用户手册

23.0

MDaemon 电子邮件服务器
用户手册

v23.0.2 - 六月 2023

目录

章节 IV 安全菜单 425

章节

1 MDaemon Messaging Server 23.0

介绍

MDaemon Technologies 的 MDaemon Messaging Server 是一个基于 SMTP/POP3/IMAP 标准的邮件服务器，支持 Windows 7、Server 2008 R2 或更高版本，并提供一套完整的邮件服务器功能。MDaemon 定位于管理任何个人用户的邮件需求，包括一套强大的集成工具，以便于管理账户和邮件格式。MDaemon 提供了一套可扩展的 SMTP、POP3、和 IMAP4 邮件服务器（其中包括 LDAP 与活动目录支持），一套集成的基于浏览器的邮件客户端，内容过滤器、垃圾邮件过滤器、丰富的安全功能等等。

MDaemon 功能

除 SMTP、POP 和 IMAP 邮件处理之外，MDaemon 还具备其他许多功能。以下仅列出一些功能。

- 作为您 MDaemon 或 MDaemon Private Cloud 许可证的插件，可以提供对病毒扫描和防护的全面支持。这提供对于实时爆发保护[535]和 MDaemon AntiVirus[558]的访问。在到达指定收件人之前，通过检测，邮件中的病毒可以被自动清除或者删除掉。此外，您可以配置 MDaemon 发送有关感染邮件的信息给管理员、发件人和收件人以提醒他们注意病毒。
- MDaemon 提供一套完整的邮件列表或邮件组管理功能，帮助您构成数量无限、一目了然的分发列表，其中可以包含本地和/或远程成员。可以设置这些列表允许或拒绝订阅请求、成为公共列表或私人列表，发表回复给列表中的每个人或邮件作者，以摘要格式发送，还可配置使用其他大量功能。
- Webmail[266]是一套 MDaemon 的集成组件。该功能使您的用户可以选用他们自己喜欢的网络浏览器而不是工作站中的独立邮件客户端来访问他们的邮箱。这款工具对于那些没有专用电脑的移动人员和用户来说，是一个接收邮件的完美解决方案。
- MDaemon Webmail具有一套完整的邮件客户端功能。您可以：收发邮件、邮件拼写检查、在多个个人文件夹中管理您的邮件，可以从 18 种语言中任选一种来显示界面，通过组日历和日程表功能来安排会议和约会，管理您的 MDaemon 账户设置（结合 Remote Administration[293]使用时），管理联系人等等。Webmail也配备了 MDaemon Instant Messenger (MDIM)[267]这款小工具，可以下载并安装到用户的本地机器上。它可以帮助您轻松访问邮件和文件夹查收新的邮件，而无需打开网页浏览器。它还包含完整的即时通信系统，能够与其他使用 MDIM 或 XMPP[312]客户端的 MDaemon 用户进行快速“交谈”。

- MDaemon 拥有大量功能帮助您确保账户的安全。垃圾邮件过滤器和 DNS 阻止列表功能帮助您终止那些 "垃圾邮件发送者"企图间接或直接发送到您域中的 "垃圾邮件"。IP 和主机屏蔽和地址 阻止列表提供了筛选和阻止某些地址和域的连接，或通过您的系统发送邮件的功能。上述功能帮助您在屏蔽所有其他 IP 的同时，允许连接特定 IP 。
- 配置了对轻量级目录访问协议(LDAP)的支持，MDaemon 能使您的 LDAP 服务器保持和它的账户用户同步。您可以用它来保持一个 LDAP 地址薄更新，以使得支持 LDAP 的邮件客户端的用户能够进行访问。您还可以选择使用活动目录或您的 LDAP 服务器作为 MDaemon 账户数据库替代 ODBC 访问数据库或者本地的 USERLIST.DAT 系统。这样，您就可以配置多个处于不同位置的 MDaemon 共享相同的账户数据库。
- MDaemon 丰富的解析功能帮助您仅使用一个拨号 POP3 邮箱即可获得整个局域网的邮件服务。此外，为整个网络提供电子邮件的服务费用仅为常规相关费用的一小部分。
- 地址别名可以将发往 "虚构"邮箱的电子邮件路由到一个有效的账户或者邮件列表。帮助个人账户与列表在一个或多个域里拥有多个邮件地址。
- 域网关功能为您本地网络或位于因特网其他位置的各种不同部门或小组提供设置独立域的选项。利用这些功能，发往此域 (由 MDaemon 作为网关)的所有邮件都将被 MDaemon 置于该域的邮箱。之后，域内的 MDaemon 服务器或邮件客户端会将这些邮件收集和分发给域内的用户。还可以使用该功能将 MDaemon 作为其他域的备份邮件服务器。
- 基于 web 的集成式远程管理 MDaemon 的 Remote Administration 293 组件与 MDaemon 和 Webmail集成，使得您的用户可以通过他们的 web 浏览器查看和编辑他们的账户设置。您能够指定您的用户可以编辑哪些设置，也可以基于每个账户分配访问许可。Remote Administration 还可以被管理员 (以及任何您允许的用户）用来查看或编辑任何 MDaemon 的设置以及任何您通过 Remote Administration 系统设置成允许被访问的文件。
- 一套内部邮件传输系统——RAW 邮件，提供一种简单方法将邮件置于邮件流中，极大简化了自定义邮件软件的开发。利用 RAW ，可将完整的邮件系统设计成使用简单的文本编辑器和若干批处理文件。
- 无所不能的内容过滤系统使得您基于来件和发件内容的自定义服务器行为成为可能。您可以插入与删除邮件报头、为邮件添加页脚、删除附件、路由副本到其他用户、向某人发送即时消息、运行其他程序等等。

MDaemon Private Cloud

MDaemon Private Cloud (MDPC) 是专门为经销商和 IT 服务供应商开发的特别版 MDaemon Messaging Server，他们希望使用 MDaemon 软件向其客户提供托管电子邮件服务。不像 MDaemon 是为内部部署使用而出售的，MDPC 建立在专门用于托管环境的新授权和代码基础之上。MDaemon Private Cloud 包含所有 MDaemon 功能及以下额外功能：

- 新的授权和收费 (每用户/每月）
- Outlook 支持
- 改进的多域控制
- 按域贴牌 (白标）
- 按域报告

- 不可计费的用户测试账户（总收费计数中不包括该计数）
- 爆发保护、MDaemon Antivirus 和 ClamAV 反病毒引擎（另外收费，可选）
- ActiveSync for MDaemon（另外收费，可选）

系统要求

有关 MDaemon 系统要求和建议的最新信息，请访问 系统要求页面，它位于 mdaemon.com。

商标

还请参阅：

MDaemon 新功能 23.0 16
升级到 MDaemon 23.0.2 50
MDaemon 的主界面 58
获得帮助 54

1.3 MDaemon 新功能 23.0

变更和新功能

MDaemon 服务器

- （23.0.2）在“设置 | 服务器设置 | MultiPOP 118”中新增一个选项，用于在检查 MultiPOP 账户时发生多次失败后发送通知电子邮件。由于临时失败并不少见，因此提供一个选项，用来选择需要多少个连续失败才触发通知。还有一个选项可以选择在通知之间等待多少天，以避免发送太多通知。可以通过编辑 \MDaemon\App\MPOPFailureNotice.dat 自定义通知电子邮件的内容和收件人。默认情况下，在 5 次失败后，将通知发送给 MultiPOP 账户持有者，每 7 天不超过一次
- 新的 MultiPOP 118 屏幕位于“服务器设置”屏幕。您可以从此页面启用/禁用 MDaemon 的 MultiPOP 服务器，并使用“*MultiPOP always deletes mail...*”选项（以前位于 MultiPOP 收集 320 页面）来为所有用户覆盖“*在 POP 服务器上保留一份邮件副本* 620”这个选项。新页面还包含 OAuth 2.0 支持选项，用于从 Gmail 和 Office 365 收集 MultiPOP 邮件。

  MultiPOP OAuth 2.0 支持用于从 Gmail 和 Office 365 收集邮件 119 — OAuth 2.0 是现代身份验证，上述服务现在需要这些身份验证，因为它们禁用了对传统/基本身份验证的支持。为了让 MDaemon 的 MultiPOP 功能使用 OAuth2.0 来代表用户从 Gmail 或 Office365 收集邮件，您必须分别向 Google 或 Microsoft 注册 MDaemon 服务器，使用 Google API 控制台或 Microsoft 的 Azure Active Directory 来创建 OAuth2.0 应用程序。这与为您的 Webmail 用户使用 MDaemon 的 Dropbox

集成[282]所需的流程类似。还请参阅 MultiPOP[119] 帮助主题来获得有关配置 OAuth 2.0 支持的更多信息。

- MDaemon 的 IMAP 服务器现在支持关键字旗标。这允许电子邮件客户端（例如 Mozilla Thunderbird）在服务器上存储“邮件标签”，这使您可以在客户端的一个实例中看到在客户端的另一个实例中设置的标签。
- 在打开大型邮件文件夹时，已改进 IMAP 服务器的性能。

安全

- (23.0.2) 在“安全 | 垃圾邮件过滤器”中新增 Spamhaus 数据查询服务（DQS）支持。请访问 https://info.spamhaus.com/getting-started-with-dqs 来了解有关 Spamhaus DQS 的更多信息
- 有一个新的“阻止登录策略违规”选项，它位于动态屏蔽[510]，如果您希望阻止不使用完整邮件地址就试图登录的任何 IP 地址，请使用此项。默认情况下，禁用该选项。还请参阅系统[414]页面来获取相应选项的更多信息，“服务器需要完整的邮件地址来进行验证”。
- 已添加“仅适用于有效账户”选项来扩展“忽略使用相同密码的身份验证尝试”这个选项，它位于验证失败跟踪[513]页面。如果您只希望在尝试登录有效账户时，忽略重复的密码身份验证尝试，请激活此选项。这就意味着，例如，如果用户在一个客户端中更新了密码，但另一个客户端仍使用旧密码运行，则仍将忽略该旧客户端的登录尝试，因为它将具有正确的登录名。尝试使用类似的密码和随机登录名称的机器人不会有同样的好处，并且一旦超过验证失败阈值就会被阻止。这有助于更快地击溃机器人。也已更新 XML API 动态屏蔽操作，以反映这些新功能。
- 已将“内容过滤器 » 附件[550]”选项添加至：*"在删除附件时在邮件正文顶部添加警告"*。在 MDaemon 从邮件中删除附件时，例如因为检测到病毒而将其删除，它会在邮件正文的顶部添加一条警告消息。如果您希望审核或修改该邮件的模板，请点击“警告”按钮。默认情况下启用此项。
- 已将此项添加至*从 AntiVirus 扫描排除可信 IP*[558]。
- 在 SSL 证书[479]被配置成供 MDaemon[481]、Webmail[483] 或 Remote Administration[487] 使用，并快要过期时，MDaemon 将向管理员发送警告邮件。
- MTA-STS[493] 现在有一个豁免列表，因此可以免除存在问题的域，而不是在在故障影响可投递性时需要关闭 MTAST。
- 已将 ClamAV AntiVirus 组件更新成 0.105.1 版本。

Webmail

- Google Drive 集成[284] — 现在可将 Webmail 链接到用户的 Google 账户，允许他们将邮件附件直接保存到其 Google Drive，并编辑和处理存储在那里的文档。要实现这一点，需要 **API Key**、**Client ID** 和 **Client Secret**。所有这些都是直接从 Google 获得的，方法是使用 Google API Console 创建一个应用程序，并在他们的服务中注册你的 MDaemon。OAuth2.0 验证组件是此应用程序的一部分，它允许您的 Webmail 用户登录 Webmail，然后通过 MDaemon 授权访问其 Google Drive 账户。一旦授权，用户可以查看他们在 Google Drive 中的文件夹和文件。此外，他们还能上传、下载、移动、复制、重命名和删除文件，以及将文件复制/移动到本地文档文件夹。如果用户想要编辑文档，点击在 Google Drive 中查看文件的选项将允许用户根据其在 Google Drive 中设置的权限对其进行编辑。Google Drive 的设置过程与

MDaemon 的 Dropbox 集成[282]和 MultiPOP OAuth 集成[118]功能类似。还请参阅 Google Drive 集成[284]来获取更多信息。

- 在除了 Lite 以外的所有主题中新增一个选项来 *"启用拖放式移动文件夹"*。这个新选项位于 Webmail 的 "文件夹"页面上的 "选项"菜单下 默认情况下启用此项。
- 通过 HTTPS 确保会话 cookie 的安全。
- 现在向 MDaemon 发送类别变更通知。
- WorldClient 不在启动时修改 robots.txt 文件。
- 内置的 web 服务器防止从 HTML 目录下载 .dll 文件。
- 为新密码输入新增长度最大值，以便显示未满足 "最多 15 个字符"的要求。
- 新增对于没有完整邮件地址的登录尝试进行报告的功能，以便支持新的阻止登录策略违规[510]这个 "动态屏蔽"选项。
- (23.0.2) 使用橙色的亮显来使 "取消延迟"选项在视觉上更明显。

Pro 主题

- 新增已读回执支持。
- 新增一个选项来禁用 HTML 编辑器上下文菜单。
- 新增调整文件夹列表大小的功能。

Remote Administration (MDRA)

23.0.2

- 新增一个勾选框来 "从 AntiVirus[558]扫描排除可信 IP"
- 在 SMTP[438]端口设置上新增 "不允许验证"选项
- 在 "设置 | 公共文件夹 | 公共文件夹管理器[258] | 编辑"中为 "ActiveSync 显示名称"新增一个选项
- 为用户列表[596]新增 4 个过滤器选项。分别是仅管理员、仅非管理员、仅全局管理员和仅域管理员
- 已在 "垃圾邮件过滤器[564]"中新增 DQS 页面 | 数据查询服务。请访问 https://info.spamhaus.com/getting-started-with-dqs 来了解有关 Spamhaus DQS 的更多信息

23.0.0

- 在 "域管理器"中，现在 Webmail设置[289]中有一个 *"允许用户通过邮件来接收双重验证的验证码"*这个选项，这样用户便能通过邮件地址接收其验证码，而不是使用 Google Authenticator 应用程序。默认情况下启用此项。
- 更改了将新 ACL 条目添加到 "查找和读取"时的默认权限。
- "测试"按钮位于：垃圾邮件过滤器 » DNS-BL » 主机[587]和设置 » 活动目录 » 验证[692]，在进程正在进行时被禁用。
- 内置的 web 服务器防止从 "模板"目录下载 .dll 文件。

- 用户现在可以通过点击在窗口右上角的用户名（例如 frank.thomas），自定义 Remote Administration 的 web 界面的外观。提供选项，允许用户将界面切换到暗模式，设置字体大小和选择首选语言。
- 已将账户删除确认更改成使用自定义的确认功能。
- 为不使用完整邮件地址的登录尝试新增“动态屏蔽”报告。

ActiveSync

- 新增一个客户端设置选项，*在将邮件移入垃圾邮件文件夹时阻止发件人*[353]。启用后，当客户端将电子邮件移动到账户的垃圾邮件文件夹时，该服务将该电子邮件的发件人或从地址添加到阻止的发件人联系人文件夹。
- 现在您可以为 ActiveSync 客户端禁用完全擦除按钮[388]因此，如果不首先禁用新的不允许出厂重置擦除[353]选项，则无法在 ActiveSync 设备上执行远程完全擦除。
- 优化了正文首选项数据，由此来使故障诊断更容易。
- 在客户端同步大型邮箱时已改进关机性能。
- 新增为邮箱和公共文件夹自定义显示名称的功能。
- 已改进关机的性能。
- ActiveSync 客户端现在可以发送到“联系人”文件夹中的“个人分发列表”。
- 已更改客户端设置对话框的布局来为新设置增添空间。

其他

- (23.0.2) 内容过滤器 - $LIST_ATTACHMENTS_REMOVED$[553] 可以用于规则操作（例如“发送便笺”和“添加警告...”）
- 在 MDaemon GUI 中，更改了将新 ACL 条目添加到“查找和读取”时的默认权限。
- 在 MDaemon GUI 中，如果您尝试将 Webmail、Remote Administration 或 XMPP BOSH 服务器端口设置为具有冲突的值，则添加了一个警告弹出窗口。
- XML API - 新增“编辑器”操作，可用于编辑 MDaemon 的各种 INI 文件
- 已更改几个插件，允许较新版本的运行，以便客户可以测试可能的修补程序/修补程序版本。

MDaemon Server 发布说明

要了解 MDaemon 23.0.2 中有关新增功能、变更和修复的完整说明，请参阅 RelNotes.html（位于 MDaemon 的\Docs\子文件夹）。

MDaemon 22.0 的新功能

变更和新功能

Webmail

Pro 主题

- 在查看邮件时，您可以将鼠标悬停在发件人的姓名上以打开一个弹出窗口，其中包含用于将发件人添加到您的 "联系人"和 "已允许"或 "已阻止发件人"文件夹的选项。
- 编写、邮件、事件、联系人、任务和便笺视图现在可以在新窗口中打开。
- 您现在可以从邮件预览窗格和邮件视图打开下一封未读的邮件。
- 在多行模式中，已将邮件片段添加到邮件列表中。
- 现在您可以为 Pro 主题用户提供 *"编辑别名显示名称"*选项，它位于 "设置 » 编写"。这允许用户编辑与其账户相关联的任何别名的显示名称。如果您希望允许上述操作，请使用新的 *"允许用户编辑其别名显示名称"*这个 Webmail设置 289。**请注意：**此项仅在 MDaemon Remote Administration (MDRA) 293 的 web 界面中可用。
- 过去被译为 "白名单"或 "黑名单"发件人的选项和链接现在被描述为 "允许"或 "阻止"发件人。此外，白名单和黑名单文件夹现在称为 "已允许发件人"和 "已阻止发件人"。
- 可以按旗标列排序邮件列表。
- 在 "任务"列表中，将以红色显示逾期任务。
- 已将 XMPP 客户端升级到 4.4.0 版本。

