfe von Hashfunktionen zu strukturieren. Bei Verwendung des Dateisystems NTFS kann es zu Leistungseinbußen kommen, falls unter dem selben Wurzelverzeichnis zahlreiche Unterverzeichnisse bestehen. Falls auf Ihrem System zahlreiche Benutzer angelegt sind, und fall Sie die Verzeichnisse für diese Benutzer über die Aufteilung `$DOMAIN$\$MAILBOX$\` hinaus weiter untergliedern wollen, können Sie hierzu das Makro `$MAILBOXFIRSTCHARSn$` einsetzen. In diesem Makro steht "`n`" für eine Zahl zwischen 1 und 10 und wird in die ersten "`n`" Zeichen des Postfachnamens umgesetzt. Ein Beispiel hierzu: Sie können die Hashfunktionen nutzen, indem Sie das Schema für die Erstellung des *Nachrichten-Verzeichnisses* etwa folgendermaßen gestalten:

```
C:
\PostfachHauptverzeichnis\$MAILBOXFIRSTCHARS4$\$M
AILBOXFIRSTCHARS2$\$MAILBOX$\.
```

Benutzer muss Kennwort für das Postfach vor der nächsten Anmeldung ändern
Diese Option zwingt den Benutzer dazu, das *Kennwort für das Postfach* zu ändern, bevor er über POP, IMAP, SMTP, Webmail oder die Remoteverwaltung auf das Benutzerkonto zugreifen kann. Meldet sich der Benutzer über Webmail oder die Remoteverwaltung an, solange diese Option aktiv ist, so kann die Anmeldung nur abgeschlossen werden, wenn der Benutzer auf Aufforderung ein neues Kennwort festlegt. Bei Nutzung dieser Option muss der Benutzer auch über die *Berechtigung zum Ändern des Kennworts* verfügen, die auf der Seite Web-Dienste 795 festgelegt wird. Nachdem der Benutzer das Kennwort geändert hat, wird die Option im Abschnitt Einzelheiten zum Benutzerkonto 714 wieder deaktiviert.

Für einzelne Benutzer kann es schwierig oder unmöglich sein, das Kennwort selbst zu ändern. Diese Option sollte daher vorsichtig eingesetzt werden.

Makros für Vorlagen

Die folgende Liste gibt Ihnen einen schnellen Überblick über die Makros, die Sie in den Schemata zur automatisierten Erstellung der Benutzerkonten verwenden können.

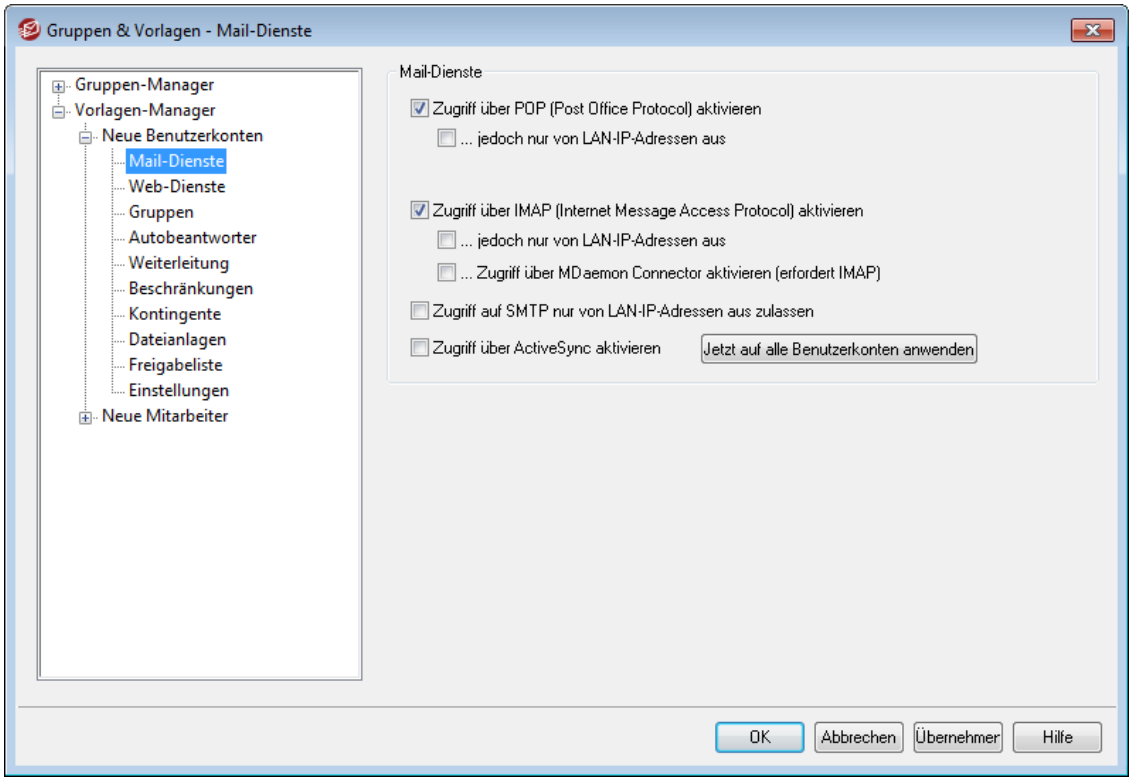
`$DOMAIN$`	Dieses Makro wird in den Domänennamen umgesetzt, der für das Benutzerkonto ausgewählt wurde.
`$DOMAINIP$`	Dieses Makro wird in die IP-Adresse umgesetzt, die mit der Domäne verknüpft ist, die für das Benutzerkonto ausgewählt wurde.
`$MACHINENAME$`	Dieses Makro wird in den Hostnamen der Standard-Domäne umgesetzt, der im Abschnitt Hostname & IP des Domänen-Managers festgelegt ist. Dieses Makro wird bei neuen Installationen jetzt auch in der Standard-Vorlage für Informationen an neue Benutzerkonten (NEWUSERHELP.DAT) verwendet.
`$USERNAME$`	Dieses Makro wird in den vollständigen Vor- und Nachnamen des Inhabers des Benutzerkontos umgesetzt. Es entspricht damit der Makrokette "$USERFIRSTNAME$ $USERLASTNAME$".
`$USERFIRSTNAME$`	Dieses Makro wird in den Vornamen des Inhabers des Benutzerkontos umgesetzt.
`$USERFIRSTNAMELC$`	Dieses Makro wird in den Vornamen des Inhabers des Benutzerkontos in Kleinbuchstaben umgesetzt.
`$USERLASTNAME$`	Dieses Makro wird in den Nachnamen des Inhabers des Benutzerkontos umgesetzt.

$USERLASTNAMELC$	Dieses Makro wird in den Nachnamen des Inhabers des Benutzerkontos in Kleinbuchstaben umgesetzt.
$USERFIRSTINITIAL$	Dieses Makro wird in den ersten Buchstaben des Vornamens des Inhabers des Benutzerkontos umgesetzt.
$USERFIRSTINITIALLC$	Dieses Makro wird in den ersten Buchstaben des Vornamens des Inhabers des Benutzerkontos in Kleinbuchstaben umgesetzt.
$USERLASTINITIAL$	Dieses Makro wird in den ersten Buchstaben des Nachnamens des Inhabers des Benutzerkontos umgesetzt.
$USERLASTINITIALLC$	Dieses Makro wird in den ersten Buchstaben des Nachnamens des Inhabers des Benutzerkontos in Kleinbuchstaben umgesetzt.
$MAILBOX$	Dieses Makro wird in den Postfachnamen des jeweiligen Benutzerkontos umgesetzt. Der entsprechende Wert wird während POP3-Verbindungen zur Übermittlung von Nachrichten auch zusammen mit dem Befehl USER übermittelt.
$MAILBOXFIRSTCHARSn$	"n" ist hierbei eine Zahl zwischen 1 und 10. Dieses Makro wird in die ersten "n" Zeichen des Postfachnamens umgesetzt.

Siehe auch:

Vorlagen-Manager 787
Gruppen-Manager 782

5.2.2.1.1 Mail-Dienste



Die Optionen in diesem Abschnitt der Vorlagen-Eigenschaften entsprechen den Optionen im Abschnitt Mail-Dienste[718] des Benutzerkonten-Editors. Ist eine Vorlage so konfiguriert, dass sie die Kategorie der Einstellungen steuert[789], die in diesem Abschnitt enthalten sind, so steuert sie die Einstellungen für die Mail-Dienste jedes Benutzerkontos, das Mitglied einer Gruppe[784] ist, mit der diese Vorlage verknüpft ist.

Mail-Dienste

Zugriff über POP (Post Office Protocol) aktivieren
Diese Option ermöglicht den Zugriff auf die Nachrichten der Benutzerkonten, die durch diese Vorlage gesteuert werden, über das Post Office Protocol (POP). Dieses Protokoll wird von nahezu allen E-Mail-Clients unterstützt.

...jedoch nur von LAN-IP-Adressen aus
Mithilfe dieser Option können Sie den Zugriff auf die Benutzerkonten über POP beschränken, sodass die Benutzer über dieses Protokoll nur von einer LAN-IP-Adresse[610] aus zugreifen können.

Zugriff über IMAP (Internet Message Access Protocol) aktivieren
Diese Option ermöglicht den Zugriff auf die Nachrichten der Benutzerkontos, die durch diese Vorlage gesteuert werden, über das Internet Message Access Protocol (IMAP). IMAP ist vielseitiger als POP und gestattet die Verwaltung der Nachrichten auf dem Server sowie den Zugriff über mehrere verschiedene E-Mail-Clients. Dieses Protokoll wird von den meisten E-Mail-Clients unterstützt.

...jedoch nur von LAN-IP-Adressen aus
Mithilfe dieser Option können Sie den Zugriff auf die Benutzerkonto über IMAP beschränken, sodass die Benutzer über dieses Protokoll nur von einer LAN-IP-Adresse[610] aus zugreifen können.

Zugriff über MDaemon Connector aktivieren (erfordert IMAP)
Diese Option steht nur in der Vorlage "Neue Benutzerkonten" zur Verfügung. Diese Option ermöglicht dem Benutzerkonto die Nutzung des MDaemon Connectors[385]. **Beachte:** Diese Option ist nur verfügbar, wenn der MDaemon Connector auf dem Server aktiv ist.

Zugriff auf SMTP nur von LAN-IP-Adressen aus zulassen
Diese Option beschränkt den Zugriff auf SMTP und lässt den Zugriff durch das Benutzerkonto nur von LAN-IP-Adressen aus. Hierdurch wird verhindert, dass Benutzerkonten E-Mail-Nachrichten über den Server versenden, solange sie nicht mit dem lokalen Netzwerk verbunden sind. Versucht ein Benutzerkonto, Nachrichten von externen IP-Adressen aus zu versenden, so wird der Verbindungsversuch abgewiesen.

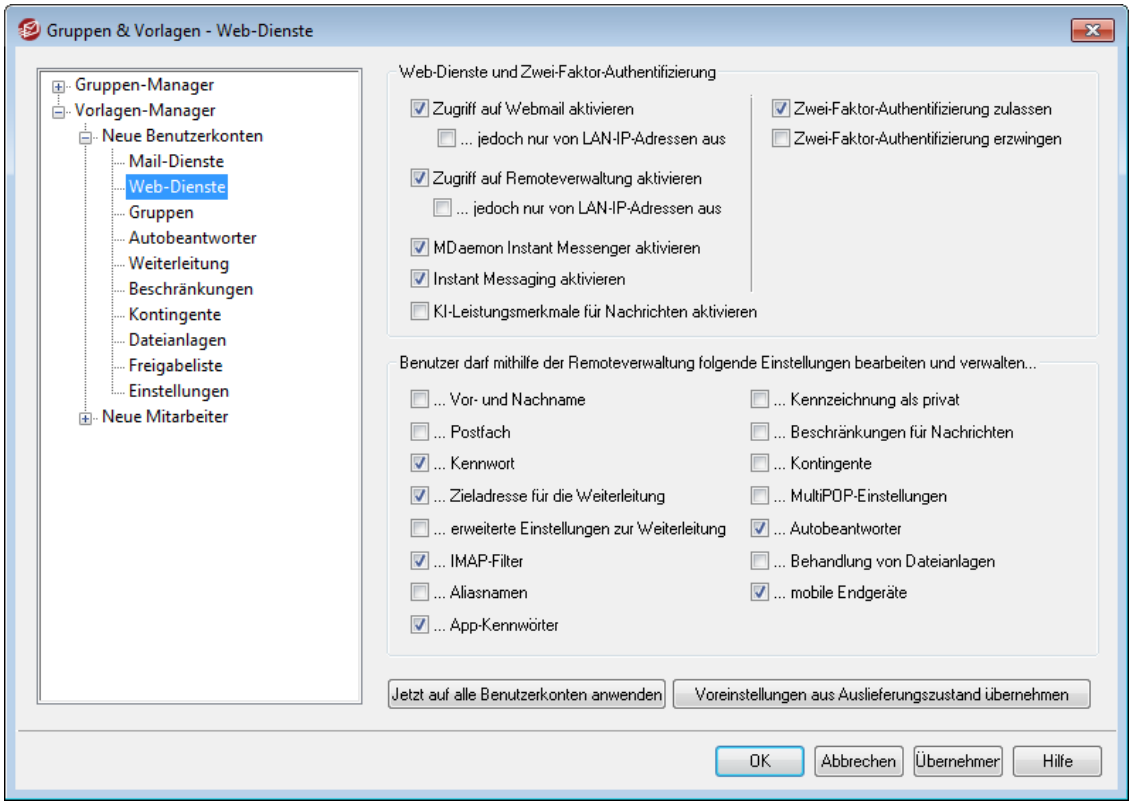
Zugriff über ActiveSync aktivieren
Diese Option steht nur in der Vorlage "Neue Benutzerkonten" zur Verfügung. Sie bewirkt, dass neue Benutzerkonten ActiveSync auf mobilen Endgeräten unterstützen. Über ActiveSync können E-Mail-Nachrichten, Kontakte, Kalender und andere Daten mit MDaemon und Webmail synchronisiert werden. Diese Einstellung entspricht der Einstellung *ActiveSync-Dienste für diesen Benutzer aktivieren* im Abschnitt ActiveSync für MDaemon[763] des Benutzerkonten-Editors.

Jetzt auf alle Benutzerkonten anwenden
Dieses Steuerelement steht nur in der Vorlage "Neue Benutzerkonten" zur Verfügung. Durch Anklicken dieses Steuerelements werden die Einstellungen aus diesem Konfigurationsdialog sofort in die Abschnitte Mail-Dienste[718] und ActiveSync für MDaemon[763] aller bestehenden MDaemon-Benutzerkonten übertragen.

Siehe auch:

Vorlagen-Eigenschaften[789]
Gruppen-Eigenschaften[784]
Vorlage "Neue Benutzerkonten"[788]
Benutzerkonten-Editor » Mail-Dienste[718]

5.2.2.1.2 Web-Dienste



Die Optionen in diesem Abschnitt der Vorlagen-Eigenschaften entsprechen den Optionen im Abschnitt Web-Dienste[720] des Benutzerkonten-Editors. Ist eine Vorlage so konfiguriert, dass sie die Kategorie der Einstellungen steuert[789], die in diesem Abschnitt enthalten sind, so steuert sie die Einstellungen für die Web-Dienste jedes Benutzerkontos, das Mitglied einer Gruppe[784] ist, mit der diese Vorlage verknüpft ist.

Web-Dienste und Zwei-Faktor-Authentifizierung

Zugriff auf Webmail aktivieren
Diese Option bewirkt, dass Benutzerkonten, die durch diese Vorlage gesteuert werden, Zugriff auf den Dienst Webmail[317] erhalten, der die Abfrage von E-Mail, die Verwaltung der Kalender und die Nutzung weiterer Leistungsmerkmale per Web-Browser zulässt.

...jedoch nur von LAN-IP-Adressen aus
Mithilfe dieser Option können Sie den Zugriff auf die Benutzerkonten über Webmail beschränken, sodass die Benutzer über diesen Dienst nur von einer LAN-IP-Adresse[610] aus zugreifen können.

Zugriff auf Remoteverwaltung aktivieren
Diese Option bewirkt, dass der Benutzer, deren Benutzerkonten über diese Vorlage gesteuert werden, die Einstellungen ihrer Benutzerkonten über die Remoteverwaltung[350] bearbeiten können. Die Benutzer dürfen dort nur jene Einstellungen bearbeiten, die Sie im Folgenden freigeben.

Ist dieses Leistungsmerkmal aktiv, und wird der Remoteverwaltungs-Server ausgeführt, so kann sich der Benutzer bei der Remoteverwaltung anmelden. Er muss dazu in einem Browser die gewünschte MDaemon-Domäne und den Port, der der Remoteverwaltung zugewiesen ist[352], angeben (z.B.

`http://example.com:1000`). Es erscheint zunächst ein Anmeldedialog und dann eine Übersicht aller Einstellungen, die der Benutzer bearbeiten darf. Nachdem er die Einstellungen bearbeitet und durch Anklicken des entsprechenden Steuerelements die Änderungen gespeichert hat, kann er sich wieder abmelden und den Browser schließen. Falls der Benutzer auch Zugriff auf Webmail hat, kann er über die erweiterten Einstellungen aus Webmail heraus die Remoteverwaltung ebenfalls aufrufen.

Falls der Benutzer ein globaler oder Domänen-Administrator ist (beides wird im Abschnitt Administrator-Rollen 757 des Benutzerkonten-Editors festgelegt), wird ihm nach der Anmeldung an der Remoteverwaltung ein anderer Konfigurationsdialog angezeigt.

...jedoch nur von LAN-IP-Adressen aus
Mithilfe dieser Option können Sie den Zugriff auf die Benutzerkonto über die Remoteverwaltung beschränken, sodass die Benutzer über diesen Dienst nur von einer LAN-IP-Adresse 610 aus zugreifen können.

MDaemon Instant Messenger aktivieren
Diese Option bewirkt, dass neue Benutzerkonten per Voreinstellung den MDIM 318 nutzen dürfen. Diese Option ist nur in der Vorlage "Neue Benutzerkonten" 788 verfügbar. Im Konfigurationsdialog Gruppen-Eigenschaften 784 steht eine ähnliche Option zur Verfügung, mit deren Hilfe der Zugriff von Gruppenmitgliedern auf den MDIM gesteuert werden kann.

Instant Messaging aktivieren
Diese Option bewirkt, dass neue Benutzerkonten per Voreinstellung die Instant-Messaging-Funktionen von MDIM nutzen dürfen. Diese Option ist nur in der Vorlage "Neue Benutzerkonten" 788 verfügbar. Im Konfigurationsdialog Gruppen-Eigenschaften 784 steht eine ähnliche Option zur Verfügung, mit deren Hilfe der Zugriff von Gruppenmitgliedern auf die Instant-Messaging-Funktionen von MDIM gesteuert werden kann.

Zwei-Faktor-Authentifizierung

MDaemon unterstützt die Zwei-Faktor-Authentifizierung (2FA) für alle Benutzer, die sich an den Webschnittstellen von Webmail und der Remoteverwaltung anmelden. Benutzerkonten, die sich an Webmail über HTTPS anmelden, können die Zwei-Faktor-Authentifizierung über den Konfigurationsdialog **Optionen » Sicherheit** aktivieren. Ab diesem Zeitpunkt muss der Benutzer bei jeder Anmeldung an Webmail oder der Remoteverwaltung einen Bestätigungskode eingeben. Der Benutzer erhält den Bestätigungskode während der Anmeldung über eine Authentifizierungs-App, die er auf seinem Mobiltelefon oder Tablet installiert. Dieses Leistungsmerkmal arbeitet mit allen Clients, die den Google Authenticator unterstützen. Die Hilfe für Webmail enthält nähere Informationen über die Einrichtung der Zwei-Faktor-Authentifizierung für die Benutzerkonten.

Zwei-Faktor-Authentifizierung zulassen
Neue Benutzerkonten 795 dürfen per Voreinstellung die Zwei-Faktor-Authentifizierung in Webmail aktivieren und nutzen. Um die Zwei-Faktor-Authentifizierung für das gerade bearbeitete Benutzerkonto zu sperren, deaktivieren Sie diese Option.

Zwei-Faktor-Authentifizierung erzwingen
Diese Option bewirkt, dass das Benutzerkonto die Zwei-Faktor-Authentifizierung für die Anmeldung an Webmail nutzen muss. Falls sie für das Benutzerkonto noch nicht eingerichtet ist, wird der Benutzer bei der nächsten Anmeldung an Webmail auf eine Konfigurationsseite umgeleitet, auf der er die Zwei-Faktor-Authentifizierung einrichten muss. Die Hilfe für Webmail enthält nähere Informationen über die Einrichtung der Zwei-Faktor-Authentifizierung für die Benutzerkonten.

Benutzer darf mithilfe der Remoteverwaltung folgende Einstellungen bearbeiten und verwalten...

Vor- und Nachname
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten, ihre *Vor- und Nachnamen* 714 zu bearbeiten.

Postfach
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten, ihre *Postfachnamen* 714 als Teil der E-Mail-Adressen zu bearbeiten.

Der Postfachname ist Teil der E-Mail-Adresse des Benutzerkontos, und diese dient zugleich als eindeutiges Identifizierungsmerkmal für das Benutzerkonto und als Benutzer- oder Anmeldename. Ändert der Benutzer den Postfachnamen, so ändert sich daher auch die E-Mail-Adresse. Nachrichten an die alte E-Mail-Adresse könnten dann abgewiesen oder gelöscht werden, oder sonst verloren gehen.

Kennwort
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten, ihre Kennwörter für ihre Postfächer zu bearbeiten. Weitere Informationen über die Kennwörter finden Sie im Abschnitt Kennwörter 847.

Zieladresse für die Weiterleitung
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten, die Zieladresse für die Weiterleitung 727 zu bearbeiten.

erweiterte Einstellungen zur Weiterleitung
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten, die erweiterten Einstellungen zur Weiterleitung 727 zu bearbeiten.

IMAP-Filter
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten, eigene IMAP-Filter 736 zu erstellen und zu bearbeiten.

Aliasnamen
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten, die Konfiguration ihrer Aliasnamen 741 über die Remoteverwaltung zu bearbeiten.

App-Kennwörter
Per Voreinstellung dürfen die Benutzer ihre App-Kennwörter[750] bearbeiten. Falls Sie Ihren Benutzern das Bearbeiten der App-Kennwörter nicht gestatten wollen, deaktivieren Sie diese Option.

Kennzeichnung als privat
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten, die Option *Benutzerkonto aus Listen "Everyone" und Ordner Öffentliche Kontakte der Domäne ausblenden* im Abschnitt Optionen[760] des Benutzerkonten-Editors zu bearbeiten.

Beschränkungen für Nachrichten
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten, die Beschränkungen für eingehende und abgehende Nachrichten zu bearbeiten, die über den Konfigurationsdialog Beschränkungen[729] erreichbar sind.

Kontingente
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten, ihre Kontingenteinstellungen[731] zu bearbeiten.

MultiPOP-Konten
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten, neue MultiPOP-Einträge[739] hinzuzufügen und den Abruf von Nachrichten für diese Einträge über MultiPOP zu aktivieren und zu deaktivieren.

Autobeantworter
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten, eigene Autobeantworter[724] zu erstellen, zu bearbeiten und zu löschen.

Behandlung von Dateianlagen
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten, die Optionen zur Behandlung von Dateianlagen zu bearbeiten, die im Abschnitt Dateianlagen[734] erreichbar sind.

mobile Endgeräte
Diese Option berechtigt die durch diese Vorlage gesteuerten Benutzerkonten zur Nutzung der Remoteverwaltung von MDaemon zur Verwaltung der Einstellungen für ihre mobilen Endgeräte, etwa für ActiveSync-Endgeräte.

Jetzt auf alle Benutzerkonten anwenden

Dieses Steuerelement steht nur in der Vorlage "Neue Benutzerkonten"[788] zur Verfügung. Durch Anklicken dieses Steuerelements werden die Einstellungen aus diesem Konfigurationsdialog auf alle bestehenden MDaemon-Benutzerkonten übertragen, deren Einstellungen für Web-Dienste nicht durch eine Vorlage für Benutzerkonten gesteuert werden.

Voreinstellungen aus Auslieferungszustand übernehmen

Dieses Steuerelement steht nur in der Vorlage "Neue Benutzerkonten"[788] zur Verfügung. Durch Anklicken dieses Steuerelements werden die Einstellungen der Vorlage "Neue Benutzerkonten" auf den Auslieferungszustand zurück gesetzt. Sie entsprechen dann den Einstellungen, die nach einer Neuinstallation gelten. Dieses Steuerelement ändert nur die Einstellungen der Vorlage, nicht jedoch die Einstellungen bestehender Benutzerkonten.

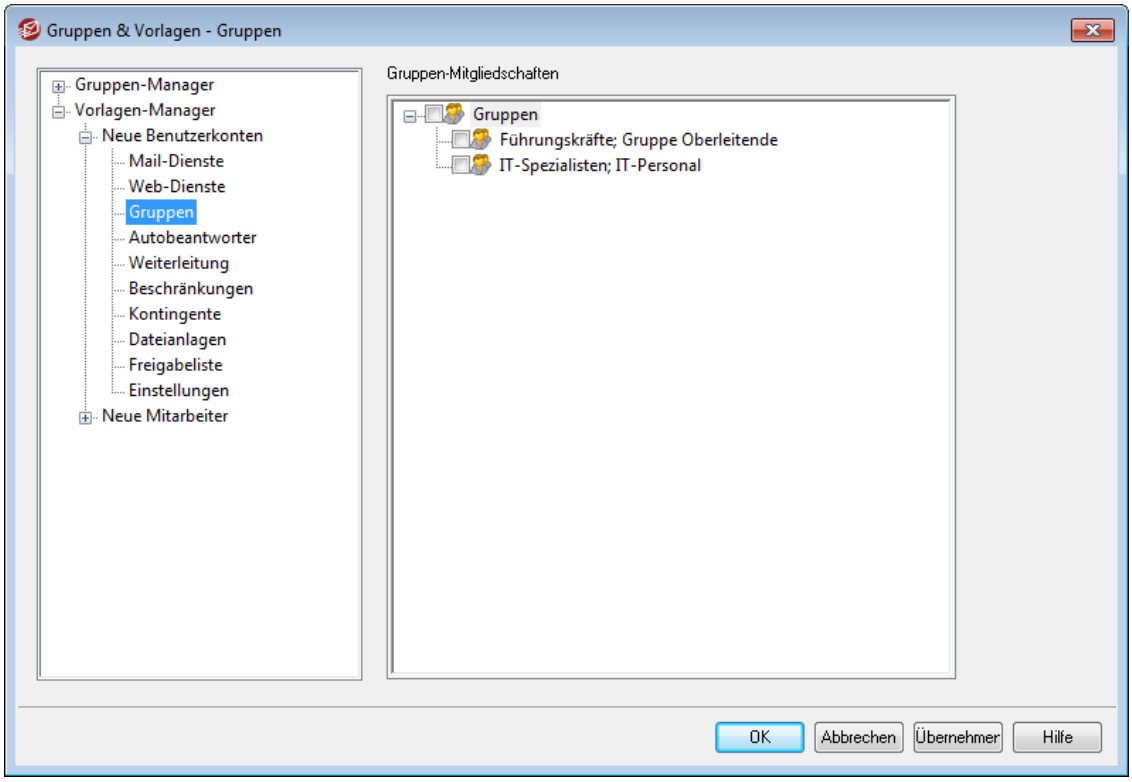
Einstellungen aus der Vorlage für neue Benutzerkonten laden

Dieses Steuerelement steht nur in benutzerdefinierten Vorlagen zur Verfügung. Durch Anklicken dieses Steuerelements werden die Einstellungen aus diesem Konfigurationsdialog auf die Voreinstellungen zurückgesetzt, die im Konfigurationsdialog Web-Dienste der Vorlage "Neue Benutzerkonten" 788 festgelegt sind.

Siehe auch:

Vorlagen-Eigenschaften 789
Gruppen-Eigenschaften 784
Vorlage "Neue Benutzerkonten" 788
Benutzerkonten-Editor » Web-Dienste 720

5.2.2.1.3 Gruppen



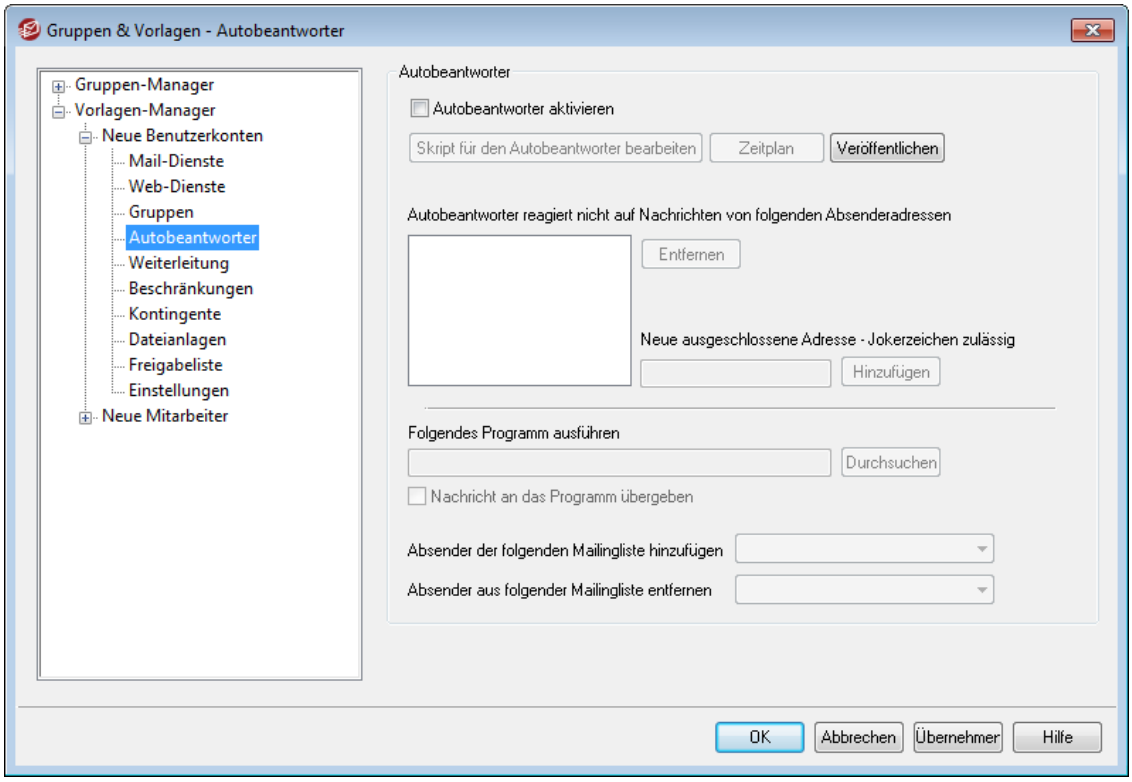
Gruppen-Mitgliedschaften

Dieser Konfigurationsdialog ist nur in der Vorlage Neue Benutzerkonten 788 verfügbar und entspricht dem Abschnitt Gruppen-Mitgliedschaften im Abschnitt Nachrichten-Verzeichnisse & Gruppen 717 des Benutzerkonten-Editors. Wenn Sie hier eine oder mehrere Gruppen auswählen, werden neue Benutzerkonten automatisch in diese Gruppen aufgenommen.

Siehe auch:

Vorlage Neue Benutzerkonten 788
Gruppen-Manager 782
Gruppen-Eigenschaften 784

5.2.2.1.4 Autobeantworter



Die Optionen in diesem Abschnitt der Vorlagen-Eigenschaften entsprechen den Optionen im Abschnitt Autobeantworter 724 des Benutzerkonten-Editors. Ist eine Vorlage so konfiguriert, dass sie die Kategorie der Einstellungen steuert 789, die in diesem Abschnitt enthalten sind, so steuert sie die Einstellungen für die Autobeantworter jedes Benutzerkontos, das Mitglied einer Gruppe 784 ist, mit der diese Vorlage verknüpft ist.

Autobeantworter sind nützliche Werkzeuge, mit denen Aktionen durch eingehende E-Mail-Nachrichten ausgelöst werden können. Eine weit verbreitete Einsatzmöglichkeit für Autobeantworter ist es, eine benutzerdefinierte Nachricht als "Anrufbeantworter" für abwesende oder anderweit an der Beantwortung eingehender Nachrichten verhinderte Benutzer zu verwenden. Eingehende Nachrichten können mit ihrer Hilfe automatische benutzerdefinierte Antwortnachrichten oder eine Programmausführung auf dem Server auslösen, wobei die Nachricht selbst über die Kommandozeile an das externe Programm übergeben wird. MDaemon-Benutzer mit Web-Zugriff 720 auf Webmail 317 oder die Remoteverwaltung 350 können diese Verwaltungswerkzeuge verwenden, um Nachrichten und Zeitpläne für den Autobeantworter selbst zu erstellen. Nachrichten der Autobeantworter stützen sich auf die Inhalte der Dateien `OOF.mrk`, die in den Verzeichnissen `\data\` unter den jeweiligen Hauptverzeichnissen der Benutzerkonten abgelegt sind. Diese Dateien unterstützen zahlreiche Makros, und die Inhalte der Nachrichten der Autobeantworter lassen sich hierdurch weitgehend dynamisch gestalten. Autobeantworter sind hierdurch sehr vielseitig einsetzbar.

Nachrichten von externen Absendern lösen Autobeantworter immer aus. Auf Nachrichten von Benutzern derselben Domäne reagieren Autobeantworter nur, falls die Einstellung *Autobeantworter reagieren auf Nachrichten aus*

eigenen Domänen im Konfigurationsdialog Autobeantworter » Einstellungen 835 aktiv ist. Dort steht auch eine weitere Option zur Verfügung, die die Anzahl der automatisch erzeugten Antwortnachrichten auf eine Antwort pro Empfänger und Tag begrenzt.

Autobeantworter

Autobeantworter aktivieren

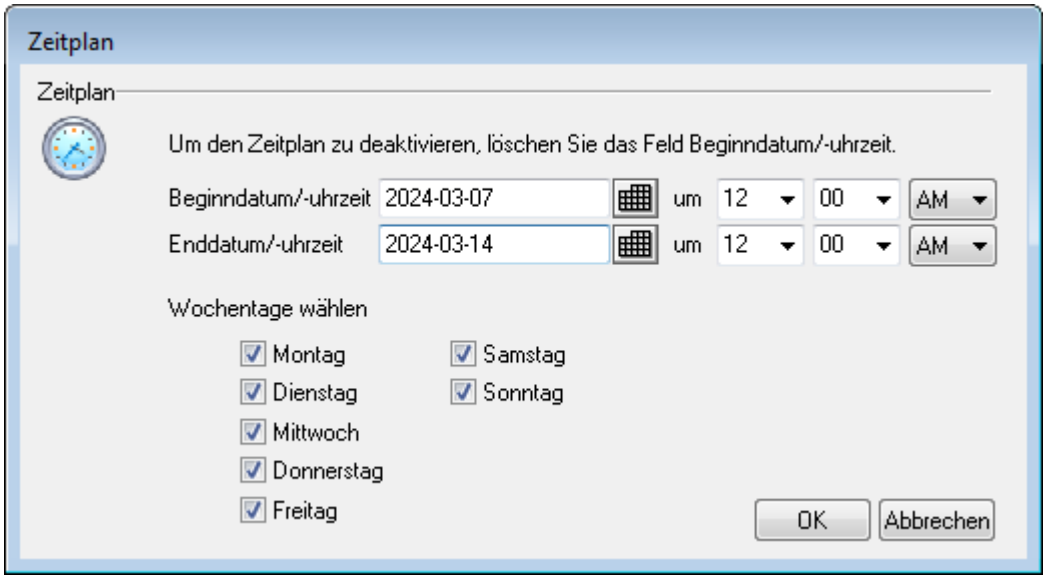
Mit dieser Option wird ein Autobeantworter für die Benutzerkonten in allen Gruppen aktiviert, mit denen diese Vorlage verknüpft ist. Nähere Informationen über Autobeantworter erhalten Sie im Abschnitt Autobeantworter 831.

Skript für den Autobeantworter bearbeiten

Durch Anklicken dieses Steuerelements können Sie die Datei des Autobeantworters für das Benutzerkonto bearbeiten. Der Name dieser Datei lautet `OOF.mrk`, und sie ist im Verzeichnis `\data\` unter dem Hauptverzeichnis des Benutzerkontos gespeichert.

Zeitplan

Ein Klick auf dieses Steuerelement öffnet den Konfigurationsdialog für die Zeitsteuerung der Autobeantworter. Dort können Daten und Uhrzeiten für Beginn und Ende der Autobeantworter festgelegt werden, während derer der Autobeantworter aktiv sein soll. Die Uhrzeit muss dabei nach US-amerikanischem Standard im 12-Stunden-Format unter Verwendung von AM und PM eingetragen werden. Soll der Autobeantworter immer aktiv sein, darf in diesem Konfigurationsdialog nichts eingetragen werden.



Veröffentlichen

Mithilfe dieses Steuerelements können Sie Datei und Einstellungen des Autobeantworters aus diesem Benutzerkonto auf ein anderes Benutzerkonto oder mehrere andere Benutzerkonten übertragen. Wählen Sie dazu die Benutzerkonten, auf die Sie die Datei und die Einstellungen übertragen wollen, und klicken Sie anschließend auf **OK**.

Autobeantworter reagiert nicht auf Nachrichten von folgenden Absenderadressen
Absender-Adressen, die hier eingetragen sind, lösen den Autobeantworter nicht aus.

Manchmal werden Nachrichten von Autobeantwortern an Adressen gesandt, die ihrerseits automatisch antworten. Dies kann einen "Ping-Pong-Effekt" auslösen; die Nachrichten werden immer wieder zwischen beiden Servern hin- und hergeschickt. Mit der oben stehenden Funktion lässt sich verhindern, dass MDaemon automatische Antwortnachrichten an solche Adressen schickt. Im Konfigurationsdialog Autobeantworter » Einstellungen 835 steht auch eine weitere Option zur Verfügung, die die Anzahl der automatisch erzeugten Antwortnachrichten auf eine Antwort pro Empfänger und Tag begrenzt.

Entfernen
Durch Anklicken dieses Steuerelements werden die gewählten Einträge aus der Liste ausgeschlossener Adressen entfernt.

Neue ausgeschlossene Adresse - Jokerzeichen zulässig
Soll eine neue Adresse ausgeschlossen werden, wird sie hier eingetragen und durch einen Klick auf *Hinzufügen* der Liste angefügt.

Bearbeiten
Durch Anklicken dieses Steuerelements können Sie das ausgewählte Skript für den Autobeantworter bearbeiten.

Ausführen eines Programms

Folgendes Programm ausführen
Hier sind Pfad und Dateiname eines Programms anzugeben, das nach dem Empfang neuer Nachrichten in den Postfächern der Benutzer aller Gruppen ausgeführt werden soll, mit denen diese Vorlage verknüpft ist. Das Programm muss unbeaufsichtigt laufen können und muss sich jedenfalls selbst beenden. Zusätzliche Befehlszeilenparameter können nach dem Dateinamen angegeben werden.

Nachricht an das Programm übergeben
Mit dieser Option wird dem oben angegebenen Programm der Name der empfangenen Nachrichtendatei als erster verfügbarer Befehlszeilenparameter übergeben. Diese Funktion ist gesperrt und wirkungslos, wenn der Autobeantworter für ein Benutzerkonto mit Nachrichten-Weiterleitung eingerichtet ist und keine Kopien der weitergeleiteten Post aufbewahrt werden (siehe Weiterleitung 727).

MDaemon übergibt den Dateinamen grundsätzlich als letzten Parameter an die Befehlszeile. Dieses Verhalten kann mit dem Makro `$MESSAGE$` geändert werden. Dieses Makro muss auf der Kommandozeile dort eingesetzt werden, wo der Dateiname stehen soll. Damit lässt sich auch eine komplex

aufgebaute Kommandozeile wie die folgende herstellen:
`logmail /e /j /message=$MESSAGE$ /q.`

Mailinglisten

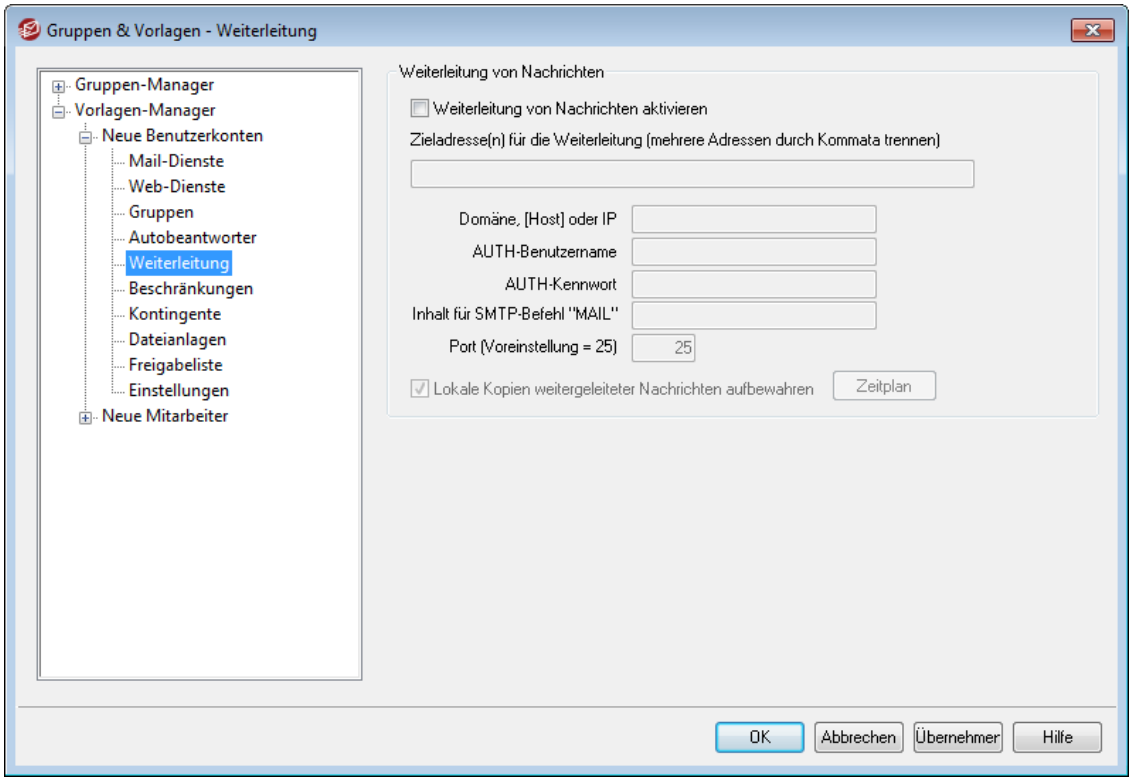
Absender der folgenden Mailingliste hinzufügen
Wird in diesem Feld eine Mailingliste eingetragen, so wird der Absender einer Nachricht durch den Autobeantworter dieser Mailingliste automatisch hinzugefügt. Automatisch arbeitende Mailingliste können so einfach erstellt werden.

Absender aus folgender Mailingliste entfernen
Wird hier eine Mailingliste eingetragen, so wird der Absender einer Nachricht durch den Autobeantworter automatisch von dieser Liste gelöscht.

Siehe auch:

Vorlagen-Eigenschaften 789
Gruppen-Eigenschaften 784
Vorlage "Neue Benutzerkonten" 788
Benutzerkonten-Editor » Autobeantworter 724

5.2.2.1.5 Weiterleitung



Die Optionen in diesem Abschnitt der Vorlagen-Eigenschaften entsprechen den Optionen im Abschnitt Weiterleitung 727 des Benutzerkonten-Editors. Ist eine Vorlage so konfiguriert, dass sie die Kategorie der Einstellungen steuert 789, die in diesem Abschnitt enthalten sind, so steuert sie die Einstellungen für die Weiterleitung jedes Benutzerkontos, das Mitglied einer Gruppe 784 ist, mit der diese Vorlage verknüpft ist.

Weiterleitung von Nachrichten

Weiterleitung von Nachrichten aktivieren
Mit dieser Option wird bestimmt, ob die eingehende Nachrichten der Benutzerkonten aller Gruppen, mit denen diese Vorlage verknüpft ist, an die Adresse im Feld *Zieladresse(n) für die Weiterleitung* weitergeleitet werden. Benutzer von MDaemon mit Web-Zugriff[720] auf Webmail[317] oder die Remoteverwaltung[350] können die Einstellungen zur Weiterleitung selbst ändern; sie müssen damit nicht einen Systemverwalter beauftragen.

Zieladresse(n) für die Weiterleitung (mehrere Adressen durch Kommata trennen)
Hier ist die Adresse anzugeben, an die eine Kopie jeder eingehenden Nachricht für die Benutzerkonten aller Gruppen, mit denen diese Vorlage verknüpft ist, automatisch weitergeleitet wird, sobald die Nachrichten in den Postfächern der Benutzers eingehen. Die Weiterleitung selbst wird mit der oben stehenden Option *Weiterleitung von Nachrichten aktivieren* ein- und ausgeschaltet. Mehrere Adressen müssen durch Kommata getrennt werden.

Domäne, [Host] oder IP
Falls Sie die weitergeleiteten Nachrichten an einen bestimmten Server leiten wollen, etwa an die MX-Hosts einer bestimmten Domäne, dann geben Sie die Domäne oder die IP-Adresse hier an. Falls Sie die Nachrichten an einen bestimmten Host leiten wollen, setzen Sie den Hostnamen in eckige Klammern (z.B. `[host1.example.com]`).

AUTH-Benutzername/Kennwort
Falls der Server, an den Sie die Nachrichten leiten, eine Echtheitsbestätigung über Benutzername und Kennwort verlangt, tragen Sie die Zugangsdaten in diese Felder ein.

Inhalt für SMTP-Befehl 'MAIL'
Falls hier eine E-Mail-Adresse angegeben wird, verwendet MDaemon diese für den SMTP-Befehl "`MAIL From`" "Nachricht von:") während des Protokolldialogs mit der Gegenstelle. Normalerweise wird für diesen Befehl die Absenderadresse verwendet. Soll der SMTP-Befehl eine leere Adresse übermitteln ("`MAIL FROM <>`"), so ist hier "[trash]" einzugeben.

Port (Voreinstellung = 25)
MDaemon übermittelt die weitergeleiteten Nachrichten über den hier angegebenen TCP-Port. Die Voreinstellung beträgt 25.

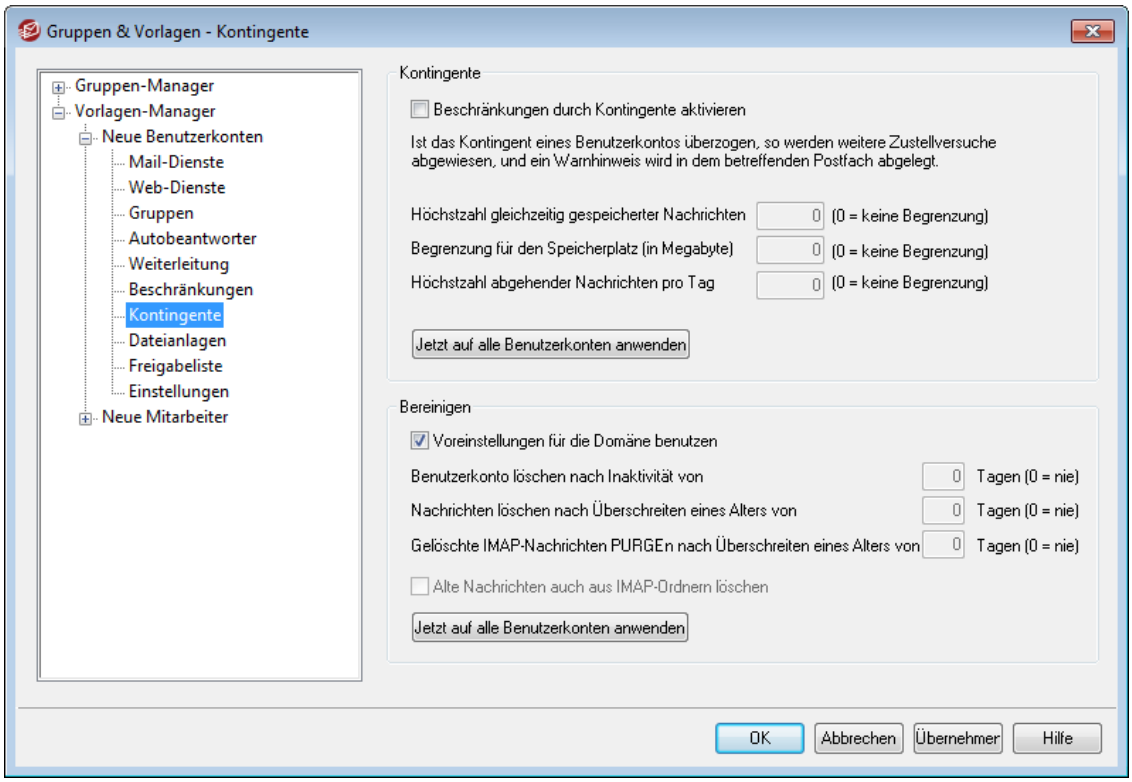
Lokale Kopien weitergeleiteter Nachrichten aufbewahren
Mit dieser Option wird festgelegt, ob MDaemon eine Kopie jeder weitergeleiteten Nachricht im Postfach des Benutzers für den späteren Abruf behalten soll.

Zeitplan
Durch Anklicken dieses Steuerelements können Sie einen Zeitplan für die Weiterleitung der Nachrichten aus diesem Benutzerkonto erstellen. Sie können Beginn und Ende der Weiterleitung mit Datum und Uhrzeit bestimmen, und Sie können die Wochentage auswählen, an denen die Weiterleitung aktiv ist.

Siehe auch:

Vorlagen-Eigenschaften 789
Gruppen-Eigenschaften 784
Vorlage "Neue Benutzerkonten" 788
Benutzerkonten-Editor » Weiterleitung 727

5.2.2.1.6 Kontingente



Die Optionen in diesem Abschnitt der Vorlagen-Eigenschaften entsprechen den Optionen im Abschnitt Kontingente 731 des Benutzerkonten-Editors. Ist eine Vorlage so konfiguriert, dass sie die Kategorie der Einstellungen steuert 789, die in diesem Abschnitt enthalten sind, so steuert sie die Einstellungen für die Kontingente jedes Benutzerkontos, das Mitglied einer Gruppe 784 ist, mit der diese Vorlage verknüpft ist.

Kontingente

Beschränkungen durch Kontingente aktivieren
Hier werden die Voreinstellungen für die Höchstzahl der Nachrichten, die im Postfach eines durch diese Vorlage gesteuerten Benutzerkontos abgelegt sein dürfen, den höchstzulässigen Speicherplatz, den die Benutzerkonten belegen dürfen (dieser Wert schließt alle entpackten und dekodierten Dateianlagen in den Dokumentenverzeichnissen der Benutzerkonten ein) und die Höchstzahl der Nachrichten getroffen, die die Benutzerkonten pro Tag über SMTP versenden dürfen. Würde die Zustellung einer Nachricht das Kontingent für ein Benutzerkonto überschreiten, so werden die Nachricht abgewiesen und eine entsprechende Warnnachricht im Posteingang des Benutzers abgelegt. Würde der Abruf von Nachrichten über MultiPOP 739 das Kontingent überschreiten, so erhält der Benutzer eine entsprechende Warnnachricht; gleichzeitig werden die

MultiPOP-Einträge für das Benutzerkonto abgeschaltet. Sie bleiben aber in der Datenbank erhalten.

Mithilfe der Option *Benutzer warnen, sobald ihr Kontingent zu folgendem Prozentsatz ausgeschöpft ist* im Menü "Benutzerkonten » Benutzerkonten-Optionen » Kontingente 805" erhalten Benutzer eine Warnnachricht, wenn sie sich der Grenze ihres Kontingents nähern. Wird das Kontingent für Höchstzahl der Nachrichten oder höchstzulässigen Speicherplatz zu mehr als dem dort festgelegten Prozentsatz ausgeschöpft, so erhält das betroffene Benutzerkonto um Mitternacht eine Warnnachricht. In ihr sind die Zahl der gespeicherten Nachrichten sowie der belegte Speicherplatz und die Prozentzahl, zu der das Kontingent ausgeschöpft ist, enthalten. Wird im Posteingang des Benutzers bereits eine Warnnachricht gefunden, so wird sie aktualisiert.

Höchstzahl gleichzeitig gespeicherter Nachrichten
Diese Option bestimmt, wie viele Nachrichten höchstens gleichzeitig für die Benutzerkonten gespeichert werden dürfen. Der Wert 0 bewirkt, dass die Zahl der Nachrichten nicht begrenzt wird.

Begrenzung für den Speicherplatz (in Megabyte)
Diese Option bestimmt, wieviel Speicherplatz die Benutzerkonten höchstens belegen dürfen, wobei auch alle Dateianlagen in den Dokumentenverzeichnissen der Benutzerkonten einbezogen werden. Der Wert 0 bewirkt, dass der Speicherplatz für die Benutzerkonten nicht beschränkt wird.

Höchstzahl abgehender Nachrichten pro Tag
Diese Option bestimmt, wie viele Nachrichten die Benutzerkonten täglich höchstens über SMTP versenden dürfen. Ist die Höchstzahl für ein Benutzerkonto erreicht, so werden alle weiteren Nachrichten abgewiesen, bis der Zähler um Mitternacht zurückgesetzt wird. Der Wert 0 bewirkt, dass die Benutzerkonten in der Zahl der Nachrichten, die sie täglich versenden dürfen, nicht begrenzt sind.

Jetzt auf alle Benutzerkonten anwenden

Dieses Steuerelement steht nur in der Vorlage "Neue Benutzerkonten" 788 zur Verfügung. Durch Anklicken dieses Steuerelements werden die Einstellungen aus diesem Konfigurationsdialog auf alle bestehenden MDaemon-Benutzerkonten übertragen, deren Einstellungen für Kontingente nicht durch eine Vorlage für Benutzerkonten gesteuert werden.

Bereinigen

Die Einstellungen in diesem Abschnitt legen fest, ob und wann ein durch diese Vorlage gesteuertes Benutzerkonto durch MDaemon gelöscht wird, falls es inaktiv wird. Es kann außerdem angegeben werden, ob alte Nachrichten, die zu einem Benutzerkonto gehören, nach einer gewissen Zeit gelöscht werden. Jeden Tag um Mitternacht löscht MDaemon alle Nachrichten, die die gesetzte Altersgrenze überschritten haben. Falls ein Benutzerkonto die Inaktivitätsgrenze erreicht hat, wird es durch MDaemon vollständig gelöscht.

Voreinstellungen für die Domäne benutzen
Die Voreinstellungen für die Bereinigung werden nach Domänen getrennt festgelegt und sind über den Konfigurationsdialog Optionen 211 des Domänen-Managers zugänglich. Falls Sie für die Voreinstellungen einer Domäne für Benutzerkonten ersetzen wollen, die durch eine Vorlage gesteuert werden, deaktivieren Sie diese Option, und tragen Sie in die folgenden Einstellungen die gewünschten Werte ein.

Benutzerkonto automatisch löschen nach Inaktivität von [xx] Tagen (0 = nie)
Hier ist anzugeben, wie lange ein Benutzerkonto inaktiv sein darf, bevor es gelöscht wird. Der Wert 0 bewirkt, dass Benutzerkonten nicht wegen Inaktivität gelöscht werden.

Nachrichten löschen nach Überschreiten eines Alters von [xx] Tagen (0 = nie)
Dieser Wert bestimmt, wie viele Tage lang eine Nachricht im Postfach eines Benutzers liegen darf, bevor sie gelöscht wird. Der Wert 0 bewirkt, dass die Nachrichten nicht wegen ihres Alters gelöscht werden. **Beachte:** Diese Option wirkt auf die Nachrichten in IMAP-Ordnern nur dann, wenn Sie auch die Option "*Alte Nachrichten auch aus IMAP-Ordnern löschen*" weiter unten aktivieren.

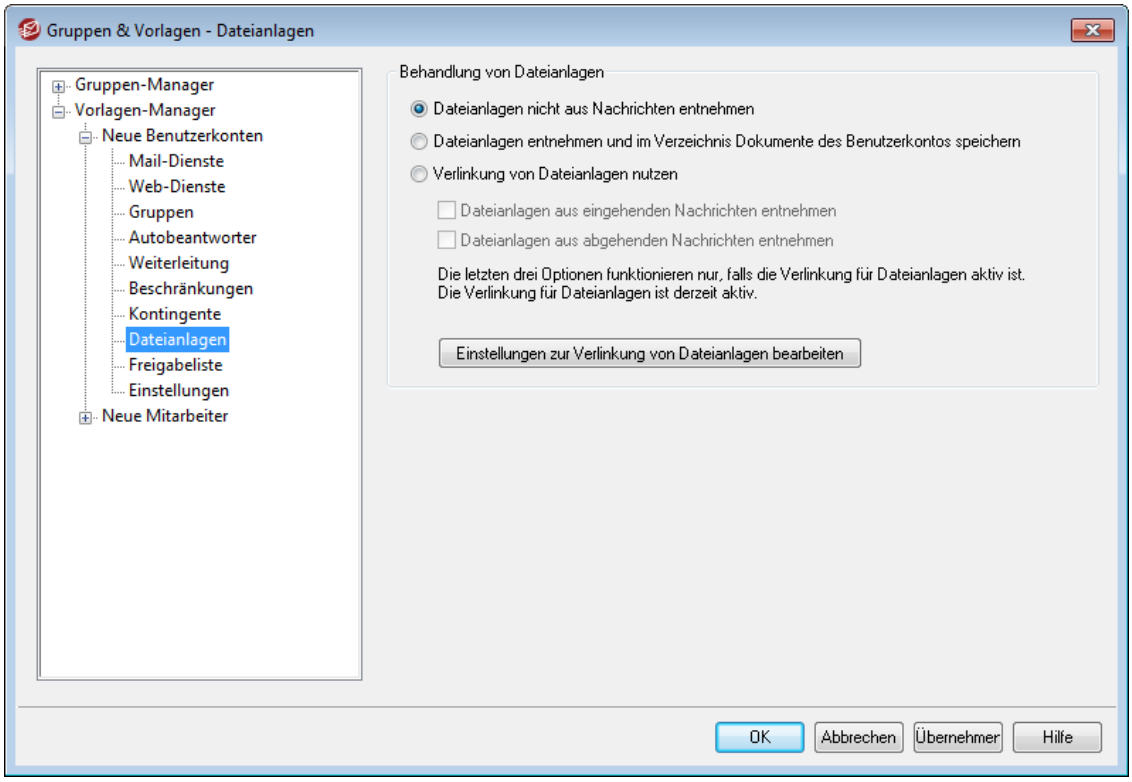
Gelöschte IMAP-Nachrichten entfernen nach Überschreiten eines Alters von [xx] Tagen (0 = nie)
Diese Option legt fest, wie lange IMAP-Nachrichten noch in den Benutzerverzeichnissen verbleiben dürfen, nachdem sie zur Löschung vorgemerkt wurden. Nachrichten, bei denen die hier angegebene Grenze überschritten ist, werden aus den Postfächern gelöscht. Der Wert 0 bedeutet, dass zur Löschung vorgemerkte Nachrichten nicht wegen ihres Alters gelöscht werden.

Alte Nachrichten auch aus IMAP-Ordnern löschen
Diese Option bewirkt, dass die Option "*Nachrichten löschen nach Überschreiten eines Alters von [xx] Tagen*" weiter oben auch auf Nachrichten in IMAP-Ordnern wirkt. Ist diese Option abgeschaltet, dann werden normale Nachrichten in IMAP-Ordnern nicht wegen Überschreitens eines Höchstalters gelöscht.

Siehe auch:

Vorlagen-Eigenschaften 789
Gruppen-Eigenschaften 784
Vorlage "Neue Benutzerkonten" 788
Benutzerkonten-Editor » Kontingente 731
Benutzerkonten-Optionen » Kontingente 852

5.2.2.1.7 Dateianlagen



Die Optionen in diesem Abschnitt der Vorlagen-Eigenschaften entsprechen den Optionen im Abschnitt Dateianlagen[734] des Benutzerkonten-Editors. Ist eine Vorlage so konfiguriert, dass sie die Kategorie der Einstellungen steuert[789], die in diesem Abschnitt enthalten sind, so steuert sie die Einstellungen für die Dateianlagen jedes Benutzerkontos, das Mitglied einer Gruppe[784] ist, mit der diese Vorlage verknüpft ist.

Behandlung von Dateianlagen

Dateianlagen nicht aus Nachrichten entnehmen
Diese Option bewirkt, dass Dateianlagen nicht aus den Nachrichten der durch diese Vorlage gesteuerten Benutzerkonten entnommen werden. Nachrichten, die Dateianlagen enthalten, werden normal verarbeitet, und an den Dateianlagen werden keine Änderungen vorgenommen.

Dateianlagen entnehmen und im Verzeichnis Dokumente des Benutzerkontos speichern
Diese Option bewirkt, dass MDaemon automatisch alle Dateianlagen, die als Base64 in MIME-Nachrichten eingebunden sind, aus den eingehenden Nachrichten für die durch die Vorlage gesteuerten Benutzerkonten entnimmt. Die entnommenen Dateianlagen werden aus der eingehenden Nachricht entfernt, dekodiert und im Dokumentenordner des jeweiligen Benutzerkontos abgelegt. In den Nachrichtentext wird dann ein Hinweis eingefügt, der über die Namen der entnommenen Dateien Auskunft gibt. Eine Verknüpfung mit der gespeicherten Dateianlage wird nicht eingefügt; die Benutzer können aber auf ihre Dokumentenordner mithilfe von Webmail[317] zugreifen.

Verlinkung von Dateianlagen nutzen
Um die Leistungsmerkmale zur Verlinkung von Dateianlagen in eingehenden und abgehenden Nachrichten zu nutzen, aktivieren Sie diese Option.

Falls diese Option aktiv ist, das Leistungsmerkmal Verlinkung von Dateianlagen im Konfigurationsdialog Verlinkung von Dateianlagen[364] aber abgeschaltet ist, werden keine Dateianlagen entnommen.

Dateianlagen aus eingehenden Nachrichten entnehmen
Ist diese Option aktiv, so werden Dateianlagen aus eingehenden Nachrichten solcher Benutzerkonten entnommen, deren Einstellungen diese Vorlage steuert. Die entnommenen Dateianlagen werden an dem Speicherort abgelegt, der im Konfigurationsdialog Verlinkung von Dateianlagen[364] festgelegt ist. In den Nachrichtentext werden URL-Verknüpfungen eingefügt; der Benutzer kann durch Anklicken dieser Verknüpfungen die entnommenen Dateianlagen abrufen. Aus Sicherheitsgründen enthalten diese Verknüpfungen keine direkt zugänglichen Dateipfade. Stattdessen enthalten sie eindeutige Kennzeichnungen (GUID), mit deren Hilfe der Server die Verknüpfung der jeweiligen Datei zuordnen kann. Die Zuordnungstabelle für die GUID wird in der Datei `AttachmentLinking.dat` gespeichert.

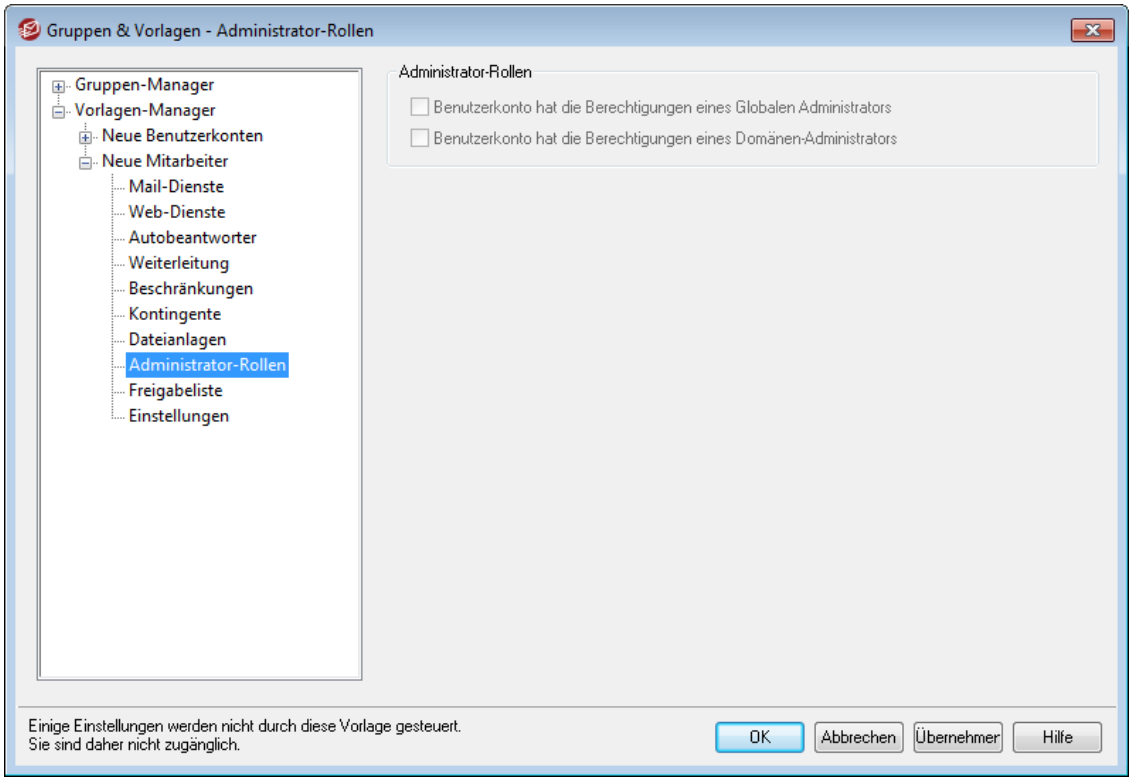
Dateianlagen aus abgehenden Nachrichten entnehmen
Ist diese Option aktiv, so werden Dateianlagen aus abgehenden Nachrichten solcher Benutzerkonten entnommen, deren Einstellungen diese Vorlage steuert. Versendet ein solches Benutzerkonto eine Nachricht mit Dateianlage, so wird die Dateianlage aus der Nachricht entnommen und gespeichert. In den Nachrichtentext wird eine URL-Verknüpfung eingefügt, mit deren Hilfe die Datei abgerufen werden kann.

Einstellungen zur Verlinkung von Dateianlagen bearbeiten
Durch Anklicken dieses Steuerelements können Sie den Konfigurationsdialog Verlinkung von Dateianlagen[364] aufrufen.

Siehe auch:

Vorlagen-Eigenschaften[789]
Gruppen-Eigenschaften[784]
Vorlage "Neue Benutzerkonten"[788]
Verlinkung von Dateianlagen[717]
Benutzerkonten-Editor » Dateianlagen[734]

5.2.2.1.8 Administrator-Rollen



Administrator-Rollen

Benutzerkonto hat die Berechtigungen eines Globalen Administrators
Diese Option gibt den Benutzern Zugriffsrechte und Berechtigungen als Administratoren für das gesamte System. Benutzer mit Berechtigungen als globale Administratoren haben im einzelnen folgende Rechte:

- Vollzugriff auf alle Einstellungen des Servers, alle Benutzer und alle Domänen, jeweils über die Remoteverwaltung
- Zugriff auf alle MDaemon-Benutzer aller MDaemon-Domänen als Kontakte ("Buddies") für Instant-Messaging
- Berechtigung zur Veröffentlichung auch in Mailinglisten, die nur für Lesebetrieb konfiguriert sind
- Berechtigung zur Veröffentlichung in allen Mailinglisten, ohne Mitglied zu sein

Ein so berechtigter Benutzer hat uneingeschränkten Zugriff auf alle Dateien und Einstellungen von MDaemon. Der Abschnitt Remoteverwaltung 350 enthält eine genaue Beschreibung der einzelnen Berechtigungsstufen für Administratoren.

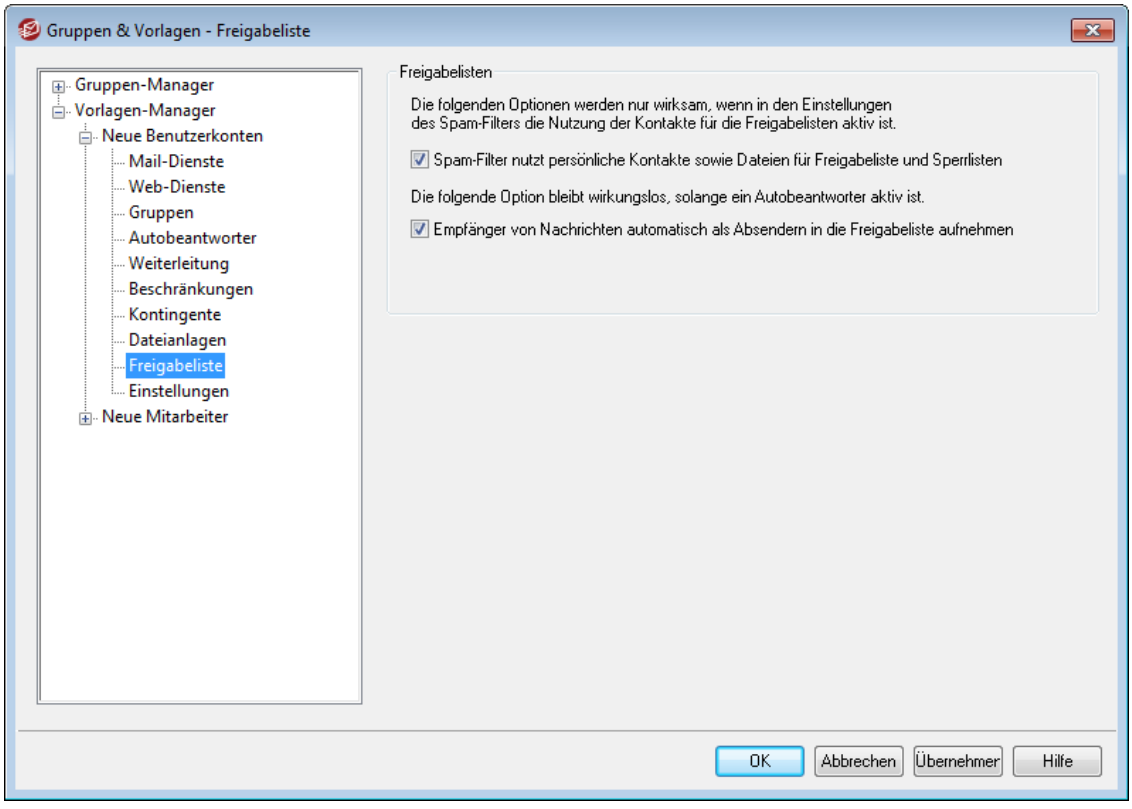
Benutzerkonto hat die Berechtigungen eines Domänen-Administrators
Diese Option gibt den Benutzern die Zugriffsrechte und Berechtigungen eines Domänen-Administrators. Diese Rechte ähneln denen der globalen Administratoren, sind aber auf die Domäne beschränkt, für die der Administrator die Administratorrechte hat, und sie sind auf die Rechte beschränkt, die ihm im Abschnitt Web-Dienste 720 zugewiesen sind. Der Abschnitt Remoteverwaltung 350 enthält weitere Informationen zu Domänen-Administratoren.

Die Optionen für die Administrator-Rollen stehen in der Vorlage für neue Benutzerkonten[788] nicht zur Verfügung. Administrator-Rollen und Administratorrechte können neuen Benutzerkonten nicht automatisch zugewiesen werden. Um einem Benutzerkonto Administratorrechte zuzuweisen, muss das Benutzerkonto mit einer benutzerdefinierten Vorlage verknüpft werden, in der dieser Abschnitt zur Verfügung steht und entsprechend konfiguriert ist. Alternativ kann das Benutzerkonto auch einzeln bearbeitet werden; die entsprechenden Berechtigungsoptionen stehen im Abschnitt Administrator-Rollen[757] des Benutzerkonten-Editors zur Verfügung.

Siehe auch:

Vorlagen-Eigenschaften[789]
Gruppen-Eigenschaften[784]
Vorlage "Neue Benutzerkonten"[788]
Benutzerkonten-Editor » Administrator-Rollen[757]

5.2.2.1.9 Freigabeliste



Die Optionen in diesem Konfigurationsdialog entsprechen den Optionen im Abschnitt Freigabeliste[758] des Benutzerkonten-Editors. Werden die Optionen durch eine Vorlage gesteuert[789], so legt die Vorlage die Einstellungen für die Freigabelisten aller Benutzerkonten fest, die Mitglied einer Gruppe[784] sind, mit der diese Vorlage verknüpft ist.

Freigabelisten

Spam-Filter nutzt persönliche Kontakte sowie Dateien für Freigabeliste und Sperrlisten
Im Abschnitt Freigabeliste (automatisch) 692 des Konfigurationsdialogs für den Spam-Filter ist eine Option enthalten, die systemweit wirkt, und die bestimmt, ob der Spam-Filter eine Nachricht automatisch als Treffer auf der Freigabeliste behandelt, falls der Absender der Nachricht in den persönlichen Kontakten oder der persönlichen Freigabeliste des lokalen Empfängers enthalten ist. Die Option bewirkt auch, dass eine Nachricht automatisch als Treffer auf der Sperrliste behandelt wird, falls ihr Absender in der Sperrliste des Benutzers gefunden wird. Die hier vorliegende Option steuert dieses Verhalten für das gerade bearbeitete Benutzerkonto. Falls die systemweite Option in der Konfiguration des Spam-Filters aktiv ist, aber nicht auf dieses Benutzerkonto wirken soll, müssen Sie diese Option hier deaktivieren. Falls die systemweite Option abgeschaltet ist, ist die vorliegende Option nicht verfügbar.

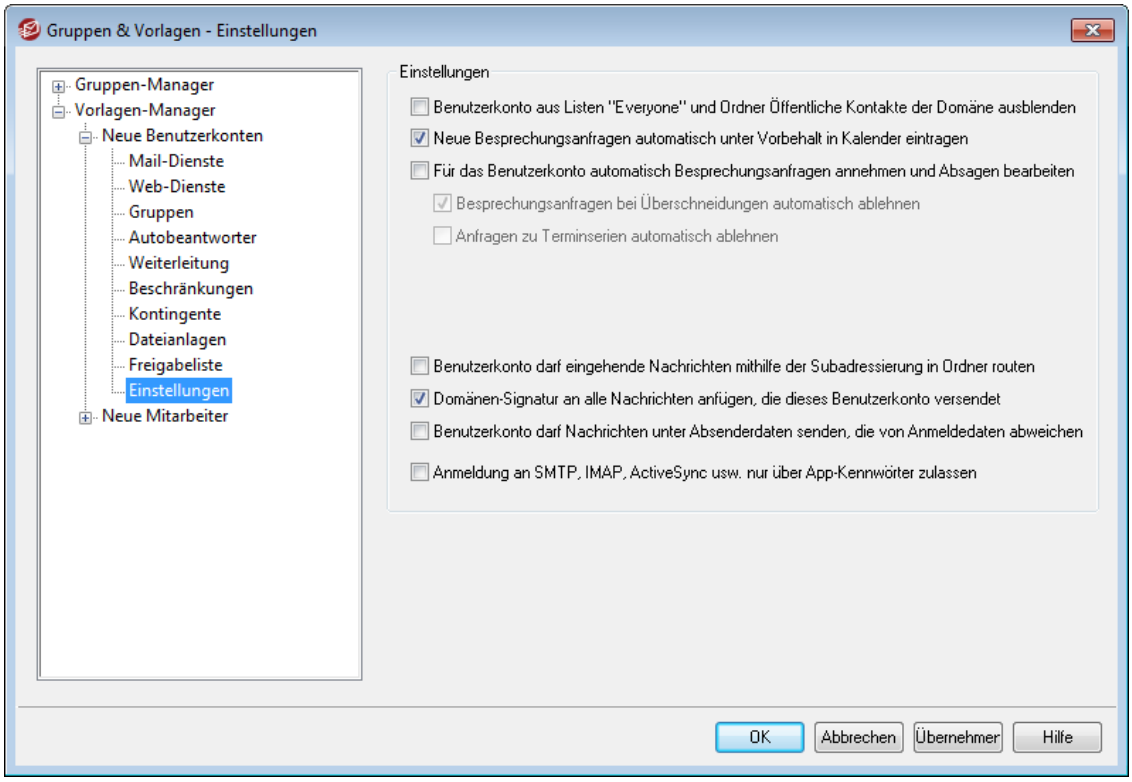
Empfänger von Nachrichten automatisch als Absendern in die Freigabeliste aufnehmen
Diese Option bewirkt, dass der Ordner Freigegebene Absender dieses Benutzerkontos immer dann aktualisiert wird, wenn das Benutzerkonto eine abgehende Nachricht an eine externe Empfängeradresse sendet. Zusammen mit der Option *Spam-Filter nutzt persönliche Kontakte sowie Dateien für Freigabeliste und Sperrlisten* weiter oben kann diese Option die Anzahl der falschen positiven Treffer des Spam-Filters erheblich verringern. Diese Option steht aber nur zur Verfügung, falls die Option *Empfänger von Nachrichten automatisch als Absendern in die Freigabeliste aufnehmen* im Abschnitt Freigabeliste (automatisch) 692 ebenfalls aktiv ist.

So lange für das Benutzerkonto ein Autobeantworter aktiv ist, ist diese Funktion automatisch gesperrt.

Siehe auch:

Vorlagen-Eigenschaften 789
Gruppen-Eigenschaften 784
Vorlage "Neue Benutzerkonten" 788
Benutzerkonten-Editor » Freigabeliste 758

5.2.2.1.10 Einstellungen



Die Optionen in diesem Abschnitt der Vorlagen-Eigenschaften entsprechen den Optionen im Abschnitt Einstellungen 760 des Benutzerkonten-Editors. Ist eine Vorlage so konfiguriert, dass sie die Einstellungen dieses Konfigurationsdialogs steuert 789, die in diesem Abschnitt enthalten sind, so steuert sie die Einstellungen jedes Benutzerkontos, das Mitglied einer Gruppe 784 ist, mit der diese Vorlage verknüpft ist.

Einstellungen

Benutzerkonto aus Listen "Everyone" und Ordner Öffentliche Kontakte der Domäne ausblenden
MDaemon erstellt automatisch eine Mailingliste mit Namen Everyone@<Domänenname> für jede Domäne; sie können benutzt werden, um alle Benutzer der jeweiligen Domäne anzusprechen. MDaemon nimmt grundsätzlich alle Benutzerkonten in die Liste auf. Diese Einstellung bewirkt, dass die durch diese Vorlage gesteuerten Benutzerkonten aus den genannten Mailinglisten ausgeblendet werden. Die Benutzerkonten erscheinen dann auch nicht in den freigegebenen oder gemeinsam genutzten Kalendern und den Ergebnismeldungen für den Befehl VRFY 94.

Neue Besprechungsanfragen automatisch unter Vorbehalt in Kalender eintragen
Diese Option bewirkt, dass Termine aus Besprechungsanfragen nach dem Eingang bei den Empfängern automatisch unter Vorbehalt in die Kalender der Empfänger der Besprechungsanfragen eingetragen werden. Diese Option ist per Voreinstellung aktiv. Deaktivieren Sie diese Option, falls Sie nicht wünschen, dass diese Option als Voreinstellung für neue Benutzerkonten genutzt wird.

Für das Benutzerkonto automatisch Besprechungsanfragen annehmen und Absagen bearbeiten
Diese Option bewirkt, dass Besprechungsanfragen, Aktualisierungen für Termine, sowie Absagen für die durch diese Vorlage gesteuerten Benutzerkonten automatisch verarbeitet werden. Erhält ein Benutzerkonto eine Besprechungsanfrage, so wird der Kalender automatisch aktualisiert. Diese Option ist per Voreinstellung für alle Benutzerkonten abgeschaltet.

Besprechungsanfragen bei Überschneidungen automatisch ablehnen
Ist die Option zum Automatischen Bearbeiten von Besprechungsanfragen aktiv, so bewirkt diese Option, dass Besprechungsanfragen immer dann automatisch abgelehnt werden, wenn sie eine Überschneidung oder einen Konflikt mit einem bereits bestehenden Termin verursachen würde. Ist die Option nicht aktiv, so wird auch eine Besprechungsanfrage angenommen, wenn dies einen Terminkonflikt hervorruft.

Anfragen zu Terminserien automatisch ablehnen
Diese Option bewirkt, dass Besprechungsanfragen, die Terminserien zum Gegenstand haben, automatisch abgelehnt werden. Andere Besprechungsanfragen werden so behandelt, wie es die vorstehenden Optionen vorsehen.

Benutzerkonto darf eingehende Nachrichten mithilfe der Subadressierung in Ordner routen
Diese Option gestattet den durch diese Vorlage gesteuerten Benutzerkonten die Nutzung der Subadressierung 762.

Domänen-Signatur an alle Nachrichten anfügen, die dieses Benutzerkonto versendet
Ist für die Benutzerkonten einer Domäne eine Domänen-Signatur 202 definiert, dann bewirkt diese Option, dass die Domänen-Signatur abgehenden Nachrichten solcher Benutzerkonten hinzugefügt wird, deren Einstellungen durch diese Vorlage gesteuert werden.

Benutzerkonto darf Nachrichten unter Absenderdaten senden, die von Anmeldedaten abweichen
Diese Option bewirkt, dass Benutzerkonten, deren Einstellungen durch diese Vorlage gesteuert werden, von der Anwendung der systemweiten Option "*Anmeldedaten für Echtheitsbestätigung müssen mit Benutzerkonto des Absenders übereinstimmen*" ausgenommen sind. Die systemweite Option ist über den Konfigurationsdialog SMTP-Echtheitsbestätigung 524 zugänglich.

Anmeldung an SMTP, IMAP, ActiveSync usw. nur über App-Kennwörter zulassen
Diese Option bewirkt, dass die Benutzerkonten in E-Mail-Clients, für die Anmeldung an SMTP, IMAP, ActiveSync und anderen E-Mail-Diensten App-Kennwörter 750 verwenden müssen. Die normalen Kennwörter 847 der Benutzerkonten müssen für die Anmeldung an Webmail oder der MDaemon-Remoteverwaltung weiterhin genutzt werden.

Wenn Sie die Nutzung von App-Kennwörtern für die genannten Anwendungsfälle erzwingen, so kann dies helfen, das Kennwort für ein Benutzerkonto gegen Brute-Force-Angriffe über SMTP, IMAP und andere Dienste zu schützen. Die Sicherheit ist in diesem Fall erhöht, da selbst bei Bekanntwerden des Kennworts für das Benutzerkonto ein Angriff über die genannten Dienste nicht möglich wäre. Ein Angreifer würde dabei nicht einmal erkennen, dass das Kennwort für das Benutzerkonto entdeckt wurde, da MDaemon für die Anmeldung an den

genannten Diensten nicht das Kennwort des Benutzerkontos sondern nur ein gültiges App-Kennwort akzeptiert. Ein weiterer Vorteil ergibt sich bei der Echtheitsbestätigung mithilfe des Active Directory. Benutzerkonten im Active Directory 815 werden nach einer bestimmten Anzahl fehlerhafter Anmeldeversuche automatisch gesperrt. Die Nutzung der App-Kennwörter kann solche Sperren verhindern, da MDaemon bei aktivierter Option nur die App-Kennwörter prüft, aber keine Echtheitsbestätigung über das Active Directory versucht.

Siehe auch:

Vorlagen-Eigenschaften 789
Gruppen-Eigenschaften 784
Vorlage "Neue Benutzerkonten" 788
Benutzerkonten-Editor » Einstellungen 760

5.3 Einstellungen für Benutzerkonten

5.3.1 Active Directory

Die Optionen im Konfigurationsdialog Active Directory (erreichbar über `Benutzerkonten » Benutzerkonten-Optionen » Active Directory`) steuern die Überwachung des Active Directorys durch MDaemon. MDaemon kann Benutzerkonten automatisch anlegen, aktualisieren, löschen und sperren, wenn die zugehörigen Benutzerkonten im Active Directory geändert werden. Darüber hinaus kann MDaemon alle öffentlichen Kontakte mit den jeweils aktuellen im Active Directory gespeicherten Informationen versorgen. Oft genutzte Datenfelder wie Postanschrift, Telefon-Nummern, geschäftliche Kontaktdaten und weitere Datenfelder der Benutzerkonten können in dieser Weise in die öffentlichen Kontakte übertragen und nach jeder Änderung im Active Directory auch in den öffentlichen Kontakten aktualisiert werden.

Anlegen von Benutzerkonten

Im Rahmen der Überwachung des Active Directorys sucht MDaemon in festgelegten Abständen nach Änderungen. Wird ein neues Benutzerkonto im Active Directory gefunden, so legt MDaemon automatisch ein neues Benutzerkonto an. Dieses neue MDaemon-Benutzerkonto enthält Vor- und Nachnamen, Anmeldenamen, Postfachnamen und Beschreibung des Benutzerkontos sowie den Status aktiv oder gesperrt aus dem Active Directory.

MDaemon fügt neue Benutzerkonten, die aufgrund von Änderungen im Active Directory erstellt werden, grundsätzlich der Standard-Domäne hinzu. Wahlweise können diese Benutzerkonten stattdessen der Domäne zugewiesen werden, die im Active-Directory-Attribut "`UserPrincipalName`" (Benutzerprinzipalname) des Benutzerkontos eingetragen ist. Bei Nutzung dieser Option erstellt MDaemon automatisch eine neue Domäne 181, falls ein Benutzerkonto einer Domäne zugewiesen werden soll, die in MDaemon noch nicht besteht.

Sie können stattdessen Ihren *Suchfilter* 818 so konfigurieren, dass er eine Gruppe im Active Directory überwacht. Wird ein Benutzer in diese Gruppe aufgenommen, oder wird die Gruppenmitgliedschaft einem Benutzerkonto hinzugefügt, so wird dieser Benutzer in MDaemon angelegt. Wird der Benutzer aus der Gruppe entfernt, so wird das Benutzerkonto in MDaemon deaktiviert, aber nicht gelöscht.

Löschen von Benutzerkonten

Wird ein Benutzerkonto aus dem Active Directory gelöscht, so kann MDaemon wahlweise die folgenden Aktionen ausführen: keine Aktion, Löschen des zugehörigen MDaemon-Kontos, Sperren des zugehörigen MDaemon-Kontos, oder Einfrieren des zugehörigen MDaemon-Kontos (in diesem Fall kann das Benutzerkonto Nachrichten noch empfangen, der Benutzer kann sie aber nicht abrufen oder sonst auf das Benutzerkonto zugreifen).

Aktualisieren von Benutzerkonten

Erkennt MDaemon Änderungen an Benutzerkonten im Active Directory, so werden die geänderten Daten automatisch in die zugehörigen MDaemon-Benutzerkonten übernommen.

Abgleich der MDaemon-Benutzerdatenbank mit dem Active Directory

Mithilfe der Option "*Vollständigen AD-Abgleich jetzt durchführen*" wird MDaemon veranlasst, das Active Directory vollständig zu durchsuchen und die MDaemon-Benutzerkonten an die Benutzerkonten des Active Directorys anzupassen. Werden dabei Active-Directory-Benutzerkonten gefunden, die zu bestehenden MDaemon-Benutzerkonten passen, so werden die MDaemon-Konten entsprechend verknüpft. Änderungen im Active Directory, die nach einem solchen Abgleich vorgenommen werden, übernimmt MDaemon automatisch in die MDaemon-Benutzerdatenbank.

Echtheitsbestätigung über das Active Directory

Benutzerkonten, die durch Abgleich mit dem Active Directory erstellt werden, sind per Voreinstellung auf die Echtheitsbestätigung über das Active Directory (AD) konfiguriert. Dabei speichert MDaemon die Kennwörter für die Benutzerkonten nicht in der eigenen Benutzerdatenbank: Stattdessen nutzt der Inhaber des MDaemon-Benutzerkontos die Anmeldedaten seines Windows-Benutzerkontos. MDaemon leitet diese zur Echtheitsbestätigung an Windows weiter.

Die AD-Echtheitsbestätigung funktioniert nur, wenn in dem entsprechenden Feld im Abschnitt Überwachung[821] der Name einer Windows-Domäne eingetragen ist. MDaemon lässt die Echtheitsbestätigung anhand der dort eingetragenen Windows-Domäne durchführen. In den meisten Fällen erkennt MDaemon die Windows-Domäne automatisch und trägt sie in das Feld ein. Falls gewünscht, kann aber auch eine andere Domäne von Hand eingetragen werden. Soll die Echtheitsbestätigung nicht nur auf eine einzelne Windows-Domäne beschränkt sein sondern alle erreichbaren Windows-Domänen umfassen, muss der Eintrag "`NT_ANY`" gewählt werden. Bleibt dieses Feld leer, so konfiguriert MDaemon neue Benutzerkonten nicht für die dynamische Echtheitsbestätigung. MDaemon erzeugt stattdessen ein Zufallskennwort, das der Systemverwalter von Hand bearbeiten muss, bevor der Benutzer auf das E-Mail-Konto zugreifen kann.

Durchgehende Überwachung

Das Active Directory wird auch dann überwacht, wenn MDaemon gerade nicht ausgeführt wird. Alle Änderungen am Active Directory werden verfolgt und durch MDaemon nach dem folgenden Programmstart verarbeitet.

Datensicherheit für das Active Directory

Die Funktionen zur Überwachung des Active Directorys, die MDaemon bereit stellt, ändern oder beeinflussen die Schema-Dateien des Active Directorys nicht. MDaemon überwacht das Active Directory nur lesend und verändert darin keine Daten.

Vorlage für das Active Directory

MDaemon nutzt für alle Änderungen an Benutzerkonten, die sich aus der Überwachung des Active Directorys ergeben, eine Vorlage ("\app\ActiveDS.dat"), mit deren Hilfe die Namen bestimmter Active-Directory-Attribute den Namen der Felder in den MDaemon-Benutzerkonten zugeordnet werden. MDaemon verknüpft beispielsweise per Voreinstellung das Active-Directory-Attribut "cn" mit dem MDaemon-Feld "FullName". Diese Verknüpfungen sind aber nicht fest vorgegeben; sie können durch Bearbeiten der Vorlage mit einem Texteditor einfach geändert werden. So kann etwa die genannte Voreinstellung "FullName=%cn%" durch "FullName=%givenName% %sn%" ersetzt werden. Nähere Informationen hierzu finden Sie in der Datei ActiveDS.dat.

Aktualisierung der öffentlichen Adressbücher

Mithilfe der Funktionen zur Überwachung des Active Directorys kann das Active Directory in bestimmten Intervallen abgefragt werden; die Ergebnisse dieser Abfrage können dann dazu benutzt werden, alle öffentlichen Kontakte in MDaemon mit den jeweils neuesten Daten zu aktualisieren. Oft genutzte Datenfelder wie Postanschrift, Telefon-Nummern, geschäftliche Kontaktdaten und weitere Datenfelder der Benutzerkonten können in dieser Weise in die öffentlichen Kontakte übertragen und nach jeder Änderung im Active Directory auch in den öffentlichen Kontakten aktualisiert werden. Um dieses Leistungsmerkmal zu nutzen, aktivieren Sie die Option "*Active Directory überwachen und öffentliche Adressbücher aktualisieren*" im Konfigurationsdialog Active Directory » Überwachung 821.

Dieses Leistungsmerkmal kann zahlreiche Datenfelder der Kontakte überwachen. Eine vollständige Übersicht der Datenfelder in öffentlichen Kontakten, die den Attributen im Active Directory zugeordnet werden können, ist in der Datei ActiveDS.dat enthalten. In diese Datei wurden mehrere neue Vorlagen für die Zuordnung von Attributen im Active Directory aufgenommen, mit deren Hilfe die Attribute genutzt werden können, um bestimmte Datenfelder in den Kontaktinformationen zu füllen. So stehen etwa %fullName% für das Feld Vor- und Nachname, %streetAddress% für die Postanschrift und andere zur Verfügung.

Damit MDaemon feststellen kann, welcher Eintrag in die Kontakte anhand der Attribute eines Active-Directory-Benutzers aktualisiert werden soll, muss die E-Mail-Adresse des Kontakts mit der im Active Directory hinterlegten Adresse übereinstimmen, und MDaemon muss diese Übereinstimmung feststellen können. Falls MDaemon keine Übereinstimmung feststellen kann, können auch keine Datenfelder aktualisiert werden. Per Voreinstellung nutzt MDaemon die Daten aus dem Attribut, das in der Datei ActiveDS.dat der Vorlage für das Postfach zugeordnet ist. MDaemon fügt an diese Daten den Namen der Standard-Domäne 181 an; die Erstellung der Adresse folgt demselben Schema wie bei der Erstellung und dem Löschen von MDaemon-Benutzerkonten auf Grundlage der Daten aus dem Active Directory. Falls dies nicht gewünscht ist, kann auch die Vorlage "abMappingEmail" in der Datei ActiveDS.dat durch Entfernen der Kommentarzeichen aktiviert werden; diese Vorlage kann jedem beliebigen Attribut im Active Directory zugeordnet werden, etwa %mail%. In allen Fällen muss aber sichergestellt sein, dass MDaemon aus dem gewünschten Attribut eine E-Mail-Adresse entnehmen kann, die zu einem gültigen lokalen Benutzerkonto gehört.

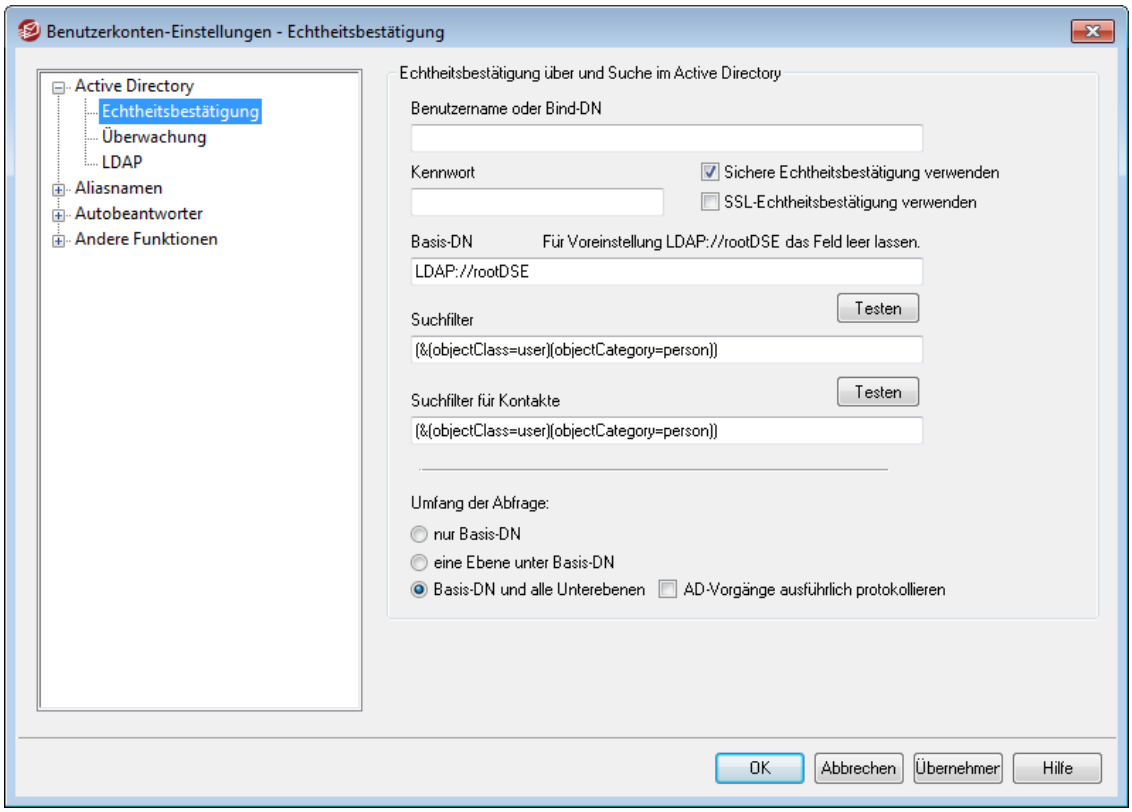
Dieses Leistungsmerkmal erstellt Kontakte automatisch, falls sie noch nicht bestehen, und aktualisiert die bereits bestehenden Kontakte. Änderungen, die außerhalb des Active Directory direkt an den Benutzerkonten vorgenommen werden, gehen bei diesem Vorgang verloren. Datenfelder der Kontakte, die keinem Attribut zugeordnet sind, bleiben unverändert; auch bestehende Daten in solchen Feldern

werden nicht verändert und gehen nicht verloren. Für MDaemon-Benutzerkonten, die als aus bestimmtem Listen ausgeblendet[760] gekennzeichnet sind, werden die Einträge in den Kontakten weder automatisch erstellt noch aktualisiert.

Siehe auch:

Active Directory » Überwachung[821]
Active Directory » Echtheitsbestätigung[818]

5.3.1.1 Echtheitsbestätigung



Für den Zugriff auf das Active Directory sind zur Nutzung aller verfügbaren Leistungsmerkmale unter Umständen besondere Berechtigungen erforderlich, die gesondert eingerichtet werden müssen.

Echtheitsbestätigung über und Suche im Active Directory

Benutzername oder Bind-DN
Hier wird der Windows-Benutzername oder der eindeutige Gesamtname (englisch "Distinguished Name", kurz DN) angegeben, den MDaemon bei der Verbindung mit dem Active Directory über LDAP verwenden soll. Das Active Directory gestattet die Nutzung eines Windows-Anmeldenamens oder eines Benutzerprinzipalnamens (UPNs) für diese Verbindung.

Wird statt eines Windows-Anmeldenamens ein DN angegeben, so muss die Option "*Sichere Echtheitsbestätigung verwenden*" weiter unten abgeschaltet sein.

Kennwort
Hier wird das Kennwort zu dem DN oder Windows-Anmeldenamen aus dem Feld *Bind-DN* angegeben.

Sichere Echtheitsbestätigung verwenden
Diese Option bewirkt, dass beim Verbindungsaufbau zum Active Directory die sichere Echtheitsbestätigung verwendet wird. Diese Option darf nicht verwendet werden, wenn im Feld *Bind-DN* statt eines Windows-Anmeldenamens ein DN eingetragen ist.

SSL-Echtheitsbestätigung verwenden
Diese Option bewirkt, dass bei Verbindungen zum Active Directory die Echtheitsbestätigung durch eine SSL-Verbindung geschützt sein soll.

Diese Option erfordert einen SSL-Server und eine entsprechende Infrastruktur im Windows-Netzwerk und dem Active Directory. Falls Unsicherheiten bestehen, ob diese Infrastruktur vorhanden ist, und diese Option genutzt werden soll, empfiehlt es sich, diese Fragen mit dem Netzwerkverwalter zu klären.

Attribut für die E-Mail-Adresse
MDaemon nutzt dieses Attribut für die Mailinglisten. Es ist nur über den Konfigurationsdialog Active Directory im Editor für Mailinglisten 299 zugänglich.

Suche im Active Directory

Basis-DN
Hier wird der DN eingetragen. Er stellt den Ausgangspunkt im Verzeichnisbaum (englisch "Directory Information Tree", kurz DIT) dar, von dem aus MDaemon das Active Directory auf Benutzerkonten und Änderungen durchsucht. MDaemon beginnt die Suche grundsätzlich beim Root-DSE, also auf der höchsten Ebene der Active-Directory-Struktur. Wird hier stattdessen ein Ausgangspunkt angegeben, der näher an der Struktur der Benutzerkonten in dem jeweils verwendeten Active-Directory-Verzeichnisbaum liegt, so kann dies die Zeit verringern, die zum Durchsuchen des DIT nach Benutzerkonten und Änderungen benötigt wird. Bleibt das Feld leer, so wird die Voreinstellung `LDAP://rootDSE` verwendet.

Suchfilter
Hier wird der LDAP-Suchfilter eingetragen, der bei der Abfrage des Active Directorys auf Benutzerkonten und Änderungen eingesetzt wird. Mithilfe dieses Filters lassen sich die Benutzerkonten, die in die Überwachung des Active Directorys einbezogen werden sollen, genauer eingrenzen.

Sie können stattdessen Ihren Suchfilter so konfigurieren, dass er eine Gruppe im Active Directory überwacht. Wird ein Benutzer in diese Gruppe aufgenommen, oder wird die Gruppenmitgliedschaft einem Benutzerkonto hinzugefügt, so wird

dieser Benutzer in MDaemon angelegt. Wird der Benutzer aus der Gruppe entfernt, so wird das Benutzerkonto in MDaemon deaktiviert, aber nicht gelöscht. Ein Beispiel hierzu: Ein Suchfilter für eine Gruppe mit dem Namen "MeineGruppe" kann folgendermaßen aussehen:

```
(|(&(ObjectClass=group)(cn=MyGroup))(&(objectClass=user)
(objectCategory=person)
(memberof=cn=MeineGruppe,ou=me,dc=domain,dc=com)))
```

Für die Attribute "ou=" und "dc=" müssen Sie die für Ihr Netzwerk zutreffenden Werte einsetzen.

Suchfilter für Kontakte
Hiermit können Sie einen gesonderten Suchfilter für die Abfrage von Kontakten anlegen. Falls Sie in dieses Feld denselben Suchfilter eintragen wie in die Option *Suchfilter* weiter oben, werden die Daten insgesamt mit nur einer Abfrage aktualisiert. Sind unterschiedliche Suchfilter konfiguriert, dann sind zwei getrennte Abfragen erforderlich.

Umfang der Abfrage:

Dieser Abschnitt steuert den Umfang, in dem das Active Directory durchsucht wird.

nur Basis-DN
Diese Option bewirkt, dass die Abfragen auf den oben angegebenen Basis-DN begrenzt bleiben. Unterhalb dieser Stelle werden keine Abfragen im Verzeichnisbaum (DIT) durchgeführt.

eine Ebene unter Basis-DN
Diese Option bewirkt, dass die Suche im Verzeichnisbaum des Active Directory auf eine Ebene unter dem oben angegebenen DN erstreckt wird.

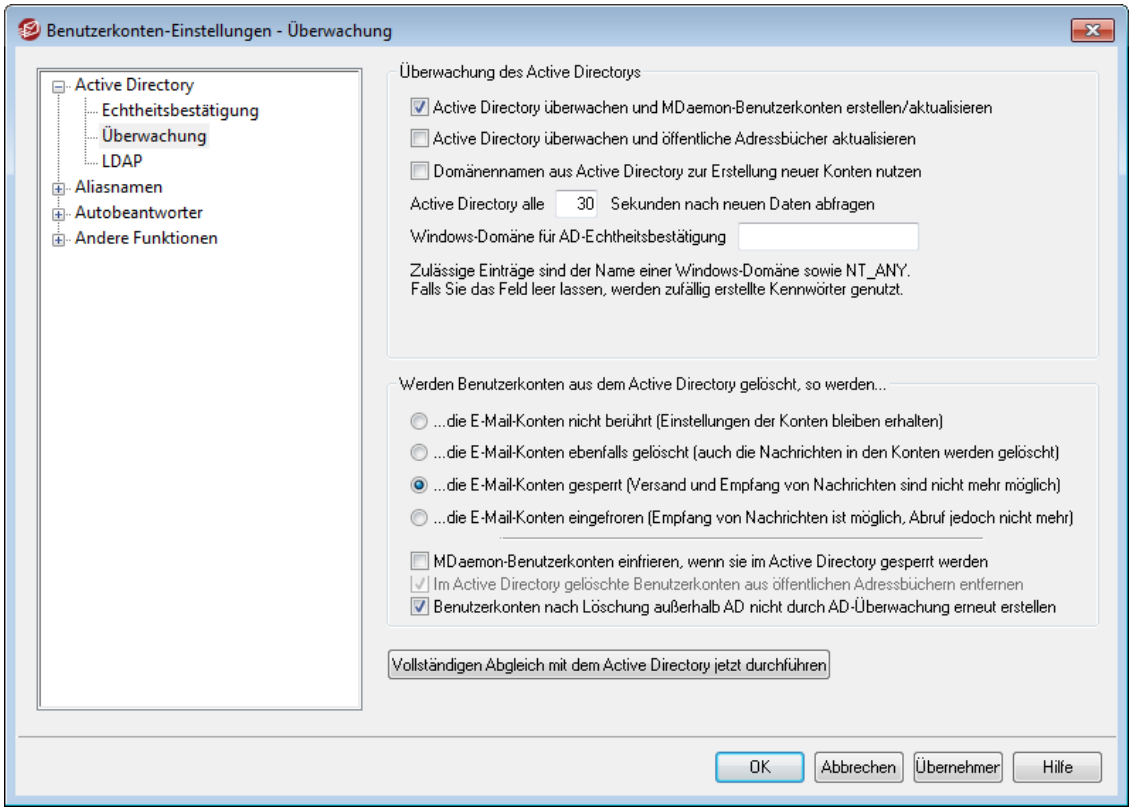
Basis-DN und alle Unterebenen
Diese Option bewirkt, dass die Suche von dem angegebenen DN auf alle Unterebenen im Verzeichnisbaum erstreckt wird. Dies ist die Voreinstellung. Gemeinsam mit der Voreinstellung Root-DSE, die weiter oben beschrieben ist, bewirkt sie, dass der gesamte Verzeichnisbaum unterhalb des Root-DSE durchsucht wird.

AD-Vorgänge ausführlich protokollieren
MDaemon protokolliert die Active-Directory-Transaktionen per Voreinstellung ausführlich. Ist ein weniger ausführliches Protokoll über die Active-Directory-Transaktionen gewünscht, so muss diese Option abgeschaltet werden.

Diese Einstellungen testen

Durch Anklicken dieses Steuerelements wird die Active-Directory-Konfiguration von MDaemon auf Funktionsfähigkeit geprüft.

5.3.1.2 Überwachung



Überwachung des Active Directorys

Active Directory überwachen und MDaemon-Benutzerkonten erstellen/aktualisieren
Diese Option bewirkt, dass das Active Directory überwacht wird. MDaemon-Benutzerkonten werden aufgrund der Änderungen im Active Directory erstellt und aktualisiert.

Active Directory überwachen und öffentliche Adressbücher aktualisieren
Diese Option bewirkt, dass mithilfe des Active Directorys alle Einträge in den öffentlichen Adressbüchern mit den jeweils aktuellsten Informationen aus dem Active Directory aktualisiert werden. Häufig benutzte Felder wie Postanschrift, Telefonnummern, geschäftliche Kontaktdaten und andere Datenfelder werden beim ersten Abgleich und nach jeder Änderung im Active Directory in die öffentlichen Kontakteinträge überführt. In dieser Weise können zahlreiche Datenfelder der Kontakte überwacht werden. Eine vollständige Liste der Datenfelder in den öffentlichen Kontakten, die Attributen im Active Directory zugeordnet werden können, ist in der Datei `ActiveDS.dat` enthalten. Weitere Informationen hierzu finden Sie im Abschnitt Aktualisierung der öffentlichen Adressbücher 817.