其他

- 当需要强密码时，现在有一个密码要求列表，在用户满足要求时显示为绿色，并勾选已满足哪些要求。此外，还添加了更多描述性错误消息，说明在提交时密码无效的问题。
- 编写选项现在包含选项来选择默认的 "发件人："地址，在编写、答复或转发邮件时将需要该地址。
- 已将 "1 分钟"设置添加到 "列表刷新时间"选项，该选项位于选项 » 个性化页面。
- 新增对于 Webmail登录页面上 CSRFTokens 的支持。在启用 *"使用跨站请求伪造令牌"*选项(位于 Webmail设置 » Web 服务器 270页面)时，启用该选项。如果您使用 Webmail的自定义模板，请在登录表单中添加隐藏输入，如下所示：<input type="hidden" name="LOGINTOKEN" value=<$LOGINTOKEN$> />
- 公共日历 - 已修改列表视图以开始停留在当前天，并显示接下来的 30 天。
- 已为邮件视图中的超链接添加自动的 URL 转换。
- 无论安装哪种语言的 MDaemon，默认文件夹的名称 (草稿、已发送邮件等)都会被翻译成 Webmail用户的语言 (以前只有英文版 MDaemon 会这样做)。
- 现在提供一个新选项，用来将双重验证的验证码发送至次要的邮件地址。
- LookOut 和 WorldClient 主题 - 已更改所有列表类别显示行为来进行匹配。

- 现在，“已允许发件人”和“已阻止发件人”文件夹拥有不同的图标来指示它们是特殊的文件夹。

Remote Administration (MDRA)

- 已在 MDRA 中添加了一个“双重验证例外 IP”页面，位于主菜单下。这允许用户在从指定 IP 地址之一连接时无需 2FA 即可登录到 Remote Admin 或 Webmail。
- 在 MDRA 中新增“*允许用户编辑其别名显示名称*”Webmail设置 289选项。如果您希望允许用户编辑与其账户关联的任何别名的显示名称，请激活此选项。这可以通过使用“*编辑别名显示名称*”选项（位于 Webmail的 Pro 主题）来实现。
- 将密码字段的 autocomplete="off" 更改为 autocomplete="new-password" 来阻止 Firefox 在登录页面之外自动补全密码。
- 已将“通知邮件编辑器”添加到“内容过滤器”的通知 552页面中。
- 新增对于登录页面上 CSRFTokens 的支持。在启用“*使用跨站请求伪造令牌*”选项（位于 MDRA 中的Remote Administration 设置页面）时，启用该选项。
- 你已经创建的任何远程或本地自定义队列 736都可以在 MDRA 中的邮件和队列部分中进行管理。

安全

- MDaemon 现在支持较新的 Windows 版本中的 TLS 1.3。Windows Server 2022 和 Windows 11 默认启用 TLS 1.3。Windows 10 版本 2004（OS 版本 19041）和更高版本具有实验性的 TLS 1.3 支持，可以通过在注册表中设置以下内容来启用入站连接：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.3\Server