Domänennamen aus Active Directory zur Erstellung neuer Konten nutzen
Diese Option bewirkt, dass neue Benutzerkonten, die aufgrund der Überwachung des Active Directorys erstellt werden, der Domäne zugewiesen werden, die im Active-Directory-Attribut "`UserPrincipalName`" (Benutzerprinzipalname) eingetragen ist. Bei Nutzung dieser Option legt MDaemon automatisch eine neue Domäne 181 an, falls ein Benutzerkonto einer noch nicht bestehenden Domäne zugewiesen werden soll. Ist diese Option abgeschaltet, so werden neue Benutzerkonten nur der Standard-Domäne 181 von MDaemon zugewiesen.

Active Directory alle [xx] Sekunden nach neuen Daten abfragen
Hier wird das Intervall angegeben, in dem MDaemon das Active Directory auf Änderungen untersucht.

Windows-Domäne für die dynamische Echtheitsbestätigung
Falls neue Benutzerkonten, die aufgrund der Überwachung des Active Directorys angelegt wurde, auf dynamische Echtheitsbestätigung konfiguriert werden sollen, muss die Windows-Domäne, anhand derer die Echtheitsbestätigung durchgeführt werden soll, hier angegeben werden. Bleibt dieses Feld leer, so erhalten neue Benutzerkonten zufällig erzeugte Kennwörter. Diese müssen von Hand nachbearbeitet werden, bevor die Benutzer Zugriff auf ihre Konten erhalten.

Werden Benutzerkonten aus dem Active Directory gelöscht, so werden...
Die folgenden Optionen bestimmen, wie MDaemon verfahren soll, falls ein Active-Directory-Konto, das einem MDaemon-Benutzerkonto zugeordnet ist, aus dem Active Directory gelöscht wird.

...die E-Mail-Konten nicht berührt (Einstellungen der Konten bleiben erhalten)
Diese Option bewirkt, dass MDaemon keine Änderungen an dem MDaemon-Benutzerkonto vornimmt.

...die E-Mail-Konten ebenfalls gelöscht (auch die Nachrichten in den Konten werden gelöscht)
Diese Option bewirkt, dass MDaemon das MDaemon-Benutzerkonto löscht, nachdem das Konto aus dem Active Directory gelöscht wurde.

Hierdurch wird das MDaemon-Benutzerkonto vollständig gelöscht. Alle Nachrichten, Ordner, Adressbücher, Kalender und sonstigen Daten des Benutzerkontos gehen verloren.

...die E-Mail-Konten gesperrt (Versand und Empfang von Nachrichten sind nicht mehr möglich)
Diese Option bewirkt, dass das MDaemon-Benutzerkonto gesperrt wird, nachdem das zugehörige Active-Directory-Benutzerkonto gelöscht wurde. Das MDaemon-Benutzerkonto besteht dann zwar noch auf dem Server, es kann aber weder Nachrichten senden noch empfangen, und es ist gegen Zugriffe von Benutzern gesperrt.

...die E-Mail-Konten eingefroren (Empfang von Nachrichten ist möglich, Abruf jedoch nicht mehr)
Diese Option bewirkt, dass MDaemon eingehende Nachrichten für das Benutzerkonto noch annimmt, das Benutzerkonto aber gegen Zugriffe des Benutzers sperrt. Die eingehenden Nachrichten gehen dabei nicht verloren, der Kontoinhaber kann sie aber nicht abrufen und auch sonst auf das Benutzerkonto nicht zugreifen, so lange es eingefroren ist.

MDaemon-Benutzerkonten einfrieren, wenn sie im Active Directory gesperrt werden
Werden Benutzerkonten im Active Directory gesperrt, so sperrt MDaemon per Voreinstellung auch die zugehörigen E-Mail-Konten. Die Benutzerkonten sind dann gegen Zugriffe gesperrt, und MDaemon stellt keine Nachrichten von dem gesperrten und an das gesperrte Konto zu. Soll nach einer Sperre im Active Directory das zugehörige MDaemon-Konto stattdessen eingefroren werden, so muss diese Option aktiv sein. Nach Einfrieren des Kontos nimmt MDaemon

eingehende Nachrichten für das Konto noch an, der Kontoinhaber kann die Nachrichten aber nicht abrufen und auch sonst nicht auf das Benutzerkonto zugreifen.

Im Active Directory gelöschte Benutzerkonten aus öffentlichen Adressbüchern entfernen
Per Voreinstellung werden Kontakte aus den öffentlichen Adressbüchern und Kontaktordnern gelöscht, wenn das zugehörige Benutzerkonto aus dem Active Directory gelöscht wird. Dies trifft aber nur dann zu, wenn der Kontakt auch ursprünglich auch durch die Leistungsmerkmale der Active-Directory-Integration 817 erstellt wurde. Falls Sie nicht wünschen, dass die Kontakte gelöscht werden, wenn die zugehörigen Benutzerkonten aus dem Active Directory gelöscht werden, deaktivieren Sie diese Option.

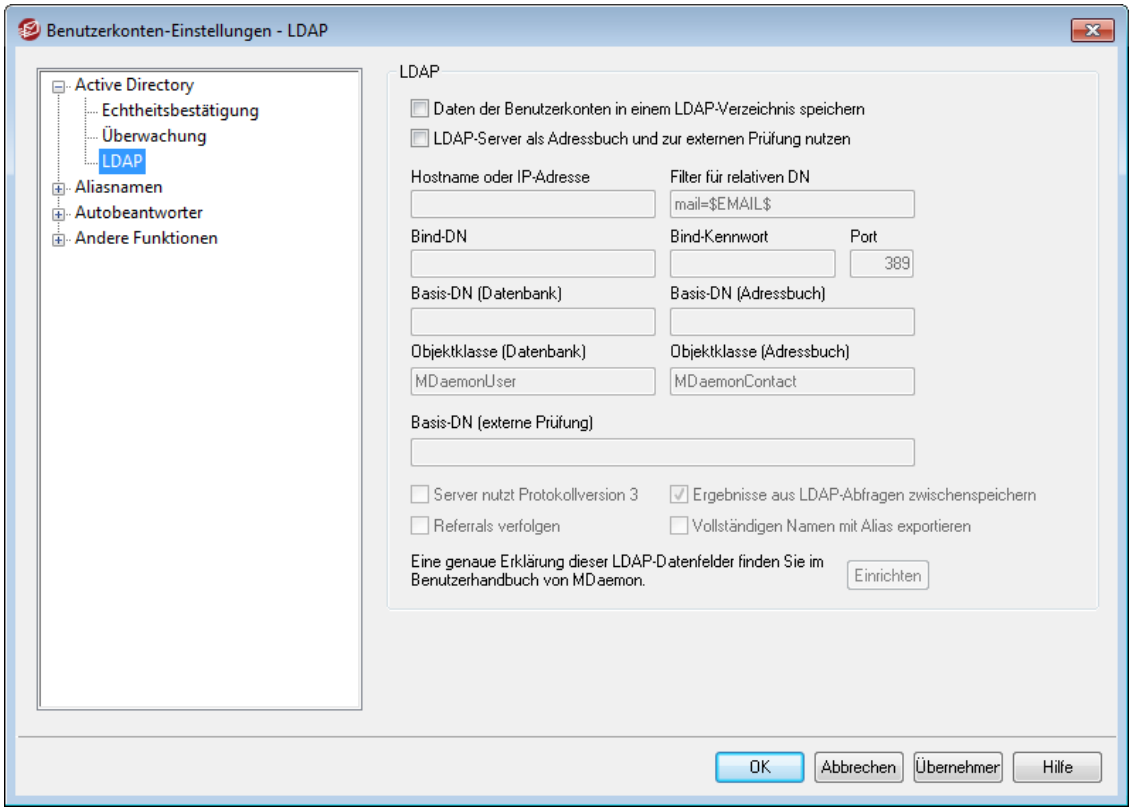
Benutzerkonten nach Löschung außerhalb AD nicht durch AD-Überwachung erneut erstellen
Wenn Sie ein MDaemon-Benutzerkonto außerhalb des Active Directorys direkt löschen (beispielsweise über die Benutzeroberfläche von MDaemon), dann wird dieses Benutzerkonto per Voreinstellung durch die Active-Directory-Überwachung nicht erneut erstellt. Falls Sie solche manuell gelöschten Benutzerkonten aufgrund des Active-Directory-Abgleichs erneut erstellen lassen wollen, deaktivieren Sie diese Option.

Vollständigen Abgleich mit dem Active Directory jetzt durchführen
Ein Klick auf dieses Steuerelement bewirkt, dass MDaemon das gesamte Active Directory abfragt und Benutzerkonten, in Übereinstimmung mit den Ergebnissen der Abfrage, anlegt, aktualisiert oder löscht. Werden Benutzerkonten im Active Directory gefunden, die zu bestehenden MDaemon-Benutzerkonten passen, so werden sie mit diesen verknüpft.

Siehe auch:

Active Directory 815
Active Directory » Echtheitsbestätigung 818

5.3.1.3 LDAP



MDaemon unterstützt Leistungsmerkmale des Lightweight Directory Access Protocol (LDAP). Sie erreichen den Konfigurationsdialog für die LDAP-Leistungsmerkmale über "Benutzerkonten » Benutzerkonten-Einstellungen » ActiveD Directory » LDAP". Sie können MDaemon so konfigurieren, dass MDaemon Daten über alle Benutzerkonten an einen LDAP-Server übermittelt und aktuell hält. MDaemon übermittelt dazu jedes Mal Daten an den LDAP-Server, wenn ein MDaemon-Benutzerkonto hinzugefügt oder gelöscht wird. Benutzer, deren Mailclients ebenfalls LDAP unterstützen, können so auf ein systemweites Adressbuch mit Einträgen über alle lokalen MDaemon-Benutzer und aller anderen Kontakte, die Sie hinzufügen, zurückgreifen.

Sie können den LDAP-Server auch als Benutzerdatenbank für MDaemon 841 verwenden. Sie benötigen dann nicht die Benutzerdatenbank in Form der Datei `USERLIST.DAT` oder einer ODBC-kompatiblen Datenbank. Diese Art der Benutzerverwaltung ist besonders nützlich, wenn Sie MDaemon-Server an verschiedenen Standorten betreiben, die alle auf dieselbe Benutzerdatenbank zugreifen sollen. Jeder MDaemon-Server in einer solchen Infrastruktur kann dann auf denselben LDAP-Server zugreifen und die Informationen zentral und nicht mehr lokal speichern.

LDAP

Benutzerdaten in einem LDAP-Verzeichnis speichern
Mit dieser Option verwendet MDaemon statt einer ODBC-Datenbank oder der lokal abgelegten Datei `USERLIST.DAT` einen LDAP-Server als Benutzerdatenbank. Diese Art der Benutzerverwaltung kann dann sinnvoll sein, wenn mehrere verschiedene MDaemon-Installationen an verschiedenen Standorten bestehen, die sich alle eine einzige Benutzerdatenbank teilen sollen. Dazu müssen die beteiligten MDaemon-Server so konfiguriert werden, dass sie zum Zweck des Austauschs

von Benutzerdaten auf denselben LDAP-Server zugreifen, anstatt die Benutzerdaten lokal zu speichern.

LDAP-Server als Adressbuch und zur externen Prüfung nutzen
Falls Sie eine ODBC-Datenbank oder die Datei `USERLIST.DAT` anstatt eines LDAP-Servers als Benutzerdatenbank verwenden, kann gleichwohl ein LDAP-Server mit den Namen, E-Mail-Adressen und Aliasnamen aller Benutzer des Systems versorgt werden und als systemweites Adressbuch für alle Benutzer dienen, deren Mailclients LDAP unterstützen. Dazu muss diese Option aktiv sein.

Diese Option bewirkt, dass die Datenbank des LDAP-Servers mit den Postfachnamen, Aliasnamen und Mailinglisten des eigenen Systems versorgt und auf dem aktuellen Stand gehalten wird. Diese Datenbank kann dann als Datenquelle für die externe Prüfung von Benutzerdaten dienen. Weitere Informationen hierzu erhalten Sie unter *Basis-DN (externe Prüfung)* weiter unten.

Eigenschaften des LDAP-Servers

Hostname oder IP-Adresse
Der Hostname oder die IP-Adresse des verwendeten LDAP-Servers sind hier einzutragen.

Filter für relativen DN
Diese Einstellung dient dazu, den relativen DN für den LDAP-Eintrag jedes Benutzers zu erzeugen. Der relative DN (RDN) ist der ganz links stehende Teil eines eindeutigen Namens. Alle gleichrangigen Einträge, die von einem gemeinsamen übergeordneten Eintrag abgeleitet sind, müssen jeweils einen eindeutigen RDN haben. Es bietet sich daher an, als RDN die jeweilige E-Mail-Adresse zu verwenden, damit keine Konflikte auftreten können. Hierfür muss das Makro $EMAIL$ ein dieses Feld eingetragen sein (also beispielsweise `mail=$EMAIL$`). Der eindeutige Name eines Benutzers wird aus dem RDN und dem weiter unten definierten *Basis-DN* zusammengesetzt.

Bind-DN
Hier wird der eindeutige Name eingetragen, der auf dem LDAP-Server über Administratorrechte verfügt. MDaemon verwendet ihn, um die Einträge für seine Benutzer auf dem aktuellen Stand zu halten. Dieser DN wird für die Echtheitsbestätigung im Rahmen der Bind-Vorgänge verwendet.

Bind-Kennwort
Dieses Kennwort wird zusammen mit dem *Bind DN* für die Anmeldung beim LDAP-Server genutzt.

Port
Hier wird der Port eingetragen, den der LDAP-Server auf eingehende Verbindungen überwacht. MDaemon verwendet ihn zum Verbindungsaufbau.

Basis-DN (Datenbank)
Hier wird der eindeutige Name (distinguished name, DN) angegeben, der für alle Benutzer von MDaemon gelten soll, wenn ein LDAP-Server statt der Datei `USERLIST.DAT` zur Verwaltung der Benutzerdatenbank eingesetzt wird. Der Basis-DN dient zusammen mit dem RDN (vgl. oben *Filter für relativen DN*) der Erstellung des eindeutigen Namens für jeden einzelnen Benutzer.

Basis-DN (Adressbuch)
Bei der Ausgabe der Benutzerkonten in ein LDAP-gestütztes Adressbuch wird der hier der Basis-DN ("Root-DN") angegeben, der in allen Einträgen der Benutzeradressbücher verwendet wird. Der Basis-DN dient zusammen mit dem RDN (vgl. oben *Filter für relativen DN*) der Erstellung des eindeutigen Namens für jeden einzelnen Benutzer.

Objektklasse (Datenbank)
Hier wird angegeben, welcher Objektklasse die einzelnen Einträge in der Benutzerdatenbank von MDaemon angehören müssen. Die einzelnen Einträge enthalten dann das Attribut `objectclass=` und den angegebenen Wert.

Objektklasse (Adressbuch)
Hier wird angegeben, welcher Objektklasse die einzelnen Einträge in den Adressbüchern der Benutzer von MDaemon angehören müssen. Die einzelnen Einträge enthalten dann das Attribut `objectclass=` und den angegebenen Wert.

Basis-DN (externe Prüfung)
Ein weit verbreiteter Nachteil von Domänen-Gateways und Servern, die als Ausfallsicherung oder "Backup-Server" arbeiten, ist, dass sie üblicherweise nicht feststellen können, ob eine eingehende Nachricht an ein bestehendes Benutzerkonto gerichtet und damit zulässig ist oder nicht. Ein Beispiel hierzu: Trifft bei dem Backup-Server der Domäne example.com eine Nachricht für `user1@example.com` ein, so kann der Backup-Server nicht feststellen, ob auf dem Hauptserver der Domäne example.com tatsächlich ein Benutzerkonto, einen Aliasnamen oder eine Mailingliste für den Namen "`user1`" besteht. Der Backup-Server hat also nur die Möglichkeit, alle eingehenden Nachrichten anzunehmen. MDaemon enthält Funktionen, mit deren Hilfe eine Prüfung solcher Adressen möglich ist und damit das Problem gelöst wird. Durch Angabe eines Basis-DN für externe Prüfung wird der zugehörige LDAP-Server mit Informationen über alle Postfächer, Aliasnamen und Mailinglisten versorgt. Der Backup-Server kann dann bei Eingang einer neuen Nachricht durch Abfrage bei diesem LDAP-Server feststellen, ob die Empfängeradresse gültig ist. Ergibt die Prüfung, dass die Adresse nicht gültig ist, wird die Nachricht abgewiesen.

Server nutzt Protokollversion 3
Diese Option bewirkt, dass für die Prüfung das LDAP-Protokoll der Version 3 genutzt wird.

Referrals verfolgen
Bisweilen ist auf einem LDAP-Server das eigentlich angeforderte Objekt nicht gespeichert; der Server kann aber über einen Verweis auf den Speicherort des Objekts verfügen und den Client dorthin verweisen. Diese Option bewirkt, dass während der Prüfung solche Verweise ausgewertet und verfolgt werden. Sie ist per Voreinstellung deaktiviert.

Ergebnisse aus LDAP-Abfragen zwischenspeichern
Diese Option bewirkt, dass die Ergebnisse der LDAP-Abfragen im Cache zwischengespeichert werden und für einen begrenzten Zeitraum für neue Abfragen zur Verfügung stehen. Diese Option ist per Voreinstellung aktiv. Falls Sie die Ergebnisse nicht zwischenspeichern wollen, deaktivieren Sie diese Option.

Vollständigen Namen mit Alias exportieren
Adressdaten, die keine Daten für Adress-Aliasnamen sind, enthalten beim Export den Vor- und Nachnamen aus dem Benutzerkonto im Feld CN. Bei Adressdaten über Aliasnamen wird in dieses Feld die tatsächliche E-Mail-Adresse des Benutzerkontos (nicht der Aliasname) eingetragen. Falls Sie statt der tatsächlichen Adresse den Vor-und Nachnamen aus dem Benutzerkonto exportieren wollen, aktivieren Sie diese Option. Der Export ist nur möglich, wenn Vor- und Nachname bekannt sind. Diese Option ist per Voreinstellung abgeschaltet.

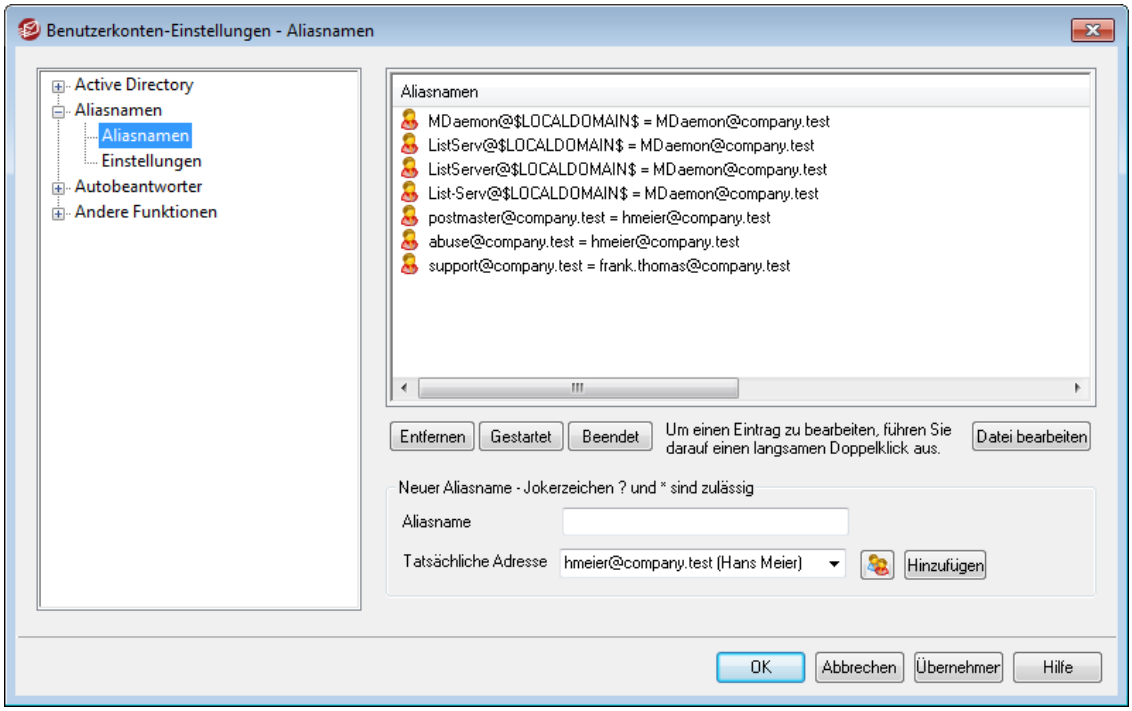
Einrichten
Durch Anklicken dieses Steuerelements wird die Konfigurationsdatei `LDAP.dat` in einem Texteditor geöffnet. In dieser Datei werden die Namen der LDAP-Attribute für die entsprechenden Felder der Benutzerkonten in MDaemon festgelegt.

Siehe auch:

Optionen zur Benutzerdatenbank 841

5.3.2 Aliasnamen

5.3.2.1 Aliasnamen



Mit Aliasnamen lassen sich für Benutzerkonten und Mailinglisten zusätzliche Postfachnamen anlegen. Das ist besonders hilfreich, wenn mehrere Postfachnamen auf dasselbe Benutzerkonto oder dieselbe Mailingliste verweisen sollen. Ohne Aliasnamen müssen getrennte Benutzerkonten für jede Adresse angelegt und die Nachrichten dann weitergeleitet oder durch komplexe Filterregeln in andere Benutzerkonten umgeleitet werden.

Soll z.B. `user1@example.com` alle Anfragen zur Buchhaltung der Domäne bearbeiten, sollen die Anfragen aber an die Adresse `billing@example.com` gerichtet werden

können, so kann ein Aliasname `billing@example.com` eingerichtet werden, der auf `user1@example.com` verweist. Werden mehrere Domänen betrieben und sollen alle Nachrichten an den Postmaster, unabhängig von der Domäne, an den Benutzer `user1@example.com` gehen, so löst ein Aliasname mit einem Jokerzeichen, `Postmaster@*`, der auf das Zielkonto verweist, dieses Problem.

Bestehende Aliasnamen

In dieser Liste erscheinen alle Aliasnamen, die derzeit auf dem System bestehen.

Entfernen
Mithilfe dieses Steuerelements können Sie den ausgewählten Eintrag aus der Liste *Bestehende Aliasnamen* entfernen.

Nach oben
Aliasnamen werden in der Reihenfolge abgearbeitet, in der sie auch in dieser Liste erscheinen. Ein Aliasname kann mit diesem Steuerelement in eine höhere Position verschoben werden.

Nach unten
Aliasnamen werden in der Reihenfolge abgearbeitet, in der sie auch in dieser Liste erscheinen. Ein Aliasname kann mit diesem Steuerelement in eine niedrigere Position verschoben werden.

Datei bearbeiten
Um die Datei `Alias.dat` in einen Texteditor zu laden, klicken Sie auf dieses Steuerelement. Sie können die Datei dann von Hand durchsuchen oder bearbeiten. Nachdem Sie die gewünschten Änderungen vorgenommen haben, schließen Sie den Texteditor; MDaemon lädt die Datei danach neu.

Aliasname
Tragen Sie hier die E-Mail-Adresse ein, die als Aliasname für die weiter unten angegebene *Tatsächliche Adresse* definiert werden soll. Die Jokerzeichen "?" und "*" sind zulässig, außerdem kann "`@$LOCALDOMAIN$`" in dem Aliasnamen als Jokerzeichen für die lokalen Domänen verwendet werden. Einige Beispiele für die zulässige Verwendung dieser Jokerzeichen sind "`user1@example.*`", "`*@$LOCALDOMAIN$`" und "`user1@$LOCALDOMAIN$`".

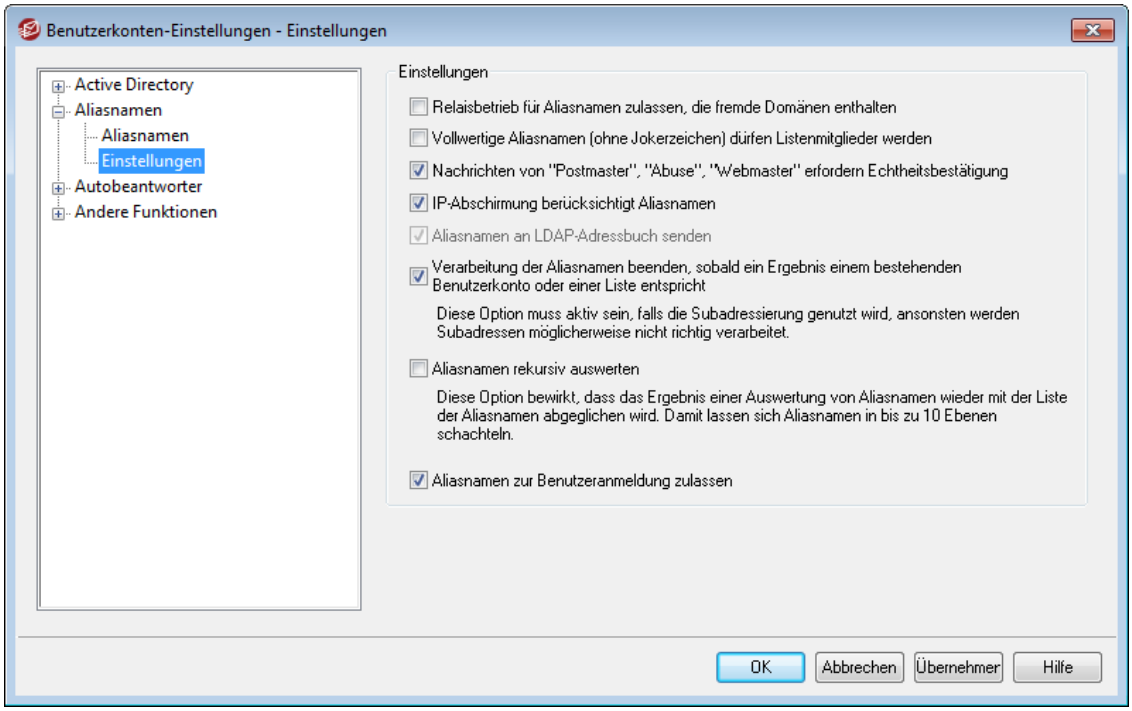
Tatsächliche Adresse
In diesem Feld wählen Sie entweder ein bestehendes Benutzerkonto aus der Liste aus, oder Sie geben eine neue Adresse oder Mailingliste an. Die hier eingetragene Adresse erhält alle Nachrichten, die an den oben angegebenen Aliasnamen gerichtet sind.

Hinzufügen
Durch Anklicken dieses Steuerelements wird der soeben angelegte Adress-Aliasname, bestehend aus dem *Aliasnamen* und der zugehörigen *tatsächlichen Adresse*, als neuer Eintrag in die Liste *Bestehende Aliasnamen* übernommen.

Siehe auch:

Aliasnamen » Einstellungen 829
Benutzerkonten-Editor » Aliasnamen 741

5.3.2.2 Einstellungen



Optionen

Relaisbetrieb für Aliasnamen zulassen, die fremde Domänen enthalten
Diese Option bewirkt, dass MDaemon den Relaisbetrieb für solche Adressen zulässt, die externe Domänen enthalten. Diese Option übergeht die Option *Relaisbetrieb nicht zulassen* im Konfigurationsdialog Relaiskontrolle 513 für solche Aliasnamen.

Vollwertige Aliasnamen (ohne Jokerzeichen) dürfen Listenmitglieder werden
Diese Funktion lässt Adress-Aliasnamen als Mitglieder der Mailinglisten von MDaemon zu. Solange diese Option abgeschaltet ist, können nur wirkliche Benutzerkonten Mitglieder einer Liste werden. **Beachte:** Auch wenn diese Funktion aktiviert ist, können Aliasnamen, die Jokerzeichen enthalten, keinesfalls Listenmitglieder werden.

Nachrichten von "Postmaster", "Abuse", "Webmaster" erfordern Echtheitsbestätigung
Ist diese Option aktiv, so nimmt MDaemon Nachrichten mit den Absenderadressen "postmaster@...", "abuse@..." und "webmaster@..." aus den eigenen Domänen nur dann zur Zustellung an, wenn diese Nachrichten über Verbindungen mit Echtheitsbestätigung übertragen wurden. Spam-Versender und Hacker wissen, dass diese Adressen auf vielen Systemen bestehen, und sie könnten daher versuchen, die Adressen als gefälschte Absenderadressen zu nutzen, um so Nachrichten über den Mailserver zu versenden. Diese Option verhindert solche missbräuchliche Nutzung, und zwar auch durch nicht berechtigte Benutzer der eigenen Domäne. Diese Option ist im Konfigurationsdialog SMTP-Echtheitsbestätigung 524 (Sicherheit » Sicherheits-Einstellungen) gespiegelt. Änderungen an der Einstellung wirken sich auf beide Konfigurationsdialoge aus.

IP-Abschirmung berücksichtigt Aliasnamen
Durch diese Option, die per Voreinstellung aktiv ist, wird die IP-Abschirmung 522 veranlasst, im Rahmen der Prüfung von Domänen/IP-Zuordnungen auf Konflikte

mit der IP-Abschirmung auch Adress-Aliasnamen auszuwerten. Die IP-Abschirmung löst dann die Aliasnamen in die Benutzerkonten auf, auf das sie verweisen. Ist die Option nicht aktiv, so behandelt die IP-Abschirmung jeden Aliasnamen wie eine Adresse, die von dem Benutzerkonto unabhängig ist, auf das er verweist. Ist also die IP-Adresse eines Aliasnamens in der IP-Abschirmung gesperrt, wird die Nachricht abgewiesen. Diese Option ist im Konfigurationsdialog IP-Abschirmung gespiegelt. Änderungen an der Einstellung wirken sich auf beide Konfigurationsdialoge aus.

Aliasnamen an LDAP-Adressbuch senden
Diese Option bewirkt, dass die Aliasnamen auch an das jeweils verwendete LDAP-Adressbuch übermittelt werden. Diese Übermittlung ist nötig, damit die Funktionen zur externen Prüfung bei Gateways zuverlässig arbeitet. Kommt die externe Prüfung nicht zum Einsatz, so ist diese Übermittlung der Aliasnamen an das LDAP-Adressbuch überflüssig. Die Option kann dann ohne Probleme deaktiviert bleiben, um die Verarbeitungsgeschwindigkeit zu erhöhen. Nähere Informationen über die externe LDAP-Prüfung finden Sie im Konfigurationsdialog LDAP 824.

Verarbeitung der Aliasnamen beenden, sobald ein Ergebnis einem bestehenden Benutzerkonto oder einer Liste entspricht
Diese Option bewirkt, dass Aliasnamens dann nicht angewendet werden, wenn sie in Konflikt mit einem bestehenden Benutzerkonto oder einer bestehenden Mailingliste stehen würden. Dieses Vorgehen betrifft üblicherweise Aliasnamen, die Jokerzeichen enthalten. Besteht beispielsweise ein Aliasname "`*@example.com=user1@example.com`", so bewirkt diese Option, dass der Aliasname nur auf Adressen angewendet wird, die auf Ihrem Server nicht bestehen. Besteht auf dem Server etwa ein Benutzerkonto "`user2@example.com`", so werden Nachrichten an "user2" direkt zugestellt, da der Aliasname auf diese Nachrichten nicht wirkt. Nur Nachrichten an nicht bestehende Benutzerkonten oder Mailinglisten würden dann an "`user1@example.com`" gesendet werden; auf diese Adressen wirkt der Aliasname. Diese Option ist per Voreinstellung aktiv.

Falls Sie die Subadressierung 762 nutzen, muss diese Option aktiv sein, sonst können Probleme bei der Verarbeitung subadressierter Nachrichten auftreten.

Aliasnamen rekursiv auswerten
Diese Option bewirkt die rekursive Auswertung von Aliasnamen. Wird sie aktiviert, wird jeder Aliasname, nachdem er verarbeitet und aufgelöst wurde, erneut mit der Liste der Aliasnamen verglichen und ggf. erneut aufgelöst. Aliasnamen können auf diese Weise bis zu 10 Ebenen tief geschachtelt werden. Denkbar wäre daher in etwa das folgende Beispiel:

```
user2@example.com = user1@example.com
zser1@example.com = user5@example.net
user5@example.net = user9@example.org
```

Dies entspricht im Ergebnis dem folgenden Aliasnamen:

```
user2@example.com = user9@example.org
```

Es bedeutet auch folgende Zuordnung:

```
user1@example.com = user9@example.org
```

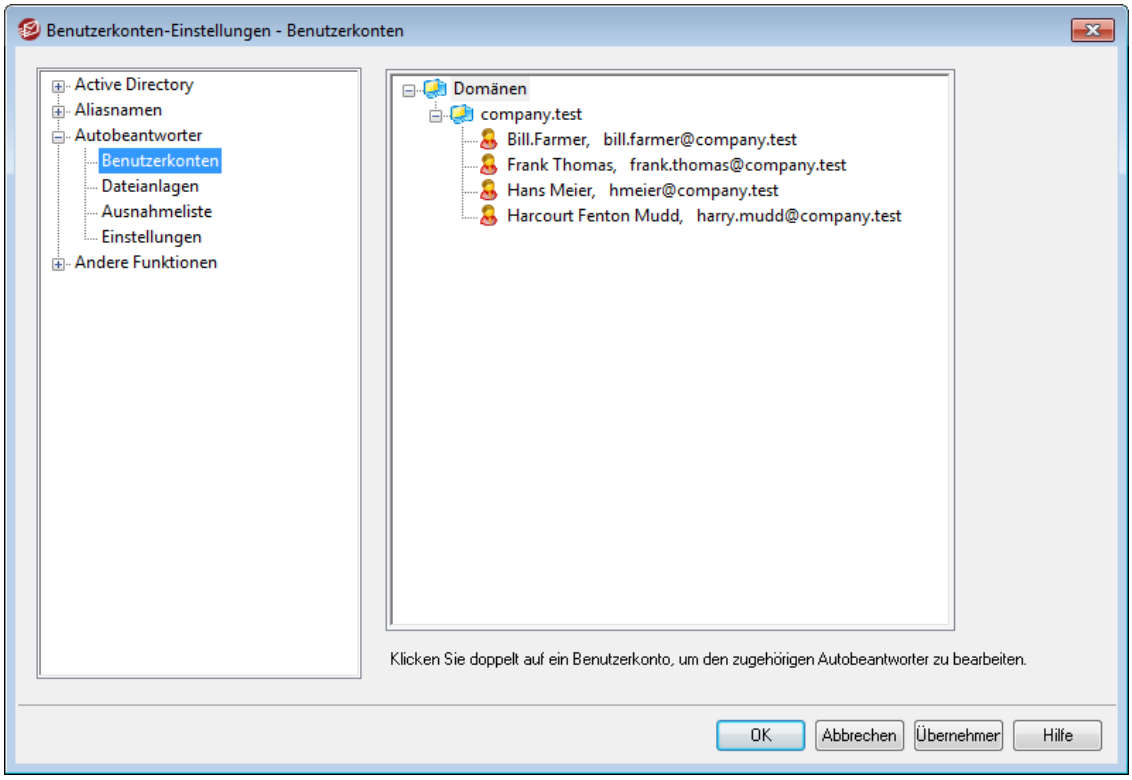
Aliasnamen zur Benutzeranmeldung zulassen
Per Voreinstellung dürfen die Benutzer für die Anmeldung an ihren Benutzerkonten statt ihres tatsächlichen Postfachnamens auch einen Alias[827] nutzen, der ihrem Benutzerkonto zugewiesen ist. Falls Sie die Nutzung der Aliasnamen zur Anmeldung nicht zulassen wollen, deaktivieren Sie diese Option.

Siehe auch:

Aliasnamen[827]

5.3.3 Autobeantworter

5.3.3.1 Benutzerkonten



Autobeantworter sind nützliche Werkzeuge, mit denen Aktionen durch eingehende E-Mail-Nachrichten ausgelöst werden können. Eine weit verbreitete Einsatzmöglichkeit für Autobeantworter ist es, eine benutzerdefinierte Nachricht als "Anrufbeantworter" für abwesende oder anderweit an der Beantwortung eingehender Nachrichten verhinderte Benutzer zu verwenden. Eingehende Post kann mit ihrer Hilfe automatische benutzerdefinierte Antwortnachrichten oder eine Programmausführung auf dem Server auslösen, wobei die Nachricht selbst über die Kommandozeile an das externe Programm übergeben wird. MDaemon-Benutzer mit Web-Zugriff[720] auf Webmail[317] oder die Remoteverwaltung[350] können diese Verwaltungswerkzeuge verwenden, um Nachrichten und Zeitpläne für den Autobeantworter selbst zu erstellen. Nachrichten der Autobeantworter stützen sich auf die Inhalte der Dateien `OOF.mrk`, die in den Verzeichnissen `\data\` unter den jeweiligen Hauptverzeichnissen der Benutzerkonten abgelegt sind. Diese Dateien unterstützen zahlreiche Makros, und die Inhalte der Nachrichten der

Autobeantworter lassen sich hierdurch weitgehend dynamisch gestalten. Autobeantworter sind hierdurch sehr vielseitig einsetzbar.

Nachrichten von externen Absendern lösen Autobeantworter immer aus. Auf Nachrichten von Benutzern derselben Domäne reagieren Autobeantworter nur, falls die Einstellung *Autobeantworter reagieren auf Nachrichten aus eigenen Domänen* im Konfigurationsdialog Autobeantworter » Einstellungen 835 aktiv ist. Dort steht auch eine weitere Option zur Verfügung, die die Anzahl der automatisch erzeugten Antwortnachrichten auf eine Antwort pro Empfänger und Tag begrenzt.

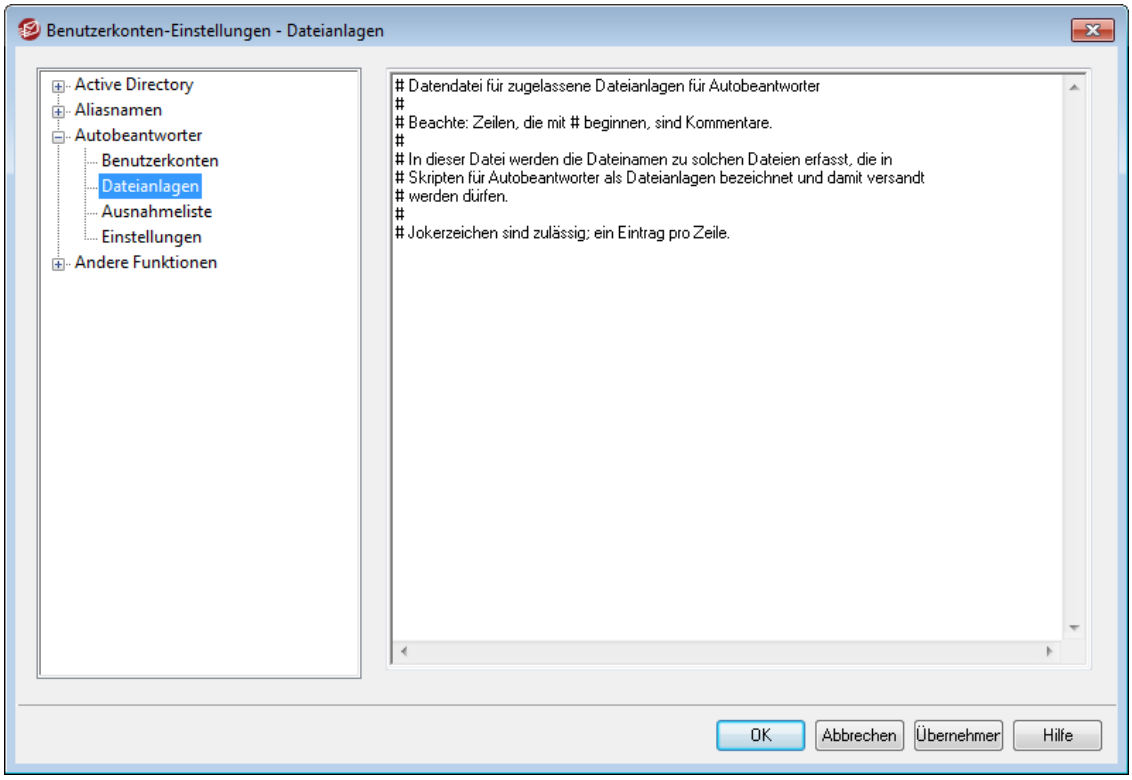
Liste der Benutzerkonten

In diesem Bereich sind alle verfügbaren lokalen Postfächer aufgeführt, für die Autobeantworter eingerichtet werden können. Durch einen Doppelklick auf einen Eintrag öffnen Sie den Konfigurationsdialog Autobeantworter 724 des zugehörigen Benutzerkontos; dort können Sie die Autobeantworter für dieses Benutzerkonto konfigurieren.

Siehe auch:

Autobeantworter » Ausnahmeliste 834
Autobeantworter » Einstellungen 835
Erstellung von Skripten für Autobeantworter 836
Benutzerkonten-Editor » Autobeantworter 724

5.3.3.2 Dateianlagen

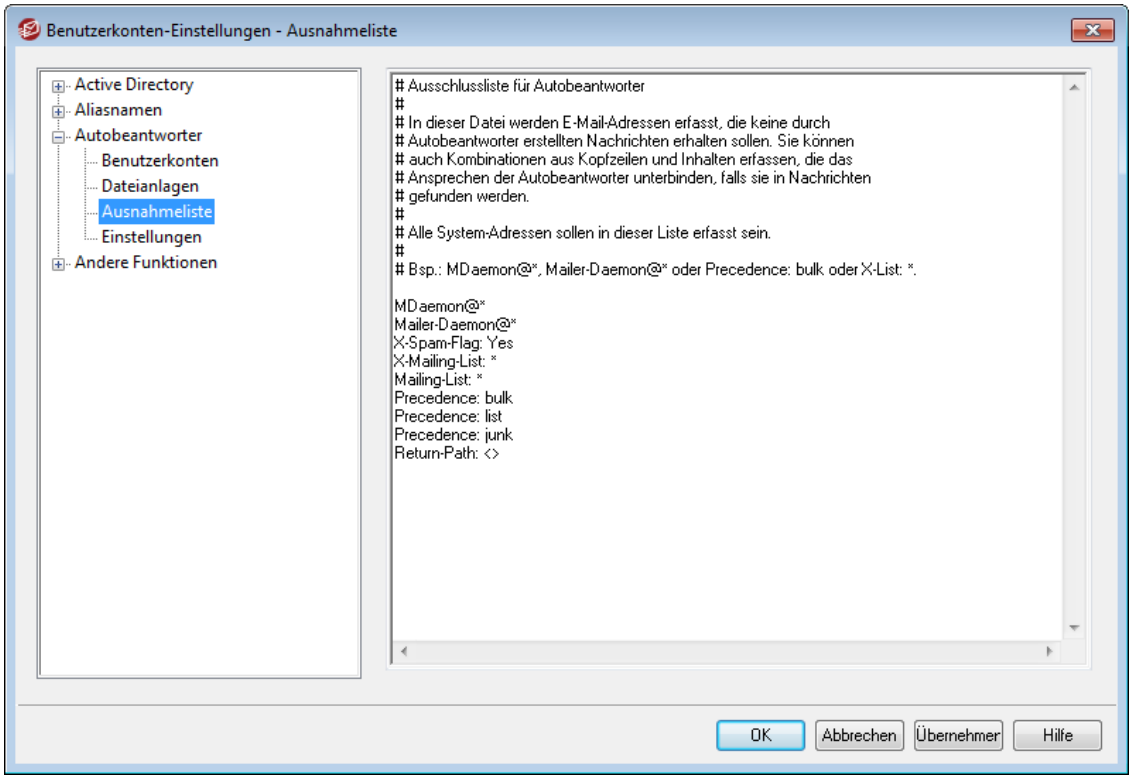


In dieser Liste erfassen Sie die vollständigen Pfade zu allen Dateien, die als Dateianlagen in Skripten für Autobeantworter[836] zugelassen sind. Im eigentlichen Skript für den Autobeantworter können Sie mithilfe des Makros **%SetAttachment %** die jeweilige Datei als Dateianlage anfügen.

Siehe auch:

Autobeantworter » Benutzerkonten[831]
Autobeantworter » Ausnahmeliste[834]
Autobeantworter » Einstellungen[835]
Erstellung von Skripten für Autobeantworter[836]
Benutzerkonten-Editor » Autobeantworter[724]

5.3.3.3 Ausnahmeliste



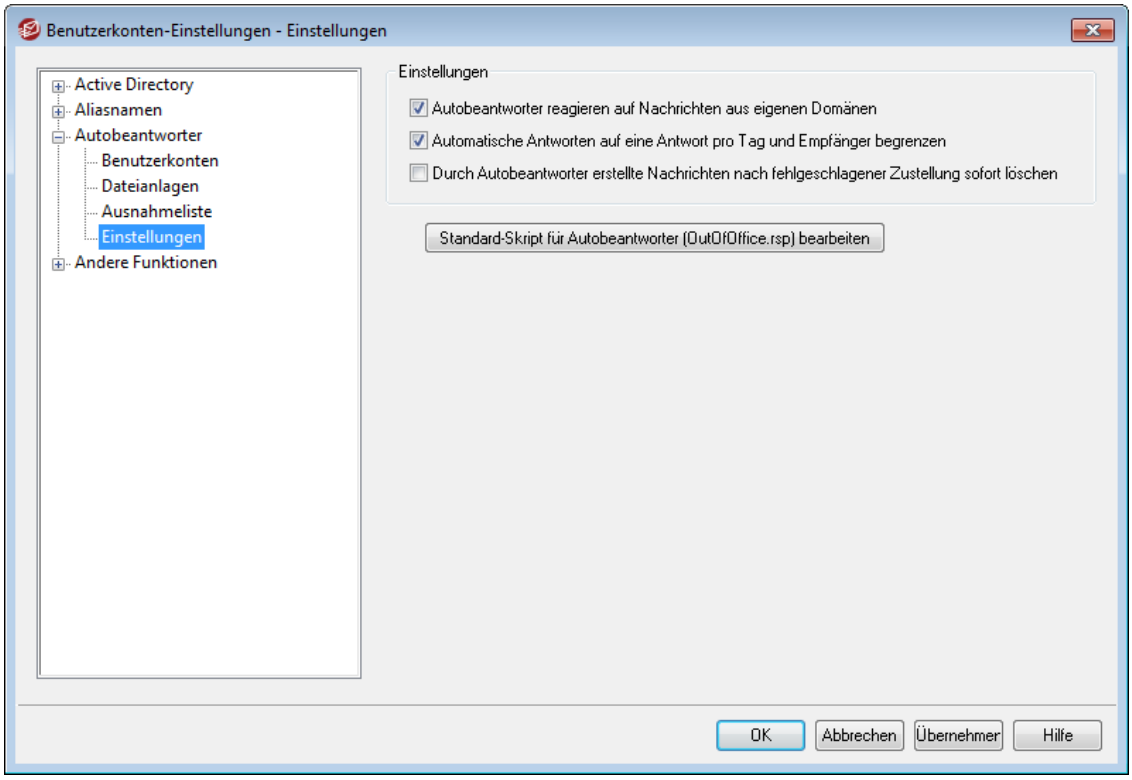
In den Konfigurationsdialog Autobeantworter » AusnahmeListe können Sie systemweite Ausnahmen für die Autobeantworter eintragen. Nachrichten von den hier eingetragenen Gegenstellen erhalten keinerlei Nachrichten von den Autobeantwortern. Als Gegenstellen können sowohl E-Mail-Adressen als auch Einträge mit Kopfzeile und Inhalt erfasst werden. Pro Zeile ist nur ein Eintrag zulässig. Jokerzeichen sind zulässig.

In diese Ausschlussliste sollten immer alle Systemadressen (z.B. mdaemon@*, mailer-daemon@* u.s.w.) eingetragen werden, um Endlosschleifen bei der Zustellung und andere Probleme zu vermeiden.

Siehe auch:

Autobeantworter » Benutzerkonten 831
Autobeantworter » Einstellungen 835
Erstellung von Skripten für Autobeantworter 836
Benutzerkonten-Editor » Autobeantworter 724

5.3.3.4 Einstellungen



Optionen

Autobeantworter reagieren auf Nachrichten aus eigenen Domänen
Diese Option bewirkt, dass nicht nur externe Nachrichten sondern auch Nachrichten aus den Domänen, die das System selbst verwaltet, die Autobeantworter auslösen. Diese Option ist per Voreinstellung aktiv. Falls die Autobeantworter nicht auf Nachrichten reagieren sollen, bei denen Absender und Empfänger derselben Domäne angehören, deaktivieren Sie diese Option.

Automatische Antworten auf eine Antwort pro Tag und Empfänger begrenzen
Diese Option begrenzt per Voreinstellung die Anzahl der durch Autobeantworter erstellten Nachrichten auf eine je Empfänger und Tag. So erhält ein Empfänger nicht dieselbe Nachricht eines Autobeantworters immer wieder, wenn er während des Tages mehrfach Nachrichten an eine Adresse sendet, für die ein Autobeantworter aktiv ist. Falls Sie wünschen, dass jede Nachricht die Antwort eines Autobeantworters auslöst, auch wenn er am selben Tag dem selben Absender bereits einmal geantwortet hat, deaktivieren Sie diese Option.

Diese Option hilft auch, Endlosschleifen in der Zustellung zu verhindern. Diese können auftreten, falls die Nachricht eines Autobeantworters an eine Adresse zurückgesandt wird, für die ebenfalls ein Autobeantworter aktiv ist. Ist diese Option aktiv, so könnte in der gezeigten Weise nur je eine Nachricht pro Tag ausgetauscht werden, ist sie nicht aktiv, so können die Nachrichten laufend hin- und hergesandt werden.

Durch Autobeantworter erstellte Nachrichten nach fehlgeschlagener Zustellung sofort löschen
Diese Option bewirkt, dass unzustellbare Nachrichten der Autobeantworter gelöscht werden, wenn sie aus der Extern-Warteschlange entfernt werden. Solche unzustellbaren Nachrichten werden dann nicht durch die Wiederholungs-Warteschlange 864 verarbeitet.

Standard-Skript für Autobeantworter (OutOfOffice.rsp) bearbeiten
Die Datei OutOfOffice.rsp ist die Standard-Nachrichtendatei für die Autobeantworter. Der Inhalt dieser Datei wird in die Datei oof.mrk der Benutzerkonten 724 kopiert, wenn diese Datei in einem Benutzerkonto fehlt oder leer ist.

Siehe auch:

Autobeantworter » Benutzerkonten 831
Autobeantworter » Ausnahmeliste 834
Erstellung von Skripten für Autobeantworter 836
Benutzerkonten-Editor » Autobeantworter 724

5.3.3.5 Erstellung von Skripten für Autobeantworter

Die Dateien OOF.mrk sind ASCII-Dateien im Format Nur-Text. Sie sind im Verzeichnis `\data\` unter dem Hauptverzeichnis jedes Benutzerkontos abgelegt. Ihr Inhalt definiert den Inhalt der Nachrichten, die durch die Autobeantworter versandt werden. Wird ein Skript durch einen Autobeantworter ausgeführt, so wird es verarbeitet und nach Makros durchsucht. Die Makros werden durch die Daten aus der eingegangenen Nachricht ersetzt, die den Autobeantworter ausgelöst hat. Zeilen, die mit dem Zeichen "#" beginnen, werden ignoriert und können für Kommentare verwendet werden. Weiter unten sind zwei Beispielnachrichten 839 aufgeführt.

Makros für Skripte des Autobeantworters

`$HEADERS$` Dieses Makro wird durch alle ursprünglichen Kopfzeilen der eingehenden Nachricht ersetzt. Dieses Makro liest alle Kopfzeilen einer eingehenden Nachricht. Der Text direkt vor dem Makro erscheint am Anfang jeder ausgewerteten Zeile.

`$HEADER:XX$` Damit wird nur die Kopfzeile "xx" der umgeformten Nachricht hinzugefügt. Ist z.B. in der Originalnachricht "TO: joe@example.com" enthalten, so gibt das Makro $HEADER:TO$ den Text "joe@example.com" aus. Enthält die Originalnachricht "SUBJECT: Dies ist der Betreff" , so ergibt das Makro $HEADER:SUBJECT$ den Text "Dies ist der Betreff".

`$BODY$` Dieses Makro gibt den kompletten Nachrichtentext außer den Kopfzeilen und dem Betreff aus. Damit auch sprachspezifische Sonderzeichen wie etwa deutsche Umlaute oder das "ß" erhalten bleiben,

liest MDaemon den Nachrichtentext als Binärdaten und erstellt so eine bitweise Kopie des Textes.

$BODY-AS-TEXT$ Dieses Makro gibt, genau wie $BODY$, den gesamten Nachrichtentext aus, jedoch liest MDaemon dabei den Text nicht binär sondern als ASCII-Text. Dies ist u.U. mit manchen Zeichensätzen nicht kompatibel. Der Text vor dieser Variable wird am Anfang jeder Zeile ausgegeben, sodass >>$BODY-AS-TEXT$ jeder Zeile der RFC-2822-Originalnachricht die Zeichen ">>" hinzufügen würde. Der Text kann auch rechts von diesem Makro hinzugefügt werden.

$SENDER$ Dieses Makro ergibt die vollständige Adresse des Absenders aus der Kopfzeile "`From:`" der eingegangenen Nachricht.

$SENDERMAILBOX$ Dieses Makro gibt den Postfachnamen des Absenders aus. Der Postfachname ist der Teil einer E-Mail-Adresse links vom @-Zeichen.

$SENDERDOMAIN$ Dieses Makro gibt den Domänennamen des Absenders aus. Der Domänenname ist der Teil einer E-Mail-Adresse rechts vom @-Zeichen

$RECIPIENT$ Dieses Makro gibt die vollständige E-Mail-Adresse des Empfängers aus.

$RECIPIENTMAILBOX$ Dieses Makro gibt den Postfachnamen des Empfängers aus. Der Postfachname ist der Teil einer E-Mail-Adresse links vom @-Zeichen.