DisabledByDefault (DWORD) = 0

Enabled (DWORD) = 1
```

- MDaemon 记录 SSL/TLS 连接使用的密码套件（例如 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384）。
- 已新增密码 717选项来让强密码要求特殊字符。为新安装默认启用，为现有安装默认禁用。
- AV 邮箱扫描程序 - 当邮箱扫描期间发现受感染的邮件时，MDaemon 的受感染计数器将增加。
- AntiVirus - 已将 ClamAV 更新到 0.104.3 版本。

ActiveSync

- 已改进文件夹同步的性能。
- ActiveSync 连接监控对话框有一个新的右键单击菜单命令，用于终止会话并阻止客户端。
- 已向客户端设置 388对话框添加一个对话框来允许 Outlook 发送使用别名的邮件。如果将 Reply-To（答复）设置为发件账户的有效别名，则通过该别名发送邮件。

- 新增对于 EAS 16.1 查找命令的支持。已删除协议限制[363]来防止 iOS 使用 EAS 16.1

其他

- 内容过滤器 - 新增对于 $CONTACT...$ 宏的支持，针对 "附加公司签名[542]"这个操作。这些宏可用于使用来自其公共联系人文件夹中发件人联系人的信息来个性化签名。还请参阅：签名宏[110]来获取支持的宏列表。
- 内容过滤器 - 已向提取附件[542]新增一个操作，并将附件链接[305]添加到邮件中。
- 现在，用于保留、隔离和坏队列的摘要邮件[734]拥有一些链接来释放、重新排队或删除每封邮件。默认情况下，启用新的 *"包含操作链接"*选项。请注意：必须设置 Remote Administration URL[294] 来生成上述链接。
- LetsEncrypt[496] - 已更新脚本来使其适用于 PS 7。
- 已新增一个延迟投递邮件撤销[99]选项来 将 "日期:"报头 替换为当前日期和时间，请启用此项。默认情况下，禁用该选项。
- MDaemon Connector[323] 已被更新为 7.0.7 版本。
- XMLAPI - 已新增对于转发调度的支持。

MDaemon Server 发布说明

要了解 MDaemon 21.5 中有关新增功能、变更和修复的完整说明，请参阅 RelNotes.html (位于 MDaemon 的\Docs\子文件夹)。

MDaemon 21.5 的新功能

主要新功能

应用程序密码[630]

应用程序密码是随机生成的强密码，用于电子邮件客户端和应用程序，有助于使您的电子邮件应用程序更加安全，因为它们无法受到双重验证[603] (2FA) 的保护。2FA 是用户登录 Webmail或 MDaemon Remote Administration (MDRA) 的一种安全方式，但电子邮件应用程序无法使用它，因为该应用程序必须能够在后台访问您的电子邮件，无需您输入身份验证器应用程序中的代码。这个应用程序密码功能允许您创建强大、安全的密码，以在您的应用程序中使用，同时仍然通过 2FA 保护您的账户密码。应用密码只能在电子邮件应用程序中使用，不能用于登录 Webmail或 MDRA。这意味着即使应用程序密码以某种方式被泄露，未经授权的用户仍然无法进入您的账户来更改您的密码或其他设置，但是您仍然可以使用账户和密码来登录您的账户，在需要时也能使用 2FA 来删除已泄露的应用程序密码，并创建一个新密码。

应用程序密码要求和推荐

- 要创建应用程序密码，必须为账户启用 2FA (您也可以选择关闭该要求[717])。
- 应用密码只能在电子邮件应用程序中使用，不能用于登录 Webmail或 MDRA。
- 每个应用程序密码在创建时仅显示一次。以后无法检索它，因此用户应该准备好在创建时将其输入到他们的应用程序中。

- 用户应该为每个电子邮件应用程序使用不同的应用程序密码，并且当他们停止使用该应用程序或设备丢失或被盗时，他们应该撤销（删除）其密码。
- 每个应用程序密码都会列出它的创建时间、上次使用时间、以及上次访问账户邮件的 IP 地址。如果用户发现“上次使用”或“上次 IP 数据”有可疑之处，该用户应该撤销该“应用程序密码”，并为他或她的应用创建一个新密码。
- 更改账户密码后，所有应用程序密码都会被自动删除——用户无法继续使用旧的应用程序密码。

为 SMTP、IMAP、ActiveSync 等要求应用程序密码

账户编辑器设置 639 页面上有一个账户选项，您可以使用它来要求*“需要应用程序密码才能登录 SMTP、IMAP、ActiveSync 等”*。

“需要应用程序密码”有助于保护账户密码免受字典和通过 SMTP、IMAP 等进行的暴力攻击。这样更安全的原因是因为即使这种攻击是猜测账户的实际密码，它也不会不起作用，因为 MDaemon 只会接受正确的应用程序密码。此外，如果 MDaemon 中的账户正在使用活动目录 689 验证，“活动目录”又被设置成在达到失败的尝试次数后锁定了账户，该选项有助于防止账户被锁定，因为 MDaemon 只会检查应用程序密码，而不尝试对“活动目录”进行身份验证。

其他新功能和改进

Pro 主题

- 现在 Mobile 主题被称为 **Pro** 主题。已对其进行扩展和改进，可以响应并适应不同类型的设备和屏幕尺寸，而不会影响功能。
- 新增“跨站点请求伪造令牌”来实现更安全的交易。默认情况下禁用此功能。要通过 MDRA 启用此项，请转至“主页 | Webmail设置 | Web 服务器 270”并勾选“使用跨站点请求伪造令牌”
- 在“设置 | 个性化”添加了一个选项，以启用深色模式，以深色背景显示 Pro 主题。
- 在打开的邮件中添加了“跟踪我的快递”的链接。
  - 默认情况下监控的运营商跟踪号码是：USPS、UPS、OnTrac、FedEx 和 DHL。
  - 默认的配置文件位于：\MDaemon\WorldClient\package_tracking.json
  - 管理员可以通过创建以下文件来添加更多运营商：\MDaemon\WorldClient\package_tracking.custom.json，它使用与默认的 package_tracking.json 文件相同的格式。至少需要一个服务名称、一个跟踪 URL 和至少一个有效的正则表达式。包含可能出现在邮件中的服务名称，以减少误报匹配的机会。
- 已将“邮件列表布局”对话框添加到较小的浏览器大小。仅显示“邮件列表密度”设置。
- 新增密码强度计。
- 已为“邮件视图”添加了图像幻灯片功能。
- 已为“联系人”列表新增卡片视图。
- 已将“新建项目”按钮从工具栏中移至桌面大小的文件夹列表上方的空间。
- 在“个人”旁边添加了一个加号图标，以在日历视图中创建一个新日历。

- 已添加带有 "编辑"选项和 "向出席者发送电子邮件"选项的事件工具提示。
- 使搜索栏对于 1200 像素或更大的浏览器窗口宽度始终可见。
- 已新增一个对话框，允许用户在将联系人添加到白名单时将其从黑名单中删除，反之亦然。
- 在创建或重命名文件夹时出错的情况下，新增了错误消息。
- 在事件、联系人、任务和便笺中添加了对 HTML 便笺的支持。
- 已使用 Jodit 替换了当前的 HTML 编辑器 (CKEditor)。
- 已更改基本的标题视图来显示 "发件人"电子邮件地址。
- 新增录音机。

其他 Webmail改进

- 当邮件中存在 List-Unsubscribe 报头时，在 "发件人"地址旁边添加了 Unsubscribe 链接。可以在 Webmail的 "设置 | 个性化"中将其禁用。
- 新增将电子邮件导入当前邮件列表的功能。
- 已更新 Dropbox 集成，以使用 Dropbox 提供的 refresh_token 重新连接用户，而无需与 OAuth 对话框交互。当 access_token 过期时，Webmail会尝试使用 refresh_token 来获取新的 access_token。不再需要的设置已从 "云应用程序"页面中删除。管理员无需对 Dropbox.com 上的 Dropbox 应用程序进行任何更改。
- 当未订阅的文件夹被隐藏时，搜索 "所有/子文件夹"请求不再搜索未订阅的文件夹。
- 新增一个名为 "跳过搜索"的勾选框，可从 "搜索所有/子文件夹"请求中排除特定文件夹。
- 在 Remote Admin 中新增一个设置，允许隐藏 "双重验证记住我"勾选框。
- 当用户会话过期时，为背景添加了模糊效果。
- 已在 "设置 | 编写"中新增自动 CC 和 BCC 功能。
- 已将一个选项添加到：WorldClient\Domains.ini [Default:Settings] PreventComposeWithAlias，由此来防止使用别名编写邮件。默认情况下，禁用该设置。
- Lite 主题 - 已向 "编写"视图添加了自动保存草稿邮件。
- 已在 "选项 | 文件夹"视图中新增一个选项来允许用户在自动完成搜索中跳过联系人文件夹。同时也在右键单击菜单中新增一个选项。
- 在用户登录时为 User-Agent 添加了 Webmail日志条目。
- 如果本地收件人启用了自动应答器，则在 "编写"视图中添加通知。
- WorldClient 主题 - 已向具有附件的事件图块添加了回形针图标。
- 新安装的附件大小最大值被设置为 25 MB。
- 已将 "全部删除"文件夹操作更改为 "空文件夹"
- WorldClient 主题 - 已在安全页面中添加了 "更改密码"和 "更改恢复电子邮件"按钮

Remote Administration (MDRA)

- 已新增拖放内容过滤规则的功能。复制、编辑和删除按钮现在位于每个相应的规则上。
- 新增"跨站点请求伪造令牌"来实现更安全的交易。默认情况下启用此功能。要禁用此项，请转至：主页 | Remote Admin 设置 | 设置，并取消勾选"使用跨站点请求伪造令牌"。
- 已在某些密码字段中添加了密码强度计。
- 已新增选项："启用双重验证记住我"至设置 | 域管理器 | 编辑 | Webmail设置 160 和主页 | Webmail设置 | 设置 289。
- 已为"动态屏蔽"新增"已阻止 IP"和"已拒绝 IP"报告。
- 已在 ActiveSync 下新增群组 396 和客户端类型 402 视图。
- 已更新 ActiveSync 诊断 361 和微调 351 页面。
- 已在报告 | 流量 | Webmail登录统计新增一个按操作系统整理的浏览器使用图表。
- 新增一些按钮，用于打开"浏览用户"和"浏览群组"弹出窗口，以将它们添加到邮件列表，它们位于：主页 | 邮件列表 | 编辑 | 新建 228。只有域或全局管理员 636 有权访问这些按钮。
- 已在"主页 | 我的账户 | ActiveSync 客户端"和ActiveSync | 客户端管理 388 页面新增"从账户擦除"选项。
- 已新增变更日志。它将记录通过 Remote Administration 所做的每一个变更。
- 已将邮件撤销 99 更新到匹配 MDaemon GUI。
- 已在安全 | 内容过滤器 | 压缩 556 页面新增"从 winmail.dat 提取附件"选项。
- 已为 MDaemon Remote Administration 新增斯洛文尼亚文。

其他 MDaemon 改进

- 已新增对于 SMTP 命令管道 (RFC 2920) 的支持。MDaemon 将分批发送 MAIL、RCPT 和 DATA 命令，而不是单独发送，从而提高高延迟网络链接的性能。始终为入站连接启用 SMTP 管道。默认情况下，它为出站连接启用，但可以在设置 | 服务器设置 | 服务器 & 投递 | 服务器 74 页面将其禁用。
- 已新增对于 SMTP CHUNKING (RFC 3030) 的支持。CHUNKING 允许传输非面向行 (non-line-oriented) 的邮件。为入站连接默认启用，为出站连接默认禁用。默认情况下，接收邮件中的裸换行符将转换为回车换行符。可以通过设置 [Special] SMTPChunkingInbound=Yes/No、SMTPChunkingOutbound=Yes/No 和 SMTPChunkingAllowBareLF=Yes/No (位于 \MDaemon\App\MDaemon.ini 中) 来更改这些默认值。
- 内容过滤器 - 已更新默认的受限附件 550 列表。
- 内容过滤器 - 已将规则操作添加至添加附件至邮件 542。
- 已将 ActiveSync 服务器启动/停止条目写入 MDaemon 的系统日志。
- 集群 - 已添加从次节点进行提醒同步的支持。

- 动态屏蔽 - 已新增选项来使用 ISO-3166 代码记录位置[510]，而不是使用名称来记录位置。
- XMLAPI - 新增对于 ActiveSync AlwaysSendMeetingUpdates 设置的支持。
- XMLAPI - 新增对于信号文件创建的支持。
- XMLAPI - 新增对于从 "设置/服务器设置/日志"进行报告/修改设置的支持。
- MDaemon Instant Messenger - 新增选择多名聊天好友进行群聊的功能，由此改进了群聊功能。此外还新增一个选项来自动接收聊天室请求。
- 位置屏蔽[477]提供一个新选项来控制是否将 "X-MDOrigin-Country"报头添加到邮件。默认情况下，启用该选项。
- 现在有一个关于是否允许用户使用别名登录的账户设置，位于：账户 | 账户设置 | 别名 | 设置[701]。默认情况下，启用该选项。
- 已将 MDaemon Connector 更新到 7.5.0 版本。
- 已将默认的投递确认邮件文本（位于 \MDaemon\App\Receipt.dat 中）更改为使用 $HEADER:X-RCPT-TO$ 宏而不是 $RECIPIENT$，以避免泄露别名解析到的实际电子邮件地址。

MDaemon Server 发布说明

要了解 MDaemon 21.5 中有关新增功能、变更和修复的完整说明，请参阅 RelNotes.html（位于 MDaemon 的\Docs\子文件夹）。

MDaemon 21.0 的新功能

主要新功能

持续聊天室[313]

MDaemon 的 XMPP 服务器现在支持持续聊天室，无需在所有用户每次离开聊天室时都重新创建聊天室。请在以下位置进行配置：设置 | Web & IM 服务 | XMPP。

病毒/垃圾邮件错误分类报告

已向 MDaemon 控制台和 Remote Administration 中的 "隔离区"、"坏队列"、"垃圾邮件陷阱"队列屏幕添加了右键单击弹出菜单选项，用来将错误分类的垃圾邮件或非垃圾邮件作为误报，报告给 MDaemon.com。而且已将类似的选项添加到 MDaemon Remote Administration。将分析这些邮件并将其投递给第三方供应商来采取纠正措施。

ActiveSync 迁移客户端 (ASMC) GUI

已创建一个 GUI 来辅助运行 ASMC（ASMCUI.exe 位于 MDaemon 的\app\ 文件夹）。这允许您稍后保存您的选项并进行撤销。ASMC 支持从 "支持协议版本 14.1"的 ActiveSync 服务器迁移邮件、日历、任务、便笺和联系人。可以在 MDaemon 的 Docs 文件夹中找到其文档，位于：\MDaemon\Docs\ActiveSync Migration Client.html。

Webmail Mobile 主题改善

为 Webmail 用户大幅度扩展和改善了 Mobile 主题。请参阅 RelNotes.html (位于 MDaemon 的\Docs\文件夹)来获取大量新增功能的完整说明。

集群改进 341

已对 MDaemon 的集群服务进行了大量改进：

- 新增一个多节点邮件路由 345选项，在集群节点之间共享邮件队列。会使用多个机器来处理和投递邮件，允许它们更平均地分配工作，并防止邮件被卡在任何发生故障的机器的队列中。
- SSL 证书会从主节点复制到从节点。
- 从节点上的队列在初始数据复制期间被冻结，从而提高了启动期间的响应速度。
- 关闭 MDaemon 后，将立即暂停复制，从而避免了与集群相关的关闭延迟。
- 可以使用 IP 地址或 DNS 名来添加集群节点。
- 现在，可以从新的 "共享网络路径"屏幕更轻松地管理共享网络路径。
- 新的 "故障诊断"屏幕上提供了日志记录和诊断工具。

其他新功能和变更

Remote Administration (MDRA)

已将数十个选项添加到 MDaemon 的 Remote Administration 界面。有关这些选项和 MDRA 变更的完整说明，请参阅 RelNotes.html (位于 MDaemon 的\Docs\文件夹)。

内容过滤器

新增在 7-Zip 压缩文件中搜索受限文件 550的功能。

自动应答器 703

自动应答器现在支持 Unicode (UTF-8)，支持使用任何语言的文本。

IMAP 过滤器 617

现在，IMAP 过滤规则可以在邮件正文中搜索特定的文本。

Webmail

- 现在，您可以通过右键单击事件，并在 LookOut 和 WorldClient 主题中选择 "发送"选项，然后从 Mobile 主题中的 "事件预览"中将事件附加到新电子邮件中。
- 已删除所有 "新建账户"功能。
- 发布日历时 (共享一个指向它的 "公共访问链接")，新增的这些选项允许您设置其默认的日历视图 (例如月/周/日)，并发布 "空闲/忙碌"日历链接。
- 新增一个选项，可以跳过每个用户的 IP 持久性检查。在 MDRA 中编辑用户账户时，请转到 Web 服务，然后选中 "为 Webmail 会话跳过 IP 持久性检查"。
- 新增在高级搜索中搜索 CC 字段的功能。

- 已将每天发送的邮件数量最大值[613]添加到现实的配额中。

用户界面

- 已删除 "设置 | 移动设备管理"，并替换为 "设置 | ActiveSync"中的 "ActiveSync 管理"对话框。
- 已删除 "ActiveSync 客户端设置"屏幕。可以在 "微调"、"域"、"群组"、"账户"和 "客户端"屏幕上自定义客户端设置。
- "ActiveSync 客户端类型"屏幕具有用于将客户端类型列入白名单和黑名单的菜单命令。
- 已在 "设置 | 邮件索引"新增屏幕，用于配置 Webmail、ActiveSync 和 Remote Administration 所使用的搜索索引的实时和每晚维护。
- 现在几个插件共享一个通用的 "故障诊断"配置屏幕。
- 已使用新的响应式系统更新了基于 MDRA 和 Webmail 浏览器的帮助系统，由此使它们在不同类型的设备上具有更高的实用性。

XML API

- XML API 文档门户的外观可以按全局和域进行自定义。请参阅帮助门户中的 "变更和开发说明"(即 http[s]://ServerName[:MDRAPort]/MdMgmtWS)，或使用 Internet Explorer 查看磁盘上的 \MDaemon\Docs\API\XML API\Help_Readme.xml 文件来获得更多信息。\MDaemon\Docs\API\XML API\Samples\Branding 中提供了示例 company.mail 目录。
- 添加了 "别名"操作，以简化 "别名"管理，解析和报告别名。
- 新增 FolderOperation Search (文件夹操作搜索)操作来搜索邮件。
- 向 QueryServiceState 和 ControlServiceState 新增 "集群服务"支持。

归档[105]

- 在本地账户之间发送邮件时，如果同时启用 "归档入站邮件"和 "归档出站邮件"，则将同时创建 "入站"和 "出站"的归档副本。
- 用于归档垃圾邮件的选项 (在 20.0 版中已删除)重新回归。
- 归档从 "垃圾邮件陷阱"释放的垃圾邮件。

组件更新

- 已将 MDaemon Connector 更新到 7.0.0 版本。
- 垃圾邮件过滤器：已更新为 SpamAssassin 3.4.4。并删除了 local.cf 中不推荐使用的设置。
- AntiVirus：已将 ClamAV 更新至 0.103.0 版本，并将 IKARUS AV 引擎更新至 6.3.0.2 版本。
- XMPP 服务器：已将数据库后端更新到 SQLite 3.33.0 版本。

MDaemon Server 发布说明

要了解 MDaemon 21.0 中有关新增功能、变更和修复的完整说明，请参阅 RelNotes.html (位于 MDaemon 的\Docs\子文件夹)。

MDaemon 20.0 的新功能

MDaemon 集群服务 341

MDaemon 新的集群服务的设计旨在：在网络上的两个或多个 MDaemon 服务器之间共享您的配置。这使您可以使用负载均衡硬件或软件，在多个 MDaemon 服务器之间分配电子邮件负载，从而可以通过减少网络拥塞和过载，并最大化电子邮件资源来提高速度和效率。如果一台服务器发生硬件或软件故障，该功能还有助于确保电子邮件系统中的冗余。还请参阅：集群服务 341来获取有关在网络上设置 MDaemon 服务器集群的更多信息。

新的 SMTP 扩展

RequireTLS (RFC 8689) 493

IETF 中的 RequireTLS 工作终于完成，并且已经实现了对此的支持。RequireTLS 允许您标记*必须*使用 TLS 的邮件。如果无法使用 TLS (或者 TLS 证书交换的参数不可接受)，则退回邮件，而不是不安全地投递邮件。默认情况下，启用 RequireTLS，但是将受 RequireTLS 进程约束的唯一邮件是被使用新的内容过滤器操作 542"*为 REQUIRETLS 标记邮件...*"的"内容过滤器"规则特别标记的邮件，或发送至<local-part>+requiretls@domain.tld (例如，arvel+requiretls@mdaemon.com)的邮件。将所有其他邮件视为已禁用该服务。此外，必须满足几个要求才能使用 RequireTLS 发送邮件。如果它们中的任何一个失败，该邮件将弹回，而不是以明文形式发送。有关这些要求以及如何设置 RequireTLS 的更多信息，请参阅：SMTP 扩展 493。有关 RequireTLS 的完整说明，请参阅：RFC 8689：SMTP 需要 TLS 选项.

SMTP MTA-STS (RFC 8461)-严格传输安全 494

IETF 中的 MTA-STS 工作完成了，并且已经实现了对此的支持。SMTP MTA 严格传输安全 (MTA-STS)是一种机制，使邮件服务供应商 (SP)能够声明其接收传输层安全 (TLS)和保护 SMTP 连接的能力，并指定发件 SMTP 服务器是否应拒绝投递给不为 TLS 提供受信任的服务器证书的 MX 主机。默认启用 MTA-STS 支持。还请参阅：SMTP 扩展 493来了解有关此设置的更多信息，MTA-STS 在以下链接有完整描述 RFC 8461: SMTP MTA 严格传输安全 (MTA-STS).

SMTP TLS 报告 (RFC 8460) 494

TLS 报告功能允许使用 MTA-STS 的域收到有关检索 MTA-STS 策略或使用 STARTTLS 协商安全通道的任何失败的通知。启用后，MDaemon 会每天向已在当天向其发送 (或尝试发送)邮件的每个启用 STS 的域发送报告。提供了多个选项来配置报告将包含的信息。默认情况下禁用 TLS 报告功能，更多详细信息请参阅RFC 8460：SMTP TLS 报告.

使用单密钥的域/公司范围的 MDPGP 加密

MDPGP 527现在支持使用单个加密密钥为所有用户加密域之间的邮件。例如，假设"domain-a"和"domain-b"希望加密它们之间发送的所有电子邮件，但不希望为域中的每个用户账户设置和管理单独的加密密钥。现在可以按照以下步骤进行操作：

"Domain-a"和 "Domain-b"分别通过自身首选的任何方式，为对方提供公共加密密钥。例如，他们可以通过右键单击 MDPGP UI 中的现有公共密钥，然后选择 "导出&电子邮件密钥"，通过电子邮件将密钥相互发送。如果他们希望创建专用于此目的的新密钥，则可以点击 "为特定用户创建密钥"按钮，然后选择为此目的放置在此处的 "_Domain Key (domain.tld)_<anybody@domain.tld>"项（尽管任何键都起作用）。一旦双方收到对方的密钥，他们将点击 MDPGP UI 上的 "导入域的密钥"按钮，然后输入域名，用于使用提供的密钥被加密的所有电子邮件。此系统不为您每个域的下拉列表创建密钥。您可以使用为所有域提供的密钥，也可以根据需要创建是域而定的密钥。

如果任何一方都已拥有希望使用的公共密钥，并且这些密钥已在密钥环上，则可以在 MDPGP UI 中右键点击该密钥，然后选择 "设置为域的密钥"。不过，请勿使用还具有相应私钥的密钥。如果您这样做，MDPGP 将加密邮件，然后立即看到解密密钥是已知的，并立即解密这封相同的邮件。

此时，MDPGP 创建了一个名为 "Encrypt all mail to <domain>（加密所有邮件到<domain>）"的 "内容过滤器"规则，该规则将对发送到该域的每封电子邮件调用加密操作。使用 "内容过滤器"意味着您可以通过启用或禁用 "内容过滤器"规则来控制此流程。您还能调整规则来微调您希望在加密邮件之前采用的条件（例如，也许要对两个域或仅对域内的某些收件人执行相同的操作）。"内容过滤器"提供各种灵活性来满足您的需求。

基于收件 IP 地址来加密出站邮件

MDPGP[527] 拥有一个新的复选框和设置按钮，您可以在其中将 IP 地址映射到特定的加密密钥。将邮件投递到这些 IP 的任何出站 SMTP 会话都将在传输之前，首先使用关联的密钥对邮件进行加密。如果邮件已被其他密钥加密，则不会完成任何工作。例如，在要确保始终对发送给某些关键合作伙伴、供应商、分支机构等的所有邮件都进行加密的情况下，此功能很有用。

用于邮件列表邮件的宏

邮件列表编辑器 » 路由[244]屏幕拥有一些新选项，允许在列表帖子的邮件正文中使用宏。这将允许您（例如）个性化每封列表邮件。列表邮件报头和页脚文件中的宏已得到长期支持，但邮件正文中从未支持它们。由于宏与个别列表成员相关，因此这个选项仅与被配置成 *"将列表邮件分别投递给每个成员"*的列表兼容。此外，出于安全目的，您可以设置此选项来要求提供列表的密码，以便在邮件正文中使用宏。如果您选择不要求密码，那么任何允许发布到列表的列表成员都被允许使用它们。请参阅邮件列表路由[244]屏幕来获取更多信息，以及可供使用的宏列表。

改善的劫持检测系统

劫持检测[473]拥有一些新选项，可以帮助防止由于密码被盗而使账户被用来狂发垃圾邮件。垃圾邮件的一个普遍特征是，由于垃圾邮件发送者试图将其发送到旧的电子邮件地址，或猜测新的电子邮件地址，因此通常将这些邮件发送给大量无效的收件人。因此，如果 MDaemon 账户在短时间内开始向大量无效收件人发送邮件，则表明该账户已被劫持，并被用于发送垃圾邮件。为了防止这种情况，MDaemon 现在可以跟踪经过身份验证的用户尝试向无效收件人发送电子邮件的次数。如果在很短的时间内发生了太多次，您可以让 MDaemon 冻结该账户（邮件管理员将收到相关邮件，他们可以通过答复来重新启用该账户）。这有助于在造成太大损失之前，自动停止被劫持的账户。**请注意：**作为这项工作的一部分，"发件人报头修改"选项已被移至其自身的发件人报头屏蔽[478]页面，来为新的 "劫持检测"选项创造空间。

延迟邮件队列和改善的邮件调用 99

为了提高 "邮件撤回"系统和 "坚持投递"报头支持的效率，MDaemon 现在具有专用于延迟邮件的队列。以前，入站队列可能会被延迟的邮件阻塞，这会减慢非延迟邮件的投递速度。新的 "延迟"队列有助于解决这个问题。"延迟"队列中的邮件由系统放置在此处，并在邮件文件名中编码了邮件被设置成何时离开队列的日期。MDaemon 每分钟检查一次队列，当邮件离开队列时，它将移至入站队列，并接受常规的邮件处理和投递。

此外，MDaemon 现在可以跟踪经过身份验证的本地用户发送的最新电子邮件的每个 Message-ID，这意味着用户现在可以撤回他们发送的上一封邮件 (但只是他们发送的上一封邮件)，只需 (单独)将 RECALL 作为主题放置在邮件中，发送给 mdaemon@system 账户。当邮件是最后发送的邮件时，无需查找并粘贴您要撤回的邮件的 Message-ID。撤回任何其他邮件时，仍然需要将 Message-ID 包含在 "主题"文本中，或附加到撤回请求的用户 "已发送"文件夹中的原始邮件中。

除了记住每个经过身份验证的用户发送的最新电子邮件之外，MDaemon 还会记住所有经过身份验证的用户发送的近 1000 封电子邮件的位置和 Message-ID。因此，即使在投递到用户邮箱之后，也可以立即从用户邮箱中撤回邮件。因此，如果用户邮件客户端和电话被撤回，邮件将消失。**请注意：**当然，这仅适用于发送给其他本地用户的邮件；一旦 MDaemon 将邮件传递到其他服务器，它就不再处于 MDaemon 的控制之下，因此无法被撤回。

验证失败日志

有一个新的 "身份验证失败"日志文件，其中包含一行，含有每个失败的 SMTP、IMAP 和 POP 登录尝试的详细信息。该信息包括使用的协议和 SessionID，以便您可以搜索其他日志、违规者的 IP、他们尝试使用的原始登录值 (有时是别名)以及与登录匹配的账户 (如果没有账户匹配则使用 "无")。

在转发/路由邮件时进行验证

MDaemon 中有几个转发选项，您现在可以在其中添加身份验证凭据。这就意味着 \APP\ 文件夹中的一些文件 (例如forward.dat、gateways.dat、MDaemon.ini 和所有 "邮件列表".grp 文件)现在有可能包含处于弱加密状态的模糊登录和密码数据。因此一如既往，您应该在命令中使用操作系统工具以及选择的任何其他措施，以保护 MDaemon 机器和目录结构免遭未授权的访问。身份验证凭证选项已被添加到：未知邮件 83、邮件列表路由 244、网关编辑器 » 转发 217、网关编辑器 » 出队 218和账户编辑器 » 转发 610。

主机验证 101

"主机验证"是一个新屏幕，您可以在其中配置任何主机的端口、登录和密码值。当 MDaemon 将 SMTP 邮件发送到该主机时，将使用此处找到的关联凭证。请注意，这些凭证属于后备之需，仅在其他针对特定任务的凭证不可用时才使用。例如，如果您使用新的 "账户编辑器 » 转发 610"或 "网关管理器 » 取消队列 218"选项来配置验证登录/密码，然后使用这些凭证，它们将取代此处配置的内容。此功能仅适用于主机名 (不适用于 IP 地址)。

已改善自定义队列和邮件路由 736

现在，您可以为任何远程队列指定主机、登录、密码、SMTP 返回路径和端口。如果提供，则使用这些新设置投递队列中的所有邮件。但是，通过设计，队列中的单封邮件仍然有可能拥有自己唯一的投递数据，这些数据将优先于这些新设置。此外，您现在可以设置任意数量的远程队列，根据您选择的条件使用内容过滤器将邮件过滤到其中，为每个队列分配自己的发送时间表，并根据您的意愿进行完全不同的路由 。

已改善域共享[93]

一段时间以来，域共享根据需要对 SMTP MAIL 发件人值执行查找。不过，通常通过 "需要身份验证"拒收邮件，而且当发件人账户位于其他服务器上时，无法执行身份验证。现在已经解决了该问题，MDaemon 可以接受邮件，而无需从其他服务器上找到的现有账户进行身份验证。可以使用以下位置新的 "安全管理器"选项禁用它：发件人验证 » SMTP 验证[438]。如果您根本不想在 SMTP MAIL 发件人上执行域共享查找，则可以使用 "域共享"选项完全禁用该功能。

"域共享"还有一个新选项，可以共享邮件列表。当邮件抵达邮件列表时，将为每个 "域共享"主机创建一个副本，同时保留该列表的版本（通过查询来进行检查）。这些主机收到副本后，会将其交付给他们所服务的列表中的所有成员。这样，邮件列表可以在多个服务器之间进行拆分，而不会损失功能。为此，每个 "域共享"主机必须在其可信 IP[435]配置中包含其他主机的 IP 地址。

最后，"域共享"拥有一个 "高级"按钮，可以打开一个文件，您可以在其中配置允许使用 "域共享"的域名。如果此文件中没有任何内容（默认情况），则所有域都可以使用 "域共享"。请参阅文件顶部的指示来获取更多信息。

已改善邮件转发的控制

首选项 » 其他[421]有一个新选项，允许管理员阻止账户邮件转发在域外发送电子邮件。如果用户将其账户配置为将 "邮件转发"发送到外部域，则邮件将被移至 "坏邮件"队列。此设置仅适用于为账户使用邮件转发选项进行转发的邮件。

账户编辑器 » 转发[610]拥有一个新的 *"调度"*按钮，允许账户配置转发的开始和停止时间。在相应的 "账户模板[679]"屏幕上也有这个按钮。这些设置配置转发开始和停止的日期和时间，但是转发仅在您选择的星期几进行。

位于 "新建账户模板[667]"的 "转发地址"字段现在也适用于账户宏。但是在新建账户时，唯一具有数据的宏是那些与账户用户的全名、域、邮箱和密码值相关的宏。因此如果您希望每个新账户转发到相同的邮件地址，但是在不同的域，您可以将此置于 "转发地址"字段：$MAILBOX$@example.com。宏也适用于 *"发送为"*、*"验证登录"*和 *"验证密码"*字段。

现在，转发邮件将更新转发账户的上次访问时间。这就意味着仅执行邮件转发操作的账户不再可能因为闲置状态而被删除。**请注意：**转发实际上必须发生，并且不能被其他配置选项所破坏，例如限制转发器可以发送邮件的位置或 "计划外"。仅配置了转发地址不会自动将账户标记为活动状态。

已改善 SMTP 验证

发件人验证 » SMTP 验证[438]拥有两个新选项。首先，*"不允许在 SMTP 端口上进行验证"*这个选项将完全禁止 SMTP 端口上的验证支持。如果 SMTP 客户端提供了 AUTH（验证），则不会在 EHLO 响应中提供 AUTH，并且会将 AUTH 视为未知命令。另一个选项用于 *"..如果他们仍然尝试，则将其 IP 添加到动态屏蔽"*。此项会将禁用 AUTH 验证期间，任何尝试验证的客户端的 IP 地址添加到 "动态屏蔽[524]"。连接也将立即终止。这些设置在所有合法账户都使用 MSA（或其他）端口来提交经过验证的邮件的配置中很有用。在这种配置中，假定在 SMTP 端口上进行任何验证的尝试都必须来自攻击者。

已改善账户管理

已扩展 "账户管理器"的过滤选项。现在，您还能根据账户是否已启用、是否正在使用 MultiPOP、是否接近配额（70%）、是否接近配额（90%）或不转发来选择显示账户。您还能在账户描述字段中搜索所需的任何文本，然后根据该文本选择账户。此外，快捷方式/右键

单击菜单具有新选项，可用于从邮件列表和组中添加或删除所有选定账户。它还具有复制现有账户来创建新账户的选项。现有账户的所有设置都将复制到新账户，全名、邮箱、密码和邮件文件夹除外。最后，"账户编辑器"的"IMAP 过滤器"屏幕有一个名为"发布"的新按钮，用于向正在编辑的账户以及该账户域中的其他所有账户添加新规则。当每个人都需要新规则时，这可以节省一些时间。

为整个域启用"勿扰"

"域管理器"的"主机名 & IP"屏幕有一个新设置，帮助您为域启用"勿扰"。启用后，域将拒绝所有用户的所有服务连接，但仍会接受来自外部世界的入站邮件。此外，您可以调度"勿扰"的开始和停止时间。例如，如果您配置2020年5月1日到2020年6月30日，时间是星期一至星期五的下午5:00到早上7:00，那么这意味着从下午5:00开始，该天的用户将无法使用该邮件服务，并且只要当前日期是2020年5月1日至2020年6月30日之间，就在上午7:01恢复。删除调度的开始日期会取消这次调度，而且有**永久将域置于"勿扰"模式**"的效果。

已改善归档

MDaemon 的简单邮件归档系统已变得更加高效和风格一致。现在，归档的工作方式如下所示：当邮件从"本地队列"投递到用户的邮件文件夹时，将在那时创建归档副本（如果已配置，则在收件人的"入站"文件夹中）。当从"远程队列"中提取邮件以进行 SMTP 传递（无论投递是否成功）时，将在那时（在发件人的"出站"文件夹中，如果已配置）创建一个归档副本。在处理"本地"和"远程"邮件时，您将在"路由"日志中看见像"ARCHIVE message: pgp5001000000172.msg"这样的行，或在"路由"日志中看见像"* Archived: (archives)\company.test\in\frank@company.test\arc5001000000023.msg"这样的行。此外，"ToArchive"队列现在作为系统队列存在（UI 中未公开）。定期检查此队列中是否有丢弃的邮件（手动、通过插件或其他方式）。在此找到邮件后，将立即将其归档并删除。如果发现不符合归档条件的邮件，则将其删除。此队列的名称为 \MDaemon\Queues\ToArchive\。邮件成功归档后，"路由"屏幕/日志将显示详细信息。此外，加密邮件的归档现在可以更一致地进行处理。默认情况下，加密邮件的未加密副本将存储在归档中。如果无法解密邮件，则将存储加密的表单。如果您希望保存加密版本，则可以使用一个选项进行存储。此外，现在有一个选项可以归档发送到公共文件夹提交地址的邮件，默认情况下处于启用状态。最后，从不归档以下类型的邮件：邮件列表流量、垃圾邮件（此选项已被弃用和删除）、带有病毒的邮件、系统级邮件和自动答复。

更高效的日志

MDaemon 不再创建空的日志文件。如果在"设置"屏幕上禁用了项目，则在启动时将不会创建其关联的日志文件。禁用某个项目时，可能已经存在的日志文件保留在原位置（未删除）。如果启用某个项目时缺少日志文件，则立即创建所需的日志文件。此变更适用于核心的 MDaemon 引擎管理的所有日志文件。动态屏蔽、即时通讯、XMPP、WDaemon 和 WebMail的日志文件在 MDaemon 外部运行，因此未更改。一些与日志有关的其他变更包括：使 ATRN 会话日志看起来正确，使所有日志的颜色保持以及记录会话和子项 ID 的方式保持一致，MultPOP 服务器不再为已超出配额的账户拆卸会话，因此在这些情况下记录时不再存在浪费现象。最后，路由日志仅记录入站和本地的队列邮件解析。如今在做出投递尝试时还记录远程队列解析。这样，您不必搜索路由日志和 SMTP（出站）日志即可查看何时处理邮件。

已改善活动目录集成

现在，您可以将 MDaemon 的"活动目录"集成功能配置为在将某人添加到"活动目录"组中时创建一个 MDaemon 账户，并且当您从"活动目录"组中删除某人时，其相应的 MDaemon 账户将被禁用（但不会删除）。要使用此功能，必须使用备用的"活动目录"搜索过滤器。还请参阅：活动目录 » 验证获取更多信息。

在 "活动目录"的 验证[692]"屏幕有一个单独的 *"联系人搜索过滤器"*选项用于搜索联系人。以前，联系人搜索是通过用户搜索过滤器完成的。此外联系人搜索过滤器还有一个单独的测试按钮。 "活动目录"搜索已经过优化，因此当搜索过滤器相同时，单个查询将更新所有数据。当搜索过滤器不同时，则需要两个单独的查询。

以下字段已添加到 ActiveDS.dat 文件模板中，以便在 "活动目录"监控创建或更新通讯簿时，将它们包含在联系人记录中：abTitle=%personalTitle%、abMiddleName=%middleName%、abSuffix=%generationQualifier%、abBusPager=%pager%、abBusIPPhone=%ipPhone% 和 abBusFax=%FacsimileTelephoneNumber%。

现在，当从 "活动目录"中删除关联账户时，默认情况下将删除公共文件夹联系人。不过，仅在联系人是由 "活动目录"集成功能创建的情况下，将其删除。这个进行控制的设置位于 活动目录监控[694]"屏幕。

当 "活动目录"监控系统创建或更新账户，而且发现邮箱值太长而无法容纳 MDaemon 邮箱值的有限空间时，它将像以前一样截断邮箱值，但是现在它还将使用完整名称来创建别名。此外在创建账户或别名时，将更新该账户的管理职位[636]屏幕，用于审计。