$RECIPIENTDOMAIN$ Dieses Makro gibt den Domänennamen des Empfängers aus. Der Domänenname ist der Teil einer E-Mail-Adresse rechts vom @-Zeichen.

$SUBJECT$ Dieses Makro ergibt den Inhalt der Kopfzeile "Betreff" ("`Subject:`").

$MESSAGEID$ Dieses Makro ergibt den Inhalt der Kopfzeile "Message-ID" ("Nachrichten-ID").

$CONTENTTYPE$ Dieses Makro ergibt den Inhalt der Kopfzeile "`Content-Type`" ("Inhalts-Typ").

$PARTBOUNDARY$ Dieses Makro gibt den Teil-Begrenzer für mehrteilige MIME-Nachrichten aus, der bei mehrteiligen Nachrichten in der Kopfzeile "`Content-Type`" zu finden ist.

$DATESTAMP$ Dieses Makro gibt eine Zeile mit Datum- und Zeitstempel nach RFC-2822 aus.

$ACTUALTO$	Manche Nachrichten enthalten ein Feld "ActualTo" ("Eigentlich an"), in dem die ursprünglich vom Absender eingegebene Zieladresse zu finden ist, wie sie vor irgendwelchen Umformungen oder Formatänderungen lautete. Dieses Makro fügt diesen Text ein.
$ACTUALFROM$	Manche Nachrichten enthalten ein Feld "ActualFrom" ("Eigentlich von"), in dem die ursprüngliche Absenderadresse zu finden ist, wie sie vor irgendwelchen Umformungen oder Formatänderungen lautete. Dieses Makro fügt diesen Text ein.
$REPLYTO$	Dieses Makro ergibt den Inhalt der Kopfzeile "ReplyTo" ("Antwort an").
$PRODUCTID$	Dieses Makro gibt die Versionsinformation für den Server MDaemon aus.
AR_START	Dieses Makro ergibt Datum und Uhrzeit, zu denen ein Autobeantworter aktiviert wird.
AR_END	Dieses Makro ergibt Datum und Uhrzeit, zu denen ein Autobeantworter deaktiviert wird.

Makros zum Einfügen und Ersetzen von Kopfzeilen

Die folgenden Makros bestimmen, welche Kopfzeilen in die durch den Autobeantworter erstellten Nachrichten eingefügt werden.

%SetSender%
Bsp.: %SetSender%=mailbox@example.com
Dieses Makro ändert, nur im Rahmen des jeweiligen Autobeantworters, den Absender der Ursprungsnachricht, bevor die Kopfzeilen der Antwortnachricht erstellt werden. Das Makro steuert damit den Inhalt der Empfängerkopfzeile TO der automatischen Antwortnachricht. War der Absender der Ursprungsnachricht beispielsweise "user2@example.com", und führt der Autobeantworter das Makro %SetSender% aus, um ihn in "user1@example.com" zu ändern, dann wird in die Kopfzeile TO der Antwortnachricht "user1@example.com" eingetragen.

%SetRecipient%
Bsp.: %SetRecipient%=mailbox@example.com
Dieses Makro ändert, nur im Rahmen des jeweiligen Autobeantworters, den Empfänger der Ursprungsnachricht, bevor die Kopfzeilen der Antwortnachricht erstellt werden. Das Makro steuert damit den Inhalt der Absenderkopfzeile FROM der automatischen Antwortnachricht. War der Empfänger der Ursprungsnachricht beispielsweise "michael@example.com", und führt der Autobeantworter das Makro %SetRecipient% aus, um ihn in "michael.mason@example.com" zu ändern, dann wird in die Kopfzeile FROM der Antwortnachricht "michael.mason@example.com" eingetragen.

%SetReplyTo%
Bsp.: %SetReplyTo%=mailbox@example.com

Steuert den Inhalt der Kopfzeile `ReplyTo` der automatisch erstellten Antwortnachricht.

%SetSubject%
`Bsp.: %SetSubject%=Neuer Betreff`
Ersetzt den Betreff der Ursprungsnachricht durch den hier angegebenen Text.

%SetMessageId%
`Bsp.: %SetMessageId%=ID String`
Ändert die Nachrichten-ID der automatisch erstellten Antwortnachricht.

%SetPartBoundary%
`Bsp.: %SetPartBoundary%=Boundary String`
Ändert den Part-Trenner.

%SetContentType%
`Bsp.: %SetContentType%=MIME type`
Ändert den Inhaltstyp der automatisch erstellten Antwortnachricht in den hier angegebenen Wert.

%SetAttachment%
`Bsp.: %SetAttachment%=Datei`
Veranlasst MDaemon, die angegebene Datei an die automatisch erstellte Antwortnachricht anzufügen. Es können hierbei nur solche Dateien als Dateianlagen angefügt werden, die im Abschnitt Dateianlagen 833 ausdrücklich aufgeführt sind.

5.3.3.5.1 Beispiel-Skripte für Autobeantworter

Ein typisches Skript für Autobeantworter in der Datei oof.mrk, das mehrere Makros für Autobeantworter nutzt, könnte folgendermaßen aussehen:

```
Sehr geehrter $SENDER$,

Ihre Nachricht wegen '$SUBJECT$' kann ich derzeit nicht
bearbeiten,
da ich mich im Urlaub befinde.

Mit freundlichem Gruß,

$RECIPIENT$
```

Mit den oben erläuterten zusätzlichen Makros lassen sich auch die Kopfzeilen bestimmen, die der automatisch erzeugten Antwortnachricht vor dem Versand an den Absender `$SENDER$` hinzugefügt werden:

```
Sehr geehrter $SENDER$,

Ihre Nachricht wegen '$SUBJECT$' kann ich derzeit nicht
bearbeiten,
da ich mich im Urlaub befinde.

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$
```

```
%SetAttachment%=c:\fotos\ich_im_urlaub.jpg
```

Dieses Skript stellt der Betreffzeile den Text "RE: " voran und fügt die angegebene Datei als Dateianlage an.

Die Zeile "%SetSubject%=RE: $SUBJECT$" wird dabei wir folgt behandelt:

1. Der Abschnitt $SUBJECT$ wird ausgewertet und durch den Betreff der Ursprungsnachricht ersetzt. Damit ergibt sich folgender Ausdruck:

   ```
   %SetSubject%=RE: Text der ursprünglichen Betreffzeile
   ```

2. MDaemon ersetzt den Betreff der Ursprungsnachricht, der noch intern gespeichert ist, durch diesen neu erstellten Text. Ab diesem Zeitpunkt wird immer dann der neue Text eingesetzt, wenn im Skript die Variable "$SUBJECT$" erscheint.

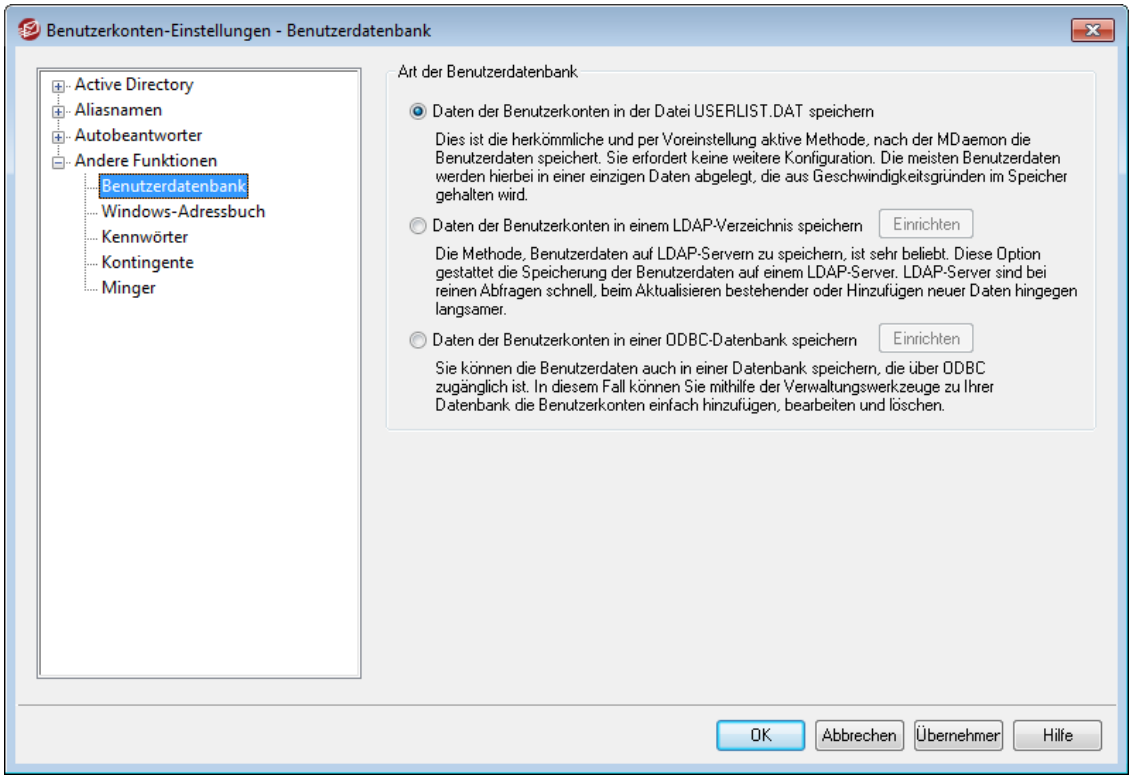
Die Platzierung der neuen Makros ist wichtig; sie müssen am Ende des Skripts stehen, um Probleme zu vermeiden. Würde beispielsweise das Makro %SetSubject% vor dem Marko $SUBJECT$ in der dritten Zeile des Skripts erscheinen, wäre der ursprüngliche Betrefftext bereits überschrieben, bevor das Makro $SUBJECT$ ausgewertet wird. Statt den ursprünglichen Betreff würde es dann nur noch den Text ausgeben, der durch das Makro %SetSubject% festgelegt wurde.

Siehe auch:

Autobeantworter » Benutzerkonten 831
Autobeantworter » Ausnahmeliste 834
Autobeantworter » Einstellungen 835
Benutzerkonten-Editor » Autobeantworter 724

5.3.4 Andere Funktionen

5.3.4.1 Benutzerdatenbank



Im Konfigurationsdialog Benutzerdatenbank (erreichbar über `Benutzerkonten » Benutzerkonten-Optionen`) legen Sie die Methode fest, nach der MDaemon Ihre Benutzerdatenbank speichern soll: in einer ODBC-Datenquelle, auf einem LDAP-Server oder in der lokalen Datei `USERLIST.DAT`.

Daten der Benutzerkonten in der Datei USERLIST.DAT speichern
Diese Option bewirkt, dass MDaemon das interne, auf der Datei `USERLIST.DAT` aufgebaute System als Benutzerdatenbank verwendet. Diese Option ist per Voreinstellung aktiv. Alle Benutzerdaten werden dabei lokal abgelegt, wobei die meisten Daten in einer einzelnen Datei abgelegt sind, die aus Gründen der Geschwindigkeit im Arbeitsspeicher gehalten wird.

Daten der Benutzerkonten in einem LDAP-Verzeichnis speichern
Diese Option bewirkt, dass MDaemon anstelle einer ODBC-Datenbank oder der lokalen Datei `USERLIST.DAT` einen LDAP-Server zur Speicherung der Benutzerdatenbank verwendet. Diese Option kann hilfreich sein, wenn sich mehrere MDaemon-Server an verschiedenen Standorten eine gemeinsame Benutzerdatenbank teilen sollen. Dazu muss jeder MDaemon-Server für den Zugriff auf denselben LDAP-Server konfiguriert sein und darf die Daten nicht lokal speichern. LDAP-Server reagieren für gewöhnlich auf Abfragen schnell und effizient, sind dafür aber bei der Aktualisierung bestehender oder dem Einfügen neuer Daten langsamer.

Einrichten
Ist die LDAP-Option gewählt, so können Sie durch Anklicken dieses Steuerelements den Konfigurationsdialog für die Einstellungen zum LDAP-Server 824 aufrufen.

Daten der Benutzerkonten in einer ODBC-Datenbank speichern
Mithilfe dieser Einstellung kann eine ODBC-kompatible Datenquelle als Benutzerdatenbank für MDaemon verwendet werden.

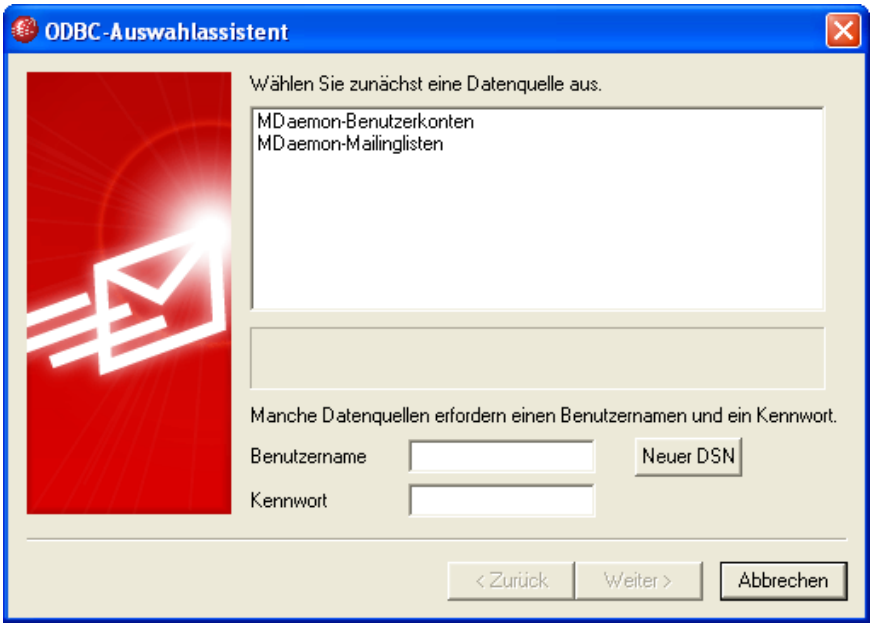
Einrichten
Ist die ODBC-Option gewählt, so können Sie durch Anklicken dieses Steuerelements den ODBC-Auswahlassistenten[842] aufrufen. Dort können Sie die gewünschte ODBC-Datenquelle auswählen und konfigurieren.

5.3.4.1.1 ODBC-Auswahlassistent - Benutzerdatenbank

Mithilfe des ODBC-Auswahlassistenten können Sie eine ODBC-kompatible Datenquelle als Benutzerdatenbank für MDaemon auswählen und konfigurieren.

Umstellen Ihrer Benutzerdatenbank in eine ODBC-gestützte Datenbank

1. Klicken Sie im Konfigurationsdialog Benutzerdatenbank (Benutzerkonten » Benutzerkonten-Optionen » Benutzerdatenbank) auf **Daten der Benutzerkonten in einer ODBC-Datenbank speichern**, und klicken Sie dann auf **Einrichten**, um den ODBC-Auswahlassistenten aufzurufen.

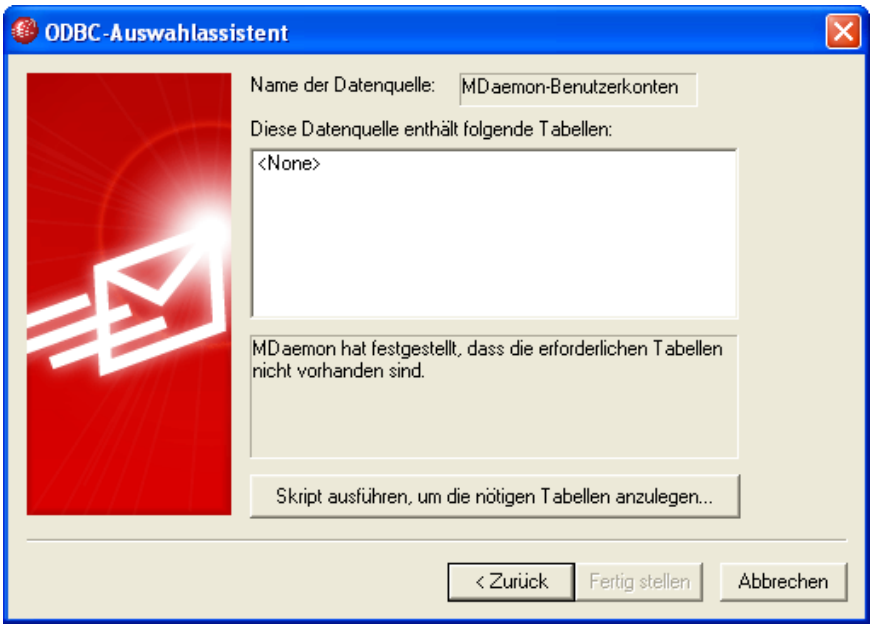


2. Wählen Sie die **Datenquelle**, die Sie für Ihre Benutzerdatenbank nutzen wollen. Falls keine kompatible Datenquelle in der Liste erscheint, klicken Sie auf **Neuer DSN**, und folgen Sie dann den Anweisungen unter **Erstellen einer neuen ODBC-Datenquelle**[844].

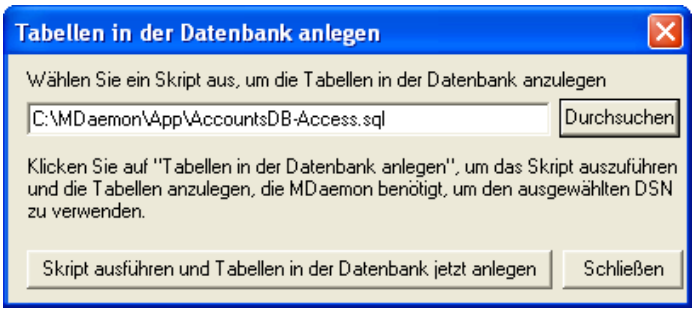
3. Falls erforderlich, geben Sie **Benutzernamen** und **Kennwort** für die Datenquelle ein.

4. Klicken Sie auf **Weiter**.

5. Falls die Datenquelle die Tabellen, die MDaemon benötigt, bereits enthält, fahren Sie mit **Schritt 8** fort. Andernfalls klicken Sie auf **Skript ausführen, um die nötigen Tabellen anzulegen...**



6. Geben Sie Pfad und Dateinamen für das Skript an (oder navigieren Sie über **Durchsuchen** zum Skript), mit dessen Hilfe Sie die Tabellen in Ihrer Datenbank-Anwendung erstellen wollen. Im Verzeichnis `\MDaemon\app\` finden Sie Skripte für einige der am weitesten verbreiteten Datenbank-Anwendungen.



7. Klicken Sie auf **Skript ausführen und Tabellen in der Datenbank jetzt anlegen**, klicken Sie dann auf **OK**, und klicken Sie schließlich auf **Schließen.**

8. Klicken Sie auf **Fertig stellen**, und klicken Sie dann auf **OK**, um den Konfigurationsdialog für die Benutzerdatenbank zu schließen.

9. Ein Datenbank-Hilfsprogramm überführt alle Benutzerkonten in die ODBC-Datenquelle und beendet MDaemon anschließend. Klicken Sie auf **OK**, und starten Sie MDaemon danach neu. MDaemon nutzt nunmehr die neue ODBC-Benutzerdatenbank.

Siehe auch:

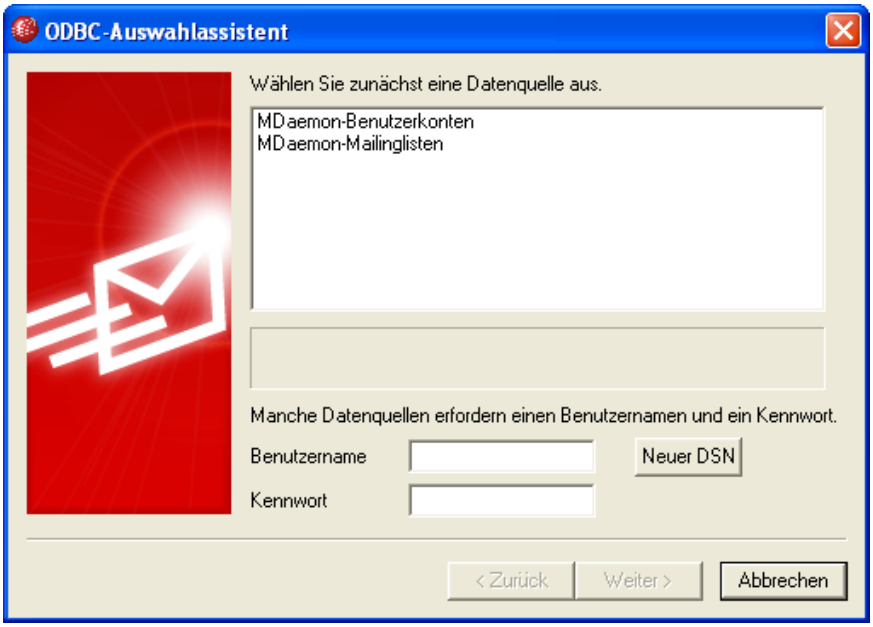
Benutzerdatenbank 841
Erstellen einer neuen ODBC-Datenquelle 844

5.3.4.1.1.1 Erstellen einer neuen ODBC-Datenquelle

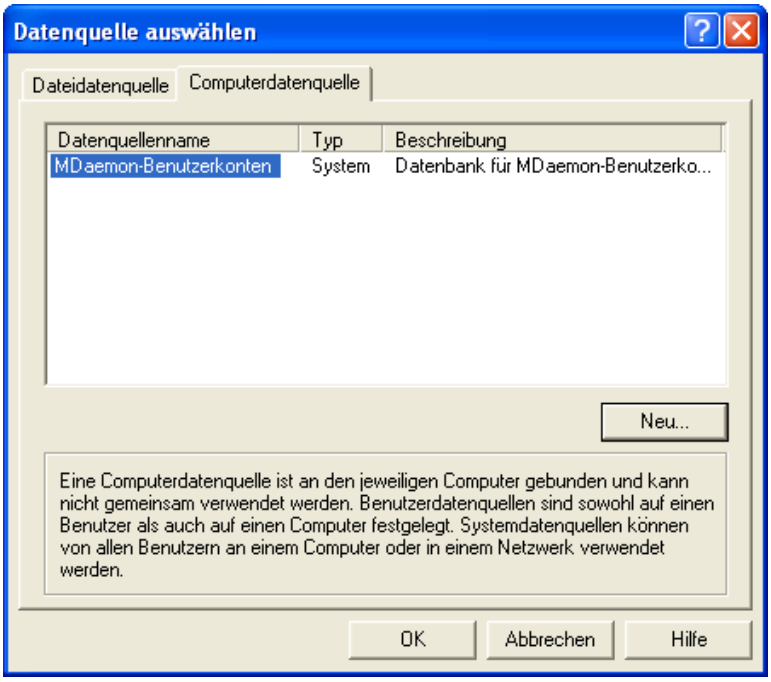
Um eine neue ODBC-Datenquelle zu erstellen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Konfigurationsdialog Benutzerdatenbank (Benutzerkonten » Benutzerkonten-Optionen » Benutzerdatenbank) auf **Daten der Benutzerkonten in einer ODBC-Datenbank speichern**, und klicken Sie dann auf **Einrichten**, um den ODBC-Auswahlassistenten aufzurufen.

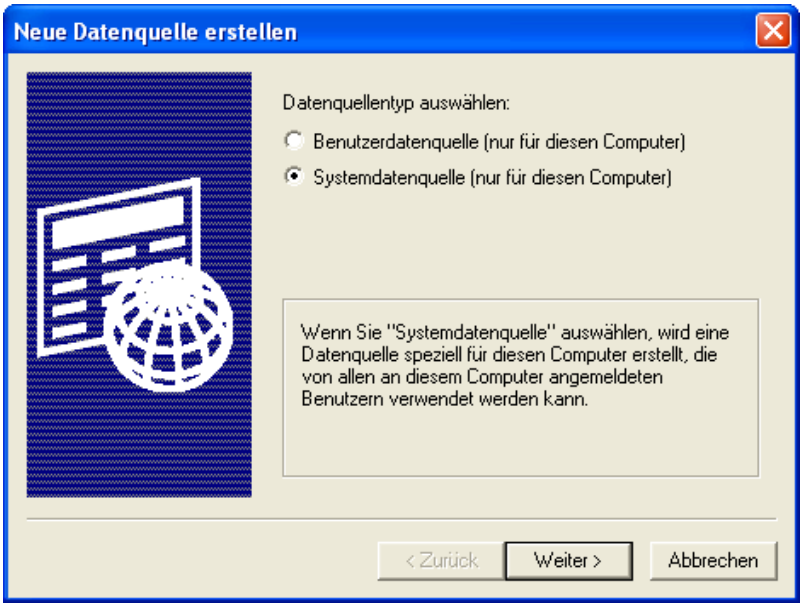
2. Klicken Sie auf **Neuer DSN**, um den Dialog zur Auswahl einer Datenquelle aufzurufen.



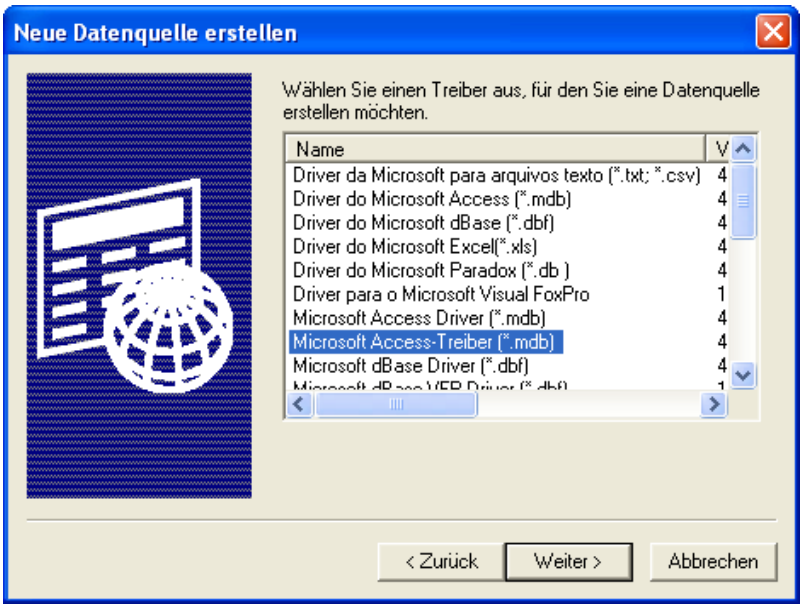
3. Wechseln Sie auf die Registerkarte **Computerdatenquelle**, und klicken Sie auf **Neu...**, um den Dialog Neue Datenquelle erstellen aufzurufen.



4. Wählen Sie **Systemdatenquelle**, und klicken Sie auf **Weiter.**



5. Wählen Sie den **Datenbanktreiber**, den Sie zur Erstellung der Datenquelle nutzen wollen, und klicken Sie auf **Weiter**.



6. Klicken Sie auf **Fertig stellen**, um den Konfigurationsdialog für den Datenbanktreiber aufzurufen. Das Erscheinungsbild dieses Konfigurationsdialogs hängt von dem ausgewählten Treiber ab (unten wird beispielhaft der Dialog für Microsoft Access gezeigt).

7. Bestimmen Sie einen **Datenquellennamen** für Ihre neue Datenquelle, und tragen Sie alle anderen Informationen ein, die der Datenbanktreiber abfragt (beispielsweise für Erstellung und Auswahl einer Datenbank, Auswahl eines Verzeichnisses oder Servers usw.).

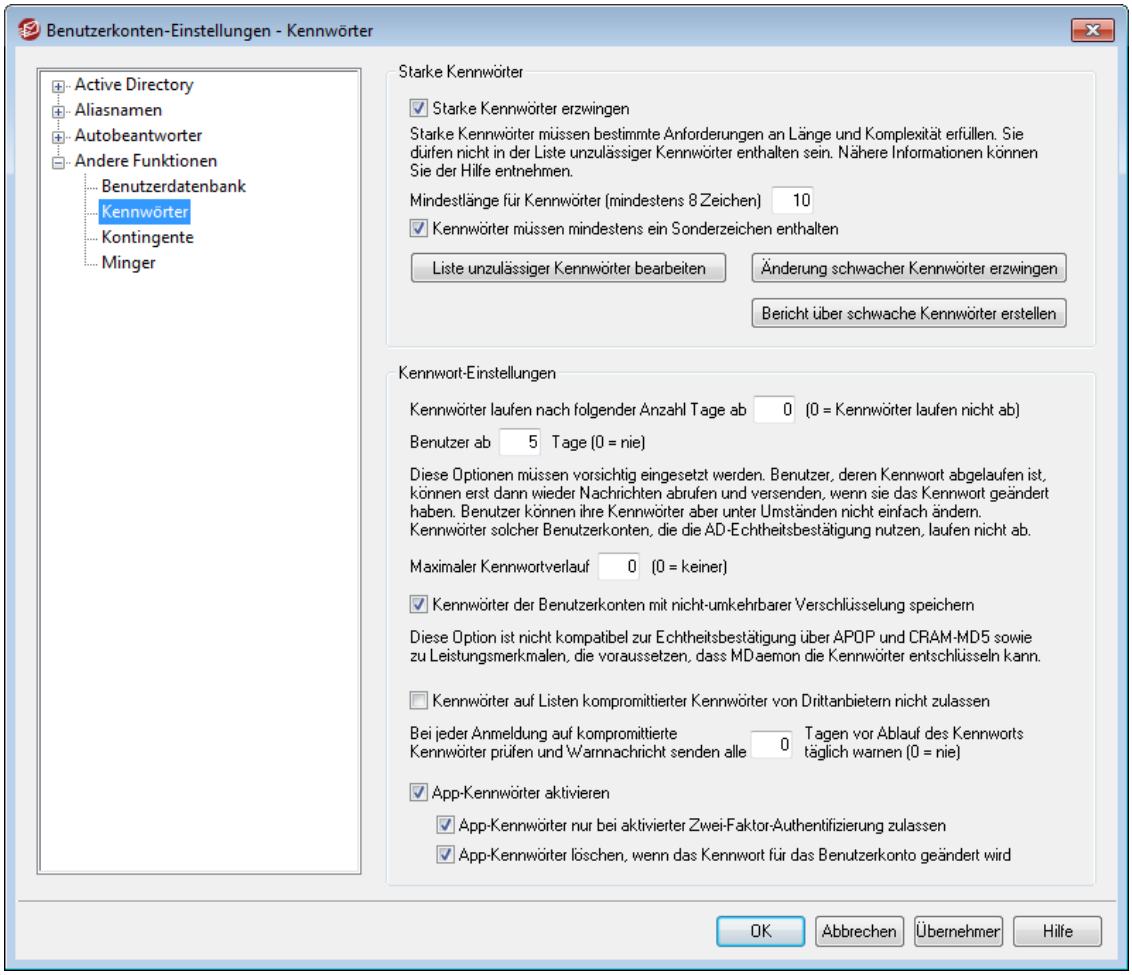
8. Klicken Sie auf **OK**, um den Dialog des Datenbanktreibers zu schließen.

9. Klicken Sie auf **OK**, um den Dialog zur Auswahl einer Datenquelle zu schließen.

Siehe auch:

Benutzerdatenbank 841
ODBC-Auswahlassistent - Benutzerdatenbank 842

5.3.4.2 Kennwörter



Starke Kennwörter

Starke Kennwörter erzwingen
Per Voreinstellung verlangt MDaemon starke Kennwörter, wenn neue Benutzerkonten erstellt oder bestehende Benutzerkonten bearbeitet werden. Falls Sie starke Kennwörter nicht verlangen wollen, deaktivieren Sie diese Option.

Starke Kennwörter müssen alle nachfolgend aufgeführten Anforderungen erfüllen:

- Sie müssen die festgelegte Mindestlänge erreichen.
- Sie müssen Groß- und Kleinbuchstaben enthalten.
- Sie müssen Buchstaben und Ziffern enthalten.
- Sie müssen mindestens ein Sonderzeichen enthalten, falls die entsprechende Option weiter unten aktiv ist.
- Sie dürfen Vor- und Nachnamen sowie Postfachnamen des jeweiligen Benutzers nicht enthalten.
- Sie dürfen nicht in der Liste der unzulässigen Kennwörter enthalten sein.

Mindestlänge für Kennwörter (mindestens 8 Zeichen)
Mithilfe dieser Option können Sie die Mindestlänge für starke Kennwörter in Zeichen festlegen. Der geringste zulässige Wert ist 8 Zeichen, eine größere Mindestlänge ist aber zu empfehlen. Die Voreinstellung beträgt bei Neuinstallationen von MDaemon 10 Zeichen. Wird dieser Wert geändert, so bleiben für die Benutzerkonten bestehende Kennwörter mit einer geringeren Mindestlänge zunächst gültig, und eine Änderung wird nicht sofort erzwungen. Sobald für solche Benutzerkonten aber eine Kennwortänderung durchgeführt wird, müssen die neuen Kennwörter die neue Mindestlänge erreichen, da sie sonst nicht angenommen werden.

Unabhängig von der hier festgelegten Mindestlänge dürfen Kennwörter länger als 72 Zeichen sein, wenn die Option "*Kennwörter der Benutzerkonten mit nicht-umkehrbarer Verschlüsselung speichern*" weiter unten aktiv ist. Falls diese Option deaktiviert ist, dann dürfen die Kennwörter höchstens 15 Zeichen lang sein.

Kennwörter müssen mindestens ein Sonderzeichen enthalten
Ist diese Option aktiv, dann müssen starke Kennwörter mindestens eines der folgenden Sonderzeichen enthalten: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~. Diese Option ist bei Neuinstallationen von MDaemon per Voreinstellung aktiv. Falls Sie Sonderzeichen in starken Kennwörtern nicht erzwingen wollen, deaktivieren Sie diese Option.

Liste unzulässiger Kennwörter bearbeiten
Durch Anklicken dieses Steuerelements können Sie die Liste der unzulässigen Kennwörter bearbeiten. Bei der Auswertung dieser Liste bleiben Groß- und Kleinschreibung unberücksichtigt. Einträge, die in dieser Liste erfasst sind, können nicht als Kennwörter verwendet werden. Neben einfachen Zeichenketten können Sie in der Liste mithilfe Regulärer Ausdrücke[657] auch komplexere Einträge erstellen, die besonders vielseitig verwendbar sind. Einträge, die mit dem Ausrufungszeichen "!" beginnen, werden als Reguläre Ausdrücke behandelt und ausgewertet.

Änderung schwacher Kennwörter erzwingen
Durch Anklicken dieses Steuerelements können Sie für alle Benutzerkonten mit schwachen Kennwörtern eine Änderung der Kennwörter erzwingen. Hierdurch werden alle Benutzerkonten mit schwachen Kennwörtern gesperrt, bis die Kennwörter geändert wurden. Die Kennwörter können durch die Administratoren mithilfe der Benutzeroberfläche von MDaemon geändert werden. Benutzer, deren Benutzerkonten gesperrt sind, können die Kennwörter auch mithilfe von Webmail oder der Remoteverwaltung selbst ändern. Versuchen Benutzer, sich mithilfe des alten Kennworts anzumelden, so werden sie aufgefordert, ein neues Kennwort festzulegen, bevor die Anmeldung abgeschlossen wird. **Beachte:** Diese Option ist nicht verfügbar, wenn die Option "*Kennwörter der Benutzerkonten mit nicht-umkehrbarer Verschlüsselung speichern*" weiter unten aktiv ist.

Bericht über schwache Kennwörter erstellen
Durch Anklicken dieses Steuerelements können Sie einen Bericht über alle MDaemon-Benutzerkonten mit schwachen Kennwörtern erstellen. Dieser Bericht wird per E-Mail an die Adresse versandt, die Sie nach dem Anklicken von OK eingeben. **Beachte:** Diese Option ist nicht verfügbar, wenn die Option

"*Kennwörter der Benutzerkonten mit nicht-umkehrbarer Verschlüsselung speichern*" weiter unten aktiv ist.

Kennwort-Einstellungen

Kennwörter laufen nach folgender Anzahl Tage ab (0 = Kennwörter laufen nicht ab)
Mithilfe dieser Option können Sie festlegen, wie lange Kennwörter für den Zugriff auf Benutzerkonten gültig bleiben, bevor die Benutzer die Kennwörter ändern müssen. Die Voreinstellung für diesen, in Tagen angegebenen, Wert beträgt 0 und bewirkt, dass die Kennwörter unbegrenzt lang gültig bleiben. Der Wert 30 bewirkt beispielsweise, dass die Benutzer ihre Kennwörter jeweils nach 30 Tagen ändern müssen. **Dieser Zeitraum rechnet von dem Tag an, an dem das Kennwort zum letzten Mal geändert wurde.** Wird hier ein Wert außer 0 eingetragen, so werden alle Kennwörter sofort als abgelaufen behandelt, die nicht innerhalb dieses Zeitraums geändert wurden. Benutzer, deren Kennwörter abgelaufen sind, können auf POP, IMAP und SMTP nicht mehr zugreifen. Diese Benutzer können sich jedoch noch bei Webmail und der Remoteverwaltung anmelden, und sie werden während der Anmeldung aufgefordert, ihre Kennwörter zu ändern. Ein Zugriff auf die eigentlichen Leistungsmerkmale in Webmail und der Remoteverwaltung ist erst nach Änderung des Kennworts wieder möglich. Über E-Mail-Clients wie Microsoft Outlook und Mozilla Thunderbird sind Änderungen der Kennwörter nicht möglich. Manche E-Mail-Clients zeigen dem Benutzer keine sinnvolle Fehlermeldung an. Die Benutzer müssen daher möglicherweise die Hilfe des Administrators in Anspruch nehmen, um zu erfahren, warum ihre Anmeldung fehlschlägt.

Benutzer können ihre Kennwörter nur dann über Webmail und die Remoteverwaltung ändern, falls ihnen im Konfigurationsdialog Web-Dienste[795] die Berechtigung zum Bearbeiten der Kennwörter erteilt ist. Unabhängig hiervon kann es auch sonst im Einzelfall für die Benutzer schwierig oder sogar unmöglich sein, die Kennwörter zu ändern. Diese Option sollte daher vorsichtig eingesetzt werden.

Benutzer ab [xx] Tagen vor Ablauf des Kennworts täglich warnen (0 = nie)
Benutzerkonten, deren Kennwort demnächst ablaufen wird, können täglich per E-Mail daran erinnert werden, dass sie ihr Kennwort ändern müssen. Mithilfe dieser Option können Sie festlegen, wie lange im Voraus MDaemon die Benutzer über den bevorstehenden Ablauf des Kennworts benachrichtigen soll. Die Benachrichtigung erfolgt einmal täglich.

Maximaler Kennwortverlauf (0=keiner)
Diese Option führt eine Kennwortchronik je Benutzerkonto. Der Wert entspricht der Anzahl der zuletzt verwendeten Kennwörter, die MDaemon für jeden Benutzer speichert. Ändern Benutzer ihre Kennwörter, so können die solche schon einmal verwendeten Kennwörter nicht verwenden, die noch im Kennwortverlauf gespeichert sind. Die Voreinstellung lautet 0; es wird dann kein Kennwortverlauf gespeichert.

Kennwörter der Benutzerkonten mit nicht-umkehrbarer Verschlüsselung speichern
Diese Option bewirkt, dass MDaemon die Kennwörter mithilfe eines Verfahrens speichert, dessen Verschlüsselung nicht umkehrbar ist. Hierdurch werden die Kennwörter gegen Entschlüsselung und Offenlegung im Klartext durch MDaemon, die Administratoren und mögliche Angreifer geschützt. MDaemon nutzt, wenn

diese Option aktiv ist, die Funktion bcrypt zur Erstellung von Kennworthashes. Hiermit werden längere Kennwörter von bis zu 72 Zeichen möglich. Die Kennwörter müssen außerdem bei Export und Import von Benutzerkonten nicht mehr offengelegt werden, bleiben aber dennoch erhalten. Einige Leistungsmerkmale sind zu dieser Verschlüsselung nicht kompatibel, insbesondere die Erkennung schwacher Kennwörter und die Leistungsmerkmale APOP und CRAM-MD5 für die Echtheitsbestätigung. Diese Leistungsmerkmale setzen voraus, dass MDaemon die Kennwörter entschlüsseln kann. Die nicht-umkehrbare Verschlüsselung ist per Voreinstellung aktiv.

Kompromittierte Kennwörter

MDaemon kann die Kennwörter der Benutzer mit einer Liste als kompromittiert bekannter Kennwörter abgleichen, die durch einen Drittanbieter bereit gestellt wird. Der Abgleich findet statt, ohne dass das Kennwort an den Anbieter übermittelt wird. Ist das Kennwort eines Benutzers in der Liste vorhanden, so bedeutet dies nicht, dass das Benutzerkonto kompromittiert oder gehackt wurde. Es bedeutet vielmehr, dass das fragliche Kennwort bereits einmal auf einem anderen System durch einen Benutzer verwendet wurde, und dass dieses verwendete Kennwort von einer Datenpanne oder einem Datenleck betroffen war. Kennwörter, die als kompromittiert bekannt und veröffentlicht sind, können durch Angreifer für Wörterbuchangriffe verwendet werden. Kennwörter, die noch nie auf anderen Systemen verwendet wurden, sind demgegenüber sicherer. Nähere Informationen hierzu erhalten Sie in englischer Sprache unter Pwned Passwords.

Kennwörter auf Listen kompromittierter Kennwörter von Drittanbietern nicht zulassen
Diese Option bewirkt, dass Kennwörter, die in der Liste kompromittierter Kennwörter gefunden werden, nicht als Kennwörter für die Benutzerkonten verwendet werden können.

Bei jeder Anmeldung auf kompromittierte Kennwörter prüfen und Warnnachricht senden alle
Mithilfe dieser Option prüft MDaemon die Kennwörter der Benutzerkonten in dem hier in Tagen konfigurierten Intervall während der Anmeldung und sendet dem Benutzer und dem Postmaster per E-Mail eine Warnmeldung, falls das Kennwort in der Liste gefunden wird. Die Warnmeldungen können mithilfe zweier Vorlagen angepasst werden, die im Verzeichnis `\MDaemon\App` abgelegt sind. Da die Anweisungen zum Ändern des Kennworts unter anderem davon abhängen, ob das Kennwort durch MDaemon verwaltet wird oder die Benutzerprüfung über das Active Directory erfolgt, stehen zwei Vorlagen zur Verfügung: `CompromisedPasswordMD.dat` und `CompromisedPasswordAD.dat`. Die Empfänger, Betreffzeile und Nachrichtentext können mithilfe von Makros individuell angepasst werden.

App-Kennwörter

App-Kennwörter 750 sind ein Leistungsmerkmal, mit dessen Hilfe sich Benutzerkonten besser absichern lassen. Dies wird erreicht durch die Verwendung sehr starker, zufällig erzeugter Kennwörter, die nur in E-Mail-Clients und E-Mail-Apps verwendet werden können, da sich diese Apps nicht durch die Zwei-Faktor-Authentifizierung 720 (2FA) schützen lassen. Nähere Informationen hierzu finden Sie im Abschnitt App-Kennwörter 750.

App-Kennwörter aktivieren
Per Voreinstellung können alle Benutzer die App-Kennwörter für ihre Benutzerkonten erstellen und verwalten. Sie müssen dazu mithilfe der Zwei-

Faktor-Authentifizierung an Webmail angemeldet sein. Sie können das Leistungsmerkmal App-Kennwörter für einzelne Benutzer deaktivieren, indem Sie den betreffenden Benutzern auf der Seite Web-Dienste die Berechtigung zum Bearbeiten der *App-Kennwörter* 720 entziehen.

App-Kennwörter nur bei aktivierter Zwei-Faktor-Authentifizierung zulassen
Per Voreinstellung müssen sich die Benutzer mithilfe der Zwei-Faktor-Authentifizierung 720 (2FA) an Webmail anmelden, um neue App-Kennwörter zu erstellen. Es wird nicht empfohlen, diese Anforderung außer Kraft zu setzen. Globale Administratoren 757 sind bei Nutzung der MDaemon-Remoteverwaltung von dieser Anforderung ausgenommen. Es empfiehlt sich aber, dass sie bei der Anmeldung an der MDaemon-Remoteverwaltung oder an Webmail stets die Zwei-Faktor-Authentifizierung nutzen.

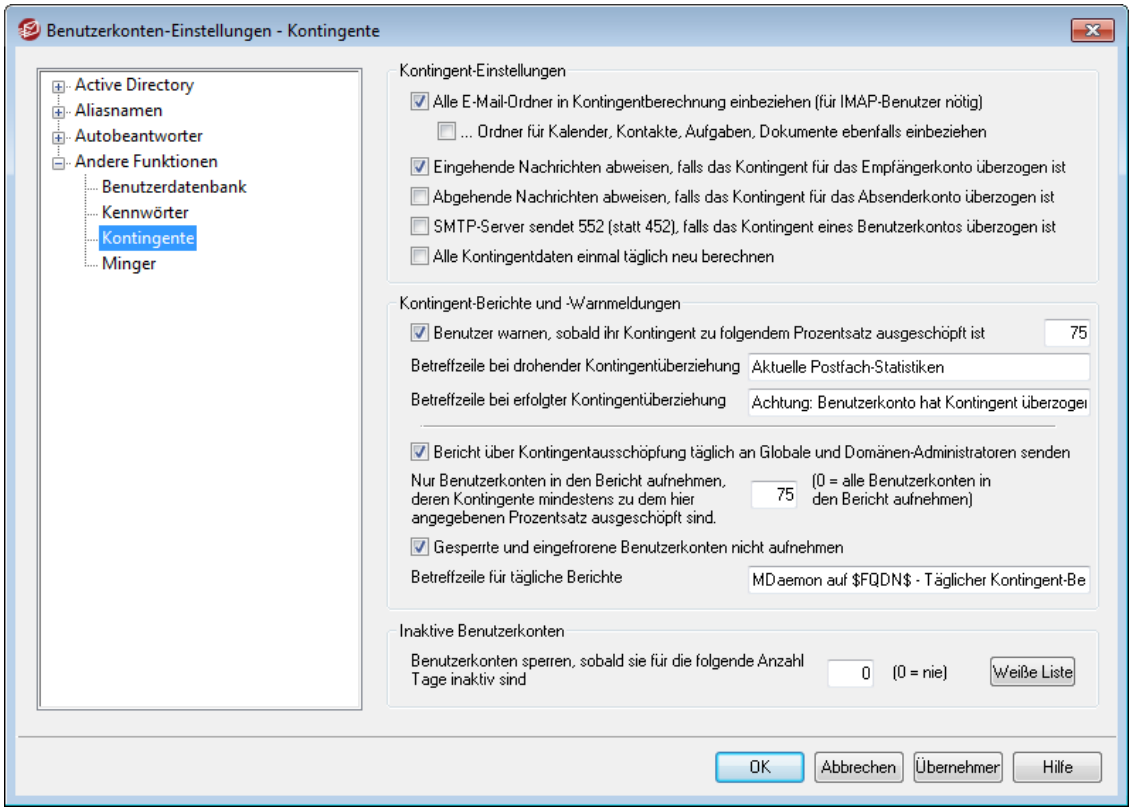
Auf der Seite Einstellungen des Benutzerkonten-Editors 760 steht die Option "*Anmeldung an SMTP, IMAP, ActiveSync usw. nur über App-Kennwörter zulassen*" zur Verfügung.

Wenn Sie die Nutzung von App-Kennwörtern für die genannten Anwendungsfälle erzwingen, so kann dies helfen, das Kennwort für ein Benutzerkonto gegen Brute-Force-Angriffe über SMTP, IMAP und andere Dienste zu schützen. Die Sicherheit ist in diesem Fall erhöht, da selbst bei Bekanntwerden des Kennworts für das Benutzerkonto ein Angriff über die genannten Dienste nicht möglich wäre. Ein Angreifer würde dabei nicht einmal erkennen, dass das Kennwort für das Benutzerkonto entdeckt wurde, da MDaemon für die Anmeldung an den genannten Diensten nicht das Kennwort des Benutzerkontos sondern nur ein gültiges App-Kennwort akzeptiert. Ein weiterer Vorteil ergibt sich bei der Echtheitsbestätigung mithilfe des Active Directory. Benutzerkonten im Active Directory 815 werden nach einer bestimmten Anzahl fehlerhafter Anmeldeversuche automatisch gesperrt. Die Nutzung der App-Kennwörter kann solche Sperren verhindern, da MDaemon bei aktivierter Option nur die App-Kennwörter prüft, aber keine Echtheitsbestätigung über das Active Directory versucht.

Siehe auch:

Benutzerkonten-Editor » Einzelheiten zum Benutzerkonto 714
Benutzerkonten-Editor » Web-Dienste 720
Benutzerkonten-Editor » App-Kennwörter 750
Reguläre Ausdrücke 657

5.3.4.3 Kontingente



Kontingent-Optionen

Alle E-Mail-Ordner in Kontingentberechnung einbeziehen (für IMAP-Benutzer nötig)
Ist diese Option ausgewählt, werden bei der Kontingentierung nach Anzahl und Größe der Nachrichten alle im Benutzerkonto eines Benutzers vorhandenen Nachrichtendateien, auch die Nachrichtendateien in allen Unterordnern, berücksichtigt. Andernfalls werden nur Nachrichtendateien im Posteingang selbst berücksichtigt. Diese Option wird üblicherweise nur für IMAP-Benutzer benötigt.

...Ordner für Kalender, Kontakte, Aufgaben, Dokumente ebenfalls einbeziehen
Aktivieren Sie dieses Kontrollkästchen, um alle Ordner für Kalender, Kontakte, Aufgaben und Dokumente ebenfalls in die Kontingentberechnung einzubeziehen.

Eingehende Nachrichten abweisen, falls das Kontingent für das Empfängerkonto überzogen ist
Ist ein Benutzerkonto durch ein Kontingent beschränkt, und ist dieses Kontingent überzogen, so nimmt MDaemon per Voreinstellung für dieses Benutzerkonto so lange keine eingehenden Nachrichten mehr an, bis der Kontoinhaber gespeicherte Nachrichten aus seinem Benutzerkonto löscht und dadurch das Kontingent wieder unterschreitet. Um eingehende Nachrichten auch dann anzunehmen, wenn das Kontingent des Empfängerkontos überzogen ist, deaktivieren Sie diese Option.

Abgehende Nachrichten abweisen, falls das Kontingent für das Absenderkonto überzogen ist
Diese Option bewirkt, dass Benutzerkonten, deren Kontingent überzogen ist, keine abgehenden Nachrichten versenden können. Abgehende Nachrichten von solchen Benutzerkonten weist MDaemon ab, bis der Kontoinhaber gespeicherte

Nachrichten aus seinem Benutzerkonto löscht und dadurch das Kontingent wieder unterschreitet. Diese Option ist per Voreinstellung abgeschaltet.

SMTP-Server sendet 552 (statt 452), falls das Kontingent eines Benutzerkontos überzogen ist
Per Voreinstellung sendet MDaemon während der Übermittlung von Nachrichten an ein Benutzerkonto mit überzogenem Kontingent in der SMTP-Verbindung den Fehlerkode 452 ("Angeforderter Vorgang nicht ausgeführt: unzureichende Speicherkapazität des Systems"). Dieser Fehlerkode zeigt der Gegenstelle an, dass sie den Vorgang später wiederholen soll. Diese Option bewirkt, dass stattdessen der Fehlerkode 552 gesendet wird, der einen dauerhaften Fehler anzeigt ("Angeforderter Nachrichten-Vorgang abgebrochen: zugewiesener Speicherplatz überschritten").

Alle Kontingentdaten einmal täglich neu berechnen
Per Voreinstellung werden zwischengespeicherte Kontingentdaten nur dann zurückgesetzt, wenn die Option "*Bericht über Kontingentausschöpfung täglich an Globale und Domänen-Administratoren senden*" weiter unten aktiv ist und die Berichte versandt werden. Um die Kontingentdaten auch während der täglichen Wartung neu zu berechnen, aktivieren Sie diese Option.

Kontingent-Berichte und -Warnmeldungen

Benutzer warnen, sobald ihr Kontingent zu folgendem Prozentsatz ausgeschöpft ist
Stellt MDaemon während der täglichen Wartungs- und Bereinigungsvorgänge 495 fest, dass ein MDaemon-Benutzerkonto den hier festgelegten Prozentsatz seiner Kontingente für die *Höchstzahl gleichzeitig gespeicherter Nachrichten* oder die *Begrenzung für den Speicherplatz,* erreicht hat, die beide mithilfe des Benutzerkonten-Editors 731 festgelegt werden, so erhält das Benutzerkonto um Mitternacht eine Warnnachricht. Die Betreffzeile dieser Warnnachricht können Sie mithilfe der Einstellung *Betreffzeile bei drohender Kontingentüberziehung* festlegen. Diese Nachricht informiert den Benutzer über die Zahl der Nachrichten, die Größe des Postfachs, den Prozentsatz, zu dem das Kontingent ausgeschöpft ist, und den Prozentsatz, zu dem das Kontingent noch frei ist. Enthält der Posteingang des Benutzers bereits eine Warnmeldung, so wird diese bestehende Meldung durch die neue Meldung ersetzt. Wird eine neue Warnnachricht in den Posteingang des Benutzers eingestellt, so wird dieser Vorgang im Protokoll System vermerkt, damit Sie davon Kenntnis nehmen können. Ist die Nachricht bereits im Posteingang vorhanden, und wird sie nur aktualisiert, so wird dieser Vorgang nicht protokolliert. Wenn der Protokolleintrag immer wieder eingetragen wird, so ist dies ein Zeichen dafür, dass der Benutzer die Warnmeldung aus seinem Posteingang löscht. Falls Sie keine solchen Warnmeldungen versenden lassen wollen, deaktivieren Sie diese Option.