"邮件列表管理器"的 活动目录[249]"屏幕现在允许您为列表成员的全名字段输入 "活动目录"属性。

"活动目录"中账户属性的变更可能触发重新创建 MDaemon 账户，即使该账户先前是在 MDaemon 中删除的也是如此。为了防止以这种方式重新创建账户，将一个新选项添加到 活动目录监控[694]"。默认情况下，在 MDaemon 中手动删除账户后将不会重新创建账户。

已改善发件人报头屏蔽[478]

"*发件人报头修改*"选项已从 "劫持检测"屏幕移至其自身的 发件人报头屏蔽[478]"屏幕，并添加了新选项。例如 "发件人报头屏蔽"现在可以检查 "发件人："报头显示名是否有看起来像邮件地址的信息。如果找到一个与实际发送电子邮件地址不匹配的地址，则可以使用实际电子邮件地址替换显示的地址。例如，如果您正在使用此功能，并且 "发件人："报头看起来类似于以下项："发件人：'Frank Thomas <friend@friend.test>' <enemy@enemy.test>"，则将其更改成："发件人：'Frank Thomas <enemy@enemy.test>' <enemy@enemy.test>"。

检查泄露的密码[717]

MDaemon 现在可以对照第三方服务中的泄露密码列表来检查用户密码。它能够执行此操作而无需将密码传输到服务，而且如果列表中存在用户的密码，并不表示该账户已被黑客入侵。这就意味着某人在某处使用了与他们的密码相同的字符，并且出现了数据泄露事件。黑客可能会在字典攻击中使用已泄露的密码，但是从未在其他任何位置使用过的唯一密码更加安全。请参阅Pwned Passwords (已泄露密码)获取更多信息。

在 "安全设置"的 密码[717]"屏幕上，MDaemon 现在提供一个选项，可以防止将账户的密码设置为 "已泄露密码"列表中的密码。它还可以每隔一定天数登录一次用户密码，如果找到密码，则向用户和邮件管理员发送警告电子邮件。通过编辑 \MDaemon\App 文件夹中的邮件模板文件，可以定制警告邮件。由于有关如何更改用户密码的说明可能取决于该账户是使用 MDaemon 中存储的密码还是使用 "活动目录"身份验证，因此有两个模板文件，CompromisedPasswordMD.dat 和 CompromisedPasswordAD.dat。宏可用于个性化邮件、更改主题和更改收件人等。

额外的功能和改善

请充分使用 MDaemon 20 中的超过 250 个新功能和改善，这一部分中还未列出大量说明。请参阅 RelNotes.html 位于 MDaemon 的 \Docs\ 子文件夹来获取此版本中包含的所有新功能、变更和修复的完整列表信息。

MDaemon 19.5 的新功能

新的 Webmail Mobile 主题

已使用具有更多功能的现代 GUI 取代了 Webmail 的 Mobile 主题。邮件列表功能现在包含个性化的类别、邮件延缓、按旗标/未读/延缓排序、排序列和邮件撤回。日历功能现在包括：导入/导出事件为 csv 或 ics 文件、添加外部日历、私有访问链接、发布日历和一次查看多个日历。编写功能现在包括延迟投递、多个签名、文本/html 邮件和电子邮件模板。其他功能包括拖放电子邮件过滤器、多个签名编辑器、更多文件夹管理选项、通知、拖放列管理和拖放类别管理等。如果在 IIS 中运行 Webmail，则需要其他配置步骤才能使用新的移动主题。请参阅知识库文章 1236 来了解更多信息。

客户端签名管理 113

现在您可以为用户配置被推送到 Webmail 和 MDaemon Connector 的电子邮件签名。可以设置默认的客户端签名 113，或者在 "域管理器"的客户端签名 170 屏幕上按域设置。使用签名宏 114（例如 $CONTACTFULLNAME$、$CONTACTEMAILADDRESS$）来使用从域的 "公共联系人"文件夹内用户的联系人那里获取的数据，对签名进行个性化。为 HTML 签名中的内嵌图像使用 $ATTACH_INLINE:filename$ 宏。输入签名文本后，它将在 Webmail 的 "编写"选项中显示为 "系统"签名，并将成为用户的默认签名。可以在 Webmail 设置 289 和域管理器 160（按域）为 Webmail 默认启用/禁用它。对于 MDaemon Connector，可以在 MC 客户端设置的签名 339 屏幕上配置签名的名称和相关设置。此功能需要 MDaemon Connector 6.5.0 或更高版本。

类别页面 288

MDaemon 的 Remote Administration (MDRA) 界面现在拥有一个类别 288 页面，位于 Webmail 选项下，用来配置 "域类别"和默认的 "个人类别"。

其他 MDRA 改善

以前只能通过 MDaemon 的应用程序界面管理的许多选项已添加到 MDRA。要了解完整列表，请参阅发布说明。

MDaemon 19.0 的新功能

TLS 服务器名称指示 (SNI) 支持 481

MDaemon 现在支持 TLS 协议的服务器名称指示 (SNI) 扩展，它允许为您的每个服务器主机名使用不同的证书。MDaemon 将查看活动证书，并在 "主题备选名称"字段中选择具有所请求主机名的证书（您可以在创建证书时指定备选名称）。如果客户端未请求主机名，或者未找到匹配的证书，则使用默认证书。

用于文件夹和项目管理的 XML-API

XML-API 已扩展为包含管理文件夹中的邮箱文件夹和项目的功能。可以使用这个 API 创建、删除、重命名和移动文件夹。项目操作支持电子邮件、日历、联系人、任务和备注。可以使用这个 API 创建、删除和移动项目。可以在 MDaemon\Docs\API\XML-API\ 文件夹中找到完整的文档说明。

Remote Administration 改进

已扩展 MDaemon 的 Remote Administration (MDRA) web 界面来包括访问以前只能使用配置会话 (即 MDaemon 的应用程序界面)管理的功能，现在有几个选项只能通过 MDRA 访问。因此，对于新的 MDaemon 安装，"启动 MDaemon"开始菜单快捷方式现在将默认打开浏览器到 MDaemon Remote Administration，而不是打开 MDaemon 配置会话。如果您希望更改此设置，请编辑 \MDaemon\App\MDaemon.ini 并设置 [MDLaunch] OpenConfigSession=Yes/No 以及 OpenRemoteAdmin=Yes/No。如果自动生成的 URL 不起作用或 MDRA 在外部 Web 服务器中运行，请设置 *Remote Administration URL* (位于设置 » Web & IM 服务 » Remote Administration » Web 服务器 294)。如果无法确定运作的 URL，则将打开 "配置会话"。最后，在 Windows 开始菜单下的 MDaemon 程序组中，现在提供有快捷方式转至 *"打开 MDaemon 配置会话"*和 *"打开 MDaemon Remote Administration"*。

Webmail改进

- Webmail用户启用其 *"显示已保存搜索文件夹"*这个选项时(位于 "选项 » 文件夹"下的 Webmail)，现在将询问用户他们是否希望将 "全部未读"和 "全部标记"这两个保存搜索文件夹添加到其列表中。他们只会在其首次登录时被问到一次。如果用户选择 "否"，他仍然可以通过点击 *"创建全部未读已保存搜索"*和 *"创建全部标记已保存搜索"*按钮 (也位于 "选项 » 文件夹"下)来手动创建这些已保存搜索。通过添加 DefaultSavedSearchesCheck=Yes (位于 [Default:UserDefaults] 下，在 MDaemon\WorldClient\Domains.ini 文件中)，管理员可以阻止 Webmail 询问用户是否希望创建这些搜索。
- 已修改一些 *WorldClient* 主题图标来使其更易查看。
- 会话到期时向浏览器选项卡标题添加 "(EXPIRED)"，这样如果用户不在 Webmail 选项卡中，则用户仍将知道会话已过期。
- 已添加删除图标，用于从自动填充列表中删除常用联系人。

MDaemon 18.5 新功能

签名宏 110

MDaemon 签名现在支持将发件人的联系信息插入签名的宏，该签名取自位于其域的公共联系人文件夹中的发件人联系人。这允许使用发件人的信息对默认和域签名进行个性化。例如 $CONTACTFULLNAME$ 插入发件人的全名，$CONTACTEMAILADDRESS$ 插入发件人的邮件地址。使用 Webmail、MDaemon Connector 或 ActiveSync 来编辑公共联系人。如果发件人不存在联系人，则使用空值。在默认签名 110 页面列出了可用宏。

用户也可以通过使用 $SYSTEMSIGNATURE$ 宏放置默认/域签名，并使用 $ACCOUNTSIGNATURE$ 放置账户签名来控制 MDaemon 签名在其邮件中的位置。

Webmail中的MDaemon即时通讯

WorldClient和LookOut主题现在具有基于浏览器的XMPP客户端，无需运行MDaemon Instant Messenger桌面应用程序或其他一些XMPP客户端应用程序即可让用户进行即时通讯。用户可以从Webmail的"选项 | 个性化"屏幕通过使用"在浏览器中启用MDaemon的即时通讯功能"这个选项来启用该功能。管理员可以使用"域管理器"(按域)、"账户编辑器"(按账户)或"群组管理器"(按组)来启用或禁用即时通讯。

MDaemon包括一个新的BOSH服务器来支持Webmail中的即时通讯。现在可以从XMPP屏幕312配置其设置(18.5.1的新功能)。

从"位置屏蔽"中免除Webmail

在Webmail中添加了用户选项，以便从"位置屏蔽"中免除"双重身份验证"登录。如果用户设置BypassLocationScreeningTFA=Yes(位于[User]部分，在User.ini文件中)，则为该用户启用"双重验证"并绕过"位置屏蔽"。这允许用户在通常被"位置屏蔽"阻止的国家/地区登录Webmail。

已改善AD集成

如果在\MDaemon\WorldClient\Domains.ini中启用了"AllowADPasswordChange"设置，其账户被设置成使用"活动目录"(AD)验证的用户现在可以在Webmail中更改其AD密码。默认情况下禁用此项。

MDRA扩展

MDaemon的Remote Administration (MDRA) web界面已得到扩展，包括对于许多功能的访问，这些功能以前只能使用MDaemon的图形用户界面进行管理。

MDaemon 18.0新功能

DNSSEC495

新的DNSSEC(DNS安全扩展)选项允许MDaemon充当非验证安全感知存根解析程序的作用，这在4033和4035作为"发送DNS查询、接收DNS响应、并能与与认知安全的递归命名服务器建立合适的安全通道的实体，该服务器代表认知安全的存根解析程序提供这些服务"。这意味着，在MDaemon的DNS查询过程中，您可以向DNS服务器请求DNSSEC服务，在查询中设置AD(真实数据)位并在并在回应中进行检查。这可以在DNS过程中为某些邮件提供额外的安全级别，但不是全部邮件，因为DNSSEC尚不受所有DNS服务器或所有顶级域名的支持。

启用时，DNSSEC服务仅适用于符合您选择标准的邮件；它可以根据您的选择广泛或狭义地请求或要求。只需指定您在DNSSEC屏幕上选择的任何"报头值组合即可，每当执行DNS查询时，MDaemon都将为符合该标准的任何邮件请求DNSSEC服务。当DNS结果未包含验证数据时，则不会产生负面后果；MDaemon只是回退到常规的DNS行为。如果您希望为某些邮件*"请求"*DNSSEC，则将"安全"添加到报头/值组合(例如"To *@example.net SECURE")。对于这些邮件，当DNS结果无法包含验证的数据，会将该邮件退回发件人。**请注意：**因为DNSSEC查找需要更多时间和资源，而且并非所有服务器都支持DNSSEC，因此默认情况下，MDaemon未配置成将DNSSEC应用于每封邮件传递。不过如果您希望为每封邮件请求DNSSEC，您可以在条件中包含"To *"来实现这点。

AntiVirus 邮箱扫描

新的 *"每隔 [n] 天扫描所有邮件"*选项位于 "安全 » AntiVirus 558"屏幕，用于定期扫描所有存储的邮件，以便在病毒定义更新可用之前检测可能已经通过系统的任何受感染的邮件来进行捕获。受感染的邮件将被移至隔离文件夹并添加 X-MDBadQueue-Reason 报头，因此在 MDaemon 中查看时您可以看见相关说明。不会隔离无法扫描的邮件。还有一个 *"配置邮箱扫描"*选项，可以扫描您希望扫描邮件的频率，以及您是希望扫描所有邮件还是只扫描那些小于特定天数的邮件。您也可以立即手动运行邮箱扫描。

从位置屏蔽免除已知的 ActiveSync 设备

启用新的从位置屏蔽免除 388这个选项 (位于 ActiveSync 客户端的设置屏幕)允许您将设备绕过位置屏蔽 477。这使得有效的用户有可能通过 ActiveSync 继续访问他或她的账户，例如当前往一个阻止验证尝试的位置时。为了免除设备，它必须使用 ActiveSync 在配置的时间范围内进行连接和验证，请在位于 "微调"屏幕的这些天后删除闲置的客户端 351这个设置中进行配置。在从 "位置屏蔽"免除设备时，还可以选择将其连接的远程 IP 地址列入白名单。这对允许其他可能从相同 IP 地址连接的客户端很有用。

新的 Webmail 和 MDRA 功能

记住我

您现在可以将 "记住我"勾选框添加到 MDaemon Webmail 和 MDaemon Remote Administration (MDRA) 的登录页面，可以分别通过位于 Webmail 设置屏幕 289和 MDRA Web Server 屏幕 294的选项来实现。启用此选项后，通过 https 端口登录的用户将看到这个勾选框。如果用户在登录时勾选此框，则将为该设备记住其凭证。然后，无论他们何时使用该设备连接到 Webmail 或 MDRA，他们都将自动登录，直至他们手动注销其帐户或其 "记住我"令牌过期。默认禁用 *"记住我"*选项，并应用至您的所有域。如果您希望为特定的 Webmail 域覆盖此设置，请使用 *"记住我"*设置，位于 MDaemon 桌面界面 "域管理器"的 Webmail 屏幕 160。

默认情况下，用户的凭证将在被强制再次登录之前记住 30 天，但您可以使用 *"这些天后过期记住我令牌"*这个选项 (位于 MDRA) 来指定不同天数。您可以将此选项设置成最大值 365 天。**请注意：**双重验证 603 (2FA) 拥有其自身的 "记住我"键值 (TwoFactorAuthRememberUserExpiration=30)，位于 [Default:Settings] 部分，Domains.ini 文件，位于 \MDaemon\WorldClient\ 文件夹。因此，当 2FA 记住我令牌过期时，即使常规令牌仍然有效，登录时也需要 2FA。

在 MDRA 中也有一个 *"重置记住我"*按钮，如果您怀疑账户可能存在安全漏洞，则可以使用此项。这会重置所有用户的记住我令牌，导致他们必须重新登录。

邮件延后

在 MDaemon Webmail 中，您现在可以在邮件列表中延后电子邮件。当邮件被延后时，它会在指定的时间内对用户隐藏。要延迟邮件，请右键点击此邮件，并在上下文菜单中选择 "延迟..."。然后选择您希望延后邮件的时间。"选择日期和时间"选项仅适用于支持日期和时间输入的浏览器。在 LookOut 主题中，通过点击工具栏中的 "查看延迟邮件"图标可以查看隐藏的邮件，在 WorldClient 主题中，请从工具栏中的视图下拉菜单中选择 "查看延迟邮件"。默认情况下启用此功能。要关闭该功能，请转到 "选项 | 个性化"，并找到收件箱设置。然后取消勾选 "启用消息延后"选框。在 Lite 和 Mobile 主题中没有延迟控件，但仍然隐藏延迟的邮件。

公共日历

在 MDaemon Webmail 中，用户可以将日历发布到可公开访问的链接。向用户提供选项，通过密码来保护日历。要发布日历，请在 LookOut 或 WorldClient 主题中，转到 "选项|文件夹"，并点击您想要发布的日历附近的 "共享文件夹"按钮。然后在对话框中，打开 "公共访问"选项卡，并按需填写显示名称或要求密码，然后点击 "发布日历"按钮。将显示确认对话框来告诉用户即将发生的情况。点击 "确定"后，警报将显示日历可用的新 URL。日历发布后，页面上也会显示链接。要取消发布日历，请点击 "取消发布日历"按钮。要更改密码或显示名称，请点击 "更新"按钮。

如果您希望全局禁用此功能，请将 EnablePublicCalendars 键值更改成 **No**，这位于 [Default:Settings] 部分，来自 Domains.ini 文件。要按用户禁用此项，请将 CanPublishCalendars=No 添加到用户的 User.ini 文件。

MDaemon 17.5 新功能

位置屏蔽 477

"位置屏蔽"一种基于地理位置的阻止系统，允许您阻止尝试从全球未经授权的区域建立的入站 SMTP、POP、IMAP、WorldClient、ActiveSync、AutoDiscovery、XML API、Remote Administration、CalDAV/CardDAV、XMPP 和 Minger 连接。MDaemon 确定与连接 IP 地址关联的国家，然后阻止该连接（如果来自受限位置），并向屏蔽日志添加一行信息。对于 SMTP，"位置屏蔽"可以选择性地阻止使用 AUTH 的连接。例如，如果您在特定国家/地区没有用户，但仍然希望能够接收来自此处的邮件，则该功能非常有用。这样您只会阻止那些试图登录到您服务器的尝试。

\MDaemon\Geo\ 文件夹包含作为主要国家 IP 数据库的数据库文件。这些文件由 MaxMind (www.maxmind.com) 提供并能按照您的需求从其站点下载更新。

针对所有协议和服务的动态屏蔽 510

MDaemon 的 "动态屏蔽"系统已被大幅度扩展，能够适用于 SMTP、POP、IMAP、Webmail、ActiveSync、AutoDiscovery、XML API、Remote Administration、CalDAV/CardDAV、XMPP 和 Minger。所有这些服务都会跟踪身份验证失败，并且所有 IP 地址都可以进行阻止。"动态屏蔽"可以在 "安全"菜单下新增的多标签对话框中进行配置。

PIM 附件

PIM（日历、联系人、任务和便笺）项目现在支持附件。可以通过 Webmail、Outlook Connector 或 CalDAV/CardDAV 将附件添加到 PIM 项目中。安排会议时，任何附件都将被发送给与会者。

SMTP 期间的 PGP 密钥交换 527

MDPGP 对话框包含一个新选项，帮助您启用公钥自动传输作为 SMTP 邮件投递过程的一部分。为此，MDaemon 的 SMTP 服务器将准许名为 RKEY 的 SMTP 命令。将电子邮件发送到支持 RKEY 的服务器时，MDaemon 将提供发送者当前首选的公钥发送给其他主机。该主机将响应，表明它已经拥有该密钥（"250 2.7.0密钥已知"）或者需要该密钥，在这种情况下密钥立即以 ASCII 形式传输（"354 Enter"键，以 CRLF.CRLF"结尾）就像电子邮件。不会传输过期或撤销的密钥。如果 MDaemon 有多个发件人的密钥，它始终会发送当前标记为首选

的密钥。如果没有首选密钥，则发送找到的第一个密钥。如果无有效密钥则不进行任何操作。只提供属于本地用户的公共密钥。