Die Vorlage für die Warnnachrichten bei drohender Kontingentüberziehung ist unter MDaemon\app\NearQuota.dat gespeichert. Aus dieser Vorlage werden die Warnnachrichten erstellt. In dieser Vorlage sind alle Makros zulässig, die für Benutzerkonten ebenfalls zulässig sind, beispielsweise $EMAIL$, $MAILBOX$ und $DOMAIN$.

Betreffzeile bei drohender Kontingentüberziehung
Hier können Sie den Text für die Betreffzeile solcher Warnnachrichten festlegen, die Benutzer erhalten, sobald ihr Kontingent zu dem oben angegebenen Prozentsatz ausgeschöpft ist.

Betreffzeile bei erfolgter Kontingentüberziehung
Benutzer, deren Kontingent überzogen ist, erhalten ebenfalls eine Warnnachricht. Sie ist ähnlich aufgebaut wie die Warnnachricht bei drohender Kontingentüberziehung. Hier können Sie den Text für die Betreffzeile solcher Warnnachrichten festlegen, die Benutzer erhalten, sobald ihr Kontingent überzogen ist.

Bericht über Kontingentausschöpfung täglich an Globale und Domänen-Administratoren senden
Diese Option bewirkt, dass die Globalen und die Domänen-Administratoren täglich einen Bericht über die Kontingente erhalten. Um diese Berichte versenden zu lassen, aktivieren Sie diese Option, und tragen Sie in das folgende Feld den gewünschten Prozentsatz ein. In die Berichte werden nur solche Benutzerkonten aufgenommen, deren Kontingente mindestens zu dem hier angegebenen Prozentsatz ausgeschöpft sind. Der Wert "0" bewirkt, dass alle Benutzerkonten immer in die Kontingent-Berichte aufgenommen werden.

Gesperrte und eingefrorene Benutzerkonten nicht aufnehmen
Per Voreinstellung enthalten die Berichte über Kontingentausschöpfung keine gesperrten und keine eingefrorenen Benutzerkonten. Um solche Benutzerkonten ebenfalls in die Berichte aufzunehmen, deaktivieren Sie diese Option.

Betreffzeile für tägliche Berichte
Mithilfe dieser Option können Sie die Betreffzeile anpassen, die MDaemon in den täglichen Bericht über die Ausschöpfung der Kontingente 852 an die Administratoren einfügt. Sie können auch den Inhalt des Berichts selbst anpassen, in dem Sie die Datei `QuotaReport.dat` im Verzeichnis `MDaemon\APP` bearbeiten.

Inaktive Benutzerkonten

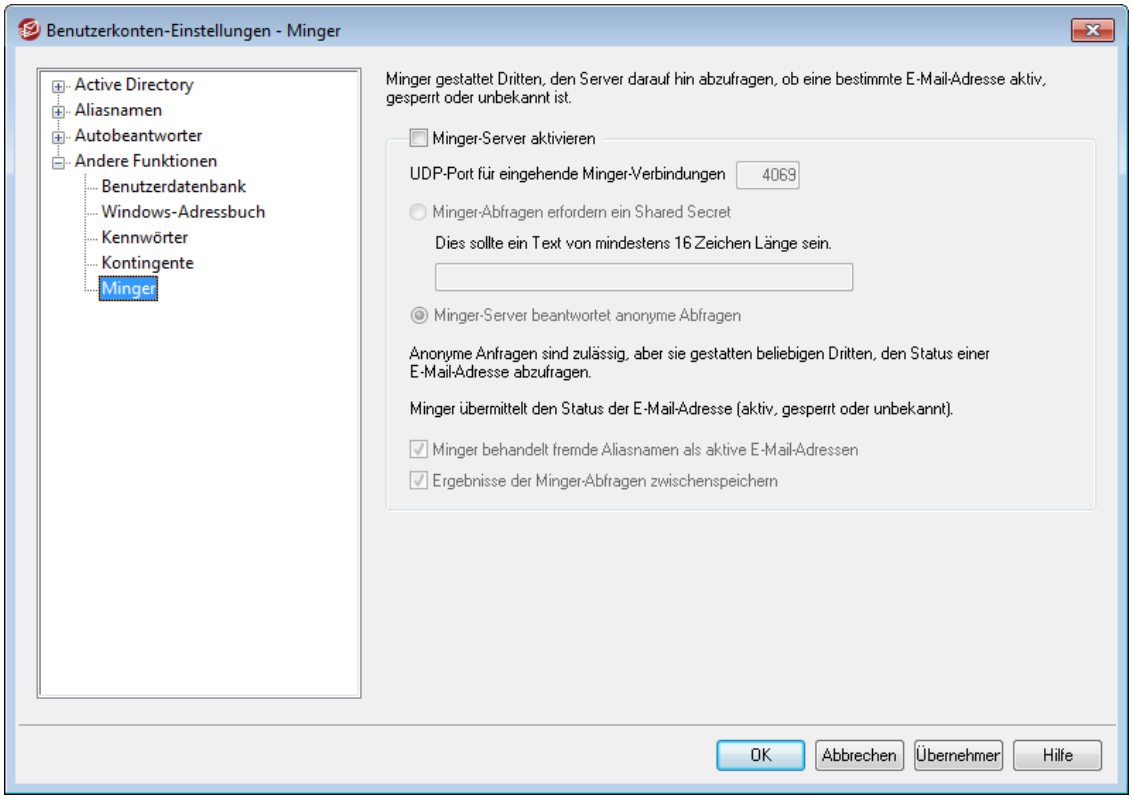
Benutzerkonten sperren, sobald sie für die folgende Anzahl Tage inaktiv sind [xx] (0=nie)
Mithilfe dieser Option können Sie Benutzerkonten automatisch deaktivieren lassen, sobald sie während der hier festgelegten Höchstzahl von Tagen durchgehend nicht aktiv waren. Sobald diese Höchstzahl erreicht ist, werden die Benutzerkonten gesperrt, und der Postmaster wird per E-Mail benachrichtigt. Er kann auf die Benachrichtigung antworten und hierdurch das Benutzerkonto wieder freischalten. Die entsprechenden Verarbeitungsvorgänge werden als Teil der Bereinigung jeden Tag im Mitternacht durchgeführt. Per Voreinstellung beträgt der Wert 0 (Option abgeschaltet).

Ausnahmeliste
Benutzerkonten, die in dieser Liste erfasst sind, werden von der Sperrung inaktiver Benutzerkonten ausgenommen.

Siehe auch:

Benutzerkonten-Editor » Kontingente 731
Vorlagen-Manager » Kontingente 805

5.3.4.4 Minger



Minger ist ein Protokoll zur Prüfung von E-Mail-Adressen auf Gültigkeit, das MDaemon Technologies entwickelt hat. Der Konfigurationsdialog für Minger ist über Benutzerkonten » Benutzerkonten-Optionen zugänglich. Die Technik von Minger gründet sich entfernt auf das Protokoll Finger; Minger ist hauptsächlich dazu geeignet, Dritten eine einfache und wirksame Methode zur Abfrage zur Verfügung zu stellen, ob eine E-Mail-Adresse gültig ist. Aus Gründen der Leistungsfähigkeit nutzt Minger UDP statt TCP; aus Sicherheitsgründen kann seine Nutzung von einer Echtheitsbestätigung abhängig gemacht werden, obwohl auch anonyme Anfragen zugelassen werden können. Der Konfigurationsdialog für Minger dient dazu, den Minger-Server in MDaemon zu aktivieren und zu deaktivieren, den verwendeten Port festzulegen (per Voreinstellung 4069), und zu bestimmen, ob für die Minger-Abfragen Echtheitsbestätigung erforderlich ist oder anonyme Anfragen zulässig sein sollen.

MDaemon verfügt auch über einen Minger-Client, der in das System der Domänen-Gateways eingebunden ist (siehe Prüfung 259). Jede Domäne, für die MDaemon als Gateway oder Ausfallsicherung arbeitet, kann für die Nutzung von Minger konfiguriert werden. MDaemon fragt dann den externen Server ab und prüft, ob die Empfängeradressen eingehender Nachrichten für die jeweiligen Domänen gültig sind. Damit ist es nicht mehr nötig, zu unterstellen, dass alle Empfängeradressen gültig seien.

Sie erhalten den neuesten Entwurf für das Minger-Protokoll unter:

http://tools.ietf.org/html/draft-hathcock-minger-05

Minger-Server

Minger-Server aktivieren
Diese Option aktiviert den in MDaemon eingebundenen Minger-Server.

UDP-Port für eingehende Minger-Verbindungen
Hier wird der Port festgelegt, den der Minger-Server auf eingehende Verbindungen überwacht. Die Internet Assigned Numbers Authority (IANA) hat die TCP- und UDP-Ports 4069 für die Nutzung durch Minger-Clients und –Server freigegeben und reserviert. Es empfiehlt sich, diesen Port nicht zu ändern, da er eigens der Nutzung durch Minger vorbehalten ist.

Minger-Abfragen erfordern ein Shared Secret
Soll für Minger-Abfragen eine Echtheitsbestätigung nach dem Shared-Secret-Verfahren verlangt werden, müssen diese Option aktiviert und ein Shared Secret von wenigstens 16 Zeichen Länge eingetragen sein. So lange diese Option aktiv ist, weist der Minger-Server Abfragen ohne Echtheitsbestätigung zurück.

Minger-Server beantwortet anonyme Abfragen
Diese Option lässt anonyme Minger-Abfragen zu. Der Minger-Client muss dabei keine Echtheitsbestätigung durchführen, bevor er Gültigkeitsprüfungen für E-Mail-Adressen durchführen darf. Dies ähnelt dem Ergebnis, das sich jetzt bereits durch den SMTP-Befehl VRFY und SMTP-Abfragen nach den Verfahren "Call back" und "Call forward" zur rückwärts gerichteten und vorwärts gerichteten Adressprüfung erzielen lässt. Minger-Abfragen sind jedoch wesentlich effizienter, und sie führen nicht zu zahlreichen abgebrochenen SMTP-Verbindungen mit entsprechenden Einträgen in den Protokolldateien, und die vermeiden auch andere Nachteile, die mit den genannten Alternativverfahren verbunden sind.

Minger behandelt fremde Aliasnamen als aktive E-Mail-Adressen
Diese Option bewirkt, dass Minger fremde Aliasnamen (Aliasnamen, die auf externe Adressen verweisen) so behandelt, wie wenn sie aktive und bekannte Adressen wären. Diese Verfahrensweise wird, unabhängig von dieser Option, erzwungen, falls eine Abfragen von SecurityGateway eingeht.

Ergebnisse der Minger-Abfragen zwischenspeichern
Per Voreinstellung speichert MDaemon die Ergebnisse der Minger-Abfragen in einem Cache. Falls Sie diese Zwischenspeicherung nicht wünschen, deaktivieren Sie diese Option.

5.4 Import von Benutzerkonten

5.4.1 Import von Benutzerkonten aus einer Textdatei

Sie erreichen die Funktion zum Import von Benutzerkonten aus kommagetrennten Textdateien über Benutzerkonten » Import » Benutzerkonten aus kommagetrennter Textdatei importieren oder über das Steuerelement *Importieren* im Benutzerkonten-Manager. Mit Hilfe dieser Funktion lassen sich Benutzerkonten schnell und einfach importieren und automatisch anlegen. MDaemon liest die Textdatei ein und kann sogar allein anhand der in ihr enthaltenen Vor- und Nachnamen die neuen Benutzerkonten. Dies funktioniert ohne Nachbearbeitung aber nur, falls die Vorlagentexte, Makros und Vorgaben für neue Benutzerkonten richtig

eingestellt sind (siehe die Vorlage "Neue Benutzerkonten"[788]). Es dürfen aber auch der Postfachname und das Kennwort für ein Benutzerkonto in der Datei enthalten sein, um damit die Vorgaben für neue Benutzerkonten für einen Eintrag zu übergehen. Alle Felder müssen durch Kommata getrennt sein.

Jede Zeile der kommagetrennten Textdatei darf nur eine einzigen Eintrag enthalten. Die erste Zeile, der sog. Feldraster, muss eine Steuerzeile sein, in der die Feldnamen in der Reihenfolge angegeben werden, in der die Inhalte der Felder in den folgenden Zeilen erscheinen. Eine Datei kann beispielsweise folgenden Inhalt haben:

```
"Mailbox", "FullName", "MailDir", "AllowAccess"
"arvel", "Arvel Hathcock", "C:\Mail\Arvel\", Y
"michael", "Michael Mason", "C:\Mail\Michael\", N
```

MDaemon stellt anhand der Reihenfolge der Feldnamen im Feldraster fest, in welcher Reihenfolge die Daten in den folgenden Zeilen erscheinen. Die Reihenfolge der Felder kann beliebig festgelegt werden, darf innerhalb der Datei aber nicht vom Feldraster abweichen. Jeder Feldname muss in Anführungs- und Schlusszeichen stehen.

Alle Werte des Typs "string" müssen in Anführungs- und Schlusszeichen stehen, und der Wert für Felder des Typs "bool" wird als `FALSE` betrachtet, falls das erste Zeichen nicht `y`, `Y`, `1`, `t` oder `T` lautet.

Für den vollständigen Namen (FullName) sind Vornamen und Nachnamen zulässig, sie dürfen aber keine Kommata enthalten.

Nach Abschluss des Importvorgangs erstellt MDaemon eine Datei namens `TXIMPORT.LOG`, die die Ergebnisse des Imports enthält und Aufschluss darüber gibt, welche Benutzerkonten erfolgreich importiert wurden, und in welchen Fällen der Import fehlgeschlagen ist. Gründe, aus denen der Import üblicherweise fehlschlägt, können ein Konflikt mit dem Postfachnamen, Vor- und Nachnamen oder Verzeichnis eines bestehenden Benutzerkontos und ein Konflikt mit einem bestehenden Aliasnamen oder Namen einer Mailingliste sein.

Weitere Informationen über die Zuordnung der einzelnen Felder enthalten die Beschreibungen für `MD_ImportUserInfo()` und `MD_ExportAllUsers()` in der Datei `MD-API.HTML` im Verzeichnis `\API\`.

Die folgenden Feldnamen sind für den Feldraster zugelassen und dienen der Zuordnung von Daten in der Textdatei zu den Datenfeldern der Benutzerkonten von MDaemon:

Feldname	Typ
MailBox	string
Domain	string
FullName	string

MailDir	string
Password	string
AutoDecode	bool
IsForwarding	bool
AllowAccess	bool
AllowChangeViaEmail	bool
KeepForwardedMail	bool
HideFromEveryone	bool
EncryptMail	bool
ApplyQuotas	bool
EnableMultiPOP	bool
MaxMessageCount	int
MaxDiskSpace	int
FwdAddress	string
FwdHost	string
FwdSendAs	string
FwdPort	string
NTAccount	string
MailFormat	string
AutoRespScript	string
AutoRespProcess	string
AddToList	string
RemoveFromList	string
PassMessageToProcess	bool
MaxUIDLCount	int
MaxMessageSize	int
RecurseIMAP	bool
MaxInactive	int
MaxMessageAge	int
MaxDeletedIMAPMessageAge	int
Comments	string
UserDefined	string

Siehe auch:

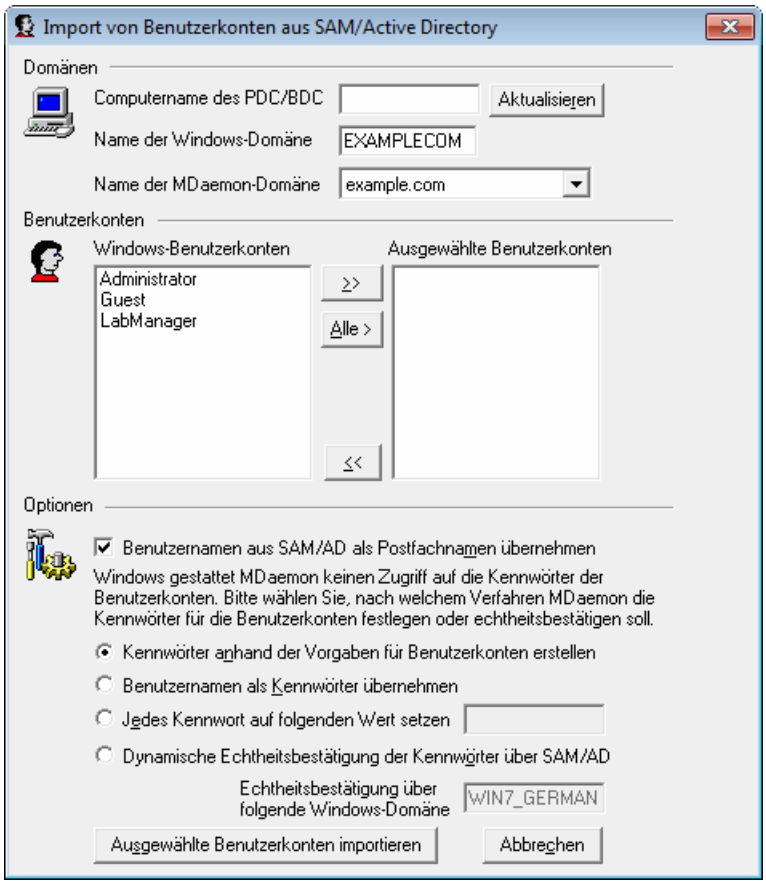
Einbindung von Windows-Benutzerkonten 859

5.4.2 Einbindung von Windows-Benutzerkonten

MDaemon unterstützt die Einbindung von Windows-Benutzerkonten. Hierzu steht die Funktion zum Import aus SAM und Active Directory zur Verfügung, die über das Menü Benutzerkonten (Benutzerkonten » Import... » Benutzerkonten aus SAM/Active Directory importieren...) erreichbar ist. Zusätzlich unterstützt MDaemon die Echtheitsbestätigung für Benutzer anhand des Active Directorys (AD). Dazu wird im Kennwortfeld eines Benutzerkontos der Name einer Windows-Domäne angegeben. MDaemon überprüft solche Benutzer dann in Echtzeit mit Hilfe der Benutzerdatenbank dieser Windows-Domäne. Bei dieser Funktion wirkt sich eine Kennwortänderung im Benutzermanager von Windows direkt auf MDaemon aus, und die Benutzer müssen sich nur eine Zugangskennung mit Kennwort merken. Neue Benutzerkonten lassen sich damit besonders einfach anlegen.

Der Sicherheitskontext des Benutzerkontos, in dem MDaemon ausgeführt wird, muss das Benutzerrecht **SE_TCB_NAME** ("Als Teil des Betriebssystems handeln") haben. Wenn MDaemon als Dienst durch das Systemkonto ("*LocalSystem*") ausgeführt wird, ist das Benutzerrecht grundsätzlich vorhanden. Ansonsten muss es in der Windows-Benutzerverwaltung dem jeweiligen Benutzerkonto hinzugefügt werden.

Import von Benutzerkonten aus SAM/Active Directory



Domänen

Computername des PDC/BDC
In diesem Feld muss der Computername des Rechners angegeben werden, dessen Windows-Benutzerdatenbank MDaemon auslesen soll. Der Eintrag \\<DEFAULT> bewirkt, dass MDaemon die Datenbank des lokalen Rechners ausliest.

Aktualisieren
Dieses Steuerelement aktualisiert die Liste der Windows-Benutzerkonten.

Name der Windows-Domäne
Hier wird der Name der Windows-Domäne angegeben, deren Benutzerkonten importiert werden sollen.

Name der MDaemon-Domäne
In dieser Auswahlliste muss die Domäne in MDaemon angegeben werden, in welche die Windows-Benutzerkonten importiert werden sollen.

Benutzerkonten

Windows-Benutzerkonten
Hier sind alle Benutzerkonten aufgeführt, die aus der Windows-Benutzerdatenbank ausgelesen wurden.

Ausgewählte Benutzerkonten
Hier sind die ausgewählten Benutzerkonten aufgeführt, die importiert werden sollen.

>>
Mit diesem Steuerelement werden die jeweils ausgewählten Einträge aus dem Abschnitt "Windows-Benutzerkonten" in den Abschnitt "Ausgewählte Benutzerkonten" verschoben.

<<
Hiermit werden die ausgewählten Einträge aus dem Abschnitt "Ausgewählte Benutzerkonten" entfernt.

Optionen

Benutzernamen aus SAM/AD als Postfachnamen übernehmen
Diese Option veranlasst MDaemon, die Postfachnamen der importierten Benutzer den Windows-Benutzernamen anzugleichen. Bei dieser Vorgehensweise muss man sich um die entsprechenden Vorlagen für neue Benutzerkonten[788] keine Gedanken machen.

Kennwörter anhand der Vorgaben für Benutzerkonten erstellen
Mit dieser Option erstellt MDaemon die Kennwörter für importierte Benutzerkonten mit Hilfe der entsprechenden Vorlage aus den Voreinstellungen für neue Benutzerkonten (siehe Vorlagen für neue Benutzerkonten[788]).

Benutzernamen als Kennwörter übernehmen
Hiermit setzt MDaemon den Namen des Benutzerkontos auch als Kennwort ein.

Jedes Kennwort auf folgenden Wert setzen
Hier kann ein feststehender Text eingetragen werden, der als Kennwort für alle importierten Benutzerkonten verwendet wird.

Dynamische Echtheitsbestätigung der Kennwörter über SAM/AD
Hiermit werden die Zugangsdaten einschließlich des Kennworts anhand des Active Directorys überprüft. MDaemon speichert selbst kein Kennwort mehr sondern prüft die Zugangsdaten, die ein Mailclient durch die Befehle USER und PASS übermittelt, in Echtzeit anhand der Windows-Benutzerdatenbank.

Echtheitsbestätigung über folgende Windows-Domäne
Hier wird der Name der Domäne angegeben, anhand deren Benutzerdatenbank MDaemon die Zugangsdaten in Echtzeit prüfen soll, wenn die dynamische Echtheitsbestätigung aktiv ist. **Hier darf nicht der Computername des Primären Domänencontrollers stehen, sondern es muss der tatsächliche Name der Windows-Domäne selbst eingetragen sein.**

Bei den Benutzerkonten, die anhand des AD dynamisch überprüft werden sollen, wird der Name der betreffenden Windows-Domäne mit zwei einleitenden Backslash-Zeichen im Feld `PASSWORD` (Kennwort) des MDaemon-Benutzerkontos gespeichert. Dieser Eintrag wird in der Datei `USERLIST.DAT` unverschlüsselt gespeichert. Soll die Echtheitsbestätigung über das AD beispielsweise innerhalb der Windows-Domäne `ALTN` erfolgen, wird im Kennwortfeld in MDaemon der Text `\\ALTN` eingetragen. Die beiden Backslash-Zeichen teilen MDaemon mit, dass das Kennwortfeld den Namen einer Windows-Domäne enthält, und dass MDaemon daher die Echtheitsbestätigung für die mit USER und PASS übermittelten Werte in Echtzeit über die Benutzerdatenbank dieser Windows-Domäne durchführen soll. Reguläre Kennwörter dürfen nicht mit zwei Backslash-Zeichen beginnen, weil dadurch immer die Prüfung über das AD ausgelöst und der Text nach den Backslash-Zeichen als Windows-Domänenname und nicht als Kennwort behandelt wird.

Die Kombination aus zwei Backslash-Zeichen und dem Windows-Domänennamen kann im Abschnitt Benutzerkonto 714 des Benutzerkonten-Managers jederzeit in das Kennwortfeld eines Benutzerkontos eingetragen werden. Die Konfiguration der dynamischen Echtheitsbestätigung über das AD ist nicht auf den hier beschriebenen Importvorgang beschränkt.

Siehe auch:

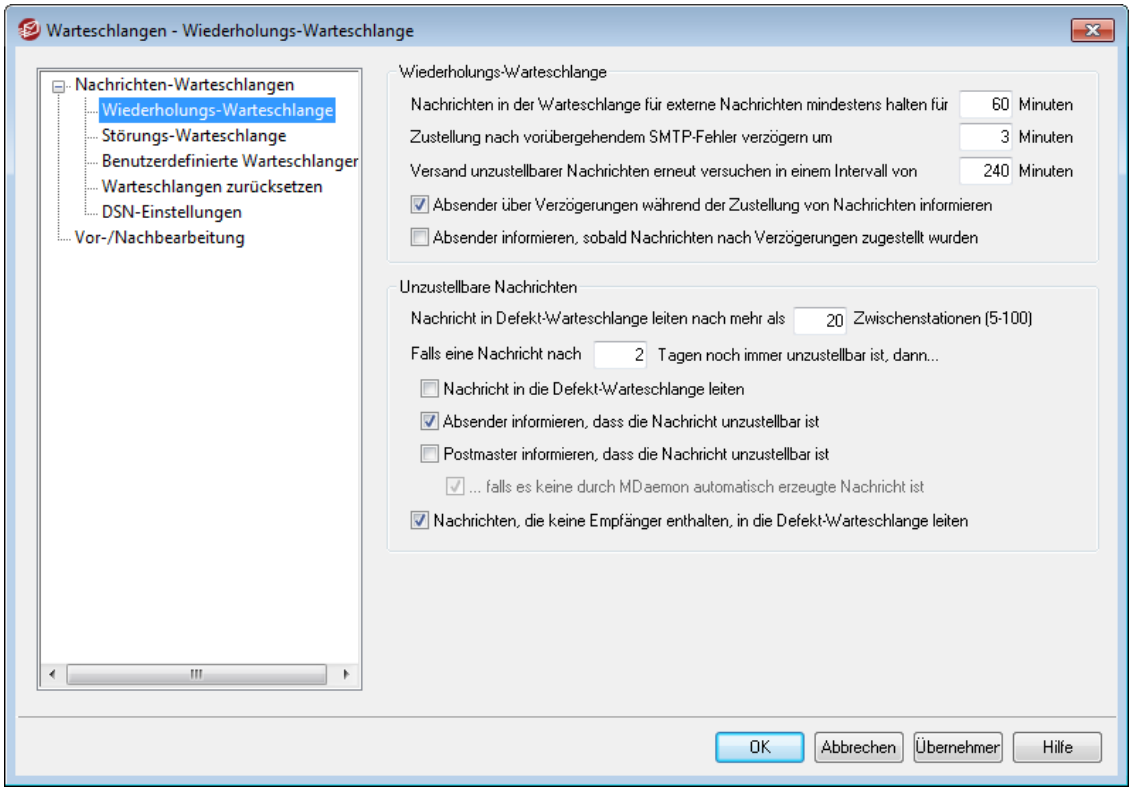
Import von Benutzerkonten aus einer Textdatei 856
Benutzerkonten-Editor » Benutzerkonto 714

Kapitel

6 Das Menü Warteschlangen

6.1 Nachrichten-Warteschlangen

6.1.1 Wiederholungs-Warteschlange



Die Wiederholungs-Warteschlange ist erreichbar über Warteschlangen » Nachrichten-Warteschlangen. Sie dient der Bearbeitung von Nachrichten durch MDaemon, die aufgrund eines nicht endgültigen Fehlers nicht zugestellt werden konnten, etwa, weil der Server der Gegenstelle vorübergehend nicht erreichbar war.

Wiederholungs-Warteschlange

Nachrichten in der Warteschlange für externe Nachrichten mindestens halten für [xx] Minuten
Hiermit wird festgelegt, wie lange eine Nachricht in der Warteschlange für externe Nachrichten verbleiben soll, bevor sie in die Wiederholungs-Warteschlange für erneute Zustellversuche verschoben wird. Die Warteschlange für externe Nachrichten versucht schneller und öfter, die Nachrichten zuzustellen als die Wiederholungs-Warteschlange.

Zustellung nach vorübergehendem SMTP-Fehler verzögern um [xx] Minuten
Tritt bei einem Zustellversuch über SMTP ein vorübergehender SMTP-Fehler (Fehlerkodes 4xx) auf, so verzögert MDaemon die weiteren Zustellversuche um die hier in Minuten angegeben Zeit. Dies verhindert, dass MDaemon erneute Zustellversuche in zu kurzer Folge unternimmt. Per Voreinstellung beträgt die Verzögerung 3 Minuten. Falls Sie keine Verzögerung bei erneuten Zustellversuchen nach vorübergehenden SMTP-Fehlern wünschen, setzen Sie den Wert auf 0.

Versand unzustellbarer Nachrichten erneut versuchen in einem Intervall von [xx] Minuten
Diese Einstellung legt das Intervall fest, in dem die Nachrichten aus der Wiederholungs-Warteschlange verarbeitet werden.

Absender über Verzögerungen während der Zustellung von Nachrichten informieren
Per Voreinstellung benachrichtigt MDaemon den Absender, wenn eine Nachricht wegen eines vorübergehend auftretenden Fehlers nicht zugestellt werden konnte und daher in die Wiederholungs-Warteschlange eingestellt wurde. Falls Sie diese Benachrichtigungen nicht wünschen, deaktivieren Sie diese Option.

Absender informieren, sobald Nachrichten nach Verzögerungen zugestellt werden
Diese Option bewirkt, dass der Absender informiert wird, sobald eine Nachricht nach einer zuvor eingetretenen Verzögerung noch zugestellt werden konnte. Diese Option ist per Voreinstellung abgeschaltet.

Unzustellbare Nachrichten

Nachricht in Defekt-Warteschlange leiten nach mehr als [xx] Zwischenstationen (5-100)
Nach den RFC-Standards muss ein Mailserver jede Nachricht jedes Mal dann mit einem Stempel versehen, wenn er sie bearbeitet. Diese Stempel können gezählt und für eine Sperre gegen Endlosschleifen im Postweg verwendet werden. Solche Endlosschleifen können manchmal wegen fehlerhafter Konfigurationen auftreten. Werden sie nicht entdeckt, erhöhen sie unnötig die Systemlast. Indem gezählt wird, wie oft eine Nachricht bearbeitet wurde, können Nachrichten in Endlosschleifen erkannt und in die Defekt-Warteschlange verschoben werden; hierbei liegt die Vermutung zugrunde, dass eine Endlosschleife vorliegt, falls eine Nachricht nach der Verarbeitung durch eine vorgegebene Anzahl von Mail-Servern ihren Adressaten immer noch nicht erreicht hat. Die Voreinstellung für diese Funktion dürfte in den meisten Fällen ausreichend sein, um Endlosschleifen zu erkennen; sie muss daher in der Regel nicht geändert werden.

Falls eine Nachricht nach [xx] Tagen noch immer unzustellbar ist, dann...
Diese Einstellung legt fest, wie viele Tage eine Nachricht in der Wiederholungs-Warteschlange verbleibt, bevor eine der nachfolgenden Aktionen durchgeführt wird. Wird in diesem Feld der Wert 0 eingetragen, so wird die Nachricht nach der ersten fehlgeschlagenen Wiederholung an den Absender zurück geleitet. Die Voreinstellung beträgt 2 Tage.

Nachricht in die Defekt-Warteschlange leiten
Ist diese Option aktiv, so werden Nachrichten in die Defekt-Warteschlange geleitet, sobald die Zeitbegrenzung aus der Option "*Falls eine Nachricht nach [xx] Tagen noch immer unzustellbar ist, dann...*" weiter oben erreicht ist.

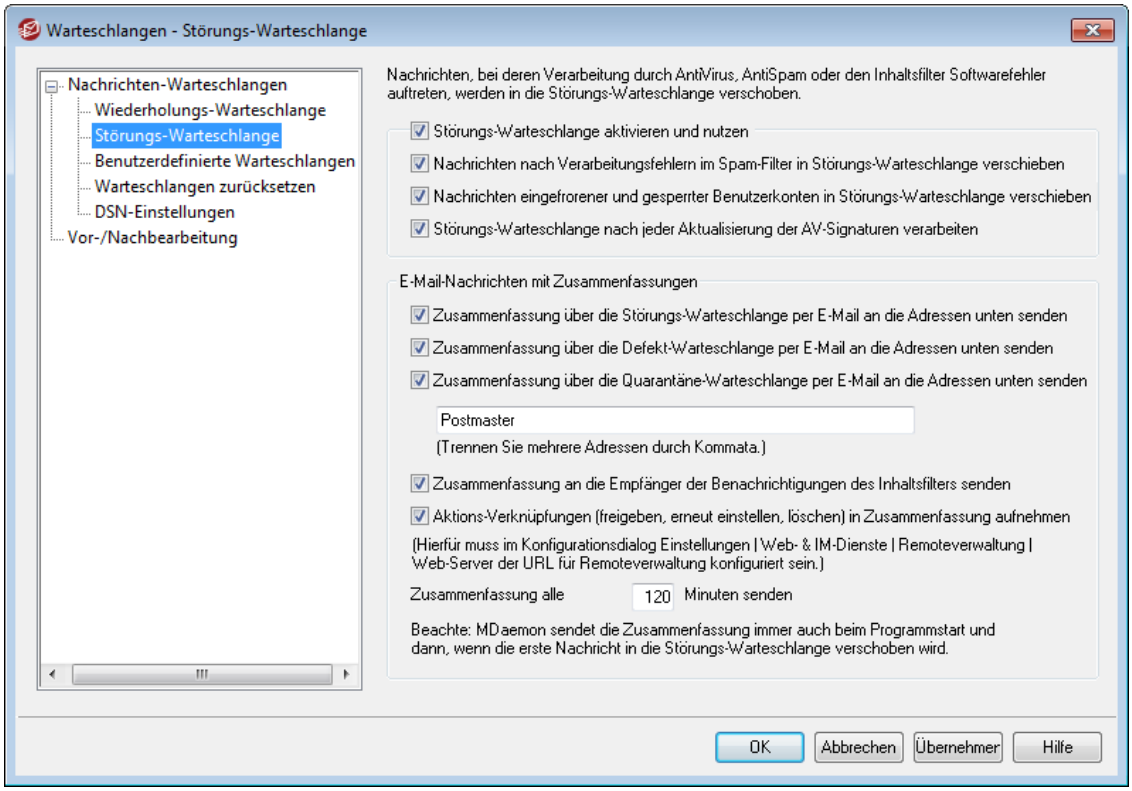
Absender informieren, dass die Nachricht unzustellbar ist
Diese Option bewirkt, dass MDaemon den Absender einer Nachricht durch eine Benachrichtigung über den Zustellstatus 872 informiert, sobald eine Nachricht dieses Absenders die Zeitbegrenzung aus der Option "*Falls eine Nachricht nach [xx] Tagen noch immer unzustellbar ist...*" erreicht hat. Die Benachrichtigung teilt dem Absender mit, dass die Nachricht endgültig vom Server entfernt wurde.

Postmaster informieren, dass die Nachricht unzustellbar ist
Ist diese Option aktiv, so wird der Postmaster benachrichtigt, wenn eine Nachricht endgültig aus der Wiederholungs-Warteschlange gelöscht wird.

...falls es keine durch MDaemon automatisch erzeugte Nachricht ist
MDaemon erhält normalerweise keine Nachricht, wenn eine automatisch erzeugte Nachricht unzustellbar ist. Da diese Information aber für den Postmaster interessant sein kann, wird er informiert, wenn solche Nachrichten nicht zugestellt werden können. Mit dieser Option lässt sich die Benachrichtigung des Postmasters von unzustellbaren automatisch erzeugten Nachrichten unterbinden. Automatisch erzeugte Nachrichten sind z.B. Empfangsbestätigungen, Nachrichten von Autobeantwortern, Ergebnisse von Änderungen am Benutzerkonto und anderes.

Nachrichten, die keine Empfänger enthalten, in die Defekt-Warteschlange verschieben
Diese Option bewirkt, dass Nachrichten, die keine Daten über einen Empfänger enthalten, in die Warteschlange für defekte Nachrichten verschoben werden. Ist diese Option deaktiviert, dann werden solche Nachrichten gelöscht. Die Option ist per Voreinstellung aktiv.

6.1.2 Störungs-Warteschlange



Die Störungs-Warteschlange ist erreichbar über Warteschlangen » Nachrichten-Warteschlangen. Diese Warteschlange nimmt Nachrichten auf, bei deren Verarbeitung durch AntiVirus, AntiSpam oder den Inhaltsfilter Softwarefehler oder Ausnahmefehler aufgetreten sind. Tritt bei der Verarbeitung einer Nachricht ein solcher Fehler auf, so wird die Nachricht in die Störungs-Warteschlange verschoben und nicht zugestellt.

Die Nachrichten verbleiben in der Störungs-Warteschlange, bis der Systemverwalter entscheidet, was mit ihnen zu geschehen hat. In der Haupt-Benutzeroberfläche von MDaemon befindet sich Steuerelement *Störungs-Warteschlange verarbeiten*, und im Menü Warteschlangen ist ein gleich lautender Eintrag enthalten. Die Nachrichten können auch durch die Option "*Erneut in die Warteschlange*" im Kontextmenü der Störungs-Warteschlange verarbeitet werden. Durch Auswahl dieser Option werden alle Nachrichten aus der Störungs-Warteschlange, je nach Empfänger, in die lokale und die externe Warteschlange eingestellt und von dort aus normal weiter verarbeitet. Tritt der Fehler, aufgrund dessen die Nachricht in die Störungs-Warteschlange verschoben wurde, erneut auf, so wird die Nachricht wiederum in die Störungs-Warteschlange verschoben. Falls die Nachrichten aus der Störungs-Warteschlange ohne Rücksicht auf die aufgetretenen möglicherweise erneut auftretenden Fehler zugestellt werden sollen, kann der Inhalt der Störungs-Warteschlange durch den Befehl "*Freigeben*" im Kontextmenü zur Zustellung freigegeben werden. Es erscheint ein Sicherheitshinweis und erinnert den Bediener daran, dass die Nachrichten vireninfiziert sein oder aus anderen Gründen den Inhaltsfilter, AntiSpam oder AntiVirus nicht richtig durchlaufen könnten.

Störungs-Warteschlange

Störungs-Warteschlange aktivieren und nutzen
Durch Aktivieren dieser Option wir die Störungs-Warteschlange aktiviert. Nachrichten, bei deren Verarbeitung durch AntiVirus und Inhaltsfilter Softwarefehler oder Ausnahmefehler auftreten, werden dann in diese Warteschlange verschoben.

Nachrichten nach Verarbeitungsfehlern im Spam-Filter in Störungs-Warteschlange verschieben
Ist diese Option aktiv, so werden Nachrichten in die Störungs-Warteschlange verschoben, falls während ihrer Verarbeitung durch den Spam-Filter Fehler aufgetreten sind.

Nachrichten eingefrorener und gesperrter Benutzerkonten in Störungs-Warteschlange verschieben
Ist diese Option aktiv, so verschiebt MDaemon automatisch solche Nachrichten in die Störungs-Warteschlange, bei denen die Benutzerkonten des Absenders oder des Empfängers oder beider Benutzer gesperrt oder eingefroren sind.

Störungs-Warteschlange nach jeder Aktualisierung der AV-Signaturen verarbeiten
Ist diese Option aktiv, so wird die Störungs-Warteschlange automatisch verarbeitet, sobald die Viren-Signaturen für AntiVirus 648 aktualisiert wurden.

E-Mail-Nachrichten mit Zusammenfassungen

Zusammenfassung über die Störungs-Warteschlange per E-Mail an die Adressen unten senden
Mithilfe dieser Option können Sie eine Zusammenfassung über die Nachrichten in der Störungs-Warteschlange in regelmäßigen Abständen an eine oder mehrere E-Mail-Adressen senden lassen. Die Empfänger-Adressen tragen Sie in das dafür vorgesehene Textfeld weiter unten ein.

Zusammenfassung über die Defekt-Warteschlange per E-Mail an die Adressen unten senden
Mithilfe dieser Option können Sie eine Zusammenfassung über die Nachrichten in der Defekt-Warteschlange in regelmäßigen Abständen an eine oder mehrere E-Mail-Adressen senden lassen. Die Empfänger-Adressen tragen Sie in das dafür vorgesehene Textfeld weiter unten ein.

Empfänger für die Zusammenfassungen
In dieses Textfeld tragen Sie die E-Mail-Adressen ein, an die die Zusammenfassungen über die Störungs- und Defekt-Warteschlangen gesandt werden sollen. Trennen Sie mehrere E-Mail-Adressen durch Kommata.

MDaemon versendet die Benachrichtigungen beim Programmstart, bei Verschieben der ersten Nachricht in die Störungs-Warteschlange, und zusätzlich in dem Intervall, das im Feld *Zusammenfassung alle [xx] Minuten senden* eingetragen ist.

Falls eine solche Benachrichtigung selbst Software- oder Ausnahmefehler verursacht, so wird sie zwar an lokale, nicht aber an externe Empfänger zugestellt.

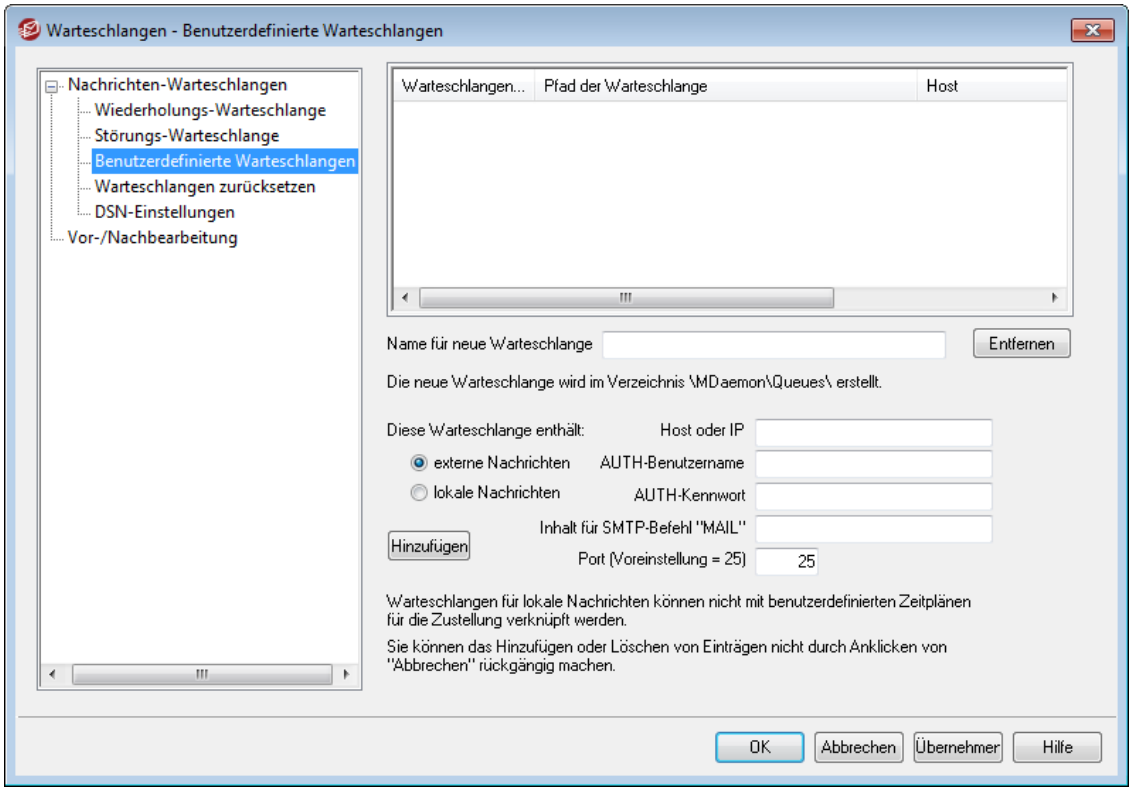
Zusammenfassung an die Empfänger der Benachrichtigungen des Inhaltsfilters senden
Diese Option bewirkt, dass zusätzlich zu den oben angegebenen Empfängern auch die Empfänger[667] der Benachrichtigungen des Inhaltsfilters eine Benachrichtigung über den Inhalt der Störungs-Warteschlange erhalten.

Aktions-Verknüpfungen (freigeben, erneut einstellen, löschen) in Zusammenfassung aufnehmen
Per Voreinstellung enthalten die E-Mail-Nachrichten mit den Zusammenfassungen der Störungs-, Quarantäne- und Defekt-Warteschlangen Verknüpfungen, mit deren Hilfe jede Nachricht freigegeben, erneut in die Warteschlange eingestellt und gelöscht werden können. Falls Sie nicht wünschen, dass diese Verknüpfungen in die Zusammenfassungen aufgenommen werden, deaktivieren Sie diese Option.

Diese Verknüpfungen können nur erstellt werden, wenn der URL für die Remoteverwaltung[352] konfiguriert ist.

Zusammenfassung alle [xx] Minuten senden
Der Wert in diesem Feld bestimmt das Intervall, in dem MDaemon die Benachrichtigungen an die angegebenen Empfänger und, falls zutreffend, auch an die Empfänger der Benachrichtigungen des Inhaltsfilters sendet.

6.1.3 Benutzerdefinierte Warteschlangen



Mithilfe des Konfigurationsdialogs Benutzerdefinierte Warteschlangen, erreichbar über Warteschlangen » Nachrichten-Warteschlangen können Sie benutzerdefinierte Warteschlangen für lokale und externe Nachrichten erstellen. Die Unterstützung für benutzerdefinierte Warteschlangen macht es möglich, dass MDaemon verschiedene Speicherorte überwacht, von denen aus Nachrichten zu versenden sind. Mithilfe des Inhaltsfilters lassen sich Nachrichten automatisch in die benutzerdefinierten Warteschlangen verschieben; für benutzerdefinierte Warteschlangen für externe Nachrichten können außerdem eigene Zeitpläne 378 angelegt werden, die bestimmen, wann diese Warteschlangen verarbeitet werden sollen.

Benutzerdefinierte Warteschlangen

In diesem Abschnitt wird für jede benutzerdefinierte Warteschlange ein Eintrag angezeigt, der auch Auskunft über den Pfad der Warteschlange und darüber gibt, ob die Warteschlange lokale oder externe Nachrichten verarbeitet.

Entfernen

Soll eine Warteschlange gelöscht werden, muss ihr Eintrag ausgewählt und dann dieses Steuerelement angeklickt werden.

> Wird eine benutzerdefinierte Warteschlange gelöscht, so werden alle benutzerdefinierten Zeitpläne und Regeln des Inhaltsfilters, die mit dieser Warteschlange verknüpft sind, ebenfalls gelöscht.

Name für neue Warteschlange

In diesem Feld geben Sie den Namen für die neue Nachrichten-Warteschlange an. Die Warteschlange wird im MDaemon-Verzeichnis `\MDaemon\Queues\` erstellt.

Warteschlange unter dem Verzeichnis Queues erstellen (Deaktivieren Sie diese Option, um einen Pfad auszuwählen.)
Ist diese Option aktiv, so wird der neue Warteschlangenname, der im Feld "*Name oder Verzeichnispfad…*" eingetragen wird, als Unterverzeichnis unter dem MDaemon-Verzeichnis `\queues\` angelegt. Wird diese Option abgeschaltet, so wird der neue Warteschlangenname als Unterverzeichnis unter dem MDaemon-Verzeichnis `\app\` angelegt. Ist diese Option deaktiviert, so kann auch ein vollständiger Pfadname in das Feld eingetragen oder über Durchsuchen ein Pfad ausgewählt werden, in dem eine neue Warteschlange angelegt werden soll.

Diese Warteschlange enthält...

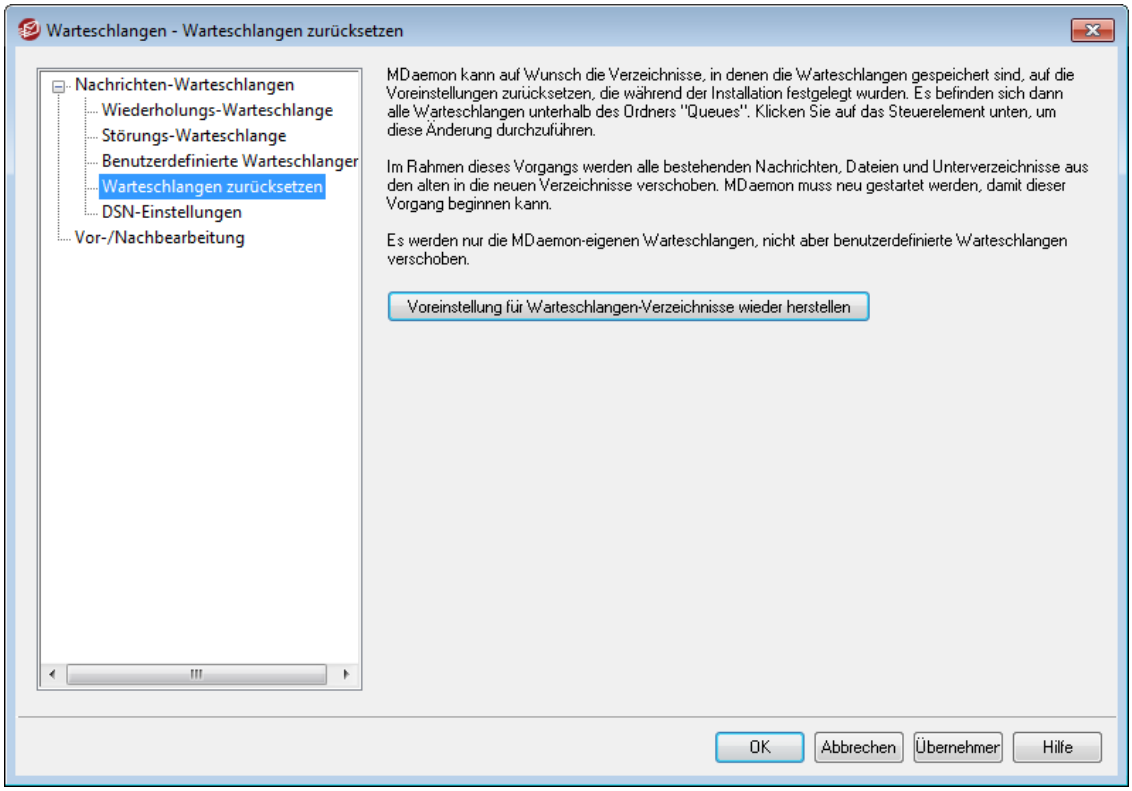
...externe Nachrichten
Soll die Warteschlange für externe Nachrichten verwendet werden, muss diese Option aktiv sein.

Anmeldedaten für die Warteschlangen
Sie können für externe Warteschlangen einen *Host* oder eine *IP*, *AUTH-Benutzernamen* und *AUTH-Kennwörter*, den *Inhalt für den SMTP-Befehl "Mail"* und einen *Port* angeben. Diese Einstellungen werden für die Zustellung aller Nachrichten aus der externen Warteschlange verwendet, der sie zugeordnet sind. Für einzelne Nachrichten in den Warteschlangen können unter Umständen abweichende Einstellungen zur Zustellung getroffen sein; in diesem Fall gehen diese abweichenden Einstellungen den hier getroffenen Einstellungen vor.

...lokale Nachrichten
Soll die Warteschlange für lokale Nachrichten verwendet werden, muss diese Option aktiv sein. **Beachte:** Warteschlangen für lokale Nachrichten unterstützen keine benutzerdefinierten Zeitpläne für die Zustellung.

Hinzufügen
Nachdem der Name und der Typ der Warteschlange festgelegt wurden, wird die Warteschlange durch einen Klick auf das Steuerelement *Hinzufügen* in die Liste der benutzerdefinierten Warteschlangen aufgenommen.

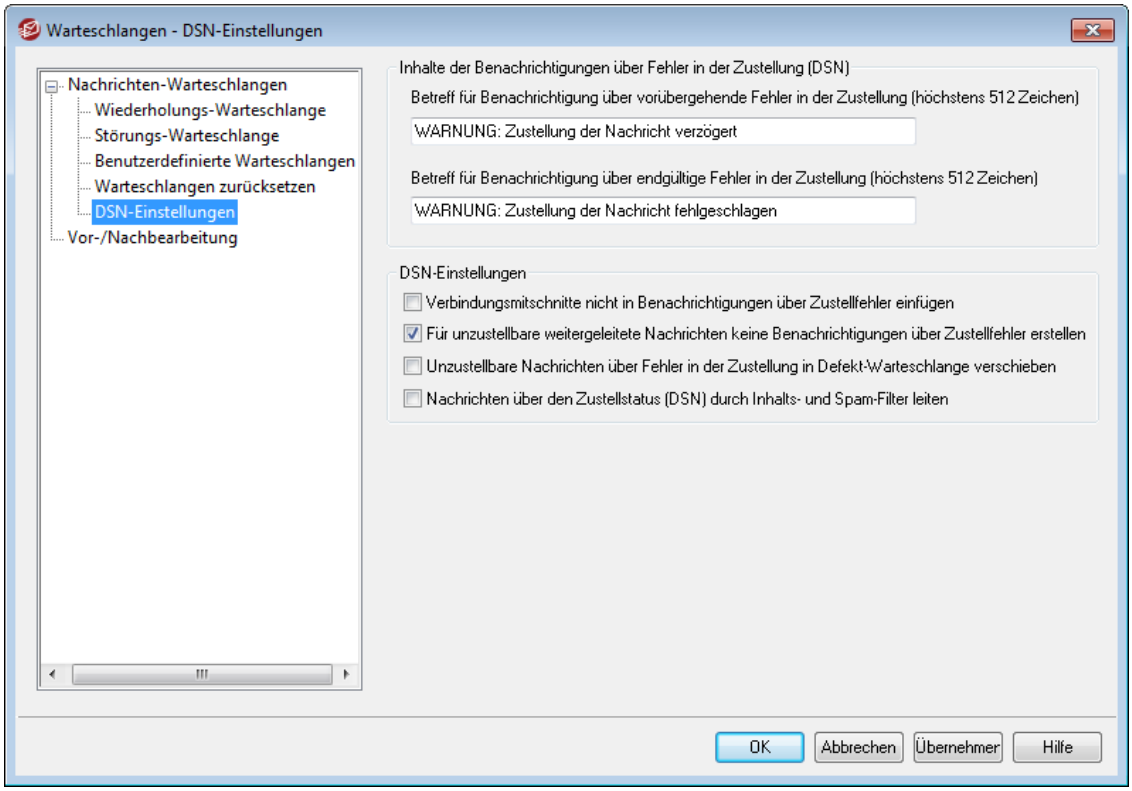
6.1.4 Warteschlangen zurücksetzen



Voreinstellung für Warteschlangen-Verzeichnisse wieder herstellen
Nach einer Neuinstallation speichert MDaemon die Nachrichten-Warteschlangen, wie etwa externe, lokale, RAW- und andere Warteschlangen per Voreinstellung in Verzeichnissen unter `\MDaemon\Queues\`. Frühere MDaemon-Versionen nutzten teils andere Speicherorte und Verzeichnisstrukturen. Falls eine bestehende MDaemon-Installation noch die alte Verzeichnisstruktur verwendet, und die Speicherorte der Warteschlangen in die neue und besser organisierte Verzeichnisstruktur überführt werden sollen, kann dies durch Klick auf dieses Steuerelement erreicht werden. MDaemon verschiebt dann alle Warteschlangen und die in ihnen enthaltenen Nachrichten und sonstigen Dateien in die neue Verzeichnisstruktur. MDaemon muss danach neu gestartet werden, damit die Änderungen wirksam werden.