公共密钥传输是作为投递用户邮件的 SMTP 邮件会话的一部分发生的。为了接受以这种方式传输的公共密钥，它必须和由密钥持有者属于的域进行 DKIM 签名 445 的邮件一起发送，其中将 i= 设置成密钥持有者的地址，而且必须准确匹配 唯一的发件人报头地址。"密钥持有者"取自密钥本身。此外，该邮件必须从发件人的 SPF 地址 440 中的主机抵达。最后，通过向 MDPGP 规则文件添加一个适当的条目 (说明在这个规则文件中)，必须为 RKEY 授权密钥持有者 (或其整个域，通过使用通配符)，指示该域可以被信任用于密钥交换。上述检查都将为您自动完成，不过您必须启用 DKIM 442 和 SPF 验证 440，否则无法有效完成这些步骤。

MDPGP 日志显示导入或删除的所有密钥的结果和详细信息，SMTP 会话日志也跟踪此活动。该进程跟踪现有密钥的删除和新的首选密钥的选定，并在这些事件发生变化时更新其发送邮件的所有服务器。

为 Outlook Connector 用户管理 Outlook 插件 340

使用 OC 客户端设置对话框中新的"插件"屏幕，您可以管理由您 Outlook Connector 用户使用的 Outlook 插件的状态。您可以允许任何或全部插件被正常使用，或者禁用任何您选择的插件。当您知道与 Outlook Connector 客户端发生冲突的特定插件时，此功能可能特别有用，从而允许您禁用该插件来避免问题。上述插件功能需要 Outlook Connector 5.0 或更高版本。

Webmail 变更

导入/导出群组/分发列表

在 LookOut 和 Webmail 主题中，已向 WorldClient 联系人文件夹中的导出和导入群组/分发列表新增一个选项。由于 Outlook 不支持导出和导入群组，该格式是 MDaemon Webmail 的特定格式。格式如下所示：

列：群组 GUID、群组名称、**GUID**、全名、电子邮件

包含群组名称或群组 GUID 的每一行被视为新群组的开头。该行上的任何 GUID、全名或电子邮件被视为这个群组/列表的第一个成员。

Excel 中的示例：

群组 GUID	群组名称	**GUID**	全名	电子邮件
	Jedis		Anakin Skywalker	ani@jedi.mail
			Leia Organa	leia.organa@jedi.mail
			Luke Skywalker	luke.skywalker@jedi.mail
			Yoda	yoda@jedi.mail
	Siths		Darth Maul	darth.maul@sith.mail
			Darth Vader	darth.vader@sith.mail
			Emperor Palpatine	emperor.palpatine@sith.mail

在导入时，会将群组 GUID 替换为新生成的 GUID。如果未包含群组名称，则该名称不会转译，显示为 "ImportedFromCSV_%GUID%"，其中 %GUID% 被替换为 GUID 的前五个字符。将群组名称右侧的单元格留空，将导致下一行是群组/列表的第一个成员。电子邮件字段是添加成员所必需的。

录音机
已向 Lookout 和 WorldClient 主题添加录音机功能。此功能需要麦克风，而且仅适用于特定的浏览器。管理员可以通过向 User.ini 文件添加 EnableVoiceRecorder=No 来按用户禁用此功能。用户被限制为录制五音轨，每轨五分钟。尝试在"录音机"会话中录制超过五轨将导致所选录音或第一个录音被新录音替换（将提示用户）。录音停止（自动或由用户停止）后，会将音轨转换为 mp3，并上传到服务器。对于每个音轨，用户都有四个选项：

- 保存到桌面
- 保存到默认的 WorldClient 文档文件夹
- 使用只包含收件人、抄送、密送、主题和纯文本邮件正文的快速对话框来发送邮件。

  只需填写收件人。当用户未输入主题或邮件正文时，将使用常规的主题和邮件正文短语。
- 打开附加音轨的新建编写视图

用户一次只能处理一个音轨。例如，只有一个音轨可以被附加到邮件中。如果用户想要将多个音轨附加到邮件中，则需要将每个录音保存到默认文档，并从那里进行附加。

新建文件夹管理功能
LookOut 和 WorldClient 主题在"选项 » 文件夹"视图和主文件夹列表视图中拥有新的文件夹管理功能。

在文件夹列表视图中（左窗格）：

- 用户可以通过拖放来将文件夹从一个父文件夹移至另一个。
- 用户还能通过再次点击它们（选定文件夹后立即操作）来重命名文件夹、为收藏夹添加昵称。
- 现在 LookOut 主题中提供按类型显示文件夹功能
- 如果已存在至少一个收藏夹文件夹（因为在添加了一个收藏夹后隐藏的收藏夹才进行显示），用户可以通过将文件夹拖放至收藏夹来进行添加（将文件夹拖出收藏夹将没有任何效果）。
- 已向 LookOut 主题添加了新建文件夹和重命名文件夹对话框

在"选项 » 文件夹"视图中，现在可以折叠文件夹树型图，而且已将"新建文件夹"对话框移至外部窗口，就和 WorldClient 主题一样。

MDaemon 17.0 新功能

XMPP 支持，用于 WorldClient Instant Messenger (WCIM)

WCIM 现在使用 XMPP 协议来进行即时通讯，而不是 WorldClient 的专属协议。这允许 WCIM 桌面客户端不仅能与其他 WCIM 客户端通信，还能与连接至 MDaemon 的 XMPP 服务器的任何第三方 XMPP 客户端（包括移动客户端）通信。此外 WCIM 现在拥有两种类型的连接："WCMailCheck"和 "WCIMXMPP"。"WCMailCheck"连接至 WorldClient，用于新的邮件通知和邮件计数。"WCIMXMPP"连接至 XMPP 服务器，用于即时通讯。因此，WCIM 用户现在将在客户端的连接屏幕（例如 "Example.com Mail"和 "Example.com WCIM"）上列出每种连接类型的条目。在更新至版本 17 时，WCIM 会将 IM 联系人从旧系统自动迁移至 XMPP，并创建一个 WCIMXMPP 账户。新的 WCIM 客户端的外观和风格在本质上时相同的，但存在一些差异，例如联系人和群聊等的管理方式。请参阅 WCIM 客户端的 "帮助"系统来了解有关变更的更多信息。

WorldClient Dropbox 集成

WorldClient 提供针对 Dropbox 的直接支持，允许用户将文件附件保存到其 Dropbox 账户，并在外发邮件中插入转至 Dropbox 文件的直接链接。要向您的 WorldClient 用户提供此功能，您必须 将WorldClient 设置为 Dropbox 应用程序，设置页面位于Dropbox 平台。这是一个简单的操作过程，您只需登录 Dropbox 账户，为具有 Dropbox 完全访问权限的应用程序创建唯一名称，指定重定向到 WorldClient 的 URI，并更改一个默认设置即可。然后，您将 Dropbox "应用密钥（app key）"和 "应用密码（app secret）"复制并粘贴到 MDaemon 中的 Dropbox 屏幕上即可。之后，当用户下次登录 WorldClient 时，您的用户将能够将其 Dropbox 账户与W orldClient 建立连接。有关如何创建 Dropbox 应用程序并将其链接到 WorldClient 的逐步说明，请参阅：创建和链接您的 Dropbox 应用.

当您创建 Dropbox 应用程序时，它最初将具有 "开发"状态。这允许多达500个 WorldClient 用户将其 Dropbox 账户链接到该应用。根据 Dropbox 的说法，"一旦您的应用程序链接了50个 Dropbox 用户，在您的应用程序能够链接其他 Dropbox 用户的功能被冻结之前，您将拥有两个星期的时间来申请并获得 "生产"状态许可，无论你的应用已经链接了多少用户（0到500）。"这就意味着，在收到 "生产"许可之前，Dropbox 集成将继续工作，但没有额外用户能够链接其账户。获取生产许可是一个简单的过程，以确保您的应用符合 Dropbox 的指南和服务条款。要了解更多信息，请参阅 "生产许可"部分，位于 Dropbox Platform 开发人员向导.

一旦您的 WorldClient 应用程序被正确创建和配置，每个 WorldClient 用户登录到 WorldClient 时，都可以选择将他们的账户连接到其 Dropbox 账户。用户需要登录到 Dropbox，并授予该应用访问 Dropbox 账户的权限。然后，该用户将使用在认证过程中传递给 Dropbox 的 URI 重定向回 WorldClient。为了安全起见，URI 必须与您指定的重定向 URI 之一相匹配，在 Dropbox.com 的应用信息页面指定。最后，WorldClient 和 Dropbox 将交换访问代码和访问令牌，这允许 WorldClient 连接到用户的 Dropbox 账户，以便用户可以在其中保存附件。交换的访问令牌每隔七天到期，这就意味着用户必须重新授权该账户才能使用 Dropbox。用户还可以手动将其账户从 Dropbox 断开，或者在必要时从 WorldClient 中的 Cloud Apps 选项屏幕重新授权。

通过 PowerShell脚本集成 Let's Encrypt

要支持 SSL/TLS and HTTPS for MDaemon、WorldClient & Remote Administration，您需要 SSL/TLS 证书。证书是由证书颁发机构（CA）颁发的小型文件，用于向客户端或浏览器验证与预期服务器建立的连接，并启用SSL／TLS／HTTPS 来保护与该服务器的连接。Let's Encrypt 是一个证书颁发机构，通过专门设计的自动化流程来

为“传输安全层 (TLS)”加密提供免费的证书，该流程使您可以免于现在复杂的手动创建、验证、签名、安装和续订用于保护网站安全的证书。

支持使用 Let's Encrypt 的自动化流程来管理证书，MDaemon 包含一个 PowerShell 脚本，位于“MDaemon\LetsEncrypt”文件夹中。ACMESharp 模块是该脚本的从属文件，需要 PowerShell 5.1 和 .Net Framework 4.7.2，这就意味着该脚本不适用于 Windows 2003。此外，WorldClient 必须监听 80 端口，否则无法完成 HTTP 挑战，该脚本也无法起作用。您需要正确设置用于 PowerShell 的执行策略，它才允许您运行这个脚本。运行该脚本将使一切为 LetsEncrypt 准备就绪，包括将一些必要的文件放置在 WorldClient HTTP 的目录中来完成 http-01 挑战。它将 SMTP 主机名 151 (属于默认域 149)用作证书域，检索证书，将其导入 Windows，并配置 MDaemon 如何使用该证书。

如果您默认域的 FQDN 151 设置不指向 MDaemon 服务器，此脚本将无法有效工作。如果您要在证书中设置备用主机名，可以通过在命令行中传递备用主机名来实现。

使用示例：

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

您无需在 AlternateHostNames 列表中包含用于默认域的 FQDN。例如，您的默认域“example.com”被配置成使用“mail.example.com”的 FQDN。您使用“imap.example.com”的备选主机名称。在您运行这个脚本时，您只需传递“imap.example.com”作为备选主机名称。此外，如果您传递了备选的主机名称，将为各个名称完成 HTTP 挑战。如果未完成全部挑战，将无法正确完成这一步。如果您不需要传递备选的主机名称，就不要在命令行中包含 -AlternateHostNames 这个参数。

如果您正在通过 IIS 运行 WorldClient，您需要使用 -IISSiteName 这个参数来为脚本传递您的站点名称。您必须安装 Microsoft 的 Web Scripting 工具，以便在 IIS 中自动设置该证书。

最后，该脚本将在名为 LetsEncrypt.log 的“MDaemon\Logs\”目录中创建一个日志文件 LetsEncrypt.log。在每次运行该脚本时将删除并重新创建这个日志文件。该日志包含脚本的启动日期/时间，但不包含每个操作的日期/时间戳。在发生错误时，会发送通知邮件。这通过使用由 PowerShell 自动创建和设置的 $error 变量来完成。如果您不想在发生错误时发送电子邮件通知，请勿在命令行中包括 -To 参数。

用来保存使用不可逆加密的邮箱密码的选项

新增密码选项 717 来保存使用不可逆加密的邮箱密码。此项保护密码不被 MDaemon、管理员或可能存在的攻击者解密。启用此项时，MDaemon 使用 bcrypt 密码散列函数。它允许更长的密码 (长达 72 字符)，而且在导出和导入账户时将保留密码，并防止密码泄露。不兼容一些取决于 MDaemon 是否能够解密密码的功能 (例如 APOP & CRAM-MD5 验证和弱密码检测)。默认情况下，启用不可逆密码。

ActiveSync 客户端批准

提供一个新的 ActiveSync 设置，可用于要求“新建客户端必须经过管理员的授权才能同步”。客户端 388 列表指示任何等待授权的客户端，管理员可以从同一屏幕为其授权。全局 353 和账户 643 客户端设置屏幕都提供这个选项。默认情况下，禁用全局选项为关闭，账户选项被设置为“继承”。

ActiveSync 通知

ActiveSync 已添加两种类型的管理通知：同步回滚通知和邮件受损通知。

同步回滚通知

如果客户端在同步操作中重复/频繁地发送过期的同步密钥，ActiveSync Service 现在可以告知管理员这个事件。

这些通知仅告诉管理员：因为客户端使用最近过期的同步密钥发出同步请求，致使服务器为给定的集合发送回滚。通知的主题为 "ActiveSync 客户端使用过期的同步密钥"。发生这个问题的原因可能是网络问题，或者之前发送至这个集合中的客户端的内容存在一些问题。在某些情况下，取决于之前的集合同步是否发送了任何项目，那里将存在一些项目 id。

回滚警报不表示客户端没有同步，而是意味着客户端可能无法完成同步，而且我们的内部系统已检测到这个可能性。为集合发出的回滚警告的频率不超过 24 小时。可以在 \MDaemon\Data\AirSync.ini 文件中的 [System] 报头下编辑以下键值：

- [System] SendRollbackNotifications=[0|1|Yes|No|True|False] (默认值是禁用)
- [System] RollbackNotificationThreshhold=[1-254]：在将通知发送至管理员之前，在给定的集合上必须发生的回滚数量。我们建议此处的值至少是 5，因为这里会存在一些网络问题。(默认值是 10)
- [System] RollbackNotificationCCUser=[0|1|Yes|No|True|False]：是否抄送给客户端发送了过期同步密钥的用户。(默认值是禁用)

ActiveSync 邮件受损通知

如果无法处理特定的邮件，ActiveSync Service 现在可以告诉管理员这件事。这些邮件都是实时发送的，以便通知管理员无法解析邮件项目，因此关于该项目的后续操作无法执行。这些邮件的主题为 "受损邮件通知"。这些项目在早期版本中会导致软件崩溃。在大多数情况下，msg 文件的内容不会是 MIME 数据。不过如果它是 MIME 数据，便可能受损。您可以使用 CMNCCUser 键来选择将这些通知抄送给受影响的用户，这样他们便能知道抵达他们邮箱的邮件不可读。对于这些邮件采取的适当措施应为移动用户邮箱中指定的 msg 文件，并对其进行分析来确定无法解析的原因和造成其处于这种存在状态的原因。可以在 \MDaemon\Data\AirSync.ini 文件中的 [System] 报头下编辑以下键值：

- [System] SendCorruptMessageNotifications=[Yes|No|1|0|True|False] (默认值是启用)
- [System] CMNCCUser==[0|1|Yes|No|True|False] (默认值是启用)

MDaemon 16.5 新功能

MDPGP 改善 527

密钥服务器支持

WorldClient

WorldClient 现在可以用作基本的公共密钥服务器。启用新的 MDPGP 选项来 *"通过 HTTP (WorldClient) 发送公共密钥"*，然后 WorldClient 将准许用于您用户公共-密钥的请求。创建请求的 URL 格式如下所示："http://<WorldClient-URL>/WorldClient.dll?View=MDPGP&k=<Key-ID>"。其中 <WorldClient-URL> 是转至您 WorldClient 服务器的路径 (例如 "http://wc.example.com")，<Key-ID> 是您所需密钥的长度为 16 个字符的密钥 id (例如 "0A1B3C4D5E6F7G8H")。密钥 id 由密钥指纹的最后 8 个字节构成 - 总共 16 个字符。

DNS (PKA1)

如果您希望 MDPGP 通过使用 PKA1 的 DNS 来查询邮件收件人的公共密钥，请启用新的 MDPGP 选项来 *"从 DNS (pka1) 收集公共密钥并缓存 [xx] 小时"*。这非常有用，因为它自动处理获取一些收件人的公共密钥，防止您或您的用户为了发送加密邮件而不得不手动获取和导入这些密钥。在进行 PKA1 查询时，将立即收集和验证找到的任何密钥 URI，并将其添加到密钥环。使用上述方式成功收集和导入密钥环的密钥将在达到此项中指定的小时数后，或按照引用它们的 PKA1 记录的 TTL 值 (这些值更大)来自动过期这些密钥。

密钥处理

跟踪密钥

MDPGP 现在始终按其主要的密钥 id 来跟踪密钥，而不是有时按密钥 id 有时按子密钥 id。因此，清理了 MDPGP 对话框的密钥列表，以便删除不必要的两栏。此外，MDPGP 现在更严格地控制其 "导出"文件夹的内容。您将始终在那里找到导出的本地用户密钥的副本。即使加密了私人密钥，为了获得更多安全性，您应该使用 OS 工具来保护这个文件夹 (以及整个 PEM 文件夹结构)免受未经授权的访问。

首选密钥

以前在密钥环中找到用于同一个邮件地址的多个不同密钥时，MDPGP 将使用它找到的第一个密钥加密邮件。现在您可以右键点击任何密钥并将其设置为首选密钥，在 MDPGP 找到多个密钥时，它将使用这个密钥。如果未声明首选密钥，MDPGP 将使用找到的第一个密钥。在解密一封邮件时，MDaemon 将尝试每一个密钥。

禁用密钥

现在将在名为 oldkeys.txt 的新文件中跟踪被禁用和检测到的密钥。以前在 plugins.dat 这个文件中跟踪被禁用的密钥。

MDPGP 签名验证

MDPGP 现在可以验证在未被加密的邮件内找到的内嵌签名。以前直到加密和签署了这封邮件，MDPGP 才能实现这点。现在在 WorldClient 中查看一封含有已验证签名的邮件时，将显示一个新图标来指示签名已受过验证。默认情况下为所有非本地用户启用签名验证，您也

可以按需指定哪些邮件地址能及不能使用该服务 (请参阅：*"精确配置谁能及不能使用 MDPGP 服务"*，位于 MDPGP 对话框[527])。

XMPP 即时通讯服务器[312]

MDaemon 现在自带 Extensible Messaging & Presence Protocol (XMPP 可扩展消息在线协议) 服务器，有时叫做 Jabber 服务器。这允许您的用户使用第三方 XMPP 客户端 (例如 Pidgin、Gajim、Swift 等) 来收发即时消息。这些客户端适用于大多数操作系统和移动设备平台。MDaemon 的 XMPP 即时通讯系统完全独立于 MDaemon 的 WorldClient Instant Messenger 聊天系统；这两个系统不能相互通信，而且不共享好友列表。