Benutzerdefinierte Warteschlangen 869 bleiben durch diese Funktion unberührt.

6.1.5 DSN-Einstellungen



Versucht MDaemon eine Nachricht zuzustellen, und tritt dabei ein Fehler auf, so übermittelt MDaemon eine Benachrichtigung über diesen Fehler in der Zustellung an den Absender der Nachricht. Eine solche Benachrichtigung wird nach dem englischen Begriff "Delivery Status Notification" (Benachrichtigung über den Status der Zustellung) auch kurz als "DSN" bezeichnet. MDaemon versendet solche Benachrichtigungen bei vorübergehenden und bei endgültigen Fehlern in der Zustellung. Mithilfe dieses Konfigurationsdialogs können Sie verschiedene Optionen für solche Benachrichtigungen konfigurieren. Sie erreichen diesen Konfigurationsdialog über Warteschlangen » Nachrichten-Warteschlangen/DSN... » DSN-Optionen.

Inhalte der Benachrichtigungen über Fehler in der Zustellung (DSN)

Betreff für Benachrichtigung über vorübergehende Fehler in der Zustellung (höchstens 512 Zeichen)
In dieses Textfeld tragen Sie die Betreffzeile für Benachrichtigungen ein, die MDaemon nach einem vorübergehenden Fehler in der Zustellung übermittelt, der eine Verzögerung in der Zustellung verursacht. Ist beispielsweise der Mail-Server des Empfängers nicht erreichbar, während MDaemon versucht, die Nachricht zu übermitteln, so versucht MDaemon in festgelegten Intervallen die Zustellung erneut und informiert den Absender mithilfe dieser Benachrichtigung von dem Problem.

Betreff für Benachrichtigung über endgültige Fehler in der Zustellung (höchstens 512 Zeichen)
In dieses Textfeld tragen Sie die Betreffzeile für Benachrichtigungen ein, die MDaemon nach einem endgültigen Fehler in der Zustellung übermittelt, der es MDaemon endgültig unmöglich macht, die Nachricht zuzustellen. Weist beispielsweise der Mail-Server des Empfängers die Nachricht ab, etwa mit der

Begründung, dass die E-Mail-Adresse des Empfängers unbekannt sei, so unternimmt MDaemon keine weiteren Zustellversuche und informiert den Absender mithilfe dieser Benachrichtigung darüber, dass die Zustellung der Nachricht endgültig fehlgeschlagen ist.

Optionen für die Benachrichtigungen über Fehler in der Zustellung (DSN)

Verbindungsmitschnitte nicht in Benachrichtigungen über Zustellfehler einfügen
Diese Option bewirkt, dass der SMTP-Verbindungsmitschnitt in Benachrichtigungen über vorübergehende und endgültige Fehler in der Zustellung nicht eingefügt wird. Diese Option ist per Voreinstellung abgeschaltet.

Für unzustellbare weitergeleitete Nachrichten keine Benachrichtigungen über Zustellfehler erstellen
Ist diese Option aktiv, so werden weitergeleitete Nachrichten, deren Zustellung endgültig fehlgeschlagen, oder deren Haltezeit in der Wiederholungs-Warteschlange 864 abgelaufen ist, in die Defekt-Warteschlange verschoben, und es wird dem ursprünglichen Absender keine Benachrichtigung über den Fehler in der Zustellung übermittelt. Diese Option ist per Voreinstellung aktiv.

Für unzustellbare Listen-Nachrichten keine Benachrichtigungen über Zustellfehler erstellen
Ist diese Option aktiv, so werden Nachrichten aus Mailinglisten, deren Zustellung endgültig fehlgeschlagen, oder deren Haltezeit in der Wiederholungs-Warteschlange abgelaufen ist, gelöscht, und es wird keine Benachrichtigung über den Fehler in der Zustellung erstellt. Ist diese Option abgeschaltet, so wird eine Benachrichtigung über den Fehler in der Zustellung an die *SMTP-"Bounce"-Adresse für diese Liste* 290 übermittelt. Diese Option ist per Voreinstellung abgeschaltet.

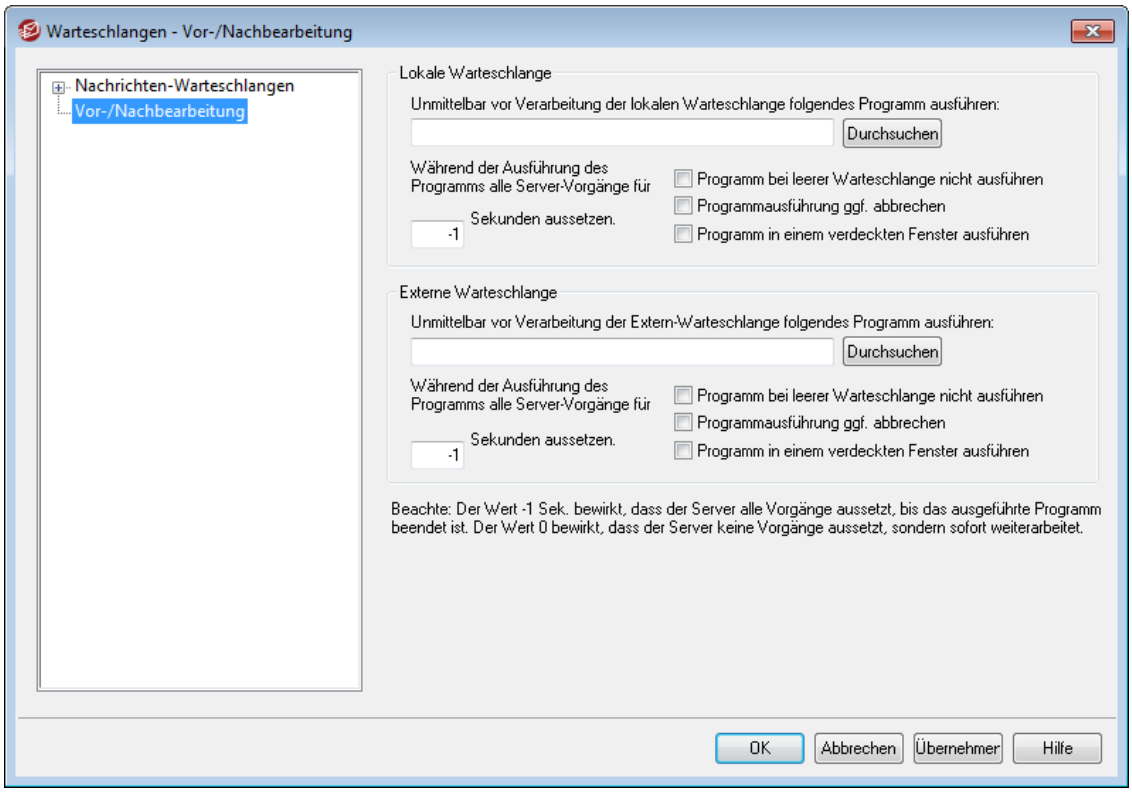
Unzustellbare Nachrichten über Fehler in der Zustellung in Defekt-Warteschlange verschieben
Diese Option bewirkt, dass Benachrichtigungen über Zustellfehler (kurz auch DSN von "Delivery Status Notifications"), bei deren Versand selbst Zustellfehler aufgetreten sind, in die Defekt-Warteschlange und nicht in die Wiederholungs-Warteschlange verschoben werden.

Diese Einstellung betrifft nur Benachrichtigungen über Zustellfehler, die MDaemon selbst erstellt hat.

Siehe auch:

Wiederholungs-Warteschlange 864

6.2 Vor-/Nachbearbeitung



Vor- und Nachbearbeitung für lokale und externe Warteschlange

Unmittelbar vor Verarbeitung der lokalen Warteschlange folgendes Programm ausführen
In diesem Feld werden Pfad und Dateiname eines Programms angegeben, das unmittelbar vor der Bearbeitung und Zustellung von Nachrichten im RFC-2822-Format aus der lokalen oder externen Nachrichten-Warteschlangen ausgeführt wird. Wird kein kompletter Pfad angegeben, sucht MDaemon das Programm zuerst im MDaemon-Verzeichnis, dann im Windows-System-Verzeichnis, danach im Windows-Verzeichnis und schließlich in den Verzeichnissen, die in der Umgebungsvariable PATH angegeben sind.

Während der Ausführung des Programms alle Server-Vorgänge für [xx] Sekunden aussetzen
Dieser Wert gibt vor, wie sich MDaemon während der Ausführung des oben angegebenen Programms verhalten soll. MDaemon kann so konfiguriert werden, dass sein Hauptthread für die angegebene Anzahl Sekunden ausgesetzt wird, während MDaemon auf das Ende des angegebenen Programms wartet. Ist das Programm vor dem Zeitablauf beendet, nimmt MDaemon die Bearbeitung sofort wieder auf. Der Wert -1 bewirkt, dass MDaemon ohne jede Zeitbegrenzung auf das Ende des Programms wartet.

Programm bei leerer Warteschlange nicht ausführen
Wenn das angegebene Programm bei leerer Nachrichten-Warteschlange nicht ausgeführt werden soll, muss diese Option gesetzt werden.

Programmausführung ggf. abbrechen
Unter Umständen beendet sich das ausgeführte externe Programm nicht selbst. Diese Option veranlasst MDaemon, die Programmausführung dann abzubrechen, wenn die in dem Feld *...alle Server-Vorgänge für x Sekunden aussetzen* angegebene Zeit abgelaufen ist. Ist dort der Wert -1 eingetragen, so ist diese Funktion wirkungslos.

Programm in einem verdeckten Fenster ausführen
Soll das externe Programm in einem versteckten Fenster ausgeführt werden, muss diese Option ausgewählt werden.

6.3 Warteschlangen- und Statistik-Manager

Der Warteschlangen- und Statistik-Manager (auch kurz "MDStats")ist in MDaemon über den Menüeintrag Warteschlangen » Warteschlangen- und Statistik-Manager erreichbar. Der Warteschlangen- und Statistik-Manager ist in vier Registerkarten unterteilt. Jede dieser Registerkarten ist für bestimmte Funktionen gedacht und in einem übersichtlichen Format gehalten, das die Bedienung sehr einfach macht.

Registerkarte Warteschlangen 876

Die Registerkarte *Warteschlangen* wird nach Programmstart immer geöffnet. Von hier aus lassen sich die Warteschlangen und die Postverzeichnisse der Benutzerkonten sehr einfach verwalten. Ein Klick auf die gewünschte Warteschlange oder das gewünschte Benutzerkonto wird eine Liste aller jeweils enthaltenen Nachrichten und wichtiger weiterer Informationen hierzu angezeigt. Diese Informationen sind Absender, Empfänger, der Inhalt der Kopfzeile "Deliver-To" ("Zustellen an"), Betreff, Größe und die Haltedauer für die gegenwärtige Position. Außerdem sind Steuerelemente vorgesehen, mit denen sich die Nachrichten zwischen den Ordnern verschieben oder aus ihnen löschen lassen.

Registerkarte Benutzer 879

Die Registerkarte *Benutzer* zeigt alle Benutzerkonten, die in MDaemon angelegt sind. Die Liste enthält den Klartextnamen, den Postfachnamen, die Anzahl der Nachrichten im Postfach, den belegten Speicherplatz und das Datum des letzten Postabrufs. Diese Liste kann auch als Textdatei und wahlweise mit Kommata als Feldbegrenzer für Datenbanken gespeichert werden.

Registerkarte Protokollübersicht 880

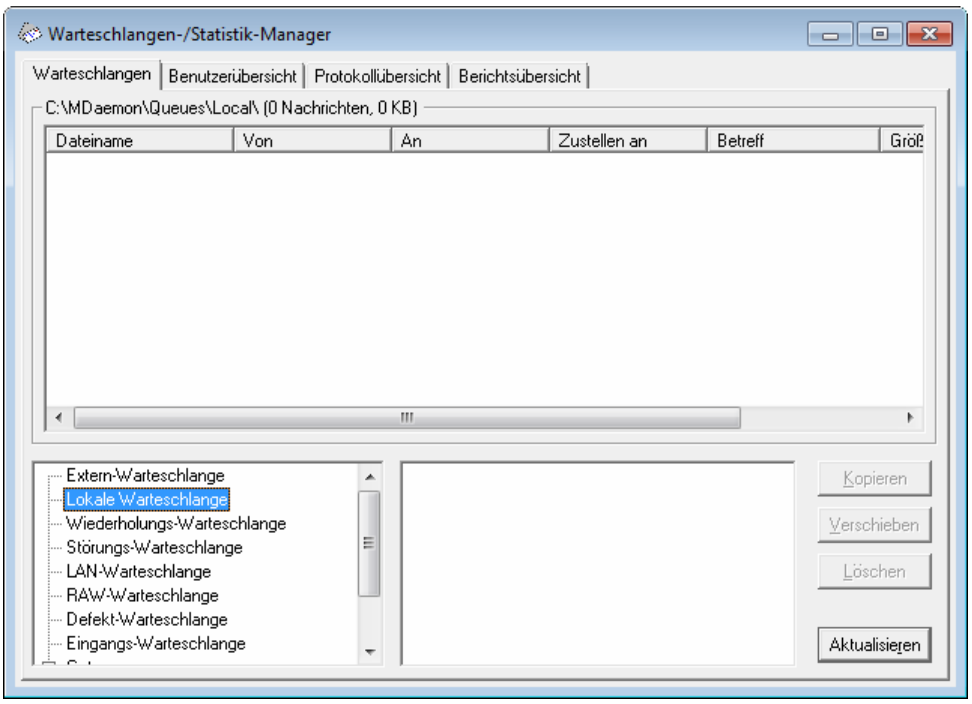
Auf dieser Registerkarte lässt sich die *Protokollübersicht* von MDaemon als einfache Liste anzeigen. Damit kann man sich schnell einen Überblick über die Server-Aktivität verschaffen, da das Protokoll zusammengefasst und in Spaltenform dargestellt wird. Die Spalten sind Nachrichtentyp (eingehend durch POP, DomainPOP, RFC 2822 u.s.w.), Gegenstelle, Absender Empfänger, Nachrichtengröße, Verarbeitungsdatum und ob die Verarbeitung erfolgreich war. Genauere Informationen zu den einzelnen Einträgen erhält man durch einen Doppelklick auf den gewünschten Eintrag. Hierdurch wird der interessierende Protokoll-Ausschnitt im Original gezeigt. Die hier angezeigten Protokolle können auch als Textdateien und wahlweise mit Kommata als Feldbegrenzer für Datenbanken gespeichert werden.

Registerkarte Berichtsübersicht 882

Die letzte Registerkarte stellt *Berichte* dar. Mit dieser Funktion kann eine Zusammenfassung aller Einstellungen von MDaemon als reine Textdatei erstellt

werden. Wegen der großen Zahl an Einstellungen und zusätzlichen Konfigurationsmöglichkeiten, die MDaemon bietet, können hiermit die Einführung von Änderungen und die Fehlersuche stark beschleunigt werden. Der Bericht wird editierbar dargestellt, sodass die Funktionen der Zwischenablage über die rechte Maustaste verfügbar sind. Vor dem Speichern der Datei lassen sich damit einfach Textteile ausschneiden und kopieren oder Anmerkungen einfügen.

6.3.1 Registerkarte Warteschlangen



Das Anzeigefenster für Warteschlangen

Wird eine Warteschlange oder ein Benutzer aus dem Bereich *Warteschlangen* ausgewählt, so erscheint eine Liste aller Nachrichtendateien der ausgewählten Warteschlange im Hauptfenster dieser Seite. Diese Liste enthält Dateinamen, Absender, Empfänger, Inhalt der Kopfzeile "Deliver-To" ("Ausliefern an"), Betreff, Größe und Datum und Uhrzeit, seit wann die Nachricht in der Warteschlange liegt.

Über diesem Fenster stehen der Pfad zu der gerade angezeigten Warteschlange, die Gesamtzahl der angezeigten Nachrichten und die Größe des Verzeichnisses.

Dateien können kopiert, verschoben oder gelöscht werden, indem eine oder mehrere aus der Liste ausgewählt werden und die gewünschte Aktion durch den entsprechenden Knopf ausgelöst wird.

Der Inhalt der angezeigten Dateien kann ebenfalls direkt von hier aus geändert werden. Die zu editierende Datei wird durch einen Doppelklick oder den Menüpunkt "Editieren" aus ihrem Kontextmenü im Editor von Windows geöffnet.

Soll MDStats standardmäßig einen anderen Editor verwenden, so muss die Datei `mdstats.ini` im Verzeichnis `\MDaemon\app\` geändert werden. In dem Eintrag "`Editor=`" im Abschnitt `[QueueOptions]` muss als Wert der Name des gewünschten Editor eingetragen werden, z.B.

> `Editor=MeinEditor.exe`. Wenn sich die Datei nicht im aktuellen Verzeichnis befindet, muss der komplette Pfadname mit angegeben werden.

Das Listenfenster kann mit den senkrechten und waagrechten Rollbalken oder, nach einem Klick auf eine beliebige Stelle innerhalb des Fensters, mit den Pfeiltasten durchgeblättert werden. Die Anzeige lässt sich nach beliebigen Spalten sortieren. Ein Klick auf eine Spaltenüberschrift sortiert nach dieser Spalte aufsteigend, ein Doppelklick sortiert absteigend. Die Spaltengröße kann geändert werden, indem man den Mauszeiger auf die Linie zwischen den Spaltenüberschriften setzt und dann die Spalte auf die neue Größe zieht.

Auswahl von Dateien

Dateien einzeln auswählen Gewünschte Datei anklicken.

Zusammenhängende Dateien auswählen

Erste gewünschte Datei anklicken, die Hochschalttaste gedrückt halten, und dann die letzte auszuwählende Datei anklicken.

Statt der Maus können auch die Pfeiltasten und Pos 1, Ende, Bild auf und Bild ab bei gedrückter Hochschalttaste verwendet werden.

Nicht zusammenhängende Dateien auswählen

Dateien bei gedrückter Strg-Taste anklicken.

Nachrichten-Warteschlangen
Ein Klick auf einen Eintrag im unteren linken Teil des Fensters zeigt die Dateiliste aus der entsprechenden Warteschlange im Hauptfenster an. Ein Klick auf Benutzerverzeichnisse zeigt alle Benutzerkonten im Fenster rechts neben dem Bereich Warteschlangen an.

Benutzerliste
Hier wird eine Liste aller Benutzer von MDaemon angezeigt, wenn im Bereich Warteschlangen (unterer linker Teil des Fensters) die Benutzerverzeichnisse ausgewählt sind. Ein Klick auf den Eintrag eines Benutzers zeigt eine Liste aller Dateien in seinem Postverzeichnis an.

Aktualisieren
Die Warteschlangen sind dynamisch, so lange MDaemon ausgeführt wird. Es werden laufend Nachrichten zwischen ihnen verschoben. Aus diesem Grund sollte dieser Knopf regelmäßig angeklickt werden, damit die Liste der angezeigten Dateien immer aktuell ist.

Durch eine Änderung in der Datei `MDstats.ini` kann MDStats veranlasst werden, die Anzeige selbsttätig zu aktualisieren. Dazu ist in der Datei im Abschnitt `[QueueOptions]` bei dem Schlüsselwort AutoRefresh ein Wert in Sekunden einzutragen, der zwischen zwei Aktualisierungen liegen soll. Der Wert 0 deaktiviert die automatische Aktualisierung. `AutoRefresh=15` würde beispielsweise die Listen alle 15 Sekunden aktualisieren.

Kopieren
Sind Dateien ausgewählt, so können sie mit diesem Knopf in eine andere Warteschlange oder ein anderes Postverzeichnis kopiert werden. Nach einem Klick auf diesen Knopf öffnet sich das Fenster Nachricht(en) kopieren, wo das Ziel der Kopieraktion ausgewählt werden kann.

Verschieben
Sind Dateien ausgewählt, so können sie mit diesem Knopf in eine andere Warteschlange oder ein anderes Postverzeichnis verschoben werden. Nach einem Klick auf diesen Knopf öffnet sich das Fenster Nachricht(en) verschieben, wo das Ziel der Verschiebeaktion ausgewählt werden kann.

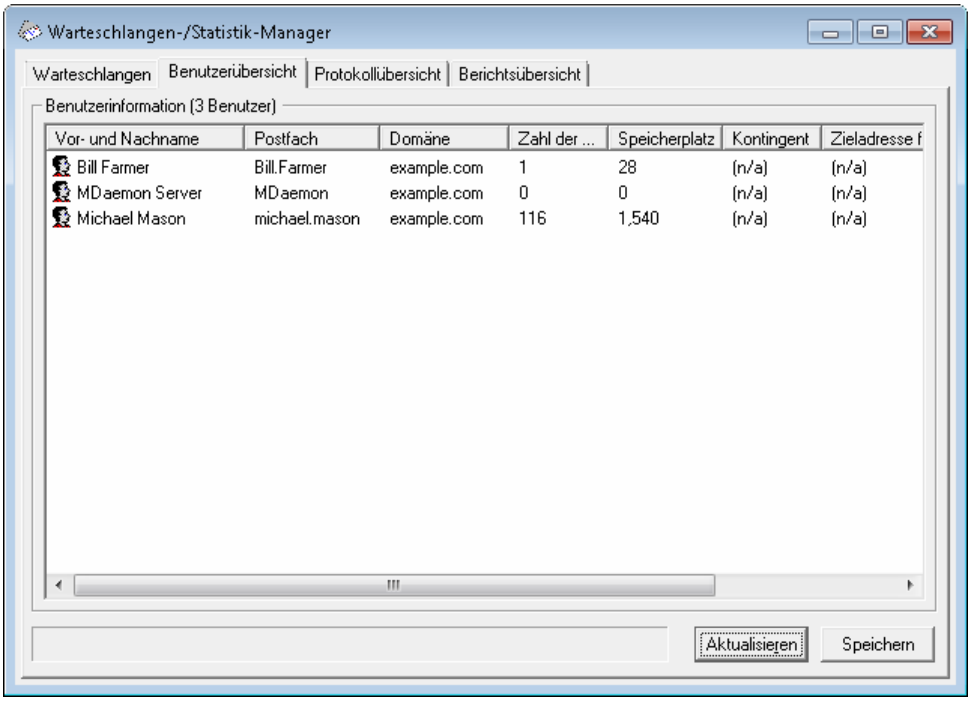
Der Dateiname ändert sich in der Regel beim Kopieren oder Verschieben. Damit im Zielverzeichnis keine gleichnamigen Dateien überschrieben werden, berechnet MDaemon immer anhand der Datei HIWATER.MRK im Zielverzeichnis den nächsten dort gültigen Dateinamen.

Löschen
Hiermit werden die jeweils ausgewählten Dateien aus dem Hauptfenster gelöscht. Vor dem endgültigen Löschvorgang wird eine Sicherheitsabfrage eingeblendet.

Die Warteschlangen sind während der Ausführung von MDaemon dynamisch, da laufend Nachrichtendateien zwischen ihnen verschoben werden. Während des Kopierens, Verschiebens oder Löschens kann daher eine Meldung erscheinen, dass MDStats den ausgewählten Vorgang nicht durchführen kann. Das passiert üblicherweise dann, wenn die gewählte Nachrichtendatei durch MDaemon vor Beginn der Aktion verschoben wurde. Mit dem Knopf Aktualisieren sollte die Dateiliste daher regelmäßig aktualisiert werden.

Durch eine Änderung in der Datei MDstats.ini kann verhindert werden, dass MDaemon Nachrichten verschiebt, die gerade vom Benutzer bearbeitet werden. Dazu wird in der Datei im Abschnitt [QueueOptions] das Schlüsselwort LockOnEdit von No auf Yes gesetzt. Damit erzeugt MDStats eine LCK-Datei, während eine Nachricht editiert wird. Diese verhindert anderweitige Dateioperationen, bis die Bearbeitung der Datei abgeschlossen ist.

6.3.2 Registerkarte Benutzer



Benutzerinformation
Sobald die Seite "Benutzer" aufgerufen wird, lädt MDStats alle Benutzerkonten aus MDaemon und zeigt sie im Fenster Benutzerinformation an. Die Liste enthält für jeden Benutzereintrag den Klartextnamen, Postfachnamen, die Domäne, zu der das Konto gehört, Anzahl und Format der gespeicherten Nachrichten, den belegten Plattenplatz (in Kilobyte), die Weiterleitungsadresse und das Datum des letzten Postabrufs. Da sich die Informationen auch in dieser Liste laufend ändern können, sind regelmäßige Aktualisierungen der List mit Hilfe des Knopfes Aktualisieren ratsam.

Das Listenfenster kann mit den senkrechten und waagrechten Rollbalken oder, nach einem Klick auf eine beliebige Stelle innerhalb des Fensters, mit den Pfeiltasten durchgeblättert werden. Die Anzeige lässt sich nach beliebigen Spalten sortieren. Ein Klick auf eine Spaltenüberschrift sortiert nach dieser Spalte aufsteigend, ein Doppelklick sortiert absteigend. Die Spaltengröße kann geändert werden, indem man den Mauszeiger auf die Linie zwischen den Spaltenüberschriften setzt und dann die Spalte auf die neue Größe zieht. Ein Doppelklick auf einen Benutzereintrag wechselt automatisch auf die Seite Warteschlangen und zeigt dort den Inhalt des zugehörigen Postverzeichnisses an.

Grundsätzlich zeigt diese Liste die Anzahl der Nachrichten und den Plattenplatz, den diese Nachrichtendateien verwenden. Andere etwa in den Postverzeichnissen vorhandene Dateien bleiben außer Betracht. Diese Werte sind dieselben, die MDaemon für ein Kontingent der Benutzer zugrundelegt. Wahlweise kann MDStats auch die physikalisch vorhandenen Dateien und den von ihnen verbrauchten Plattenplatz anzeigen. Hierzu muss in der Datei `MDstats.ini` im Abschnitt `[UserOptions]` das Schlüsselwort `ShowQuota=No` gesetzt werden.

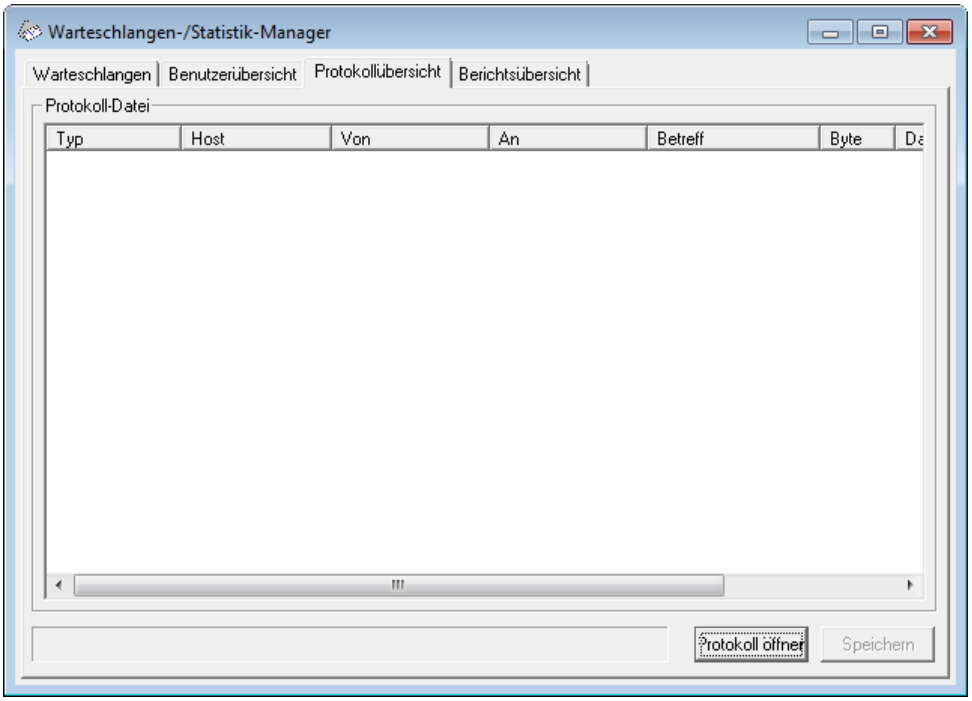
Die Postverzeichnisse enthalten Dateien mit dem Namen "`hiwater.mrk`", aus denen MDStats Teile der angezeigten Benutzerinformation liest. Diese Dateien dürfen im Normalfall nicht gelöscht werden, da MDStats dann die Benutzerinformationen nicht mehr vollständig anzeigt.

Aktualisieren
Statistikdaten der Benutzer wie etwa die Anzahl der Nachrichten in den Postfächern und der belegte Plattenplatz ändern sich laufend. Daher kann die Liste mit einem Klick auf diesen Knopf leicht aktualisiert und somit sichergestellt werden, dass alle angezeigten Daten im Moment der Aktualisierung richtig sind.

Fortschrittsbalken
Im Feld Benutzerinformation können sehr umfangreiche Listen angezeigt werden. Daher erscheint während länger dauernder Vorgänge der Fortschrittsbalken, um während der Verarbeitung großer Dateien anzuzeigen, dass das Programm beschäftigt ist.

Speichern
Die Informationen aus der Liste können durch Anklicken dieses Knopfes entweder als reine Textdatei oder als Textdatei mit Kommata als Feldbegrenzern für Datenbanken gesichert werden. Nachdem Pfad und Dateiname angegeben sind, fragt MDStats nach, ob die Datei Kommata als Feldbegrenzer enthalten soll.

6.3.3 Registerkarte Protokollübersicht



Protokollzusammenfassung
In dieser Liste wird die Protokolldatei von MDaemon in übersichtlicher Form angezeigt, nachdem sie mit dem Knopf Protokoll durch einen normalen Windows-Dialog geladen wurde. Diese Anzeige ermöglicht es, sich schnell und einfach einen Überblick über die abgeschlossenen Transaktionen von MDaemon zu verschaffen,

ohne erst die zusätzlichen Informationen zu überspringen, die in den Protokolldateien von MDaemon u.U. enthalten sind. MDStats filtert die interessanten Informationen Nachrichtentyp (eingehend durch POP, DomainPOP, RFC 2822 usw.), Gegenstelle während der Übermittlung der Nachricht, Absender, Empfänger, Nachrichtengröße, Verarbeitungszeitpunkt und erfolgreiche Übermittlung heraus und zeigt sie tabellarisch an.

Um den Wortlaut des Protokolls zu einem beliebigen Eintrag einzusehen, genügt ein Doppelklick auf diesen Eintrag. Damit wird der entsprechende Ausschnitt aus dem Protokoll in einem Fenster angezeigt. Mit Hilfe der Zwischenablage, deren Funktionen aus dem Kontextmenü zugänglich sind, können Teile des Textes zum Speichern oder Nachbearbeiten in einen Texteditor kopiert werden.

Das Listenfenster kann mit den senkrechten und waagrechten Rollbalken oder, nach einem Klick auf eine beliebige Stelle innerhalb des Fensters, mit den Pfeiltasten durchgeblättert werden. Die Anzeige lässt sich nach beliebigen Spalten sortieren. Ein Klick auf eine Spaltenüberschrift sortiert nach dieser Spalte aufsteigend, ein Doppelklick sortiert absteigend. Die Spaltengröße kann geändert werden, indem man den Mauszeiger auf die Linie zwischen den Spaltenüberschriften setzt und dann die Spalte auf die neue Größe zieht.

Auf der Seite Protokoll werden Protokolleinträge angezeigt, die mit Hilfe der Optionen zum detaillierten oder zusammengefassten Protokollieren der E-Mail-Übertragung erstellt werden. Es wird dringend empfohlen, statt der Zusammenfassung die Protokollierung im Detail zu verwenden, da bei der Zusammenfassung nur wenige Informationen in MDStats angezeigt werden können. Da MDStats die Protokolldaten bereits zusammenfasst und in eine übersichtliche Form bringt, die Betrachtung der Originaleinträge aber gleichwohl ermöglicht, muss MDaemon das Protokoll nicht bereits bei der Erstellung zusammenfassen.

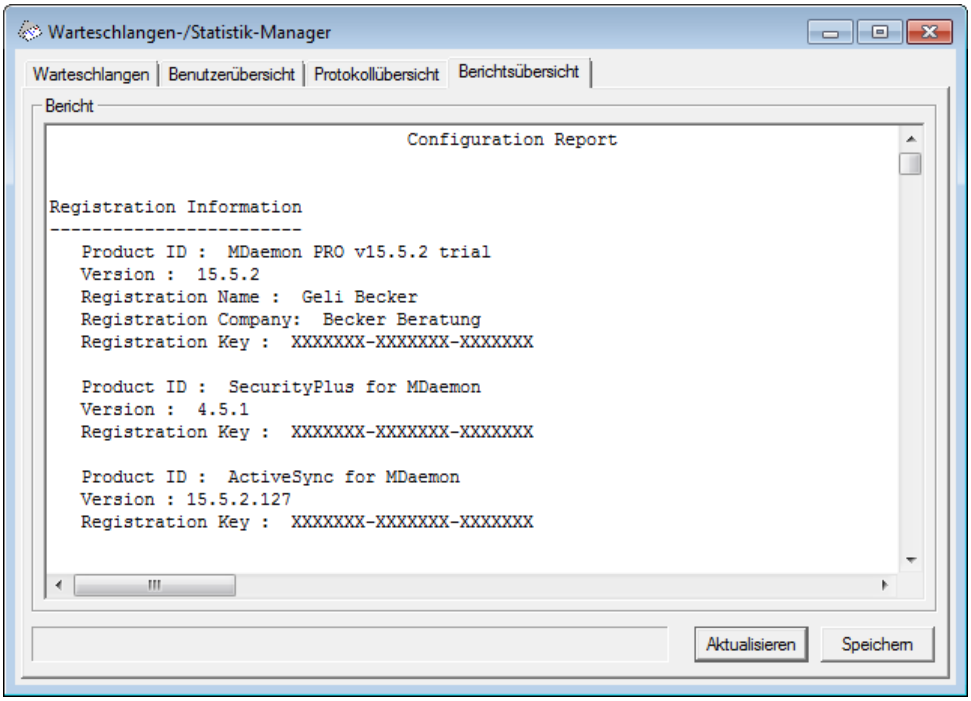
Protokoll öffnen
Ein Klick auf dieses Steuerelement öffnet ein Dateiauswahlfenster, aus dem die gewünschte Protokolldatei ausgesucht werden muss. Wird dieses Steuerelement angeklickt, während MDStats bereits einen Protokollauszug anzeigt, so kann die neue Datei wahlweise an die bereits angezeigte Datei angehängt werden.

Nachdem ein Protokoll angezeigt wurde, erscheint ein Fenster mit einer Statistik zu diesem Protokoll. Wird der Protokollauszug gespeichert, so wird diese Statistik daran angehängt.

Fortschrittsbalken
Da Protokolle sehr groß sein können, erscheint am unteren Rand des Fensters ein Fortschrittsbalken, der während der Verarbeitung großer Dateien anzeigt, dass MDStats beschäftigt ist.

Speichern
Die Informationen aus dem Protokoll-Report können durch Anklicken dieses Knopfes entweder als reine Textdatei oder als Textdatei mit Kommata als Feldbegrenzern für Datenbanken gesichert werden. Nachdem Pfad und Dateiname angegeben sind, fragt MDStats nach, ob die Datei Kommata als Feldbegrenzer enthalten soll.

6.3.4 Registerkarte Berichtsübersicht



Bericht
Auf dieser Seite zeigt MDStats eine übersichtliche und leicht lesbare, aber umfassende Darstellung aller bei MDaemon verfügbaren Einstellungen an. Damit wird die Zeit, die der Administrator zur Prüfung der zahlreichen Einstellungen benötigt, deutlich verringert, außerdem wird die Fehlersuche bei Problemen in der Konfiguration vereinfacht.

Das Listenfenster kann mit den senkrechten und waagrechten Rollbalken oder, nach einem Klick auf eine beliebige Stelle innerhalb des Fensters, mit den Pfeiltasten durchgeblättert werden. Die Anzeige lässt sich nach beliebigen Spalten sortieren. Der dargestellte Text kann direkt in dem Fenster editiert werden, sodass sich Anmerkungen leicht einfügen lassen. Es steht zusätzlich die Funktionen der Zwischenablage zur Verfügung; sie sind nach einem Klick auf die rechte Maustaste über das Kontextmenü zugänglich.

Aktualisieren
Mit einem Klick auf diesen Knopf wird der angezeigte Bericht über die Konfiguration von MDaemon aktualisiert.

Fortschrittsbalken
Wie in den anderen Programmteilen von MDStats, so zeigt auch hier ein Fortschrittsbalken während umfangreicher Dateioperationen an, dass MDStats beschäftigt ist.

Speichern
Hiermit kann der gerade angezeigte Bericht gespeichert werden. Es wird ein normaler Windows-Dialog geöffnet, in dem Pfad und Dateiname für die zu speichernde Datei ausgewählt werden.

6.3.5 Anpassung des Warteschlangen- und Statistik-Managers

6.3.5.1 Die Datei MDstats.ini

Anpassung des Warteschlangen-/Statistik-Managers
Die nachfolgend aufgeführten Einstellungen können in der Datei `MDstats.ini` im Verzeichnis `\app\` unter dem Hauptverzeichnis von MDaemon geändert werden:

[MDaemon]

AppDir=C:\mdaemon\app\	Pfad zum Verzeichnis \app\ von MDaemon.

[QueueOptions]

Editor=NOTEPAD.EXE	Editor, der bei einem Doppelklick auf eine Nachricht oder bei der Auswahl "Bearbeiten" aus dem Kontextmenü der Nachricht gestartet werden soll.
LockOnEdit=No	Legt fest, ob während der Bearbeitung einer Nachricht eine LCK-Datei angelegt werden soll, die ein Verschieben der Nachricht außerhalb der Warteschlange verhindert.
AutoRefresh=Yes	Intervall in Sekunden zwischen der automatischen Aktualisierung der Anzeige. 0 sperrt diese Funktion.
ShowDirectories=Yes	Unterverzeichnisse der Warteschlangen zusätzlich zu den Nachrichten anzeigen. Die Verzeichnisse erscheinen als <Verzeichnisname>.

[UserOptions]

ShowQuota=Yes	Legt fest, ob die Benutzeranzeige das Kontingent (Nachrichtenzahl und dadurch belegter Platz wie in dem Kontingent durch MDaemon) oder physikalische Dateiinformationen (Dateianzahl und insgesamt belegter Platz) anzeigt.

[LogOptions]

ShowUnknown=Yes	Zeigt auch Verbindungen an, bei denen MDStats nicht feststellen konnte, ob sie vom Typ ein-, abgehend, SMTP oder POP waren.
ShowSmtpInbound=Yes	Eingehende SMTP-Verbindungen anzeigen.
ShowPopInbound=Yes	Eingehende POP-Verbindungen zeigen (Postabruf).
ShowSmtpOutbound=Yes	Abgehende SMTP-Verbindungen anzeigen.
ShowPopOutbound=Yes	Abgehende POP-Verbindungen anzeigen (MultiPOP, DomainPOP).
ShowRFC822=Yes	Lokale Postzustellung nach RFC822 anzeigen.
ShowSmtpHelo=Yes	Domänenname aus dem Befehl HELO bei eingehenden SMTP-Verbindungen in der Spalte "Host" anzeigen.
IgnoreEmptyPop=Yes	POP-Verbindungen ignorieren, in denen nichts übertragen wurde.
ShowImap=Yes	IMAP-Verbindungen anzeigen.
[Remap]	Mapping von Netzwerklaufwerken, damit MDStats auf einem anderen Rechner laufen kann als MDaemon.
C:=\\server\c	Beim Einlesen der Datei MDaemon.ini wird "C:" durch "\\server\c" ersetzt.
[Special]	
OnlyOneInstance=No	lMDStats kann, wenn dieses Schlüsselwort auf Yes gesetzt ist, nur einmal gleichzeitig ausgeführt werden. Jeder weitere Programmstart bringt das bereits laufende Programm in den Vordergrund.

Siehe auch:

Befehlszeilenparameter für MDStats 884

6.3.5.2 Befehlszeilenparameter für MDStats

Beachte: Die nachfolgend aufgeführten Befehlszeilenparameter ignorieren Groß- und Kleinschreibung.

Zahl 1 bis 8	Zeigt die ausgewählte Warteschlange an.
1	Warteschlange für externe Post
2	Warteschlange für lokale Post

3	Wiederholungs-Warteschlange
4	LAN-Warteschlange
5	RAW-Warteschlange
6	Defekt-Warteschlange
7	Warteschlange für SMTP eingehend
8	Speicher-Warteschlange
/L[N] [Quelldatei] [Zieldatei]	Dies erzeugt einen Protokoll-Report. Der Parameter N bewirkt, dass die Zieldatei keine Kommata als Feldbegrenzer enthält.
/A	Beim Erstellen eines Protokoll-Reports werden die neuen Daten an die Zieldatei angehängt; sie wird nicht überschrieben.

Kapitel VII

7 Zusätzliche Leistungsmerkmale von MDaemon

7.1 MDaemon und Text-Dateien

MDaemon nutzt eine Reihe von Textdateien dafür, Daten, Vorlagen für automatisch durch das System erstellte Nachrichten und Konfigurationsinformationen zu speichern. Diese Vorgehensweise ermöglicht einen hohen Grad an Flexibilität. Sie können von MDaemon aus neue Textdateien über den Menüpunkt Datei » Neu erstellen. Diese Funktion kann zum schnellen Anlegen neuer Textdateien, etwa für Autobeantworter und andere Leistungsmerkmale von MDaemon, nützlich sein.

Bearbeiten der Dateien von MDaemon

Die verschiedenen Datendateien, die MDaemon nutzt, sind reguläre Textdateien, die Sie beispielsweise mit Notepad bearbeiten können. Sie können diese Dateien aus MDaemon mithilfe des Menüpunkts Datei » Öffnen » Leere Textdatei einfach öffnen. Per Voreinstellung wird dabei im MDaemon-Verzeichnis `\app\` nach Dateien mit den Endungen `*.txt` gesucht. Durch Auswahl des Dateityps "Alle Dateien" können Sie auch auf die weiteren Dateien zugreifen, die sich in dem Verzeichnis befinden.

7.2 Fernsteuerung des Servers über E-Mail

MDaemon gestattet den Fernzugriff auf viele Leistungsmerkmale mithilfe besonderer E-Mail-Nachrichten mit bestimmtem Inhalt, die auf dem regulären Transportweg an das Systemkonto von MDaemon ("`MDaemon@<Domäne von MDaemon>`") übermittelt werden. Solche Nachrichten werden auch als Steuernachrichten bezeichnet. Steuernachrichten, die an den Server gerichtet sind, werden im Nachrichtenverzeichnis des Systemkontos gespeichert; die Vorgehensweise unterscheidet sich dem Grunde nach nicht von normalen Benutzerkonten.

Manche Befehle setzen ein gültiges Benutzerkonto auf dem Server voraus. Solche Befehle können nur dann ausgeführt werden, wenn die Steuernachricht, in der sie enthalten sind, über eine SMTP-Verbindung mit Echtheitsbestätigung über SMTP AUTH übermittelt wurde.

Die Befehle, die in den Steuernachrichten verwendet werden können, zerfallen in zwei Hauptgruppen: Mailinglisten 888 und Allgemeine E-Mail-Dienste 890.

Siehe auch:

Steuerung von Mailinglisten 888
Steuerung allgemeiner E-Mail-Dienste 890

7.2.1 Steuerung von Mailinglisten und Dateikatalogen

Die nachfolgend aufgeführten Befehle erfordern kein Benutzerkonto auf dem Server. Die Parameter in eckigen Klammern sind wahlfrei. So könnte z.B. "`Name [Adresse]`" nur als "`Michael`" oder mit dem zusätzlichen Parameter als "`Michael user1@example.com`" angegeben werden. Die Steuernachrichten müssen an "mdaemon@[Domäne von MDaemon]" gerichtet sein; jeder Befehl und die zugehörigen Parameter müssen auf eine eigenen Zeile im Nachrichtentext gesetzt werden.

BEFEHLE	PARAMETER	BESCHREIBUNGEN

SUBSCRIBE	Listenname [Adresse] [{Vor-/Nachname}] [(Kennwort)]	Der Absender wird neues Mitglied der Mailingliste, falls der Listenname richtig ist und die Liste Bestellungen per E-Mail erlaubt. Wird nach dem Listennamen eine E-Mail-Adresse angegeben, so wird statt der Absenderadresse der Nachricht diese Adresse neues Mitglied. Der Klartextname des Mitglieds kann in geschweifter Klammer mit angegeben werden (z.B. {Bill F}. Ist das richtige Kennwort in Klammern angegeben, so ist die Bestellung auch möglich, wenn die Liste ungeschützte Bestellungen per E-Mail ignoriert.
		Beispiele:
		`SUBSCRIBE liste@example.com`
		`SUBSCRIBE liste@example.com me@example.com {Bill F}`
		`SUBSCRIBE liste@example.com you@example.org (Kennwort)`

UNSUBSCRIBE oder SIGNOFF	Listenname [Adresse] [(Kennwort)]	Der Absender wird aus der angegebenen Mailingliste gestrichen, falls der Listenname richtig ist und der Absender ein Mitglied der Liste ist. Wird nach dem Listennamen eine E-Mail-Adresse angegeben, so wird statt der Absenderadresse diese Adresse aus der Mitgliederliste gestrichen. Wird das Listenkennwort in Klammern angegeben, so ist die Abbestellung auch möglich, wenn die Liste ungeschützte Abbestellungen per E-Mail ignoriert.
		Beispiele:
		`UNSUBSCRIBE liste@example.com (Kennwort)`
		`SIGNOFF liste@example.com me@example.com`

DIGEST	Listenname [Adresse]	Der Absender erhält die Mailingliste ab sofort im Digest-Format. Wird eine E-Mail-Adresse gesondert angegeben, so wird deren Versandart auf Digest umgestellt.
		Beispiele:
		`DIGEST liste@example.com`
		`DIGEST liste@example.com benutzer1@example.com`

NORMAL	Listenname [Adresse]	Der Absender erhält die Mailingliste im Normalformat, nicht als Digest. Wird eine E-Mail-Adresse gesondert angegeben, so wird deren Versandart auf Normalformat geändert.
		Beispiele:
		`NORMAL liste@example.com`
		`NORMAL liste@example.com benutzer1@altn.com`

NOMAIL	Listenname [Adresse]	Dieser Befehl sperrt die angegebene Adresse vorübergehend für Post aus der Liste. Wird keine gesonderte Adresse angegeben, so wird der Absender gesperrt. Beispiele: `NOMAIL liste@example.com me@example.com`

MAIL	Listenname [Adresse]	Dieser Befehl gibt die angegebene Adresse für Nachrichten aus der Liste wieder frei. Wird keine gesonderte Adresse angegeben, so wird der Absender freigegeben.
		Beispiele:
		`MAIL liste@example.com`
		`MAIL liste@example.com me@example.com`

REALNAME	Listenname [Adresse] {Vor-/Nachname}	Der Befehl ändert den Inhalt des Feldes Vor- und Nachnamen für die angegebene Adresse, die bereits Abonnent der Mailingliste sein muss. Der Vor- und Nachname muss in geschweifter Klammer angegeben werden. Beispiel: `REALNAME liste@example.com {Bill Farmer}`
LIST	[Listenname] [Listenkennwort]	Fordert Informationen über eine Mailingliste an. Falls der Name der Liste nicht angegeben wird, wird eine Zusammenfassung aller Listen ausgegeben. Falls das Listenkennwort angegeben wird, werden mehr Informationen über die Mailingliste ausgegeben. Beispiel: `LIST liste@example.com Lz$12`

Siehe auch:

Fernsteuerung des Servers über E-Mail 888
Steuerung allgemeiner E-Mail-Dienste 890

7.2.2 Steuerung allgemeiner E-Mail-Dienste

Die folgenden allgemeinen Befehle für die Steuerung von E-Mail-Funktionen können in Steuernachrichten per E-Mail an das Systemkonto versandt werden. Die Steuernachrichten müssen an "mdaemon@[Domäne von MDaemon]" gerichtet sein; jeder Befehl und die zugehörigen Parameter müssen auf eine eigenen Zeile im Nachrichtentext gesetzt werden.

BEFEHLE	PARAMETER	BESCHREIBUNGEN
HELP	keine	Verarbeitet die Datei NEWUSERHELP.DAT und sendet eine Nachricht mit dem sich hieraus ergebenden Inhalt an den Absender.

STATUS	keine	Hiermit wird ein Statusbericht über den Zustand des Servers und gerade durchgeführte Aktionen zurückgesandt. Da es sich hierbei um vertrauliche Informationen handelt, muss der Benutzer, der die Anforderung übermittelt, als Administrator echtheitsbestätigt sein. Beispiel: STATUS

Siehe auch:

Fernsteuerung des Servers über E-Mail 888
Steuerung von Mailinglisten 888

7.3 Die Spezifikation für RAW-Nachrichten

7.3.1 Die Spezifikation für RAW-Nachrichten

MDaemon unterstützt von Haus aus das einfache aber effiziente Nachrichtenformat RAW. Der Zweck des Formats RAW ist es, ein einfaches und standardisiertes Format zur Verfügung zu stellen, das Serversysteme wie MDaemon dazu verwenden können, wesentlich komplexere Nachrichten nach RFC 2822 zu erstellen. Die Software an den Arbeitsplätzen braucht sich dabei um die Einhaltung irgendwelcher Internet-Standards für E-Mail nicht zu kümmern, da hierfür der Server zuständig ist.

Nachrichten im Format RAW bestehen aus einigen zwingend nötigen und anderen wahlfreien Kopfzeilen und dem Nachrichtentext selbst. Die meisten Kopfzeilen bestehen aus einem Schlüsselwort und danach dem Wert in spitzen Klammern (<>). Jede Kopfzeile endet mit der Zeichenfolge <CRLF>. Die Kopfzeilen sind vom Nachrichtentext durch eine Leerzeile getrennt, in ihnen sind Groß- und Kleinschreibung unbeachtlich, und außer den Kopfzeilen from (Absender) und to (Empfänger) sind keine Kopfzeilen zwingend erforderlich. Die gesamte Datei mit Kopfzeilen und Nachrichtentext muss im ASCII-Format als Text vorliegen und die Endung `raw` tragen (wie etwa "`meine-nachricht.raw`"). Um die Nachricht dann zu versenden, wird die RAW-Datei in der RAW-Warteschlange (üblicherweise unter "`C:\MDaemon\Queues\Raw`") von MDaemon abgelegt.

Umgehen des Inhaltsfilters

RAW-Nachrichten durchlaufen grundsätzlich, wie sonstige Nachrichten auch, den Inhaltsfilter. Soll eine bestimmte RAW-Nachricht nicht durch den Inhaltsfilter verarbeitet werden, so muss ihr Dateiname mit "`p`" oder "`P`" beginnen. Eine Nachricht "`P_meine-nachricht.raw`" würde beispielsweise den Inhaltsfilter nicht durchlaufen, wohingegen "`meine-nachricht.raw`" durch den Inhaltsfilter verarbeitet werden würde.

Umgehen Nachrichten den Inhaltsfilter, so können sie auch nicht durch DKIM signiert werden. Falls MDaemon so konfiguriert ist, dass alle Nachrichten signiert werden, kann dies zu Problemen bei der Zustellung führen. Soll MDaemon eine RAW-Nachricht signieren, obwohl sie den Inhaltsfilter nicht durchläuft, so kann dies durch Einfügen der weiter

> unten beschriebenen Option `x-flag=sign` erreicht werden.

RAW-Kopfzeilen

From <mailbox@example.com>	Dieses Feld enthält die E-Mail-Adresse des Absenders.
To <mailbox@example.com [, mailbox@example.com]>	Dieses Feld enthält die Adresse(n) der Empfänger. Mehrere Empfänger werden durch Kommata getrennt.
ReplyTo <mailbox@example.com>	Antwort auf die Nachricht wird an diese Adresse geleitet.
CC <maibox@example.com[, mailbox@example.com]>	Die Empfänger von Durchschlägen dieser Nachricht werden hier angegeben. Mehrere Empfänger werden durch Kommata getrennt.
Subject <Text>	Falls gewünscht, wird hier der Betrefftext eingegeben.
Header <Kopfzeile: Inhalt>	Hiermit können bestimmte Kopfzeilen in die Nachricht aufgenommen werden. Mithilfe dieser Option können auch benutzerdefinierte oder nicht standardisierte Kopfzeilen in die RAW–Nachrichten eingefügt werden.

Besondere durch RAW unterstützte Felder

Dateianlagen und -Kodierung

`x-flag=attach <Pfad zur Datei, Methode> [-x]`

Beispiel: `x-flag=attach <c:\utils\pkzip.exe, MIME> -x`

Dieser X-FLAG benützt den Wert "ATTACH" und zwei Parameter hierzu in spitzen Klammern. Der erste Parameter ist der vollständige Pfad zu der anzuhängenden Datei. Der zweite Parameter wird vom ersten durch Kommata getrennt und gibt das gewünschte Kodierverfahren für die Dateianlage an. MDaemon unterstützt hier zwei Verfahren. Die Methode MIME veranlasst den Server, das Internet-Standardverfahren Base64 zu verwenden. Die Methode ASCII veranlasst den Server, die Datei einfach in die Nachricht zu importieren. Der wahlfreie Parameter –X veranlasst den Server, die Datei zu löschen, nachdem sie an die Nachricht angehängt wurde.

Nachricht über Zustellstatus

`x-flag=confirm_delivery`

Bei der Konvertierung von RAW-Nachrichten, die diesen Befehl enthalten, ins Format RFC 2822 wird der Befehl in eine Kopfzeile nach dem Schema "Return-Receipt-To: <sender@example.com>" umgeformt.

Spezielle Kopfzeilen und Inhalte in RFC-2822-Nachrichten einsetzen

```
header <Kopfzeile: Inhalt>
```

Soll eine bestimmte Kopfzeile mit einem bestimmten Inhalt in eine RFC-2822-Nachricht eingesetzt werden, die aus einer RAW-Datei erstellt werden soll, so kommt in der RAW-Nachricht das Makro HEADER zum Einsatz. Soll z.B. die Kopfzeile "Ausgeliefert-von: mail-server@example.com" in die RFC-2822-Nachricht eingefügt werden, so müsste der Eintrag in der RAW-Nachricht "header <Ausgeliefert-von: mail-server@example.com>" lauten. Es ist wichtig, zu beachten, dass das Makro "header" immer Namen und Inhalt der Kopfzeile erfordert. Die Anzahl der "header"-Makros in einer RAW-Nachricht ist nicht beschränkt.

RAW-Nachrichten über DKIM signieren

```
x-flag=sign
```

Wird dieser Befehl in eine RAW-Nachricht eingefügt, so wird diese Nachricht über DK/DKIM signiert. Dieser Befehl soll nur bei Nachrichten eingesetzt werden, die den Inhaltsfilter nicht durchlaufen (deren Dateinamen also mit "p" oder "P" beginnen). In normalen RAW-Nachrichten, die durch den Inhaltsfilter verarbeitet werden, soll dieser Befehl nicht eingesetzt werden; diese Nachrichten können auch ohne den Befehl signiert werden.

Alle RAW-Nachrichten, die der Inhaltsfilter selbst erstellt, werden automatisch mit dem Befehl `x-flag=sign` versehen.

Beispiele für Nachrichten im RAW-Format

Beispiel 1:

```
from <mdaemon@altn.com>
to <user01@example.com>

Hallo John!
```

Beispiel 2:

```
from <user01@example.com>
to <user09@example.net>
subject <Angeforderte Dateien>
X-FLAG=CONFIRM_DELIVERY
X-FLAG=ATTACH <c:\docs\files\data01.zip, MIME> -X

Hier sind die Dateien, die Sie haben wollten.
```

7.4 Signal- oder Semaphore-Dateien

MDaemon reagiert auf eine Reihe von Dateien, die sehr vielseitig eingesetzt werden können, die sog. Signal- oder Semaphore-Dateien. MDaemon prüft das Unterverzeichnis `\APP\` regelmäßig auf das Vorhandensein solcher Dateien. Wird eine solche Datei gefunden, so werden die mit ihre verknüpfte Aktion ausgeführt und die Datei danach gelöscht. Hiermit können Systemverwalter und Software-Entwickler

MDaemon leicht steuern, ohne die Benutzeroberfläche zu bedienen. Es folgt eine Liste aller Signaldateien und der zugehörigen Aktionen:

DATEINAME	AKTION
ACLFIX.SEM	Bereinigt die Zugriffskontrolllisten (ACL).
ADDUSER.SEM	Diese Signaldatei erstellt neue Benutzerkonten. Sie veranlasst MDaemon, die neuen Einträge an das Ende der Datei USERLIST.DAT anzufügen, ohne die Benutzerdatenbank womöglich zeitraubend neu aufbauen zu müssen. In dieser Datei muss in jeder Zeile ein komplettes Benutzerkonto stehen; der Aufbau ist im Abschnitt Benutzerverwaltungsfunktionen im API zu MDaemon beschrieben (vgl. MD-API.html im Unterverzeichnis \docs\API\). Es können mehrere Benutzerkonten angegeben werden, jedoch nur eines pro Zeile, da MDaemon die Datei zeilenweise verarbeitet. Die Signaldatei kann während der Bearbeitung durch Anlegen der Datei ADDUSER.LCK für MDaemon gesperrt werden, sodass MDaemon sie erst liest, wenn die LCK-Datei gelöscht ist. Ein Beispiel für ADDUSER.SEM ist die Datei ADDUSER.SMP im APP-Verzeichnis. Sie kann mit jedem Texteditor geöffnet werden.
ALERT.SEM	MDaemon zeigt allen gerade angemeldeten Webmail-Benutzern den vollständigen Inhalt dieser Datei in einem Popup-Fenster, sobald sie erstellt wurde. Das Popup erscheint jedoch nicht sofort und bei allen Benutzern gleichzeitig, es wird vielmehr bei jedem Benutzer dann angezeigt, wenn er mit seinem Browser eine Aktion in WorldClient durchführt. **Beachte:** Anders als die anderen hier dargestellten Signaldateien bezieht sich diese Datei nur auf WorldClient. Sie darf daher nicht im Verzeichnis \app\, sondern sie muss im Verzeichnis \MDaemon\WorldClient\ abgelegt werden.
ALIAS.SEM	Veranlasst MDaemon, die Alias-Datenbank neu zu laden.
AUTORESPEXCEPT.SEM	Veranlasst MDaemon, die Ausschluss-Liste für die Autobeantworter neu zu laden.
BATV.SEM	Datendateien des Schutzes gegen Rückstreuung (BATV) werden neu geladen.
BAYESLEARN.SEM	Diese SEM-Datei löst den Bayes'schen Lernvorgang von Hand aus. Es tritt dieselbe Wirkung ein, wie wenn der Lernvorgang über den Konfigurationsdialog des Spam-Filters von Hand begonnen wird. Beachte: Diese Signaldatei löst

	den Bayes'schen Lernvorgang auch dann aus, wenn diese Funktion sonst abgeschaltet ist.
BLACKLIST.SEM	Datendateien der Sperrlisten werden neu geladen.
CFILTER.SEM	Lädt die Regeln des Inhaltsfilters neu, leert den Cache des Inhaltsfilters, und lädt die Freigabeliste (keine Filterung)[695] des Spam-Filters neu.
CLEARQUOTACOUNTS.SEM	Die Ergebnisse der Kontingentprüfung für die Benutzer werden in der Datei quotacounts.dat gespeichert. Sollen die dort gespeicherten Werte gelöscht werden, so muss die E-Mail-Adresse des Benutzers, dessen Werte gelöscht werden sollen, in diese Datei eingetragen werden. Danach muss sie im Verzeichnis \app\ abgelegt werden. Der Eintrag „*" auf einer eigenen Zeile bewirkt die Löschung aller Kontingentdaten aus dem Cache.
DELUSER.SEM	Mit dieser Signaldatei lassen sich ein oder mehrere Benutzerkonten löschen. In der Datei müssen die Adressen jedes einzelnen zu löschenden Benutzerkontos eingetragen sein, und zwar eine Adresse pro Zeile. Die Datei muss den Namen "DELUSER.SEM" erhalten und im Unterverzeichnis …\app\ abgelegt werde. MDaemon löscht dann zunächst die Benutzerkonten und anschließend die Datei DELUSER.SEM. Falls Sie ein Benutzerkonto löschen, das zugehörige Nachrichtenverzeichnis aber bestehen lassen wollen, fügen Sie der Adresse das Zeichen ^ hinzu (z.B. `frank@example.com^`).
DNS.SEM	Diese Signaldatei bewirkt, dass die Windows-DNS-Server[108] und die DNS-Einstellungen des Spam-Filters neu geladen werden.
DOMAINSHARING.SEM	Datendatei für verteilte Domänen wird neu geladen
EDITUSER.SEM	Hiermit lassen sich einzelne Einträge der Datei `USERLIST.DA` gezielt ändern, ohne dass die gesamte Datei möglicherweise zeitaufwändig neu erstellt werden müsste. Um einzelne Benutzerdatensätze in der Datei `USERLIST.DAT` zu aktualisieren, erstellen Sie eine Datei namens `EDITUSER.SEM`, und nehmen Sie in diese Datei die Datensätze, die Sie aktualisieren wollen, jeweils vollständig auf. Setzen Sie dabei jeden Datensatz auf eine eigene Zeile. Die neuen Datensätze ersetzen dann die bestehenden Datensätze. Jeder Datensatz muss mit dem Format für die Datei `USERLIST.DAT` übereinstimmen, wie es in dem Artikel Datenformat der Datei Userlist in der Wissensdatenbank in englischer Sprache beschrieben ist, und jeder Datensatz

	muss zusätzlich mit der E-Mail-Adresse des zu ersetzenden Datensatzes und einem Komma beginnen. MDaemon verarbeitet die Datei EDITUSER.SEM zeilenweise nacheinander. Sie können die Datei EDITUSER.LCK erstellen und so die Datei EDITUSER.SEM gegen Verarbeitung sperren, während Sie sie bearbeiten. MDaemon verarbeitet die Datei EDITUSER.SEM erst dann, wenn die Datei EDITUSER.LCK wieder gelöscht ist. Sie können ein Beispiel für die Datei für EDITUSER.SEM einsehen, indem Sie im Verzeichnis \APP\ die Datei EDITUSER.SMP mit einem Texteditor öffnen.
EXITNOW.SEM	MDaemon beendet sich selbst.
GATEWAYS.SEM	MDaemon hält aus Gründen besserer Leistung die Liste der Gateways im Speicher. Die Datei GATEWAYS.SEM im APP-Verzeichnis bewirkt, dass MDaemon die Datei gateways.dat neu lädt.
GREYLIST.SEM	Datendatei der Grauen Liste wird neu geladen.
GROUPS.SEM	Liste der Benutzergruppen wird neu geladen.
GRPLIST.SEM	Lädt dynamisch die Namen der Mailinglisten neu.
HANGUPG.SEM	Veranlasst einen „sanften" Abbruch der von MDaemon hergestellten DFÜ-Verbindung. MDaemon wartet erst, bis alle Mail-Verbindungen beendet sind und trennt dann die Verbindung.
HANGUPR.SEM	Veranlasst einen sofortigen Abbruch der DFÜ-Verbindung, die MDaemon hergestellt hat. Achtung: Die Verbindung wird ohne Rücksicht auf gerade laufende Mail-Verbindungen getrennt, sodass diese Funktion vorsichtig einzusetzen ist.
HOSTSCREEN.SEM	Datendatei für den Host-Filter wird neu geladen.
IPSCREEN.SEM	Datendatei für den IP-Filter wird neu geladen.
IPSHIELD.SEM	Die Datei IPShield.dat wird im Hauptspeicher gehalten, um den Zugriff darauf zu beschleunigen. Nutzen Sie die Signaldatei IPSHIELD.SEM, um die Datendatei erneut in den Hauptspeicher zu laden.
LDAPCACHE.SEM	Cache für LDAP- und Gateway-Benutzerdaten wird neu geladen.

LOCKSEMS.SEM	Verhindert die Abarbeitung aller anderen Signaldateien, bis diese Datei gelöscht wird.
LOGSETTINGS.SEM	Protokolleinstellungen werden neu geladen.
MDSPAMD.SEM	Freigabeliste des Spam-Filters und MDSpamD werden neu geladen, Konfigurationsdaten von MDSpamD werden neu initialisiert.
MINGER.SEM	Beendet den Minger-Server[855] und startet ihn danach neu.
MXCACHE.SEM	Veranlasst MDaemon, den MX-Cache neu zu laden.
NODNSBL.SEM	Freigabeliste für DNS-BL wird neu geladen.
NOPRIORITY.SEM	Veranlasst MDaemon, die Datei `NoPriority.dat` erneut zu laden.
ONLINE.SEM	MDaemon erstellt diese Datei, sobald eine DFÜ-Verbindung zum ISP hergestellt ist und löscht sie nach Ende der Verbindung wieder. Hiermit lässt sich leicht feststellen, wann MDaemon die RAS oder das DFÜ-Netzwerk verwendet.
POSTDIAL.SEM	MDaemon erzeugt diese Nachricht unmittelbar nach Trennung einer selbst gewählten DFÜ-Verbindung.
PREDIAL.SEM	MDaemon erzeugt diese Datei unmittelbar vor einem Verbindungsaufbau über RAS oder DFÜ-Netzwerk. Hierdurch kann andere Software feststellen, wann die Schnittstellen freigegeben werden müssen, weil sie von MDaemon gebraucht werden.
PRIORITY.SEM	Veranlasst MDaemon, die Datei PRIORITY.DAT neu zu laden.
PROCBAD.SEM	Die Defekt-Warteschlange wird abgearbeitet.
PROCDIG.SEM	Alle Digest-Nachrichten werden sofort versandt.
PROCHOLDING.SEM	Inhalt der Störungs-Warteschlange wird verarbeitet und zugestellt.
PROCNOW.SEM	MDaemon startet sofort einen Verarbeitungsdurchlauf für Nachrichten. **Beachte:** Sie können auch eine Nachricht an "`procnow@example.com`" senden; MDaemon erstellt dann die

	Datei PROCNOW.SEM file. Daher dürfen Sie "procnow" nicht als Teil eines Postfachnamens verwenden.
PROCREM.SEM	MDaemon startet sofort einen Verarbeitungsdurchlauf für Nachrichten und bearbeitet die externen Nachrichten.
PROCRETR.SEM	Die Wiederholungs-Warteschlange wird verarbeitet.
PRUNE.SEM	MDaemon bereinigte alte Nachrichten und Benutzerkonten; derselbe Vorgang wird um Mitternacht automatisch ausgeführt.
PUBLICSUFFIX.SEM	Lädt die Liste öffentlicher Domänenendungen[553] neu.
QUEUE.SEM	Diese Signaldatei aktiviert und deaktiviert die Nachrichten-Warteschlangen. Sie kann eine beliebige Anzahl Zeilen enthalten. Auf jeder Zeile muss einer der nachfolgend aufgeführten Ausdrücke stehen, und es ist nur ein Ausdruck pro Zeile zulässig: ENABLE INBOUND (Eingangs-Warteschlange freigeben), ENABLE REMOTE (Warteschlange für externe Nachrichten freigeben), ENABLE LOCAL (Warteschlange für lokale Nachrichten freigeben), oder DISABLE INBOUND (Eingangs-Warteschlange anhalten), DISABLE REMOTE (Warteschlange für externe Nachrichten anhalten), DISABLE LOCAL (Warteschlange für lokale Nachrichte anhalten).
RESTART.SEM	Startet MDaemon neu.
RESTARTCF.SEM	Startet CFEngine.exe (die ausführbare Datei des Inhaltsfilters) neu.
RESTARTWC.SEM	Startet MDaemon Webmail neu. Diese Signaldatei wirkt nur, falls Webmail unter dem eigenen, mitgelieferten Web-Server ausgeführt wird[322].
RELOADCACHE.SEM	MDaemon lädt alle im Cache zwischengespeicherten Einstellungen und Dateien neu, jedoch nicht die Einstellungen und Dateien des Inhaltsfilters.
REVERSEEXCEPT.SEM	Ausschlussliste der Rückwärtssuche wird neu geladen.
SCHEDULE.SEM	Veranlasst MDaemon, die Datei SCHEDULE.DAT neu zu laden.

SPAMHONEYPOTS.SEM	Datendateien der Spam-Honeypots werden neu geladen.
SPF.SEM	Datendateien für SPF, DKIM und VBR werden neu geladen.
SUPPRESS.SEM	Einstellungen der Sperrlisten werden neu geladen; zwischengespeicherte Einstellungen für Domänen werden gelöscht.
TARPIT.SEM	Lädt die Datendateien der Teergrube neu.
TRANSLAT.SEM	Veranlasst MDaemon, die Datenbank für die Kopfzeilen-Umsetzung neu zu laden.
TRAY.SEM	Stellt das Symbol für MDaemon im Infobereich (Systray) wieder her.
TRUST.SEM	MDaemon hält aus Gründen besserer Leistung die Liste der vertrauten Domänen und IP-Adressen im Speicher. TRUST.SEM veranlasst, dass diese neu geladen werden.
UPDATEAV.SEM	Veranlasst eine sofortige Aktualisierung der Viren-Signaturen.
UPDATESA.SEM	Veranlasst eine Aktualisierung des Spam-Filters.
USERLIST.SEM	Veranlasst MDaemon, die Datei USERLIST.DAT neu zu laden und die Mailingliste EVERYONE.GRP neu zu erstellen. Nach Änderungen an der Datei USERLIST.DAT ist dies sinnvoll, wenn MDaemon die Datei neu laden soll.
WATCHDOG.SEM	MDaemon prüft alle 10 – 20 Sekunden, ob diese Datei im Verzeichnis APP vorhanden ist und löscht sie jeweils sofort. Die Datei kann von anderen Programmen verwendet werden, um zu prüfen, ob MDaemon noch läuft. Bleibt sie länger als 20 Sekunden bestehen, so ist MDaemon wahrscheinlich abgestürzt.

7.5 Laufzettel (Route-Slips)

Die Kopfzeilen einer Nachrichtendatei, die auf ihre Zustellung wartet, enthalten üblicherweise alle Daten, dir erforderlich sind, um die Nachricht an den gewünschten Empfänger zuzustellen. Diese Kopfzeilen werden in der Nachrichtendatei selbst gespeichert (z.B. die Kopfzeile X-MDaemon-Deliver-To), und sie teilen MDaemon mit, wo und an wen die Nachricht zugestellt werden soll. Manchmal ist es aber erforderlich oder erwünscht, diese Informationen zu übergehen und bestimmte Alternativdaten über die Zustellung vorzugeben. Die Laufzettel (engl. "Route Slips") stellen einen entsprechenden Mechanismus zur Verfügung. Ein Laufzettel ist eine

Datei, die MDaemon mit sehr genauen Informationen darüber versorgt, wo und an wen eine Nachricht zugestellt werden soll. Liegt für eine bestimmte Nachricht ein Laufzettel vor, so nutzt MDaemon die Informationen aus dem Laufzettel und nicht die Leitwegdaten aus der Nachricht selbst, um zu bestimmen, wo und an wen die Nachricht zugestellt wird.

Laufzettel haben die Dateiendung `RTE`. Heißt z.B. die Nachrichtendatei `MD0000.MSG`, so muss der zugehörige Laufzettel `MD0000.RTE` heißen und in demselben Verzeichnis (derselben Warteschlange) liegen wie die Nachrichtendatei.

Die Laufzettel sind nach folgendem Schema aufgebaut:

```
[RemoteHost]
DeliverTo=example.net
```

In diesem Abschnitt wird MDaemon der Servername mitgeteilt, an den diese Nachrichtendatei zu senden ist. MDaemon versucht dann immer, eine direkte Verbindung so schnell wie möglich herzustellen. Es darf nur ein Name angegeben werden.

```
[Port]
Port=xxx
```

Hier wird die Portnummer angegeben, auf der MDaemon eine TCP/IP-Verbindung zur Gegenstelle herstellen soll. Für SMTP ist die Voreinstellung 25.

```
[LocalRcpts]
Rcpt0=adresse@example.com
Rcpt1=andere-adresse@example.com
Rcpt2=ganz-andere-adresse@example.com

[RemoteRcpts]
Rcpt0=adresse@example.net
Rcpt1=andere-adresse@example.net
Rcpt2=ganz-andere-adresse@example.net
```

In diesen Abschnitten des Laufzettels werden beliebig viele lokale und externe Empfänger für die `MSG`-Datei angegeben. Die Adressen der lokalen und externen Empfänger müssen getrennt in den jeweiligen Abschnitten `[LocalRcpts]` und `[RemoteRcpts]` eingetragen werden.

Laufzettel sind zwar praktisch, um Nachrichten zuzustellen oder umzuleiten, sie sind aber meist nicht erforderlich. MDaemon verwendet sie z.B. für geroutete Nachrichten aus Mailinglisten. Wenn eine Mailingliste so eingestellt ist, dass nur eine Kopie einer Listennachricht an einen anderen Server geroutet werden soll, so wird dazu ein Laufzettel verwendet. Dies ist eine sehr effiziente Zustellungsmethode, falls an sehr viele Adressen zugestellt werden muss, da unabhängig von der Zahl der Empfänger immer nur eine Nachrichtendatei gebraucht wird. Diese Routingmethode ist aber nicht überall zugelassen. Da die Zustellung an die endgültigen Empfänger durch die Server der Empfänger durchgeführt werden muss, begrenzen viele Server die Anzahl der gleichzeitig möglichen Empfänger.

Kapitel VII

8 Erstellen und Verwenden von SSL-Zertifikaten

MDaemon versieht die über das Menü SSL & TLS erstellten Zertifikate mit einer Eigensignatur. Der Aussteller des Zertifikats, die sog. Zertifizierungsstelle oder Certificate Authority (regelmäßig als CA abgekürzt), ist dabei gleich dem Herausgeber des Zertifikats. Diese Vorgehensweise ist zulässig, die Zertifizierungsstelle ist aber auf den Systemen der Benutzer noch nicht in den Listen der vertrauenswürdigen Zertifizierungsstellen eingetragen. Dies führt beim Verbindungsaufbau zu Webmail oder zur Remoteverwaltung über HTTPS zu einem Sicherheitshinweis, der den Benutzer fragt, ob er die Seite aufrufen und das Zertifikat installieren will. Sobald der Benutzer diesem Vorgehen zugestimmt und die Webmail-Domäne als vertrauenswürdige Zertifizierungsstelle eingestuft hat, erscheinen beim Verbindungsaufbau zu Webmail oder zur Remoteverwaltung keine Sicherheitshinweise mehr.

Stellen die Benutzer die Verbindung zu MDaemon über einen Mailclient, wie etwa Microsoft Outlook, her, so wird ihnen die Installation des Zertifikats nicht angeboten. Die Benutzer können wählen, ob sie das Zertifikat vorübergehend nutzen wollen, obwohl es nicht als vertrauenswürdig eingestuft ist; sie müssen außerdem bei jedem Verbindungsaufbau zum Mailserver nach einem Neustart des Mailclients diese Frage beantworten. Um dies zu vermeiden, können Sie entweder ein Zertifikat von einer anerkannten Zertifizierungsstelle beziehen, wie etwa Let's Encrypt, oder Sie können Ihr eigensigniertes Zertifikat exportieren und über E-Mail oder auf anderem Weg an Ihre Benutzer übermitteln. Die Benutzer können dann das Zertifikat manuell installieren und als vertrauenswürdig kennzeichnen, sodass weitere Warnmeldungen vermieden werden.

Erstellen eines Zertifikats

Um in MDaemon ein Zertifikat zu erstellen, gehen Sie folgendermaßen vor:

1. Rufen Sie den Konfigurationsdialog für SSL & TLS auf (erreichbar unter **Sicherheit » Sicherheits-Einstellungen » SSL & TLS » MDaemon**).

2. Aktivieren Sie das Kontrollkästchen **SSL, STARTTLS und STLS aktivieren**.

3. Tragen Sie in das Textfeld **Hostname** den Domänennamen ein, zu dem das Zertifikat gehört (z.B. "`mail.example.com`").

4. Tragen Sie in das Textfeld Name der **Organisation/Firma** den Namen der Organisation oder des Unternehmens ein, dem das Zertifikat gehört.

5. Tragen Sie in das Textfeld **Weitere Hostnamen...** alle weiteren Domänennamen ein, zu denen Ihre Nutzer unter Verwendung dieses Zertifikats gesicherte Verbindungen herstellen (z.B. "`*.example.com`", "`example.com`", "`mail.altn.com`", usw.).

6. Wählen Sie eine Schlüssellänge für das Zertifikat aus.

7. Wählen Sie Land oder Region aus, in der sich der Server befindet.

8. Klicken Sie auf **OK**.

Nutzung eines Zertifikats eines anderen Ausstellers

Auch ein gekauftes oder sonst von einer anderen Stelle als MDaemon ausgestelltes Zertifikat kann verwendet werden. Es muss dazu mithilfe der Microsoft-Management-Konsole in den Zertifikatsspeicher eingelesen werden, den MDaemon verwendet. Hierzu sind unter Windows XP folgende Schritte nötig:

1. Klicken Sie in der Windows-Taskleiste auf **Start** » **Ausführen...,** und geben Sie in das Textfeld "**mmc /a**" ein.
2. Klicken Sie auf **OK**.
3. Klicken Sie in der Microsoft Management Console in der Menüleiste auf **Datei** » **Snap-In hinzufügen/entfernen...** (oder drücken Sie **Strg-M**).
4. Klicken Sie auf der Registerkarte Eigenständig auf **Hinzufügen...**
5. Klicken Sie im Konfigurationsdialog *Eigenständiges Snap-In hinzufügen* auf **Zertifikate** und dann auf **Hinzufügen**.
6. Im Konfigurationsdialog *Zertifikat Snap-In* wählen Sie **Computerkonto**, und klicken Sie dann auf **Weiter**.
7. Im Konfigurationsdialog *Computer auswählen* wählen Sie **Lokalen Computer**, und klicken Sie dann auf **Fertig stellen**.
8. Klicken Sie auf **Schließen**, und klicken Sie auf **OK**.
9. Ist das Zertifikat, das Sie importieren, eigensigniert, so klicken Sie unter *Zertifikate (Lokaler Computer)* im rechten Bereich des Fensters auf **Vertrauenswürdige Stammzertifizierungsstellen** und dann auf **Zertifikate**. Falls es nicht eigensigniert ist, klicken Sie auf **Eigene Zertifikate**.
10. Klicken Sie in der Menüleiste auf **Aktion** » **Alle Aufgaben** » **Importieren...** und dann auf **Weiter**.
11. Geben Sie Pfad und Dateinamen zu dem Zertifikat an, das Sie importieren wollen (navigieren Sie nötigenfalls mithilfe von Durchsuchen), und klicken Sie auf **Weiter**.
12. Klicken Sie erneut auf **Weiter,** dann klicken Sie auf **Fertig stellen**.

MDaemon zeigt nur Zertifikate an, deren private Schlüssel dem Standard "Privater Informationsaustausch (PKCS #12)" entsprechen. Falls das importierte Zertifikat nicht in der Liste erscheint, kann es nötig sein, eine PEM-Datei zu importieren, die sowohl den Schlüssel für das Zertifikat als auch den privaten Schlüssel enthält. Zum Import dieser Datei sind ebenfalls die oben aufgeführten Schritte erforderlich; die Datei wird hierdurch in das Format PKCS #12 umgewandelt.

Verwaltung Ihres Zertifikats mithilfe von Let's Encrypt

Let's Encrypt ist eine Zertifizierungsstelle (auch Certificate Authority, kurz CA), die mithilfe eines automatisierten Verfahrens unentgeltlich Zertifikate zur Verfügung stellt. Dieses Verfahren soll die derzeit noch weit verbreiteten und komplexen Verfahren der manuellen Erstellung, Echtheitsprüfung, Signatur, Installation und Verlängerung von Zertifikaten für die Sicherung von Websites ablösen.

Um dieses Verfahren zu unterstützen, steht Ihnen der Konfigurationsdialog Let's Encrypt 596 zur Verfügung. Mithilfe dieses Konfigurationsdialog wird das automatische Verfahren zur Verwaltung eines Zertifikats unterstützt, das Let's Encrypt bereitstellt. Sie können hier ein PowerShell-Skript einfach konfigurieren und ausführen, das im Verzeichnis "`MDaemon\LetsEncrypt`" abgelegt ist. Wenn Sie dieses Skript ausführen, wird hierdurch das System für Let's Encrypt eingerichtet, und insbesondere werden die für die erfolgreiche Abwicklung der http-01-Challenge erforderlichen Dateien in das HTTP-Verzeichnis von Webmail kopiert. Das Skript nutzt als Domäne für das Zertifikat den SMTP-Hostnamen 184 der Standard-Domäne 181 und fügt etwa konfigurierte *Weitere Hostnamen* ein, ruft das Zertifikat ab, importiert es in Windows, und konfiguriert MDaemon so, dass das Zertifikat für MDaemon, Webmail und die Remoteverwaltung genutzt wird. Darüber hinaus erstellt das Skript im Verzeichnis "`MDaemon\Logs\`" die Protokolldatei `LetsEncrypt.log`. Diese Protokolldatei wird immer dann, wenn das Skript ausgeführt wird, gelöscht und neu erstellt. Sie beinhaltet Datum und Uhrzeit, wann das Skript ausgeführt wurde. Falls Sie eine *E-Mail-Adresse des Administrators für Benachrichtigungen* angegeben haben, werden im Fehlerfall Benachrichtigungen an diese Adresse versandt. Nähere Informationen finden Sie im Abschnitt Let's Encrypt 596.

Siehe auch:

SSL & TLS 577

Kapitel

9 Glossar

ACL—Abkürzung für den englischen Begriff **A**ccess **C**ontrol **L**ists, Zugriffskontroll-Listen. ACL ist eine Erweiterung des Internet Message Access Protocols (kurz IMAP4), mit dessen Hilfe Sie eine Zugriffsliste für jeden IMAP-Nachrichten-Ordner erstellen können. Hierdurch können Sie Ihre Ordner für andere Benutzer freigeben, die ebenfalls über ein Benutzerkonto auf Ihrem Mailserver verfügen. Sie können weiter für jeden Benutzer den Umfang seiner Zugriffsrechte festlegen. So können Sie beispielsweise bestimmen, ob ein Benutzer Nachrichten löschen, als gelesen oder ungelesen markieren oder in Ordner kopieren darf, neue Unterordner anlegen kann, und vieles mehr. Ordner, die in dieser Weise freigegeben wurden, können nur durch E-Mail-Clients mit ACL-Unterstützung genutzt werden, und nur solche Clients können auch die Berechtigungen definieren. Unterstützt der verwendete Client keine ACL, so können Sie die Berechtigungen auch über MDaemon setzen.

ACL werden in RFC 2086 umfassend beschrieben. Sie erhalten dieses Dokument unter:

http://www.rfc-editor.org/rfc/rfc2086.txt

ASCII—Wird "as-kieh" ausgesprochen und ist das Akronym für den englischen Begriff "**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange" (Amerikanischer Standardzeichensatz für den Informationsaustausch). Dies ist der weltweit genutzte Standardkode, in dem alle lateinischen Buchstaben, Ziffern und Satzzeichen als siebenstellige Binärzahlen ausgedrückt werden, wobei jedem Zeichen eine Zahl von 0 bis 127 zugewiesen ist (d.h. 0000000 bis 1111111). Der ASCII-Kode für den Buchstaben M lautet beispielsweise 77. Die meisten Rechner nutzen die ASCII-Kodes, um Text darzustellen; sie können so Daten an andere Rechner übermitteln. Die meisten Texteditoren und Textverarbeitungsprogramme können Dateien im ASCII-Format speichern (die entstehenden Dateien werden üblicherweise als ASCII-Dateien bezeichnet). Die meisten Datendateien — insbesondere solche, die numerische Daten enthalten — werden jedoch nicht im ASCII-Format gespeichert.

Es bestehen einige umfangreichere Zeichensätze, die über 128 zusätzliche Zeichen verfügen, da sie nicht 7 sondern 8 Bit nutzen. Diese Zusatzzeichen werden genutzt, um Symbole und Schriftzeichen darzustellen, die in der englischen Sprache nicht genutzt werden. Das Betriebssystem DOS nutzt einen Zeichensatz, der unter anderem ASCII-Zeichen enthält und als erweiterter ASCII-Zeichensatz bezeichnet wird. Es besteht jedoch noch ein Standard, der einem universellen Zeichensatz noch näher kommt, ISO Latin 1, den viele Betriebssysteme und Web-Browser nutzen.

ATRN—Vgl. unten ETRN und ODMR.

Backbone—Ein oder mehrere Verbindungswege, die den Haupt-Datenverkehr in einem Netzwerk verarbeiten. Der Begriff bezeichnet keine absoluten Größenverhältnisse, da die Verbindungswege außerhalb des Backbones in einem größeren Netz den Umfang des Backbones in einem kleineren Netz übersteigen können.

Bandbreite—Die Datenmenge, die in vorgegebener Zeit über eine Netzwerk- oder Modemverbindung übermittelt werden kann, gemessen üblicherweise in Bit pro Sekunde (bps). Eine voll beschriebene Seite Text hat etwa 16.000 Bit; ein schneller Modem kann sie in 1 bis 2 Sekunden übertragen. Abhängig von der

Komprimierung benötigen vollständige Videodateien etwa 10.000.000 Bit pro Sekunde.

Bandbreite kann bildlich wie eine Autobahn dargestellt werden. Die Autobahn stellt die Verbindung dar; die Fahrzeuge, die sie befahren, stellen die Computer-Daten dar. Je breiter die Autobahn (je größer die Bandbreite), desto mehr Fahrzeuge können sie befahren.

Baud—Die Baud-Rate ist ein Maß dafür, wie häufig Trägersignale auf einer Telefonleitung wechseln. Es ist eine Messgröße für die Übertragungsgeschwindigkeit von Modemen. Langsamere Modemen werden üblicherweise nach ihrer Baud-Rate, schnellere Modemen in Bit pro Sekunde gemessen. Die Baud-Rate und Bit pro Sekunde sind nicht notwendig gleich bedeutend, da jedes Signal in Hochgeschwindigkeitsverbindungen mehr als ein Bit kodieren kann.

Bit—Ein einzelne Binärziffer (englisch **B**inary Dig**it**), die kleinste Einheit Computerdaten, die als einstellige Zahl in Base-2 (0 oder 1) dargestellt wird. Abgekürzt üblicherweise mit dm Buchstaben "b", wie in "bps" (Bit pro Sekunde). Eine voll beschiebene Seite Text hat etwa 16.000 Bit.

Bitmap—Die meisten Grafikdateien, die Computer anzeigen, und alle im Internet verfügbaren Grafiken, sind Bitmaps. Ein Bitmap ist eine Anordnung von Bildpunkten ("Bits"), die wie ein Bild aussehen, solange man sie nicht zu nahe am Bildschirm betrachtet oder die Grafik zu sehr vergrößert, sodass die Bildpunkte einzeln sichtbar werden und der Gesamteindruck, den sie vermitteln, verloren geht. Gängige Formate für Bitmaps sind u.a. BMP, JPEG, GIF, PICT, PCX und TIFF. Da Bitmap-Grafiken üblicherweise aus vielen Bildpunkten bestehen, erscheinen sie in hoher Vergrößerung nicht mit glatten Kanten sondern "pixelig". Vektorgrafiken (wie sie üblicherweise in CorelDraw, PostScript und CAD-Software angelegt werden) lassen sich wesentlich besser skalieren, da sie auf geografischen Formen basieren, die mathematisch berechnet sind und nicht nur durch "zusammengewürfelte" Bildpunkte dargestellt werden.

Bps—"**B**it **P**ro **S**ekunde" ist eine Maßeinheit für die Übertragungsgeschwindigkeit von Daten zwischen zwei Rechnern. Ein Modem mit 33.6 kbps kann etwa 33.600 Bit pro Sekunde übermitteln. Kilobit (1.000 Bit) pro Sekunde und Megabit (1.000.000 Bit) pro Sekunde werden als "kbps" und "Mbps" abgekürzt.

Browser—Kurzform für "Web-Browser"; Browser sind Anwendungen, in denen Webseiten angezeigt werden. Sie interpretieren HTML-Kode, Text, Hypertext-Verknüpfungen, Bilder, JavaScript und andere Elemente. Die am weitesten verbreiteten Browser sind der Internet Explorer und der Netscape Communicator.

Byte—Eine Gruppe Bits (üblicherweise 8), die ein einzelnes Zeichen darstellen. Ein Byte enthält 8 Bit, machmal auch mehr, je nach Messung. "Byte" wird mit dem Buchstaben "B" abgekürzt.

Cache—Zwischenspeicher, wird ausgesprochen wie "Käsch". Es gibt verschiedene Arten von Caches, die alle unlängst genutzte Informationen speichern, sodass sie für erneuten Zugriff schneller verfügbar sind. Web-Browser benutzen etwa Caches, um Seiten, Grafiken, URLs und andere Elemente von Websites zu speichern, die Sie vor kurzem aufgesucht haben. Kehren Sie zu einer gecachten Seite zurück, so muss der Browser nicht alle Elemente erneut laden. Da der Zugriff auf den Cache auf der lokalen Festplatte weit schneller ist als der Zugriff über die Internet-Verbindung, beschleunigen Caches den Surfvorgang deutlich.

MDaemon speichert die IP-Adressen der Domänen im IP-Cache, an die Sie unlängst Nachrichten übermittelt haben. MDaemon muss damit die IP-Adressen bei der Zustellung weiterer Nachrichten an dieselben DOmänen nicht erneut auflösen. Hierdurch kann die Zustellung deutlich beschleunigt werden.

CGI—Abkürzung für **C**ommon **G**ateway **I**nterface; ein Satz regeln, die beschreiben, wie ein Web-Server mit anderer Software auf demselben Rechner kommuniziert und wie die andere Software (das "CGI-Programm") mit dem Web-Server kommuniziert. Jede Software kann CGI-Software sein, falls sie Eingabe- und Ausgaberoutinen nach dem CGI-Standard beherrscht. CGI-Programme sind üblicherweise kleine Programme, die Daten von einem Web-Server empfangen und verarbeiten, etwa den Inhalt eines Formulars in eine E-Mail-Nachricht überführen oder die Daten sonst nachbearbeiten.CGI-Programme werden oft in dem Verzeichnis "cgi-bin" einer Website abgelegt und können, müssen aber nicht, in dem URL, der sie aufruft, erscheinen.

cgi-bin—Der am häufigsten genutzte Verzeichnisname auf einem Web-Server, in dem CGI-Programme abgelegt werden. Der Teil "bin" in "cgi-bin" ist eine Abkürzung für "binary" ("binär"), da viele Programme auch als "Binaries" oder Binärdateien bezeichnet werden. Tatsächlich sind die meisten CGI-BIN-Programme Textdateien, Skripte, die durch an anderen Stellen abgelegte Programme ausgeführt werden.

CIDR—Abkürzung für "**C**lassless **I**nter-**D**omain **R**outing"; ein neues System zur IP-Adressierung, das die älteren auf den Klassen A, B und C basierenden Systeme ablöst. IP-Adressen in CIDR-Schreibweise sehen wie normale IP-Adressen aus, denen ein Schrägstrich und eine Zahl hinzugesetzt wird; dieser Zusatz heißt auch IP-Präfix. Ein Beispiel:

123.123.0.0/12

Der IP-Präfix bestimmt, wie viele Adressen durch die CIDR-Adresse umfasst sind; je niedriger die Zahl, desto mehr Adressen umfasst sie. Im Beispiel kann der Präfix "/12" genutzt werden, um 4.096 Adressen der früheren Klasse C anzusprechen.

CIDR-Adressen verringern den Umfang der Routingtabellen und machen innerhalb geschlossener Organisationen mehr IP-Adressen verfügbar.

CIDR wird in den RFCs 1517-1519 beschrieben; diese Dokumente sind verfügbar unter:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

Client—Ein Software-Programm, das eine Verbindung mit einem *Server* herstellt und mit ihm Daten austauscht. Der Server befindet sich meist auf einem anderen Rechner, entweder im lokalen Netzwerk oder an anderer Stelle. Jeder *Client* ist für die Interaktion mit bestimmten *Servern* vorgesehen, und jeder Server benötigt einen geeigneten Client. Ein Web-*Browser* ist ein Client, der mit Web-*Servern* kommuniziert.

Common Gateway Interface—Siehe CGI.

Cookie—Im Computer-Jargon ist ein *Cookie* ein Datensatz, den ein Web-Server an Ihren Web-Browser sendet;e r wird dort gespeichert und bei Ihrer Rückkehr auf

dieselbe Site sowie beim Aufsuchen anderer Sites für verschiedene Zwecke eingesetzt. Erhält ein Web-Server von einem Web-Browser eine Anforderung, die einen Cookie enthält, so kann er die Daten aus dem Cookie für beliebige Zwecke nutzen, etwa die Daten, die dem Benutzer zurückgesandt werden, anpassen, oder ein Protokoll der Anforderungen des Benutzers führen. Cookies werden oft zur Speicherung von Kennwörtern, Benutzernamen, Voreinstellungen, Informationen über Warenkörbe und andere Zwecke genutzt, die mit der Website in Zusammenhang stehen. Websites können sich durch Cookies scheinbar an Benutzer, ihre früheren Besuche und ihre Aktionen auf der Site "erinnern".

Ihre Browser-Einstellungen bestimmen, ob Sie Cookies annehmen, und wie lange Sie sie speichern. Cookies verfallen meist nach einer vorbestimmten Zeit und werden im Hauptspeicher gehalten, bis der Browser beendet wird; zu diesem Zeitpunkt können sie auf Festplatte gespeichert werden.

Cookies haben **keinen** Lesezugriff auf Ihre Festplatte. Sie können jedoch dazu eingesetzt werden, Informationen über Sie und die Zugriffe auf bestimmte Websites zu gewinnen, die ohne Cookies nicht verfügbar wären.

Dateianlage—Eine Datei, die an eine E-Mail-Nachricht angehängt wurde (englisch auch "Attachment"). Da die meisten E-Mail-Systeme nur reinen Text als E-Mail-Nachrichten versenden können, müssen Binärdateien oder formatierte Textdokumente (etwa Dateien aus Textverarbeitungen) erst kodiert werden, bevor sie versandt werden können. Nach dem Empfang müssen sie entsprechend dekodiert werden. Es sind mehrere Kodierverfahren verfügbar — zwei der am weitesten verbreiteten sind Multipurpose Internet Mail Extensions (MIME) und Unix-to-Unix encode (UUencode). Der Server MDaemon kann bei eingehenden Nachrichten die Dekodierung der Dateianlagen entweder dem Mailclient des Empfängers überlassen oder die Dateianlagen automatisch dekodieren und sie in einem bestimmten Verzeichnis ablegen, bevor die Nachricht an den lokalen Benutzer zugestellt wird.

DFÜ-Netzwerk—Bestandteil von Windows (auch: Remote Access Services, RAS) für den Verbindungsaufbau mit einem Netzwerk über eine Wählverbindung. Falls Ihr Computer nicht über ein LAN mit dem Internet verbunden ist, benötigen Sie einen Wählzugang bei einem Einwahlpunkt (POP) eines Internet Service Providers (ISP), um den Zugriff aufs Internet zu erhalten. Ihr ISP muss u.U. bestimmte Informationen bereit stellen, wie etwa die Adresse des Standard-Gateways und die IP-Adresse für Ihren Rechner.

Das DFÜ-Netzwerk ist über die Systemsteuerung und die Netzwerkeinstellungen zugänglich. Für jeden Dienst kann eine getrennte Wählverbindung konfiguriert werden; die Profile oder Telefonbuch-Einträge können mithilfe von Verknüpfungen an beliebigen Stellen abgebildet werden.

Default—Englischer Begriff für eine Voreinstellung oder Standard-Einstellung in Computer-Programmen. Default-Einstellungen werden genutzt, falls der Benutzer keine abweichenden Einstellungen festgelegt hat. Beispielsweise ist die Standard-Schrift im Netscape Communicator "Times". Diese Einstellung wird beibehalten, falls der Benutzer sie nicht ändert. Standard-Einstellungen sind meist die Einstellungen, die die meisten Benutzer verwenden.

Im Englischen wird der Begriff auch als Verb verwendet. Falls eine benutzerdefinierte Einstellung nicht funktioniert oder dem Programm Daten zur Abarbeitung einer Aufgabe fehlen, fällt es meist auf die Standard-Einstellungen zurück, was mit "default" beschrieben wird.

DHCP—Akronym für "**D**ynamic **H**ost **C**ontrol **P**rotocol". Server in Netzwerken können mithilfe dieses Protokolls den Rechnern im Netzwerk dynamisch IP-Adressen zuweisen. Ein DHCP-Server wartet auf einen Verbindungsaufbau eines anderen Rechners und weist ihm dann eine IP-Adresse aus einer gespeicherten Liste zu.

DHCP wird im RFC-2131 beschrieben; das Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc2131.txt

Domänen-Gateway—Siehe Gateway.

Domänenname—Der eindeutige Name, der eine Website im Internet identifiziert. Beispielsweise ist "mdaemon.com" der Domänenname von MDaemon Technologies. Jeder Domänenname enthält mindestens zwei durch Punkt getrennte Teile; der am weitesten links stehende Teil ist der speziellste Teil, während der Teil rechts der allgemeinste Teil ist. Jeder Domänenname verweist auf die IP-Adresse eines einzelnen Servers, aber ein einzelner Server kann mehr als einen Domänennamen haben. Beispielsweise können "mail.mdaemon.com", "smtp.mdaemon.com" und "example.com" alle auf denselben Server verweisen wie "mdaemon.com", aber "mdaemon.com" kann auf zwei verschiedene Server verweisen. Clients können mithilfe bestimmter Methoden auf Alternativ-Server verwiesen werden, falls der Haupt-Server ausfällt oder aus anderen Gründen nicht erreichbar ist.

Domänennamen können auch registriert sein, ohne einem bestimmten Rechner zugeordnet zu sein. Der Grund dafür ist meist, dass der Inhaber des Domänennamens noch keine Website erstellt hat, oder dass er E-Mail-Adressen, aber keine Website in der Domäne betreibt. Im letzten Fall muss jedoch ein mit dem Internet verbundener Rechner zur Verfügung stellen, der den Domänennamen und seine E-Mail-Nachrichten verarbeiten kann.

Der Begriff Domänennamen wird oft als "Domäne" abgekürzt. Der Begriff "Domäne" hat noch andere Bedeutungen und kann sich auf andere Einrichtungen beziehen, wie etwa Windows-Domänen oder Objektklassen; diese Begriffe dürfen nicht verwechselt werden.

Domänennamen werden in den RFCs 1034-1035 beschrieben; diese Dokumente sind verfügbar unter:

http://www.rfc-editor.org/rfc/rfc1034.txt

http://www.rfc-editor.org/rfc/rfc1035.txt

DomainPOP—Eine durch MDaemon Technologies entwickelte Technik, die Teil des Mailservers MDaemon ist. DomainPOP erlaubt die Bereitstellung von E-Mail-Diensten für ein ganzes Netzwerk oder eine Arbeitsgruppe mithilfe eines einzelnen POP-Postfachs bei einem ISP. Früher musste der E-Mail-Server eines Unternehmens ständig mit dem Internet verbunden sein, um im Netzwerk E-Mail-Dienste zur Verfügung zu stellen, stand ein solcher Server nicht zur Verfügung, mussten die einzelnen Personen Postfächer beim ISP des Unternehmens haben. DomainPOP benötigt nur ein einzelnes Postfach. Der ISP sammelt alle Nachrichten für den Domänennamen des Unternehmens in dem Postfach, DomainPOP ruft die Nachrichten ab und wertet sie darauf hin aus, an welche Mitarbeiter sie gerichtet sind. DomainPOP übernimmt dann die Weiterverteilung an die einzelnen Mitarbeiter. Auf diese Weise kann ein einzelnes Postfach über eine Wählverbindung ein vollständiges Netzwerk mit E-Mail versorgen.

Download—Englische Bezeichnung für "Herunterladen", der Vorgang, durch den Ihr Computer Daten von einem anderen Computer abruft und lädt. Informationen aus dem Internet werden beispielsweise durch Herunterladen von anderen Rechnern empfangen. Das Gegenstück hierzu ist der *Upload*, das *Hochladen*. Falls Sie Informationen an einen anderen Rechner senden wollen, *laden* Sie sie *hoch*.

E-Mail—Kurzform von "Electronic mail", elektronischer Post. Auch andere Schreibweisen (E-mail, e-mail, email usw.) sind gelegentlich anzutreffen. E-Mail ist die Übermittlung von Textnachrichten über Kommunikationsnetzwerke. In den meisten Computer-Netzwerken steht ein E-Mail-System in irgendeiner Form zur Verfügung. Manche E-Mail-Systeme sind auf einzelne Computer-Netzwerke beschränkt, andere haben Netzübergänge (Gateways) in andere Netzwerke (sodass sie standortübergreifende Kommunikation ermöglichen) oder ins Internet (sodass sie weltweite Kommunikation ermöglichen).

Die meisten E-Mail-Systeme nutzen *E-Mail-Clients* (auch als *Mailclient* oder schlicht *Client* bezeichnet), die Texteditoren und andere Werkzeuge zum Verfassen von Nachrichten enthalten, sowie mindestens einen *Server*, der die Nachrichten von den Clients entgegen nimmt und an die Bestimmungsorte leitet. Meist wird eine Nachricht auf dem Client verfasst und zur Zustellung an die *E-Mail-Adresse* (kurz *Adresse*), die in der Nachricht angegeben ist, an den Server geleitet, die sie an den Server des Empfängers weitergibt. Ist der Empfänger der Nachricht eine lokale Adresse, die durch den selben Server versorgt wird, so kann sie auch auf diesem Server verbleiben. Schließlich stellt der Empfänger der Nachricht eine Verbindung zu dem Server her und ruft mithilfe seines eigenen Mailclients die Nachricht ab. Der gesamte Vorgang vom Absenden der Nachricht bis zur Bereitstellung beim Server des Empfängers dauert meist nur wenige Sekunden oder Minuten.

E-Mail-Nachrichten können neben Text auch *Dateianlagen* enthalten. Jede gewünschte Datei kann Dateianlage sein: Grafiken, Textdateien, Programme, andere E-Mail-Nachrichten und vieles mehr. Da die meisten Systeme aber nur den Versand von Textnachrichten unterstützen, müssen die Dateianlagen erst kodiert (in Textform umgewandelt) werden, bevor sie versandt werden können. Der Empfänger muss sie wieder dekodieren. Die beteiligten Mailclients erledigen diesen Vorgang üblicherweise automatisch.

Alle Internet-Dienstleister bieten E-Mail-Dienste an. Die meisten unterhalten auch Gateways, sodass Sie Nachrichten mit Benutzern anderer E-Mail-Systeme austauschen können. Obwohl die Systeme unterschiedliche Protokolle für den Datenaustausch nutzen können, machen bestimmte gemeinsame Standards den Austausch von Nachrichten zwischen nahezu allen verfügbaren Systemen möglich.

E-Mail-Adresse—Ein Name oder eine Zeichenkette, die ein bestimmtes elektronisches Postfach in einem Netzwerk bezeichnet, das E-Mail empfangen kann. E-Mail-Adressen sind die Kennzeichnungen für jene Orte, von denen Nachrichten gesendet und an denen sie empfangen werden können. E-Mail-Server benötigen die E-Mail-Adressen, um die Nachrichten an ihr Ziel weiterzuleiten. Das Format der E-Mail-Adressen unterscheidet sich je nach Netz; im Internet haben alle E-Mail-Adressen das Format "postfachname@example.com".

Ein Beispiel hierzu:

```
Michael.Mason@example.com
```

E-Mail-Client—Langform für *Mailclient* oder *Client* für E-Mail. E-Mail-Clients sind Anwendungen, die dem Benutzer das Versenden, Empfangen und Organisieren von E-Mail gestatten. Sie heißen Clients, weil die E-Mail-System eine Client-Server-Architektur nutzen; ein Client erstellt die Nachrichten und sendet sie an den Server, der sie an den Server des Empfängers weiterleitet; von dort geht die Nachricht an den Client des Empfängers. E-Mail-Clients werden meist als gesonderte Software-Pakete auf dem Rechner des Benutzers installiert; Produkte wie MDaemon enthalten jedoch einen Webmail-Client, der dem Benutzer über seinen Web-Browser bereit gestellt wird. Der Browser wird dadurch zum Mailclient, und ein eigener Client auf dem Rechner des Benutzers ist nicht mehr nötig. Der Komfort und die Flexibilität in der Nutzung werden hierdurch deutlich erhöht.

Ethernet—Die meistgenutzte Verbindungsart in lokalen Netzwerken (LAN). Die beiden meist verbreiteten Varianten sind 10BaseT und 100BaseT. Ein Ethernet auf Basis von 10BaseT kann Daten mit bis zu 10 Mbps (Megabit pro Sekunde) über eine kabelgebundene oder kabellose Verbindung übermitteln. Ein Ethernet auf Basis von 100BaseT kann Daten mit bis zu 100 Mbps übermitteln. Ein Gigabit-Ethernet kann Daten mit bis zu 1.000 Mbps übermitteln; es ist bei manchen Apple-Computern anzutreffen.

ETRN—Akronym für den Begriff **E**xtended **TURN**. Dies ist eine Erweiterung für SMTP, mit deren Hilfe ein SMTP-Server von einem anderen SMTP-Server den Versand von bereit gehaltenen Nachrichten anfordern kann (manchmal auch Versandauslösen oder Aufforderung zur Freigabe wartender Nachrichten genannt). Das SMTP-Protokoll sieht den ABruf von Nachrichten nicht vor (E-Mail wird meist nur über POP3 oder IMAP abgerufen); diese Erweiterung befähigt daher den SMTP-Server, der den Befehl ETRN erteilt, die Gegenstelle zum Aufbau einer neuen SMTP-Verbindung zu veranlassen und dann die Nachrichten zu übermitteln, die für die anfordernde Gegenstelle bereit gehalten werden.