XMPP 服务器作为 Windows 服务安装，而且默认的服务器端口是 5222 (通过 STARTTLS 的 SSL) 和 5223 (专用的 SSL)。如果在 MDaemon 中启用 XMPP 服务器，它将使用 MDaemon 的 SSL 配置。此外，一些 XMPP 客户端为主机名称的自动发现使用 DNS SRV 记录。请参阅 http://wiki.xmpp.org/web/SRV_Records 获取更多信息。

用户通过使用其电子邮件和密码的所选 XMPP 客户端进行登录。不过一些客户端需要将邮件地址划分成单独的组件来进行登录。例如有些客户端不需要 "frank@example.com"，而要求您使用 "frank" 作为登录/用户名，将 "example.com" 用作域。

对于多用户/群聊天服务，客户端通常将其显示成 "房间" 或者 "会议"。当您希望开始一个群聊天会话时，请创建一个房间/会议 (为其命名)，然后邀请其他用户进入这个房间。大多数客户端无需您输入会议的服务器位置，您只需输入会议名称即可。在要求您这么做时，请将 "conference.<your domain>" 用作位置 (例如 conference.example.com)。一些客户端要求您使用以下格式输入名称和位置："room@conference.<your domain>" (例如 Room01@conference.example.com)。

一些客户端 (例如 Pidgin) 支持用户搜索服务，允许您按姓名或邮件地址搜索服务器中的用户，这使联系人的添加更加简便。通常您不必提供搜索位置，不过如被要求，请使用 "search.<your domain>" (例如 search.example.com)。在进行搜索时，可以将 % 符号用作通配符。因此您可以在邮件地址字段中使用 "%@example.com" 来显示邮件地址以 "@example.com" 结尾的所有用户的列表。

OC 客户端设置的集中管理[326]

使用 "OC 客户端设置" 对话框来集中管理您 Outlook Connector 用户的客户端设置。使用您需要的客户端设置来配置各个屏幕，这样 MDaemon 会将这些设置推送到相应的客户端屏幕，每次将一名 Outlook Connector 用户连接到服务器。自上次 OC 客户端连接和接收设置以来，只有在更新和改变设置时，才发送最新设置。如果您启用了提供的选项来 *"允许 OC 用户覆盖推送的设置"* 时，用户可以在其个别客户端上覆盖任何推送的设置。如果禁用了此项，将锁定所有客户端屏幕；Outlook Connector 用户可以不做任何变更。

要允许必须不同于各名用户或域的特定设置，OC 客户端设置支持以下宏，例如 $USERNAME$、$EMAIL$ 和 $DOMAIN$。在将设置推送到一个客户端时，会将这些宏转换成视用户或域而定的数据。注意不要将任何静态值放入应该使用宏的任何字段，例如不要将 "Frank Thomas" 这样的信息放入您的 "姓名" 字段。这会使每名连接到 MDaemon 的 Outlook Connector 用户将其姓名设置成 "Frank Thomas"。方便起见，在常规[328]屏幕上存在一个 "宏引用" 按钮，它显示所支持宏的一个列表。

对于使用 MDaemon Private Cloud (MDPC) 的用户，在域管理器[149]上的另一个 "OC 客户端设置" 对话框用来按域控制 Outlook Connector 客户端设置。

默认情况下禁用此功能，而且该功能仅适用于使用 Outlook Connector 客户端版本 4.0.0 或更高版本。

"发件人："报头保护/修改 473

这个新的安全功能修改入站邮件的 "发件人："报头，来使报头的仅姓名部分包含姓名和邮件地址。这是为了抵御垃圾邮件和攻击中通常使用的策略，即伪装成邮件来自其他人。在显示邮件列表时，邮件客户端通常仅显示发件人的姓名，而不是姓名和邮件地址。要查看邮件地址，收件人必须先打开邮件或采取一些其他操作，例如右键点击条目或将鼠标悬停在姓名上等。出于这个原因，攻击者通常在可见的 "发件人"报头放置合法的人名或公司名称来构建邮件，并隐藏不合法的电子邮件地址。例如，一封邮件的实际 "发件人："报头可以是 "Honest Bank and Trust"<lightfingers.klepto@example.com>，但是您的客户端可能只将"Honest Bank and Trust"作为发件人显示。该功能更改报头的可见部分来显示两部分，其中电子邮件地址优先。在上例中，现在会将发件人显示成 "lightfingers.klepto@example.com -- Honest Bank and Trust"，清楚为您指示这是伪造的欺诈邮件。默认情况下禁用此项，而且仅适用于指向本地用户的邮件。

已改善 IP 屏蔽 468

"IP 屏蔽"现在拥有一个新的 "导入"按钮，您可以使用该按钮来导入 APF 或 .htaccess 文件中的 IP 地址数据。现在 MDaemon 对这些文件的支持包括：

- 支持 "拒绝发件人"和 "允许发件人"
- 只导入 IP 值（非域名）
- 允许 CIDR 表示法，不过不允许部分 IP 地址。
- 每行可以包含任何数量的由空格分隔或逗号分隔的 IP 地址。例如 "deny from 1.1.1.1 2.2.2.2/16"和 "3.3.3.3, 4.4.4.4, 5.5.5.5"等。
- 将忽视由 # 开头的行。

自动安装产品更新 420

利用 "自动更新"功能，您可以配置 MDaemon 在存在针对已安装产品的更新时通知邮件管理员，或者您可以自动下载和安装更新。这包括 MDaemon、SecurityPlus 和 Outlook Connector。可以为各个产品单独控制自动安装更新，每次安装更新后需要重启服务器。在检测到更新时下载安装程序文件，不过将在您指定的时间进行安装和重启。将在 MDaemon 系统日志中记录所有安装活动，并在更新后通知邮件管理员。请参阅更新 420对话框获取更多信息。

WorldClient 变更

类别 288

WorldClient 支持 LookOut 和 WorldClient 主题中的邮件类别。用户可以通过前往 "选项 » 列"并勾选 "邮件列表"部分中的 "类别"来向邮件列表添加 "类别"列。要为一封或多封邮件选择类别，请选择这些邮件并右键点击其中一封。使用上下文菜单来设置类别。

- 管理员可以创建自定义类别。有两种文件用于这个目的：DomainCategories.json 和 PersonalCategories.json。

- 默认情况下全局启用“域类别”。要禁用此项，请打开 MDaemon\WorldClient\Domains.ini，并在 [Default:Settings] 部分将“DomainCategoriesEnabled=”的值从“是”更改成“否”。
- 默认情况下用户可以添加并编辑其自己的类别。如果您希望禁用此项，您可以将“anEditPersonalCategories=”的值从“是”更改成“否”来按用户或全局实现这点。用户选项位于 [User] 部分（User.ini 文件中），全局选项位于 Domains.ini 文件的 [Default:UserDefaults] 部分下。
- 如果启用了“域类别”，而且不允许用户编辑个人类别，则该用户只能看见 DomainCategories.json 中列出的类别。
- 如果禁用了“域类别”，而且不允许用户编辑个人类别，则该用户只能看见 PersonalCategories.json 中列出的类别。
- CustomCategoriesTranslations.json 文件用来支持您多种语言的定制类别名称。向该文件添加任何必要的定制类别翻译，可以使 WorldClient 识别被保存成事件、便笺或任务的类别。

要了解此处提到的这些文件的相关详细信息，请参阅：MDaemon\WorldClient\CustomCategories.txt。

白名单和黑名单 292

默认情况下，您可以为 WorldClient 用户隐藏白名单和黑名单文件夹。要实现这点，请打开 MDaemon\WorldClient\Domains.ini，并在 [Default:UserDefaults] 部分下，将“HideWhiteListFolder=”或“HideBlackListFolder=”的值从“否”更改成“是”。您可以通过编辑 User.ini 文件（位于 [User] 部分下）来为特定的用户隐藏或显示这些文件夹。

检查附件

在 LookOut 和 WorldClient 主题中，现在提供一个选项，如果在邮件的主题或正文中提到附件，则在发送邮件前检查编写完的邮件是否存在附件。这帮助您避免意外发送不含附件的可能存在附件的邮件。

双重验证 603

您现在可以控制是否允许账户使用或要求使用“双重验证”(2FA)。新建账户 672模板上存在两个新选项，用来控制新建账户的默认设置。Web 服务 603屏幕上也提供相应的选项来为个别账户控制 2FA。

MDaemon 16.0 新功能

MDaemon Remote Administration (MDRA) UI 更新

MDRA 的用户界面不再使用框架，而且已将其更新成使用优先响应移动设备的设计。浏览器支持仅限于 IE10+、最新版本的 Chrome、最新版本的 Firefox 和最新版本的 Safari（Mac 和 iOS）。已知在使用 Android stock 浏览器时会发生与滚动相关的问题，不过 Chrome 可以在 Android 设备上流畅运行。

该设计完全基于正在使用的窗口大小。无论用户正在使用手机、平板电脑、还是计算机，相同的窗口大小具有相同的外观。该版本最重要的变更是菜单。宽度小于等于 1024 像素时，将在浏览器的左侧隐藏菜单。可以使用两种方式来显示菜单。如果使用触屏设备，向右滑动

即可显示次级菜单。无论设备是否正在使用，在其左上角还有一个“菜单”按钮，它将显示次级菜单。轻击菜单顶部附近带有左箭头的菜单标题，将显示主菜单。此外，右上角的帮助、关于和注销菜单也将基于屏幕宽度进行变化。屏幕宽度大于等于 768 像素时，将显示文字形式的帮助、关于和注销。屏幕宽度为 481 - 767 像素时，仅显示图标。屏幕宽度小于等于 480 像素时，仅显示一个“齿轮”图标，在点击该图表时将显示一个含有帮助、关于和注销选项的下拉菜单。具有多列的列表视图有一个开/关列的按钮，可以通过点击工具栏最右的灰色向右箭头按钮进行访问。设置页面不再被设计成 MDaemon GUI 的复刻版，而是基于浏览器的宽/高对位置和大小进行了重新设计。

Spam bot 检测 475

名为“Spambot 检测”的新功能跟踪各个 SMTP MAIL（返回-路径）使用了一段指定时间的 IP 地址。如果短时间内数量异常的 IP 地址使用了相同的返回-路径，这就表明 Spambot 网络在作祟。当然这也可能指示邮件系统完全合法的使用（没有应对此功能检测内容的规则）。不过，实验表明只要一直在使用相同的返回路径，该功能便能有效检测分布式 Spambot 网络。如果检测到 Spambot，就会立即断开与其通信的连接，并供您选择是否将返回路径值添加到黑名单长达一段您指定的时间。您还可以选择将所有 Spambot IP 列入黑名单长达一段用户定义的时间。

CardDAV 308

MDaemon 现在支持通过 CardDAV 协议同步联系人。MDaemon 的 CardDAV 服务器允许经过验证的 CardDAV 客户端访问保存在 MDaemon 中的联系人信息。注意，CardDAV 客户端是 Apple Contacts（包含于 Mac OS X）、Apple iOS（iPhone）和 Mozilla Thunderbird（通过 SOGO 插件）。要了解有关 CardDAV 和配置 CardDAV 客户端的更多详细信息，请参阅：CalDAV & CardDAV 308。

面向 WorldClient 和 Remote Administration 的双重验证

MDaemon 现在为登录 WorldClient 或 MDaemon 的 Remote Administration web 界面的用户支持“双重验证”（例如 2-步验证）。通过 HTTPS 登录到 WorldClient 的任何用户可以在“**选项 » 安全**”屏幕上为账户激活“双重验证”。然后用户在登录 WorldClient 或 Remote Administration 时必须输入验证码。可以从安装在用户的移动设备或平板电脑上的验证器应用程序获取该代码。该功能专为支持 Google Authenticator 的任何客户端而设计。

基于 ActiveSync 协议的迁移客户端

MDaemon 现在自带一个基于 ActiveSync 协议的迁移客户端（ASMC.exe）。它支持从支持协议版本 14.1 的 ActiveSync 服务器迁移邮件、日历、任务、便笺和联系人。提供一个单独的文档来说明这一模块的使用。可以在 \MDaemon\Docs 文件夹中找到。

XML API 用于大量管理任务

MDaemon 现在自带基于 API 通过 http(s) 的 XML。因此，现在可以在能够向服务器发出 http(s):// 发送请求的任何平台上使用任何语言来写入 MDaemon 管理客户端。在 MDaemon Pro 中，只对已验证的全局管理员提供此功能，而在 MDaemon Private Cloud 中，已验证的域管理员也能进行一部分可用操作。这个 API 还生成一个网站，其中含有关于 API 规范的文档。安装默认值将其安装在 http://servername:RemoteAdminPort/MdMgmtWS/，不过出于额外安全性，可以将其设置成任何 url。

可用操作包括：

- 帮助
- CreateDomain
- DeleteDomain
- GetDomainInfo
- UpdateDomain
- CreateUser
- DeleteUser
- GetUserInfo
- UpdateUser
- CreateList
- DeleteList
- GetListInfo
- UpdateList
- AddDomainAdministrator
- DeleteDomainUsers
- GetDomainList
- GetVersionInfo
- GetQueueState
- GetServiceState
- SetAddressRestriction
- GetAddressRestriction

现在，已使用 Javascript、Powershell、VBScript、C、C++ 和 VisualBasic 语言对命令行管理客户端进行了写入/测试。简单的 HTML 和 Javascript 测试站点被用作基于 web 的管理控制台的概念验证，可以在若干主流浏览器中有效运作。虽然这款 API 还未经测试，不过完全可以预期它能与使用 PHP、Perl和其他开发平台的 web 服务器顺利协作。

还请参阅：

介绍 14
升级到 MDaemon 23.0.2 50
MDaemon 的主界面 58

1.4 升级到 MDaemon 23.0.2

以下是您将 MDaemon 从之前的版本升级到版本 23.0.2 时，可能需要特别考虑与注意的事项列表。要了解 MDaemon 23.0.2 中有关新增功能、变更和修复的完整说明，请参阅 RelNotes.html (位于 MDaemon 的\Docs\子文件夹)。

版本 23.0.2

- 已恢复 Outbreak Protection (爆发保护)功能 Please review your Outbreak Protection settings[535], as they may have been reset to their default values.

版本 23.0.1

- Cyren Anti-Virus 已被 IKARUS Anti-Virus 取代。Cyren 最近在几乎没有提前通知的情况下，宣布停止运营的计划。这就需要我们找到一个新的反病毒合作伙伴。经过彻底的评估，IKARUS 因其出色的检测率和速度而脱颖而出。IKARUS Anti-Virus 每10分钟自动更新一次定义。如果您的 AntiVirus 许可证已过期，则禁用使用 IKARUS 的扫描。
- 已删除 Cyren Outbreak Protection (爆发保护)。Cyren 最近在几乎没有预警的情况下宣布了停止运营的计划。我们正在积极研究和考虑可行的反垃圾邮件技术，作为我们软件产品中现有反垃圾邮件机制的适当补充。
- [26778] IMAP 关键字旗标支持现在可以通过在 \MDaemon\App\MDaemon.ini中设置 [Special] IMAPKeywordFlags=Yes/No 来启用或禁用。默认情况下，当从 23 之前的版本更新 MDaemon 时，将禁用 IMAP 关键字旗标，以避免 Thunderbird 邮件客户端中潜在的邮件标签丢失问题。当 Thunderbird 连接到支持关键字旗标的 IMAP 服务器时，它会使用从服务器读取的标签，覆盖其本地邮件标签，这些标签最初是空白的。默认情况下，对于新安装和从 23.0.0 版本更新时，启用 IMAP 关键字旗标。

版本 22.0.0

- 已弃用 32-位 MDaemon。MDaemon 22.0 和更高版本将仅提供 64 位版本。如果您当前正在我们支持的 64 位操作系统上运行 32 位版本，您只需在现有安装的基础上安装 64 位版本即可。
- 强密码长度最小值[717]必须至少为 8 个字符。如果在更新到 MDaemon 22 之前，将长度最小值设置为少于 8 个字符，它将更改为 8。现在，新安装的强密码的默认长度最小值是 10。
- MDaemon 不再使用 "白名单"和 "黑名单"术语。在大多数情况下，现在它们变成了 "允许列表"和 "阻止列表"。具有用来豁免 IP 和地址等的 "白名单"的功能现在有一个 "豁免列表"。按用户的垃圾邮件过滤器联系人文件夹现在被命名为 "已允许发件人"和 "已阻止发件人"。首次启动 MDaemon 22 时，将重命名所有账户的文件夹。

版本 21.5.0

- "X-MDOrigin-Country"报头 (位置屏蔽[477]可将其添加到邮件)，现在将包含双字母的 ISO 3166 国家和洲代码，而不是完整的国家和洲名称。请务必更新您可能在此报头中查找特定值的任何过滤器。
- 将 Webmail "Mobile"主题重命名为 "Pro"后，使用 Mobile 主题并启用了 "记住我"选项的用户可能会产生一点副作用。这些用户可能发现他们无法打开附件。要解决此问题，他们必须退出其 Webmail账户，然后重新登录即可。

版本 21.0.2

- 在 "设置 » 首选项 » 其他"页面中，用于将系统生成的所有邮件管理员通知复制到全局管理员和域管理员的设置，现在适用于更多通知，例如 "账户冻结和禁用"、"无此类用户"、"磁盘错误"、"磁盘空间不足"以及 "Beta"和 "AV 过期"。如果您认为管理员不适合接收这些通知，则必须禁用这些设置。

版本 20.0.3

- MDaemon 将移除 "AlertExceedsMax yes"，它位于 ClamAV 的 clamd.conf 文件，原因是它引起太多 "Heuristics.Limits.Exceeded"AV 扫描失败。

版本 20.0.1

- "设置 | 首选项 | Windows 服务"中的网络资源访问设置现在将 MDaemon 服务（以及 Remote Administration 和 XMPP Server 服务）配置成作为指定账户运行，而不是以系统管理员身份运行 MDaemon，然后再以该账户运行特定的进程和线程。当更新到此版本时，安装程序将更新服务来以指定账户运行。