Der Befehl `TURN` ,der hierfür meist eingesetzt wird, stellt ein Sicherheitsrisiko dar, da er ohne jede Echtheitsbestätigung oder Prüfung bewirkt, dass die SMTP-Verbindung umgekehrt wird, und dass sofort mit dem Versand von Nachrichten begonnen wird. Ob der anfordernde Server zur Anforderung berechtigt war, wird nicht geprüft. Der Befehl `ETRN` beginnt eine neue SMTP-Verbindung und kehrt nicht die Richtung der bestehenden Verbindung um. Falls also ein Server unter gefälschter Identität den Befehl erteilt, so versucht die Gegenstelle, an den wirklichen Empfänger zuzustellen. Es besteht ein Vorschlag für einen Standard zur Echtheitsbestätigung beim Befehl TURN (`ATRN`); dieser Standard kehrt ebenfalls die Richtung der SMTP-Verbindung um, erfordert aber vorherige Echtheitsbestätigung. Dieser neue Standard würd als On-Demand Mail Relay (ODMR, Postrelais bei Bedarf) bezeichnet. MDaemon unterstützt ETRN und ODMR-ATRN.

ETRN wird in RFC 1985 beschrieben; das Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc1985.txt

ODMR wird in RFC 2645 beschrieben; das Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc2645.txt

FAQ—Abkürzung für "**F**requently **A**sked **Q**uestions" (häufig gestellte Fragen). FAQ sind Dokumente, die Antworten auf die meist gestellten Fragen zu einem bestimmten Thema liefern. Die erscheinen meist als Liste, wobei unter jeder Frage die Antwort aufgeführt ist. In größeren FAQ werden oft alle Fragen am Beginn

des Dokuments aufgeführt; Verknüpfungen verweisen dann auf die Antworten im Dokument. FAQ werden oft als Ausgangspunkt für technischen Support und Anweisungen zur Fehlerbehebung genutzt; hat der Benutzer Zugriff auf ein FAQ, das seine Frage beantwortet, so kann er viel Zeit sparen und muss sich nicht mit dem technischen Support in Verbindung setzen.

File Transfer Protocol—Siehe FTP.

Firewall—Im Computer-Jargon wird ein *Firewall* durch verschiedene Sicherheitsmaßnahmen gebildet, entweder auf Grundlage von Software oder Hardware, die ein Computer-Netzwerk in mindestens zwei Teile untergliedern oder den Zugriff darauf in sonstiger Weise auf bestimmte Benutzer begrenzen. Es kann beispielsweise wünschenswert sein, die Homepage einer Website im Netzwerk allen Benutzern zugänglich zu machen aber nur den eigenen Angestellten den Zugang zu einem geschlossenen Bereich zu ermöglichen. Unabhängig von der dabei verwendeten Zugangskontrolle (Kennwort, Beschränkung von Verbindungen auf bestimmte IP-Adressen usw.) geht man davon aus, dass sich der geschlossene Bereich hinter einem Firewall befindet.

FTP—Abkürzung für "**F**ile **T**ransfer **P**rotocol" (Protokoll zur Dateiübertragung). Eine häufig genutzte und effiziente Methode, um Dateien über das Internet von einem Rechner auf einen anderen zu übermitteln. Es stehen besondere Client/Server-Anwendungen hierfür zur Verfügung, die FTP-Server und FTP-Clients genannt werden. FireZilla ist beispielsweise einer der meist verwendeten Clients. FTP-Clients können üblicherweise neben der Dateiübertragung zahlreiche weitere Funktionen ausführen und sind sehr nützliche Produkte. Auch einige Web-Browser unterstützten das File Transfer Protocol, manchmal aber nur zum Herunterladen. Die meisten FTP-Server sind "anonyme FTP-Server"; das bedeutet, dass jeder auf sie zugreifen und Daten herunterladen kann. Dazu werden meist der Benutzername "anonymous" und als Kennwort die E-Mail-Adresse angegeben. Manchmal können Dateien von anonymen FTP-Sites auch ohne Anmeldung geladen werden; sie werden durch Anklicken einer Verknüpfung abgerufen. Browser, die FTP unterstützen, können meist eine Verbindung zu einer FTP-Site herstellen, indem "ftp://" statt "http://" an den Beginn eines URLs gesetzt wird.

FTP wird in RFC-959 beschrieben; dieses Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc959.txt

Gateway—Computer und Software, die Daten zwischen zwei Anwendungen oder Netzwerken vermitteln, deren Protokolle und Schnittstellen sich unterscheiden. "Gateway" ist auch die Bezeichnung für den Netzübergang zwischen zwei Systemen. Der ISP ist beispielsweise der Gateway des Benutzers zum Internet.

Der Mailserver MDaemon kann für andere Domänen als E-Mail-Gateway arbeiten; hierzu stehen die Funktionen Domänen-Gateways zur Verfügung. MDaemon sammelt die Nachrichten für eine Domäne und stellt sie zum Abruf durch die Domäne bereit. MDaemon wird dadurch zum Gateway für die Domäne. Dies ist insbesondere für Domänen nützlich, die keine ständig aktive Internet-Verbindung haben, und für Domänen, in denen eine Ausfallsicherung durch Backup-Server für den Fall gewünscht ist, dass der eigentliche Server ausfällt.

GIF—Abkürzung für "**G**raphics **I**nterchange **F**ormat" (Format zum Austausch von Grafikdateien). Ein verbreitetes Format für Grafikdateien, und das meist verwendete Format für Grafiken im Internet. GIF nutzt eine indizierte Farben oder eine Palette mit einer bestimmten Farbanzahl; dies verringert die Dateigröße deutlich, besonders, wenn die Grafik große Anteile derselben Farbe enthält. Die

geringere Größe erleichtert die schnelle Übermittlung zwischen Systemen und ist der Grund für die Verbreitung im Internet. Die Methode zur GIF-Komprimierung wurde ursprünglich von CompuServe entwickelt; daher werden die Dateien noch häufig als CompuServe GIF bezeichnet.

Grafische Benutzeroberfläche—Siehe GUI.

GUI—Abkürzung für "**G**raphical **U**ser **I**nterface" (grafische Benutzerschnittstelle, auch grafische Benutzeroberfläche). Die GUI erlaubt die Interaktion mit Computern und Anwendungen mit Hilfe einer Maus oder eines vergleichbaren Eingabegeräts und das Anklicken grafischer Steuerelement auf dem Bildschirm, das die Eingabe von Textbefehlen ersetzt. Die Betriebssysteme Microsoft Windows und Apple Mac sind beide GUI-gestützt, die Idee der GUI stammt, obwohl sie von Apple erstmals praktisch eingesetzt wurde, eigentlich von Xerox.

Host—Jeder Computer in einem Netzwerk, der als Server für andere Computer desselben Netzwerks arbeitet. Auf dem Host können Web-Server, E-Mail-Server und andere Dienste ausgeführt werden, und er stellt meist mehrere Dienste gleichzeitig bereit. Der Begriff Host wird auch im Sinne von "hosten" als Verb gebraucht. Ein Host, auf dem ein E-Mail-Server betrieben wird, "hostet" die E-Mail-Dienste.

In Peer-to-Peer-Netzwerken sind die Rechner meist gleichzeitig Host und Client. Ein Rechner kann etwa die Drucker für das Netzwerk hosten, aber gleichzeitig Client sein, der E-Mail-Nachrichten abruft und Dateien von einem anderen Host lädt.

HTML—Abkürzung für "**H**ypertext **M**arkup **L**anguage" ("Hypertext-Auszeichnungssprache"). Die Programmiersprache, in die im World Wide Web genutzten Hypertext-Dokument erstellt werden. Ein HTML-Dokument ist, einfach gesagt, ein reines Textdokument, das Formatierungsbefehle und Tags enthält, die der Web-Browser des Benutzers auswertet und in die vollständige Darstellung einer Website mit formatiertem Text und Farben umsetzt. Ein Browser, der etwa ein HTML-Dokument mit dem Inhalt "<B>Text</B>" erhält, stellt das Wort Text in Fettdruck dar. Da reine Textdateien meist sehr gklein sind, können sie über das Internet schnell übermittelt werden.

HTTP—Abkürzung für **H**ypertext **T**ransfer **P**rotocol ("Hypertext-Übertragungsprotokoll") ist das Protokoll für die Übertragung von Hypertext-Dokumenten zwischen zwei Rechnern über das Internet. HTTP erfordert einen Client (meist einen Web-Browser) und einen HTTP-Server als Endpunkte der Verbindung.

HTTP wird in RFC-2616 beschrieben; dieses Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc2616.txt

Hypertext—Jeder Text, der Verknüpfungen mit anderen Dokumenten oder Stellen im selben Dokument enthält. Manchmal wird auch der Text als Hypertext-Verknüpfung oder nur als Verknüpfung oder Link bezeichnet. Hypertext kann ein Wort oder ein Satz sein und enthält die Verknüpfung bereits, sodass ein Klick auf den Text den Benutzer an die Stelle führt, auf die der Hyperlink verweist. Hypertext-Verknüpfungen sind meist deutlich sichtbar, da der Text unterstrichen und in einer anderen Farbe dargestellt wird, dies ist jedoch nicht unbedingt gegeben. Die Erscheinung von Hypertext unterscheidet sich manchmal nicht von normalem Text, sein Vorhandensein wird aber fast immer durch einen grafische Effekt dargestellt, wenn der Mauszeiger über dem Hypertext steht.

Hypertext Markup Language—Siehe HTML.

IMAP—Abkürzung für **I**nternet **M**essage **A**ccess **P**rotocol (Protokoll für Zugriff auf Nachrichten via Internet) ist ein an der Universität Standford entwickeltes Protokoll zum Abruf und zur Verwaltung von E-Mail-Nachrichten. Die neueste Version ist IMAP4, die POP3 ähnelt aber einige zusätzliche Funktionen enthält. IMAP4 ist am besten bekannt als Protokoll für die Verwaltung von E-Mail-Nachrichten auf dem Server statt auf dem lokalen Rechner des Benutzers. Nachrichten können nach Schlüsselwörtern durchsucht, in Ordnern abgelegt, zum Abruf gekennzeichnet und in anderer Weise behandelt werden. Sie befinden sich dabei immer auf dem Server. IMAP stellt daher geringere Anforderungen an die Rechner der Nutzer und zentralisiert die E-Mail-Funktionen, sodass Benutzer von verschiedenen Standorten auf ihre Daten zugreifen können.

IMAP wird RFC-2060 beschrieben; dieses Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc2060.txt

IMAP4-ACL-Erweiterung—Siehe ACL.

Internet—Das Internet entstand 1969 für die Nutzung durch die Streitkräfte der USA, ursprünglich als Kommunikationsnetzwerk, das während eines Atomkrieges nicht zerstört werden konnte. Es besteht heute aus Millionen Computern und Netzwerken weltweit. Das Internet ist als dezentrale Struktur entworfen; es wird nicht durch einzelne Unternehmen, Organisationen oder Staaten kontrolliert. Jeder Host (oder Rechner) im Internet ist von anderen unabhängig und kann alle Informationen und Dienste anbieten, die seine Betreiber wünschen. Dennoch werden die meisten Informationen auf ihrem Übertragungsweg durch Backbones geleitet, der sehr schnelle Verbindungen hoher Bandbreite zur Verfügung stellt und von den größeren ISPs und Organisationen kontrolliert wird. Die meisten Nutzer greifen über einen Onlinedienst wie AOL oder einen anderen ISP auf das Internet zu, der an mindestens einen Backbone angebunden ist.

Es wird oft angenommen, das *World Wide Web (WWW)* und das Internet seien dasselbe; dies trifft aber nicht zu. Das WWW ist nur Teil des Internet, es stellt nicht das gesamte Internet dar. Es ist der sichtbarste und meist genutzte Teil, der hauptsächlich kommerziellen Interessen dient, aber es ist nur ein Teil des Internet.

Intranet—Ein Internet für geschlossene Benutzergruppen, das streng auf das Netzwerk eines Unternehmens oder einer Organisation beschränkt ist. Obwohl sich Intranet je nach Anwendungszweck stark unterscheiden, können sie alle Leistungsmerkmale bieten, die auch das Internet bereit stellt. Sie können eigene E-Mail-Systeme, Datei-Verzeichnisse und Websites haben, durchsucht werden, Hypertext-Dokumente veröffentlichen und vieles mehr. Der Hauptunterschied zwischen Intranets und dem Internet ist, dass ein Intranet vergleichsweise klein und nur einer geschlossenen Benutzergruppe zugänglich ist.

IP—Abkürzung für "**I**nternet **P**rotocol" ("Internet-Protokoll", wie beispielsweise in TCP/IP). Internet-Protokolle ermöglichen den Datenaustausch zwischen Systemen über das Internet. Nutzen zwei Gegenstellen dasselbe Internet-Protokoll, so können sie unabhängig von ihren Plattformen und Betriebssystemen Daten austauschen. Der Begriff IP wird auch als Abkürzung für die IP-Adresse benutzt. Derzeit ist Standard-Version 4 des Internet-Protokolls (IPv4) aktuell.

Das Internet-Protokoll wird in RFC-791 beschrieben; dieses Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc791.txt

IP-Adresse—Die Internet-Protokoll-Adresse, mit deren Hilfe ein bestimmtes TCP/IP-Netzwerk und die Hosts oder Computer in diesem Netzwerk identifiziert werden. Die Adresse ist eine 32-bittige numerische Adresse, die vier Zahlengruppen enthält. Die Zahlengruppen liegen zwischen 0 und 255 und sind durch Punkte getrennt (z.B. "127.0.0.1"). Innerhalb eines abgeschlossenen Netzwerks muss jeder Computer eine eindeutige IP-Adresse haben, die zufällig vergeben werden kann. Jeder Computer im Internet muss aber eine registrierte IP-Adresse haben, damit Doppelvergaben vermieden werden. Jede IP-Adresse im Internet kann fest (statisch) oder dynamisch sein. Statische Adressen ändern sich nicht und bezeichnen immer denselben Standort oder Computer im Internet. Dynamische IP-Adressen ändern sich und werden meist durch ISPs an Computer vergeben, die nur vorübergehend mit dem Internet verbinden sind, etwa Kunden mit Wählzugang zum Internet. Auch für Wählzugänge können aber feste IP-Adressen vergeben werden.

ISPs und größere Organisationen versuchen üblicherweise, einen IP-Adressbereich ("Range") vom InterNIC Registration Service zu erhalten, sodass alle Clients in ihrem Netz oder alle Nutzer ihrer Dienste ähnliche Adressen haben. Diese Adressen werden in drei Klassen unterteilt: Klasse A, B und C. Bereiche der Klassen A und B werden von sehr großen Organisationen genutzt und unterstützen 16 Millionen und 65.000 Hosts. Bereiche der Klasse C sind für kleinere Netzwerke geeignet und unterstützen 255 Hosts. Bereiche der Klassen A und B sind wegen der Knappheit der verfügbaren Adressen nur schwer zu erhalten, sodass viele Unternehmen stattdessen mehrere Bereiche der Klasse C nutzen müssen. Wegen der Knappheit an IP-Adressen wurde ein neues Protokoll für IP-Adressen, CIDR, geschaffen, das das bisherige System schrittweise ablöst.

Der derzeitige Protokoll-Standard IPv4 wird in RFC-791 beschrieben; dieses Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc791.txt

IP der Version 6 (IPv6) ist in RFC-2460 beschrieben; dieses Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc2460.txt

CIDR ist in den RFCs 1517-1519 beschrieben; diese Dokumente sind verfügbar unter:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

IP-Nummer—Siehe IP-Adresse.

ISP—Abkürzung für **I**nternet **S**ervice **P**rovider (im deutschsprachigen Raum meist Internet-Provider); ein Dienstleister, der Endkunden den Zugang zum Internet vermittelt. Die meisten ISPs bieten ihren Kunden verschiedene Internet-Dienste, wie etwa Zugriff auf WWW, Newsgroups und News-Server usw. Die Benutzer stellen zum ISP meist eine Wählverbindung oder eine andere Art der Verbindung her; der ISP verbindet sie mit einem Router, der dann die Verbindung zum Internet-Backbone vermittelt.

Java—Eine Entwicklung von Sun Microsystems. Java ist eine netzwerkorientierte Programmiersprache für Computer, deren Syntax C/C++ ähnelt, die sich aber nicht auf Funktionen sondern auf Klassen stützt. Für Internet-Anwendungen wird sie oft zur Programmierung von Applets eingesetzt, dies sind kleine Programme, die in Webseiten eingebunden sind. Die Programme können automatisch abgerufen und im Browser des Benutzers ausgeführt werden und stellen viele Funktionen zur Verfügung, die durch HTML oder sonstige Skript-Sprachen nicht umsetzbar wären, ohne dass dabei die Gefahr von Viren und Schäden am Rechner zu befürchten wäre. Java ist effizient und benutzerfreundlich und wird daher bei vielen Entwicklern von Software und Hardware immer beliebter.

JavaScript—Eine Entwicklung von Netscape, die nicht mit Java verwechselt werden darf. JavaScript erweitert die Fähigkeiten von HTML und gestattet die Entwicklung interaktiver Webseiten. JavaScript ist eine weit entwickelte und einfach einsetzbare Programmiersprache, die deutlich leichter einzusetzen ist als Java und andere Sprachen, aber deswegen auch in gewisser Weise begrenzt ist. Trotz diesen Beschränkungen ist die sehr hilfreich, um interaktive Elemente in Websites einzusetzen. JavaScript kann beispielsweise Formulardaten vorbearbeiten, bevor sie an den Web-Server übergeben werden und Reaktionen auf Benutzeraktionen, wie das Anklicken von Links und Formularelementen bewirken. Auch die Steuerung von Plugins und Applets auf der Grundlage der Benutzeraktionen ist möglich, und viele weitere Funktionen werden unterstützt. JavaScript wird in den Text der HTML-Dokumente eingebunden und durch Web-Browser interpretiert und ausgeführt.

JPEG—Ein Grafikformat, das in der Komprimierung von Grafiken mit großer Farbtiefe und Fotografien weitaus effizienter als GIF ist. GIF ist das Format der Wahl für Grafiken, die wiederkehrende Formen und große einheitliche Farbflächen enthalten, JPEG ist für Grafiken mit uneinheitlichen Mustern und vielen verschiedenen Farben deutlich besser geeignet. JPEG wird meist für Grafiken mit großer Farbtiefe und Fotodarstellungen im Internet genutzt. Der Begriff ist eine Abkürzung für "**J**oint **P**hotographic **E**xperts **G**roup", den Namen der Gruppe, die das Format entwickelt hat.

kbps—Geläufige Maßeinheit für Übertragungsgeschwindigkeiten von Modemen (z.B. 56 kbps). Abkürzung für "**K**ilo**b**it **P**ro **S**ekunde". Die Einheit bezeichnet 1 Kilobit (1.000 Bit) Daten, die pro Sekunde übermittelt oder verarbeitet werden. Beachte - Dieser Begriff darf nicht mit Kilobyte verwechselt werden, 1 Kilobyte enthält etwa achtmal so viele Daten wie ein Kilobit.

Kilobyte—Ein Kilobyte (K oder KB) sind 1.000 Byte Computerdaten. Genau genommen wären es 1.024 Byte (2^10 = 1024), im normalen Sprachgebrauch wird aber zur einfacheren Handhabung auf 1.000 abgerundet.

LAN—Abkürzung für **L**ocal **A**rea **N**etwork ("lokales Netzwerk"); ein Computer-Netzwerk, das auf ein einzelnes Gebäude oder eine bestimmte Fläche begrenzt ist, bei dem meist alle Netzwerkgeräte (Computer oder Workstations) mit Kabeln oder anderen Verbindungsarten an das Netzwerk angebunden sind. Die meisten größere Unternehmen unterhalten ein LAN, das die Verwaltung und den Austausch von Informationen zwischen den Mitarbeiter deutlich erleichtert. In den meisten LANs sind ein E-Mail- oder Chat-System und gemeinsam genutzte Netzwerkgeräte, wie Drucker, vorhanden, sodass nicht alle Geräte für alle Arbeitsplätze beschafft werden müssen. Sind die einzelnen Endstellen über Telefonleitungen, Funkverbindungen oder Satelliten-Verbindungen angebunden, so spricht man von einem Wide Area Network (Weitverkehrsnetzwerk, WAN).

Latenz—Die Zeit, die ein Datenpaket für die Übermittlung über eine Netzwerkverbindung braucht. Während das Datenpaket gesendet wird, entsteht eine Verzögerung oder Latenz, bis die Gegenstelle den ordnungsgemäßen Empfang des Datenpakets bestätigt. Latenz ist neben der Bandbreite einer der Faktoren, die die Geschwindigkeit der Verbindung bestimmen.

LDAP—Abkürzung für **L**ightweight **D**irectory **A**ccess **P**rotocol, ein Protokoll für Verzeichnisdienste, das eine Vereinfachung gegenüber dem Directory Access Protocol (DAP) darstellt. Das Verzeichnissystem ist eine hierarchische Struktur, die aus den folgenden Ebenen besteht: Die höchste Ebene "root", dann Land, Organisation, Organisationseinheit und individuelle Endstelle in der Einheit. Jeder LDAP-Eintrag besteht aus Attributen mit einem eindeutigen Identifikationsmerkmal, dem Distinguished Name (DN). Da das Protokoll standardoffen ist, ist es effizient und kann über viele Server verteilt werden. LDAP kann schließlich für nahezu jede Anwendung jeder Plattform den Zugriff auf Verzeichnisinformationen wie E-Mail-Adressen, Organisationen usw. weltweit.

LDAP ist in RFC-2251 beschrieben; das Dokument ist verfügbar unter

http://www.rfc-editor.org/rfc/rfc2251.txt

Link—Siehe Hypertext.

Listen-Server—Eine Serveranwendung, die E-Mail-Nachrichten an mehrere Empfänger verteilt, indem sie die Nachricht an eine einzelne Adresse richtet. Wird eine E-Mail-Nachricht an eine Mailingliste auf dem Listen-Server versandt, so wird sie an die Mitglieder der Liste automatisch weiter verteilt. Mailinglisten haben meist eine einzige normale E-Mail-Adresse (etwa mailingliste@example.com), aber diese Adresse spricht die gesamte Liste der Mitglieder und nicht nur einen bestimmten Empfänger oder ein bestimmtes Postfach an. Wird jemand Mitglied einer Mailingliste, so fügt der Server seine Adresse der Liste hinzu und leitet künftige Listennachrichten auch an dieses Mitglied. Bestellt jemand die Liste ab, so entfernt der Server die zugehörige Adresse aus der Liste; sie erhält dann keine Nachrichten aus der Liste mehr.

Der Begriff "listserv" wird oft allgemein für beliebige Liste-Server verwendet. Listserv® ist jedoch eine Marke von L-Soft International, Inc. und wird für ein spezielles Programm genutzt, das Eric Thomas 1986 für BITNET entwickelt hat. Neben den anderen Funktionen hat der Server MDaemon auch umfassende Funktionen für die Verwaltung von Mailinglisten und den zugehörigen Funktionen.

Logon—Kode oder eine Zeichenfolge, mit der sich ein Benutzer an einem Rechner identifiziert. Meist muss auch ein Kennwort angegeben werden, um Zugriff zu erhalten.

Viele Begriffe werden gleichbedeutend mit "Logon" verwendet, wie etwa *login*, *Benutzername*, *Benutzer*, *user ID*, *sign-in*. Logon wird auch in der Bedeutung "einloggen", anmelden gebraucht; ein Benutzer loggt sich an einem Server ein.

Mailingliste—Auch als E-Mail-Gruppe oder Verteilerliste bezeichnet; eine Mailingliste ist eine Liste von E-Mail-Adressen, die durch eine einzelne E-Mail-Adresse angesprochen werden können, etwa "mailingliste@example.com". Geht eine Nachricht bei dem Listen-Server ein, so wird die Nachricht automatisch an alle Mitglieder der Mailingliste gesendet. Neben den anderen Funktionen hat der Server MDaemon auch umfassende Funktionen für die Verwaltung von Mailinglisten und den zugehörigen Funktionen. Listen können öffentlich oder privat (jeder oder nur Mitglieder können veröffentlichen oder die Liste bestellen),

moderiert (jede Nachricht muss genehmigt werden, bevor sie veröffentlicht wird) sein, im Digest-Format oder als individuelle Nachrichten gesendet werden und auf vielfältige andere Art eingesetzt werden.

Megabyte—Technisch eigentlich 1.048.675 Byte (oder 1.024 Kilobyte); umgangssprachlich wird Megabyte ("MB") jedoch auf 1.000.000 Byte abgerundet.

MIME—Abkürzung für **M**ultipurpose **I**nternet **M**ail **E**xtensions (Mehrzweck-Erweiterungen für Internet Mail), ein 1992 durch die Internet Engineering Task Force (IETF) verabschiedeter Standard für die Kodierung von Dateien, die keine Textdateien sind, in Internet-Nachrichten. Da über E-Mail üblicherweise nur reine Textdateien übermittelt werden können, müssen andere Dateien erst in das Textformat umgesetzt werden, bevor sie anderen Empfänger übermittelt werden. Ein E-Mail-Programm ist MIME-kompatibel, wenn es Dateianlagen mit MIME kodieren und dekodieren kann. Wird eine MIME-kodierte Nachricht versandt, so werden die Art der Kodierung und die Methode zur Dekodierung in der Nachricht angegeben. Es bestehen viele vordefinierte MIME-Typen, wie etwa "image/jpeg" und "text/plain". Es können aber auch eigene MIME-Typen definiert werden.

Der MIME-Standard wird auch durch Web-Server genutzt; sie identifizieren damit die Dateien, die sie an Web-Browser senden. Web-Browser unterstützen verschiedene MIME-Typen und können daher auch Dateien anzeigen und ausgeben, dir nicht im HTML-Format vorliegen. Die Liste der MIME-Typen und der zugehörigen Anwendungen können im Browser auch einfach aktualisiert werden; er kann dadurch auch neuen Dateiformate unterstützen.

MIME ist in den RFCs 2045-2049 beschrieben; diese Dokumente sind verfügbar unter:

http://www.rfc-editor.org/rfc/rfc2045.txt

http://www.rfc-editor.org/rfc/rfc2046.txt

http://www.rfc-editor.org/rfc/rfc2047.txt

http://www.rfc-editor.org/rfc/rfc2048.txt

http://www.rfc-editor.org/rfc/rfc2049.txt

Mirror—Ein Server (meist ein FTP-Server), der dieselben Dateien spiegelt, die auch auf einem anderen Server verfügbar sind. Daher auch die Bezeichnung als Mirror- oder Spiegel-Server. Er hat meist den Zweck, einen zweiten Speicherort zur Verfügung zu stellen, von dem die Dateien zusätzlich zum Haupt-Server abgerufen können. Der Begriff der Spiegelung bezieht sich auch auf Konfigurationen, bei denen Daten auf mehr als einen Massenspeicher gleichzeitig geschrieben werden. Dies dient der Ausfallsicherung, sodass beim Ausfall eines Massenspeichers keine wichtigen Informationen verloren gehen.

Modem—Ein Wort, das aus den Begriffen **Mo**dulator-**Dem**odulator gebildet wird. Ein Modem ist ein Gerät, das an einen Computer angeschlossen wird un den Datenaustausch mit anderen Computern über Telefonleitungen erlaubt. Der Modem setzt die Digitaldaten des Computers in analoges Format um (moduliert sie) und sendet sie dann an den anderen Modem, der die Daten wieder in Digitalformat umsetzt (demoduliert). Ein Modem ist also ein kombinierter Analog-Digital-Analog-Wandler. Die Geschwindigkeit für die Datenübermittlung wird durch die Baud-Rate (z.B. 9.600 Baud) oder in Kilobit pro Sekunde (z.B. 28,8 kbps) ausgedrückt.

MultiPOP—Ein Bestandteil des Server MDaemon, der Nachrichten über das POP3-Protokoll von verschiedenen anderen E-Mail-Servern für die Benutzer des eigenen Servers abrufen kann. Benutzer von MDaemon können damit E-Mail-Konten auf anderen E-Mail-Servern unterhalten und deren E-Mail-Nachrichten durch MDaemon abrufen und gemeinsam bereit stellen lassen. Sie erhalten so alle Nachrichten über dasselbe Postfach.

NAT—Siehe Network Address Translation.

Netzwerk—Mindestens zwei Computer, die mit einander verbunden sind. Zweck des Netzwerks ist die gemeinsame Nutzung von Ressourcen und Informationen durch verschiedene Systeme zu ermöglichen. Gängige Beispiele sind die gemeinsame Nutzung von Druckern, DVD-Laufwerken, Festplatten, Dateien usw.

Es gibt viele Arten von Netzwerken; die meist genutzten sind lokale Netzwerke und Weitverkehrsnetzwerke (LAN und WAN). In einem LAN sind die einzelnen Computer nahe beieinander angeordnet, meist im selben Gebäude. Sie werden meist auch direkt kabelgebunden verschaltet, wobei auch drahtlose Verbindungen sich immer weiter verbreiten. Die Computer in einem WAN liegen meist weit auseinander (in anderen Gebäuden oder Städten) und sind über Kommunikationsverbindungen, Telefonleitungen, Satellitenverbindungen u.ä. miteinander verbunden.

Das Internet selbst ist ebenfalls ein Netzwerk. Es wird auch als Netzwerk der Netzwerke beschrieben.

Network Address Translation—Technik zur Umsetzung von Netzwerkadressen. Sie bewirkt, dass ein Netzwerk zwei verschiedene Arten von IP-Adressen für öffentlichen und internen Verkehr nutzen kann. Meist wird dies als Firewall eingesetzt, um die Netzwerksicherheit zu erhöhen. Ein Computer hat dabei im Verkehr mit Computern außerhalb des LANs eine bestimmte öffentliche, im LAN aber eine ganz andere private Adresse. Hardware und Software an der Schnittstelle zwischen LAN und Internet steuert den Datenverkehr mithilfe dieser Adressen. Damit können mehrere Rechner eine öffentliche IP-Adresse gemeinsam nutzen. Die Adresse im LAN wird nach außen nicht bekannt, auch direkte Verbindungen von außen zu den Computern im LAN sind nur mithilfe besonderer Maßnahmen möglich.

Network News Transfer Protocol—See NNTP below.

Netwerkkarte—Eine Netzwerkkarte (englisch auch Network Interface Card oder NIC) ist eine Schaltung, die einen Rechner mit einem Netzwerk verbindet. Netzwerkkarten stellen dauernd verfügbare Verbindungen her, wohingegen Modemen nur vorübergehende Verbindungen vermitteln, etwa für Wählzugänge ins Internet. Die meisten Netzwerkkarten eignen sich nur für bestimmte Netzwerktypen und Protokolle, wie etwa Ethernet, Token Ring und TCP/IP.

NIC—Siehe Netzwerkkarte.

NNTP—Network **N**ews **T**ransfer **P**rotocol (Prokotoll für Übermittlung von Nachrichten in Netzwerken) ist das Protokoll, über das in USENET-Newsgroups Nachrichten übermittelt werden. Die meisten Browser und E-Mail-Clients verfügen auch über NNTP-Clients.

NNTP ist in RFC-977 beschrieben; das Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc977.txt

Node—Ein einzelner Computer, der mit einem Netzwerk verbunden ist.

ODMR—On-**D**emand **M**ail **R**elay ("Postrelais bei Bedarf") ist ein neues Protokoll, das E-Mail-Servern den Betrieb erleichtern soll, die nur zeitweise Verbindung zum Internet und keine feste IP-Adresse haben. Sie können damit Nachrichten ähnlich wie solche Server mit fester IP-Adresse haben, die den Befehl ETRN verwenden können. Die Nutzung des ESMTP-Befehls ETRN erfordert eine feste IP-Adresse und ist bei Systemen mit dynamischen IP-Adressen nicht möglich. Für sie steht keine allgemein verfügbare Lösung zur Verfügung. ODMR löst das Problem durch den Befehl ATRN (TURN mit Echtheitsbestätigung oder Authenticated TURN), der den Datenverkehr in der SMTP-Verbindung umkehrt (wie es auch beim älteren Befehl TURN der Fall war) und dabei zusätzliche Sicherheit bietet. Der SMTP-Server mit dynamischer IP-Adresse kann dann eine Internet-Verbindung herstellen und die Nachrichten an sich per SMTP übermitteln lassen, er muss sie nicht durch POP oder IMAP abrufen. Diese Lösung befriedigt den Bedarf an günstigen Lösungen für solche Unternehmen, die einen eigenen Mailserver brauchen, eine statische IP-Adresse aber nicht erhalten können.

ODMR ist in RFC 2645; das Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc2645.txt

OEM—Original **E**quipment **M**anufacturer ("Hersteller von Original-Ausrüstung") ist ein oft falsch verstandener und angewandter Begriff. Ein OEM ist ein Unternehmen, das die Produkte und Ausrüstung eines anderen Unternehmens unter seinen oder anderen Marken und in eigener Verpackung vertreibt. Beispielsweise ist HyperMegaGlobalCom, Inc. ein OEM, da das Unternehmen Computer-Komponenten von anderen Unternehmen einkauft, sie zu benutzerindividuellen Produkten zusammenfasst und sie dann unter der Marke "HyperMegaGlobalCom" verkauft. Der Zulieferer von HyperMegaGlobalCom kann auch ein OEM sein, falls er seinerseits von Dritten zukauft. "OEM" ist deswegen verwirrend, weil OEMs nicht die eigentlichen Original-Hersteller sind, wie es der Begriff vermuten lassen könnte. OEMs sind die Unternehmen, die Produkte lediglich umpacken, kombinieren und vertreiben. Dennoch hat es sich eingebürgert, diese Wiederverkäufer und nicht die ursprünglichen Hersteller als OEM zu bezeichnen.

On the fly—Der Begriff "on the fly" wird meist in zwei Bedeutungen verwendet. Er bezeichnet eine Tätigkeit, die "schnell" oder einfach während einer anderen Tätigkeit nebenbei erledigt werden kann. Beispielsweise kann eine Buchhaltungssoftware das Erstellen von Konten während der Eingabe der Umsatzzahlen ermöglichen. Der eigentliche Vorgang wird dabei nur kurz unterbrochen, um die andere Tätigkeit auszführen. Die andere Bedeutung ist, dass etwas automatisch oder dynamisch erzeugt werden kann und nicht fest vorgegeben ist. Informationen, die in einem Cookie gespeichert werden, können die Erstellung einer an den Benutzer angepassten Website "on the fly" veranlassen. Es muss dabei kein Profil manuell angelegt werden, sondern das Aussehen der Site ändert sich beim Besuch unmittelbar.

Original Equipment Manufacturer—Siehe OEM.

Paket—Eine Dateneinheit, die ein Computer über ein Netzwerk sendet (daher auch Datenpaket). Daten, die ein Computer aus einem LAN oder dem Internet empfängt, werden immer als Pakete übermittelt. Die ursprüngliche Datei oder Nachricht wird in diese Pakete aufgeteilt, übermittelt und beim Empfänger wieder zusammengesetzt. Jedes Paket enthält Kopfdaten (Header), die Quelle und Ziel angeben, einen Inhaltsblock und einen Kode zur Fehlerkorrektur. Es ist auch

nummeriert, sodass eingehende Pakete in der richtigen Reihenfolge zusammengesetzt werden können. Die Übermittlung von Paketen wird auch als "Paketvermittlung" bezeichnet. Pakete werden auch als "Datagramme" bezeichnet.

Paketvermittlung—Der Vorgang der Übermittlung von Paketen über das Internet. Anders als bei der Leitungsvermittlung (wie etwa bei analogen Telefonleitungen), bei denen die Daten als kontinuierlicher Datenstrom über denselben Pfad oder Verbindungweg gesendet werden, werden paketvermittelte Daten in Pakete unterteilt, die nicht über dieselbe Route ans Ziel gelangen müssen. Da die Daten aufgeteilt sind, können mehrere Benutzer Daten gleichzeitig über denselben Verbindungsweg senden.

Parameter—Ein Parameter ist ein Wert oder eine Eigenschaft. Im Computer-Jargon ist es jeder Wert, den der Benutzer oder ein anderes Programm an ein Programm übergeben. Name und Kennwort, Einstellungen, Schriftgröße usw. sind Parameter. In der Programmierung ist ein Parameter ein Wert, der an eine Subroutine oder Funktion zur Verarbeitung übergeben wird.

PDF—Abkürzung für **P**ortable **D**ocument **F**ormat, ein stark komprimiertes plattformübergreifendes Dateiformat, das Adobe Systems Incorporated entwickelt hat. Es erfasst Formatierung, Text und Inhalt von Dokumenten aus verschiedenen Anwendungen. Ein Dokument kann damit auf verschiedenen Computern und Plattformen immer gleich aussehen und ausgedruckt werden (was bei vielen Textverarbeitungen nicht möglich ist). Zum Betrachten von PDFs ist der Adobe Reader nötig, eine kostenlose Anwendung von Adobe Systems. Es wird auch ein Plugin für die Anzeige von PDFs im Browser angeboten. PDFs von Websites können damit direkt betrachtet und müssen nicht erst heruntergeladen und dann in einem gesonderten Programm geöffnet werden.

Parsen—In der Linguistik ist Parsen das Zerlegen einer Sprache in ihre grammatikalischen Bestandteile, die dann analysiert werden; so kann ein Satz in Verben, Adjektive, Substantive usw. zerlegt werden.

In der Informatik ist Parsen das Aufteilen einer Computersprache in Einzelteile, die dann für den für den Computer nutzbar werden. Ein Parser in einem Compiler nimmt jedes Statement, das ein Entwickler geschrieben hat, und teilt es in Bestandteile auf, die dann zur Ausführung weiterer Aktionen und zur Erstellung von Instruktionen genutzt werden, aus denen ein ausführbares Programm entsteht.

Der Server MDaemon und andere Produkte parsen oft E-Mail-Nachrichten, um ihre Empfänger zu bestimmen oder sie mithilfe von Filtern und anderen Werkzeugen bearbeiten zu lassen.

Ping—Akronym für **P**acket **In**ternet **G**roper. Ein einfaches Internet-Programm, das feststellt, ob eine bestimmte IP-Adresse erreichbar ist und auf Anforderungen reagiert. Dazu wird eine Echo-Anforderung im Format des Steuerprotokolls Internet Control Message Protocol (ICMP) an die Gegenstelle gesendet und auf Antwort gewartet. "Ping" wird oft auch als Verb "pingen" eingesetzt, so kann etwa ein Benutzer einen Server pingen. Das Pingen einer IP-Adresse erfoglt durch die Eingabe des Befehls "ping" mit der IP-Adresse oder Domäne als Parameter auf der Befehlszeile. Ein Beispiel: "Ping 192.0.2.0."

ICMP ist in RFC-792, das Echo-Protokoll ist in RFC-862 beschrieben; diese Dokumente sind verfügbar unter

http://www.rfc-editor.org/rfc/rfc792.txt

http://www.rfc-editor.org/rfc/rfc862.txt

POP—Abkürzung für **P**ost **O**ffice **P**rotocol (Postfach-Protokoll). POP wird auch als POP3 bezeichnet und ist das am weitesten verbreitete Protokoll zum Abruf von Nachrichten von einem Mailserver. Die meisten Mailclients nutzen das POP-Protokoll, wobei viele auch das neuere IMAP-Protokoll unterstützen. POP2 wurde Mitte der 1980-erjahre zum Standard und brauchte SMTP zum Nachrichtenversand. Es wurde durch die neuere Version POP3 ersetzt, die auch ohne SMTP funktioniert.

POP3 ist in RFC-1939 beschrieben; das Dokument ist hier verfügbar:

http://www.rfc-editor.org/rfc/rfc1939.txt

Port—In Netzwerken mit TCP/IP- und UDP-Verkehr, wie auch im Internet, ist der Port der Endpunkt einer logischen Verbindung und wird durch eine Zahl von 0 bis 65535 gekennzeichnet. Die Ports von 0 bis 1024 sind für bestimmte wichtige Protokolle und Dienste reserviert. Web-Server laufen meist auf Port 80, SMTP-Server auf Port 25 und POP-Server senden und empfangen Nachrichten auf Port 110. Nur ein Programm kann einen Port zur selben Zeit nutzen oder sich "an ihn binden". Beim Browsen im Internet laufen Server oft auf besonderen Ports, deren Nummer der Benutzer durch Doppelpunkt getrennt an den Domänennamen anhängen muss, etwa "www.example.com:3000".

Ports sist auch die Bezeichnung für die Anschlüsse für Peripheriegeräte an Computern, etwa serielle Ports, Parallel-Ports, USB-Ports usw.

Port wird auch im Sinne von Portierung gebraucht; Portierung ist die Übertragung eines Programms von der Plattform, für die es entwickelt wurde, auf eine andere Plattform. Windows-Anwendungen könnten beispielsweise nach UNIX portiert werden. Die übertragene Anwendung wird gelegentlich als "Port" bezeichnet.

Postfach—Ein Bereich im Hauptspeicher oder auf einem Massenspeicher, der einer bestimmten E-Mail-Adresse für die Ablage ihrer Nachrichten zugewiesen ist. In jedem E-Mail-System hat ein Benutzer ein privates Postfach, in dem die für ihn bestimmten Nachrichten nach Empfang abgelegt werden. Der Postfachname bezeichnet den Teil der E-Mail-Adresse rechts vom Zeichen @, etwa "user01" bei "user01@example.com"; hierbei ist Frank der Name des Postfachs und "example.com" der Name der Domäne.

PPP—Bezeichnet das Point-to-Point-Protokoll, den Internet-Standard für Wählverbindungen. PPP ist ein Regelsatz, der bestimmt, wie über eine Modemverbindung Datenpakete mit anderen Systemen im Internet ausgetauscht werden.

PPP ist in RFC-1661 beschrieben; das Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc1661.txt

Protokoll—Im Computer-Jargon sind Protokolle Richtlinien und Standards, nach denen Server und Anwendungen kommunizieren. Es bestehen zahlreiche Protokolle für verschiedenste Anwendungen, etwa TCP/IP, SLIP, HTTP, POP3, SMTP, IMAP, FTP usw.

RAS—Remote Access Services, siehe DFÜ-Netzwerk.

Registrierung—Sprachlich richtig eigentlich "Registratur"; eine Datenbank von Microsoft Windows, in der Konfigurationsdaten über die auf dem Computer installierte Software erfasst sind. Sie umfasst Benutzereinstellungen, Zuordnungen von Dateierweiterungen, Bildschirmhintergründe, Farbschemata und vieles mehr. Sie ist in folgende sechs Teile untergliedert:

HKEY_User—Speichert Benutzerdaten für alle Benutzer des Systems.

HKEY_Current_User—Einstellungen für den gerade angemeldeten Benutzer.

HKEY_Current_Configuration—Speichert Einstellungen für Anzeige und Drucker.

HKEY_Classes_Root—Dateizuordnungen und OLE-Daten.

HKEY_Local_Machine—Einstellungen zu Hardware, Betriebssystem und installierten Anwendungen.

HKEY_Dyn_Data—Leistungsdaten.

Während der Installation von Programmen schreibt die Installationsroutine meist Informationen in die Registratur. Die Registratur kann mithilfe von "regedit.exe" auch von Hand bearbeitet werden; das Programm gehört zu Windows. Bei der Bearbeitung muss aber vorsichtig vorgegangen werden, da eine fehlerhafte Bearbeitung zu schwer wiegenden Funktionsstörungen und Ausfällen führen kann.

RFC—Abkürzung für **R**equest **F**or **C**omments ("Aufforderung zur Abgabe von Kommentaren") ist der Name der Vorgehensweise, einen Standard im Internet zu definieren. Der Begriff bezeichnet gleichzeitig das Ergebnis, in das der Prozess mündet. Jeder neue Standard und jedes neue Protokoll werden im Internet als RFC veröffentlicht. Die Internet Engineering Task Force (IETF) moderiert die Diskussionen, bis der neue Standard schließlich verabschiedet wird. Kommentare sind für verabschiedete Standards zwar nicht mehr verlangt, doch behält das Ergebnis den Titel RFC bei, er wird durch die laufende Nummer ergänzt. Beispielsweise ist RFC-822 (jetzt ersetzt durch RFC-2822) ein offizieller Standard oder "RFC" für E-Mail. Protokolle, die offiziell als Standard-Protokolle verabschiedet werden, tragen zusätzlich eine Standardnummer, unter der sie im Dokument Internet Official Protocol Standards ("Offizielle Internet-Protokoll-Standards") aufgeführt sind (dieses trägt die Bezeichnungen STD-1 und derzeit RFC-3700). Die RFCs stehen im Internet an vielen Stellen zur Verfügung, nur der RFC-Editor ist aber eine "amtliche" Quelle. Er ist erreichbar unter http://www.rfc-editor.org/.

Das Dokument Internet Official Protocol Standards ist verfügbar unter:

http://www.rfc-editor.org/rfc/std/std1.txt

RTF—Rich **T**ext **F**ormat ("Ausgestaltetes Textformat") ist ein universelles, durch Microsoft entwickeltes Dateiformat für fast alle Textverarbeitungen. Anders als reine Textformate kann RTF Formatierungen, Informationen über Schriftarten, Schriftfarben und anderes enthalten. Die Dateigröße von RTF-Dateien kann, verglichen mit anderen Dokumentenformaten wie Microsoft Word (*.doc und *.docx) und Adobe PDF, sehr groß sein.

Server—Ein Computer oder Programm, das einen bestimmten Service für Clients auf anderen Computern zur Verfügung stellt. Der Begriff kann sich auf Software, etwa einen SMTP-Server, oder den Computer beziehen, auf dem die Software ausgeführt wird. Ein einzelner Server-Rechner kann verschiedene Serverdienste ausführen. Der Server im Netzwerk kann beispielsweise Web-Server, E-Mail-Server und Fax-Server gleichzeitig sein.

SMTP—Abkürzung für **S**imple **M**ail **T**ransfer **P**rotocol ("einfaches Protokoll zur Übermittlung von Nachrichten"). Dies ist das meist genutzte Protokoll für den Versand von Nachrichten von Servern im Internet untereinander oder von Clients an Server. SMTP besteht aus Regeln, nach denen Programme bei Empfang und Versand von Nachrichten zusammenarbeiten, Sobald eine Nachricht über SMTP bei einem Server eingegangen ist, wird sie üblicherweise dort gespeichert und kann dann durch den Client über POP, IMAP und andere Protokolle abgerufen werden.

Das Protokoll SMTP ist in RFC-2821 beschrieben; das Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc2821.txt

Spam—Unerwünschte ("Junk") Nachrichten im Internet. Spam bezeichnet meist unverlangte kommerzielle Nachrichten, manchmal auch überhaupt alle unerwünschten Nachrichten. Ein Spammer erlangt Millionen von E-Mail-Adressen aus verschiedenen Quellen und sendet an diese dann Spam oder Werbenachrichten. Spam kann sich auch auch Newsgroups und Diskussionsgruppen beziehen und dort die unerwünschte Veröffentlichung von Werbe-und sonstigen Nachrichten bezeichnen.

Spam wird im Internet schnell zu einem immer ernster zu nehmenden Problem, da viel Zeit und Serverressourcen auf seine Bearbeitung verwendet werden. Spammer versuchen manchmal, den Ursprung der Nachrichten zu verschleiern, etwa durch gefälschte Adressen oder durch den Versand der Nachrichten über verschiedene Server. Die Abwehr von Spam gestaltet sich daher schwierig. MDaemon enthält mehrere Funktionen zur Abwehr von Spam, etwa Sperrlisten für DNS (DNS-BL), IP-Abschirmung, IP-Filter, Relaiskontrolle und viele mehr.

Der Ursprung des Begriffs "Spam" als Bezeichnung für unerwünschte Nachrichten ist umstritten, allerdings wird weithin akzeptiert, dass der Begriff aus einem Sketch der Gruppe Monty Python stammt, in dem das Word "Spam" immer weiter wiederholt wurde. Es kann sich aber auch um eine abwertende Bezugnahme auf das Produkt gleichen Namens aus dem Hause Hormel handeln.

TCP/IP—Transmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol wird meist als Grundlage des Internet angesehen. Es ist ein Satz grundlegender Kommunikationsprotokolle, mit deren Hilfe Hosts im Internet kommunizieren können. Es ist auch das meist verwendete Protokoll in LANs. Es besteht aus zwei Schichten. Die oberste Schicht TCP verwaltet die Zerlegung und Zusammensetzung der Dateien in Datenpakete zur Übermittlung über das Netzwerk. IP, die untere Schicht, bearbeitet die Adressierung der Pakete, sodass sie ihre Ziele erreichen. TCP ist in RFC-793, IP in RFC-791 beschrieben. Diese Dokumente sind verfügbar unter:

TCP - http://www.rfc-editor.org/rfc/rfc793.txt

IP - http://www.rfc-editor.org/rfc/rfc791.txt

Telnet—Ein Befehl und ein Programm für den Verbindungsaufbau mit Gegenstellen im Internet, die den Zugriff über Telnet gestatten. Der Befehl Telnet stellt die Verbindung her und zeigt die Anmeldeaufforderung des Servers. Falls ein Benutzerkonto auf dem Server besteht, kann der Benutzer die für ihn freigegebenen Ressourcen, wie Dateien, E-Mail usw. einsehen. Telnet hat den Nachteil, dass es ein Befehlszeilenprogramm ist, das UNIX-Befehle nutzt.

Das Protokoll TELNET ist in den RFCs 854-855 beschrieben; diese Dokumente sind verfügbar unter:

http://www.rfc-editor.org/rfc/rfc854.txt

http://www.rfc-editor.org/rfc/rfc855.txt

Terminal—Ein Gerät, mit dessen Hilfe Befehle an einen entfernten Computer übermittelt werden können. Ein Terminal besteht aus Tastatur, Bildschirm und einfachen Schaltungen. Meistens werden Personal Computer verwendet, um Terminals zu simulieren.

Tiff—Abkürzung für **T**agged **I**mage **F**ile **F**ormat. Dies ist ein universelles Grafikformat für die Nutzung auf mehreren Plattformen. TIFF kann Farbtiefen zwischen 1- und 24-Bit verarbeiten.

Treiber—Ein kleines Programm, das mit einem bestimmten Gerät kommuniziert. Treiber enthalten die Informationen, die der Computer und andere Programme benötigen, um das Gerät anzusprechen, zu steuern und zu erkennen. Bei Windows-Rechnern sind Treiber oft in dynamische Verbindungsbibliotheken (englisch Dynamic Link Libraries, DLL) gefasst. Bei Mac-Systemen brauchen die meisten Geräte keine Treiber; ist aber ein Treiber nötig, so wird er meist als System-Erweiterung bereit gestellt.

UDP—User **D**atagram **P**rotocol ist eines der Protokolle, die gemeinsam den TCP/IP-Protokollstapel ergeben. UDP wird als zustandsloses Protokoll bezeichnet, da es den Empfang von Datenpaketen nicht bestätigt.

UDP ist in RFC-768 beschrieben; das Dokument ist verfügbar unter:

http://www.rfc-editor.org/rfc/rfc768.txt

Unix—Unix, auch UNIX, ist ein Betriebssystem, das in den 1960-erjahren in den Bell Labs entstand. Es wurde für Mehrnutzerbetrieb konzipiert und ist das beliebteste Betriebssystem für Server im Internet. Es stehen viele Betriebssysteme auf Grundlage von UNIX zur Verfügung, wie etwa Linux, GNU, Ultrix, XENIX und andere.

URL—Jeder Datei und jedem Server im Internet ist ein Ressourcenbezeichner, der sog. **U**niform **R**esource **L**ocator (URL), zugewiesen. Dies ist die Adresse, die der Benutzer in den Browser eingibt, um eine bestimmte Adresse aufzusuchen oder eine Datei zu erhalten. URLs dürfen keine Leerzeichen enthalten und enthalten nur vorwärtsgerichtete Schrägstriche. Sie sind in zwei Teile gegliedert, die durch "://" getrennt sind. Der erste Teil legt das Protokoll oder die Ressource für den zugriff fest (z.B. http, telnet, ftp usw.), der zweite Teil ist die eigentliche Adresse der Datei oder des Servers (z.B. www.altn.com oder 127.0.0.1).

Uuencode—Eine Reihe von Algorithmen für die Umsetzung von Dateien in 7-Bit-ASCII-Zeichen für die Übermittlung über das Internet. Es wurde als Unix-to-Unix-Encode standardisiert, ist aber nicht mehr nur auf UNIX-Rechner beschränkt. Es wird als häufig eingesetzte Methode zur Dateiübermittlung zwischen unterschiedlichen Plattformen auch für die Übermittlung E-Mail-Nachrichten genutzt.

Verschlüsselung—Sicherheitsmaßnahme, durch die Informationen in einer Datei kodiert oder geschleiert werden, sodass die Informationen erst nach Entschlüsselung oder Dekodierung lesbar werden. E-Mail wird häufig verschlüsselt, damit ein Dritter, der die Kommunikation abfängt oder mitschneidet, ihren Inhalt nicht lesen kann. Die Nachricht wird beim Versand verschlüsselt und nach Erreichen des Empfängers entschlüsselt.

WAN—Abkürzung für **W**ide **A**rea **N**etwork (Weitverkehrsnetzwerk). Es arbeitet ähnlich wie ein LAN, erstreckt sich aber über mehrere Gebäude oder sogar Städte. WANs setzen sich manchmal aus kleineren LANs zusammen, die verbunden sind. Das Internet kann als das größte WAN der Welt gelten.

Zip—Bezeichnet eine komprimierte oder "gezippte" Datei, meist mit der Dateiendung ZIP. Das "Zippen" von Dateien ist das Komprimieren mindestens einer Datei in eine Archivdatei, um Speicherplatz zu sparen und die Übertragung an einen anderen Computer zu beschleunigen. Die Dateien aus einem ZIP-Archiv müssen vor der Nutzung erst mithilfe des entsprechenden Programms, beispielsweise PKZip oder WinZip, entpackt werden. Im Internet stehen zahlreiche kostenlose und kostenpflichtige Archivprogramme bereit, die diesen Standard unterstützen.

Zugriffsliste—Siehe ACL.

Index

- 2 -

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- J -

- K -

- L -

- M -

- N -

- O -

- P -

- Q -

- R -

- S -

- T -

- U -

- V -

- W -

- X -

- Z -