- 由于对 clamd.conf 中的许多设置做出变更，而且不赞成使用，因此安装程序现在将覆盖现有的 clamd.conf。如果您已自定义 clamd.conf，则需要在安装后检查并更改 clamd.conf。

版本 20.0.0

- 请仔细阅读完整的发布说明中标记为任务[8930]的部分，因为其中涉及对 "活动目录"集成系统的更改，并且您可能会发现过去已中断的事情现在可以开始工作。请注意在此部分所做的所有变更，并仔细阅读发布说明的这一部分。请注意在此部分所做的所有变更，并仔细阅读发布说明的这一部分。
- MDaemon 20.0 需要 Windows 7、Server 2008 R2 或 newer。
- "首选项 » 其他[421]"拥有两个新的复选框，用于控制是否应将定期发送给 "Postmaster"（邮件管理员）别名的系统生成的通知电子邮件也发送给全局和域级别的管理员。默认情况下启用这两个选项。域管理员被限制为仅接收针对其域和发行说明的那些电子邮件。全局管理员会收到所有信息，包括队列摘要报告、统计信息报告、发行说明、（对于所有域而言）找到的 "没有此类用户"、磁盘错误通知、账户冻结和禁用通知（与域管理员一样，他们可以取消冻结并重新启用）、有关许可证和测试版本即将到期的警告、"垃圾邮件摘要"报告等。如果您认为管理员不适合接收这些通知，则必须禁用这些设置。
- 自动应答器的存储方式已发生变化。现在将账户自动应答器的文本保存为 OOF.MRK 文件，置于账户的 DATA 文件夹中，该文件夹是账户根邮件文件夹内新的子文件夹。自动应答器脚本文件不再保存在 APP 文件夹中，并且不在账户之间进行共享。首次启动 MDaemon 时，它将把所有现有的自动应答器文件和设置迁移到每个账户的正确位置中。AUTORESP.DAT 文件已过时，而且随每个视账户而定的 .RSP 文件（将保留 OutOfOffice.RSP 和非视账户而定的文件供您参考并作为示例）。如果您希望将一个自动应答器配置快速分配给多个账户，则可以使用新的 "发布"按钮，位于 "账户设置 » 自动应答器[607]"。此按钮会将现有自动应答器脚本文本和当前账户的所有设置复制到您选择的其他账户。此外，编辑自动应答器文件[607]按钮帮助您编辑默认的自动应答器脚本（OutOfOffice.rsp）。此默认值被复制到账户 OOF.MRK，前提是 OOF.MRK 丢失或为空。

- 账户签名文件的存储方式已发生变化。签名文件被另存为 SIGNATURE.MRK，保存在该账户的 DATA 文件夹中，它是该账户根邮件文件夹内一个新的子文件夹。首次启动 MDaemon 时，它将把所有现有的签名文件迁移到每个账户的正确位置中。根 MDaemon 签名文件夹将不再包含特定于账户的签名文件，但仍保留在原处，因为它可能仍包含 MDaemon Administration 和 "内容过滤器"所需的项目。原始的 "签名"文件夹优先于迁移，被备份到 \Backup\20.0.0\Signatures\。最后，会将各个账户的 ADMINNOTES.MRK 从该账户的根邮件文件夹移至新的 DATA 子文件夹。
- 垃圾邮件过滤器 » 白名单（自动）[575] 已将默认值更改成禁用 *"..仅使用 DKIM 进行验证的白名单地址"*这个选项，启用此功能后，对于许多人来说存在些限制，并且阻止地址簿白名单对 MultiPOP 和 DomainPOP 邮件起作用。如果您不喜欢这样，请重新启用此设置。
- 首选项 » UI[411] 选项中用来 *"居中所有 UI 对话框"*的选项已被重置成为所有人 "启用"的默认设置。您可以按需禁用此项。这样可以防止屏幕在创建时超出屏幕范围，但这样做有时会导致难以选择多个重叠的屏幕。
- 安全管理器 » 屏蔽 » 位置屏蔽[477]——已将这个功能的默认值从禁用改为启用。启用 "位置屏蔽"后，即使未阻止特定国家/地区，也将始终记录连接的国家/地区（如果知道）。因此，即使您不想阻止任何国家/地区，也可以启用 "位置屏蔽"（无需选择要阻止的任何国家/地区），以便可以显示和记录国家/地区。由于此设置的默认设置已发生变化，因此您应该查看 "位置屏蔽"配置的正确性。MDaemon 将插入 "X-MDOrigin-Country"报头，其中列出要进行内容过滤或其他目的的国家和地区。
- 已删除垃圾邮件过滤器扫描的 2 MB 硬编码固定大小限制。现在，可以扫描的邮件大小没有理论限制。不过如果这对您而言是个问题，您仍然可以配置你自己的限制，但在此项中使用 "0"表示无限制。您应该审核 "垃圾邮件过滤器 » 设置[584]"屏幕来确保已将此项设置成您需要的值。
- 在主界面的 "队列"屏幕中添加了 "发件人域"和 "收件人域"这两列。因此，必须一次性重置已保存的列宽。一旦您按照自己的喜好设置了列宽，它们就会被记住。
- 默认情况下，"主机屏蔽"现在适用于 MSA 连接。该选项位于：安全管理器 » 屏蔽 » 主机屏蔽[470]。
- 默认情况下，MDaemon IMAP、WebMail 和 ActiveSync 服务器不再提供对已禁用账户的共享文件夹的访问。您可以使用一个位于 "服务器设置 » 公共 & 共享文件夹[97]"的新设置来更改上述配置。

版本 19.5.2

- 已删除 *"允许的 RSET 命令最大值"*这些选项（位于 "服务器设置 » 服务器[74]"屏幕），因为它们是位于 "SMTP 屏蔽[472]"上一些相同功能的重复项，在本质上缺少灵活性。"SMTP 屏蔽"版本是 "动态屏蔽"系统的一部分，它考虑了更多因素（例如，它具有白名单，考虑了身份验证状态等）。已将您的一些较旧的值移至 "SMTP 屏蔽"。请检查这些值来确保其正确性。这些选项（推荐）的正确默认值是：将 *"阻止发送这么多 RSET 的 IP"*设置成 **"20"**，将 *"阻止 IP 后关闭 SMTP 会话"*这个选项设置 "启用/已勾选"。

版本 19.5.1

- 已更新 LetsEncrypt[496] 功能来使用 ACME v2。需要这种更新的原因在于 LetsEncrypt 不再继续支持 ACME v1。现在需要 PowerShell 5.1 和 .Net Framework 4.7.2 在使用 LetsEncrypt。

版本 19.5.0

- 已将一些设置（例如注册密钥）从 \MDaemon\App\MDaemon.ini 移至 \MDaemon\LocalData\LocalData.ini。如果您需要恢复以前的 MDamon 版本，早期版本的安装程序找不到位于新位置的设置，因此要询问您输入注册密钥。可以通过将设置复制回 MDaemon.ini，或先恢复到 MDaemon.ini 的备份版来避免这一点。

版本 19.0.0

- 已扩展 MDaemon 的 Remote Administration (MDRA) web 界面来包括访问以前只能使用配置会话（即 MDaemon 的应用程序界面）管理的功能，现在有几个选项只能通过 MDRA 访问。因此，对于新的 MDaemon 安装，"启动 MDaemon"开始菜单快捷方式现在将默认打开浏览器到 MDaemon Remote Administration，而不是打开 MDaemon 配置会话。如果您希望更改此设置，请编辑 \MDaemon\App\MDaemon.ini 并设置 [MDLaunch] OpenConfigSession=Yes/No 以及 OpenRemoteAdmin=Yes/No。如果自动生成的 URL 不起作用或 MDRA 在外部 Web 服务器中运行，请设置 *Remote Administration URL*（位于设置 » Web & IM 服务 » Remote Administration » Web 服务器 294）。如果无法确定运作的 URL，则将打开"配置会话"。最后，在 Windows 开始菜单下的 MDaemon 程序组中，现在提供有快捷方式转至*"打开 MDaemon 配置会话"*和*"打开 MDaemon Remote Administration"*。
- 已弃用和删除 SyncML。
- MDaemon 的磁盘空间计算在几个地方不一致（例如有时使用 1000，有时使用 1024 字节进行千字节计算）。这已被修复为始终使用 1024。因此，用户的磁盘空间配额值可能与以前的版本略有不同。请检查并做出您认为需要的任何调整（如果有的话）。
- 现在默认启用"仅在发生故障时发送防病毒更新通知 555"这个选项。在更新到 MDaemon 19 时，将在第一次启动 MDaemon 时启用此选项。

还请参阅：

介绍 14
MDaemon 新功能 23.0 16
MDaemon 的主界面 58

1.5 获得帮助

技术支持选项

技术支持是整个 MDaemon Technologies 客户体验的重要部分。我们希望您在首次购买了我们的产品并安装之后就从中获得最大收益，我们也在尽自己的最大努力确保解决所有的问题直到您满意为止。要了解最新的客户服务信息，技术支持选项，自助支持资源，产品信息及更多详情，请访问以下 MDaemon Technologies 技术支持页面，位于：
www.mdaemon.com/support/

MDaemon Beta 测试

MDaemon Technologies 为我们的产品维持活跃的 beta 测试团队。如果您希望加入 MDaemon 测试版团队，请发送电子邮件到 MDaemonBeta@mdaemon.com。

Beta 团队是为那些希望在 MDaemon 软件正式发布之前获得它们并加入其测试的人员成立的；它不是备选的技术支持方案。只有通过以下概述的方法，才能获得 MDaemon 的技术支持：www.mdaemon.com/support/。

联系我们

运营时间
周一至周五上午 8:30 - 下午 5:30，中部标准时间
周末与美国节假日除外
客户服务或销售
美国免税：866-601-ALTN (2586)
国际：817-601-3222
sales@helpdesk.mdaemon.com

技术支持
www.mdaemon.com/support/

培训
training@mdaemon.com

业务发展/联盟
alliance@mdaemon.com

传媒/分析师
press@mdaemon.com

渠道/经销商咨询
请访问渠道伙伴页面了解更多信息。

企业总部

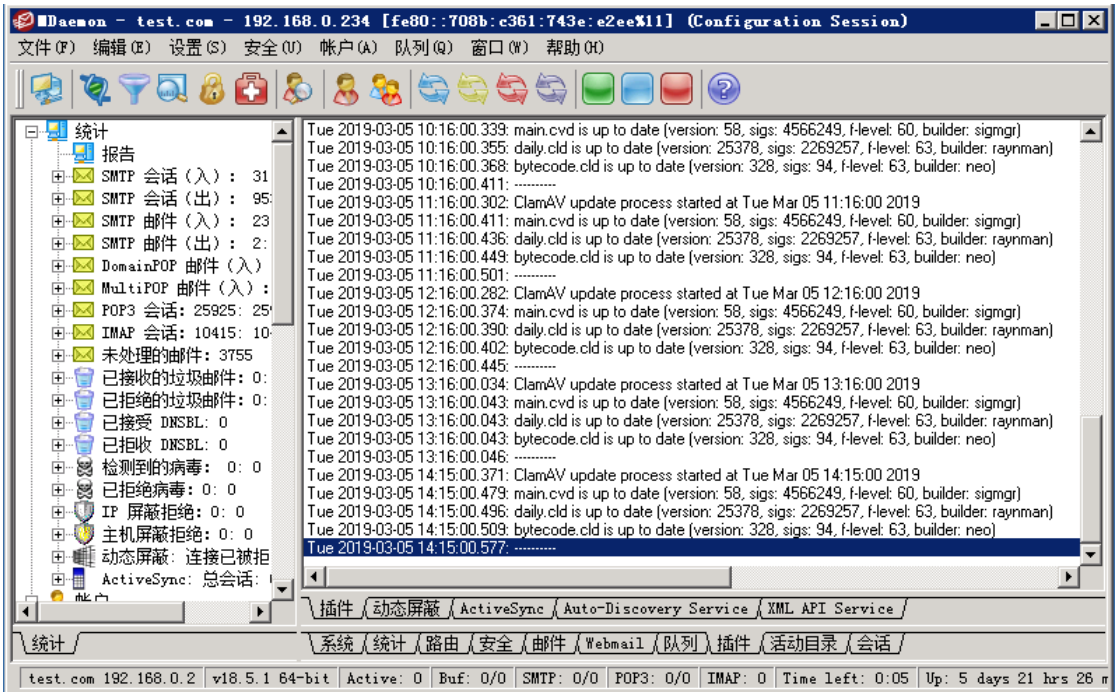
MDaemon Technologies
4550 State Highway 360, Suite 100
Grapevine, Texas 76051
美国免税：866-601-ALTN (2586)
国际：817-601-3222
传真：817-601-3223

商标

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

章节

2 MDaemon 的主界面



MDaemon 的主图形用户界面 (GUI)为您提供关于 MDaemon 的资源、统计、活动会话以及等待处理的队列邮件的重要信息。其中还提供可以轻松激活或关闭 MDaemon 各种服务器的选项。GUI 的选项卡面板帮助您查看服务器及其入站与出站连接的最新执行情况。

统计

默认情况下，统计窗口在 MDaemon 主界面的左窗格中。该窗格包含四个部分：统计、账户、队列和服务器。

"*统计*"部分含有以下统计：包括 MDaemon 收发的邮件数量、POP 和 IMAP 会话数、已接收和拒收的垃圾邮件、以及病毒等。这些统计从 MDaemon 启动时开始计数，还提供右键单击快捷菜单，帮助您清除计数器。

当您点击 "重置根节点计数"选项时，将重置所有计数器，不仅是您右键点击的那个选项。此外，在 "设置» 首选项» GUI"中有一个选项，用于 "*重启后保留根节点邮件计数器*。"否则将重置计数器，不管 windows 是否重启。

"*账户*"部分含有用于 MDaemon、MDaemon Connector 和 ActiveSync 的条目。取决于您的产品许可证，每个条目都列出已用账户数和所剩账户数。

"*队列*"部分含有针对各个邮件队列的条目，以及各个队列所含有的邮件数量 (若存在)。您可以右键点击每个队列条目以打开快捷菜单，其中包含一个或多个以下选项，取决于您所选择的队列：

查看队列——该选项切换主窗口到队列选项卡并显示所选的队列。将显示队列中所有邮件的列表，您可以右键单击任何邮件以打开快捷菜单，其中包含大量选项，与那些在队列与统计管理器中的可用选项类似，例如复制、移动与编辑等等。

队列和统计管理器——打开 "队列"与 "统计管理器"以抵达 "队列页面"，其上会显示所选的队列。

立即处理——该选项 "重新排队"所有在队列中的邮件并尝试将它们处理为正常投递。如果您尝试处理包含在 "保持队列"、"坏队列"或其他类似队列中的邮件，那么这些邮件可能会遇到相同的错误，即将它们置于首位并退回至相同的队列。

冻结/解冻队列——临时停止对所选队列的处理，或如果队列当前处于停止状态那么可以继续进行处理。

释放——从保持队列释放邮件。MDaemon 将忽略遇到的错误信息，尝试投递邮件——即使这些邮件遇到导致它们被移至此队列的原始错误，也不会将它们退回到 "保持队列"。

重新排队——只对 "保持队列"有用，并和以上的 *"立即处理"*具有相同的效果。

启用/禁用队列——启用或禁用 "保持队列"。禁用时，不顾遇到的错误，不会将邮件移动到保持队列。

"*服务器*"部分包含用于 MDaemon 内每个服务器的条目，而且每个条目都列出服务器的当前状态："活动"或者 "闲置"。以下列出的每个服务器的条目用于每个域 (可用时)，以及该服务器或域当前正在使用的端口和 IP 地址。快捷菜单提供控件，用于切换每个服务器的活动和不活动状态。在服务器处于闲置状态时，其图标将变为红色。

事件跟踪与日志记录

主界面上默认的右边窗格包含一组标签，显示 MDaemon 其各种服务器与资源的当前活动和状态，并且它们会被持续地更新以反映当前服务器的状态。一有操作完成，每个活动会话与服务器活动就会被记录到正确的选项卡中。如果您已选择记录那些活动，显示在这些选项卡上的信息会被镜像到日志目录内的日志文件中。

MDaemon GUI 的主窗格中包含以下选项卡：

系统——在启动程序时，"系统"选项卡会显示一个初始化进程的日志，它可以提醒您 MDaemon 的配置或状态可能存在的问题。它还显示活动，例如启用/禁用 MDaemon 的各种服务器。

统计——该标签显示服务器的统计报告，对应包含在各种根节点计数器里的信息，这些根节点计数器在 "统计与工具"窗格中的 "统计"选项卡上。如果您希望更改此报告中的字体或字体大小，您可以编辑 MDaemon.ini 文件中的以下部分：

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

此外，每晚午夜，在内容过滤器的收件人 555 屏幕上列出的 Postmaster 和其他所有地址将通过邮件收到一份报告的副本。这份报告和您使用在 "常规电子邮件控制 754 "中列出的 "状态"邮件命令所生成的报告是一样的。如果您不希望发送这份报告，请禁用 *"在午夜将统计报告发送给邮件主管员"*选项，其位于 "首选项"下的其他 421 屏幕。

路由——显示通过 MDaemon 解析的每封邮件的路由信息 (收件人、发件人、邮件 ID 等等)。

安全——点击此选项卡将在其上显示和安全相关的若干其他选项卡。

内容过滤器——此选项卡列出 MDaemon 的内容过滤器[540]操作。当一封邮件符合某一"内容过滤器"的邮件规则条件时，就会在此处记录这封邮件的相关信息及操作。

AntiVirus——AntiVirus[539]操作都列在这个选项卡上。扫描某封邮件是否存在病毒时，会在此处记录该邮件的相关信息及操作。

反垃圾邮件——显示 MDaemon 的所有垃圾邮件过滤器[564]和拦截活动。

MDSpamD——列出所有 MDaemon Spam Daemon[573]活动。

SPF — 显示所有发件人策略框架[440]活动。

DKIM——列出所有 DomainKeys Identified Mail(域密钥标识邮件)[442]活动。

DMARC——列出所有 DMARC[449]活动。

VBR——该选项卡显示 VBR 证书[460]活动。

MDPGP——该选项卡显示 MDPGP[527]活动。

屏蔽——此选项卡显示缓送[503]与动态屏蔽[472]活动。

验证失败——此选项卡(和相应的日志文件)包含每个失败的 SMTP、IMAP 和 POP 登录尝试的详细条目。该信息包括使用的协议和 SessionID，以便您可以搜索其他日志、违规者的 IP、他们尝试使用的原始登录值(有时是别名)以及与登录匹配的账户(如果没有账户匹配则使用"无")。您可以右键单击此选项卡中的一行，并将违规者的 IP 地址添加到阻止列表中。

MTA-STS — 显示与 SMTP MTA 严格传输安全(MTA-STS)相关的所有活动。

邮件——点击此选项卡会在其上显示若干与邮件相关的其他选项卡。

SMTP(入站)——此选项卡上显示所有使用 SMTP 协议的入站会话活动。

SMTP(出站)——此选项卡上显示所有所有使用 SMTP 协议的出站会话活动。

IMAP——在此选项卡上记录使用 IMAP 协议的邮件会话。

POP3——当用户使用 POP3 协议从 MDaemon 收集邮件时，会在此处记录该活动。

MultiPOP——此选项卡显示 MDaemon 的 MultiPOP 邮件收集活动。

DomainPOP——此选项卡显示 MDaemon 的 DomainPOP 活动。

LDAP——显示 LDAP 服务器活动。

Minger——显示 Minger[724]服务器活动。

RAW——在此选项卡上记录 RAW 或由系统生成的邮件活动。

MDaemon Connector — 显示所有 MDaemon Connector[323]活动。

Webmail

Webmail — 显示 MDaemon Webmail的邮件活动。

ActiveSync — 该选项卡显示 ActiveSync 的活动。

队列 — 从此选项卡可抵达其上的另一行选项卡，每个选项卡对应每个邮件队列，例如：本地、远程、保持、隔离，贝叶斯垃圾邮件等等。

插件 — 显示所有与任何 MDaemon 插件相关的活动。

活动目录 — 显示与 "活动目录"有关的所有活动。

会话 — 点击此选项卡，其上会显示若干其他选项卡。这些标签显示连接到 MDaemon 的每个活动条目。无论连接的是出站或进站的 SMTP、POP、IMAP、Webmail，或 ActiveSync，每一个启用进程的信息都会在这里显示。双击活动会话以显示会话窗口[69]，它将显示 SMTP 会话在处理时的记录。

显示在这些选项卡上的信息不会对实际存储在日志文件中的数据量有任何影响。然而，MDaemon 对关于记录在那些文件中的信息类型和数量具有很强的适应性。有关日志记录选项的更多信息，请参阅日志记录[136]对话框。

事件跟踪窗口的快捷菜单

如果您右键单击任何一个事件跟踪窗格的选项卡，将打开一个快捷菜单。该菜单提供大量选项，用于选择、复制、删除或保存指定选项卡的内容。该菜单的 *"打印/复制"*选项将会在记事本中打开任何当前选中的内容，可以用来打印或保存到文件。 *"删除"*选项将删除您已选定的文本。 *"搜索"*选项将打开一个窗口，您可以在此指定一个单词或短语以在日志中进行搜索。MDaemon 将会在所有的日志文件中查找该文本字符串，接着所有包含那个字符串的会话记录将合并到一个文件并在记事本中打开以让您查看。该功能的实际应用是搜索一个特定的邮件-ID 报头，以便从包含此邮件 ID 会话记录的所有日志中提供编辑。在某些选项卡上，还有一些选项可以向 MDaemon.com 报告已被误分类为垃圾邮件或包含病毒的邮件，或者应被分类为这类 (即误报或误报)的邮件。将分析这些被报告的邮件，并将其投递给第三方供应商来采取纠正措施。

MDaemon GUI 的布局并不局限于以上描述的默认位置。您可以点击菜单栏上的 "窗口» 切换窗格"来切换它们的位置。

综合日志视图

在 MDaemon 菜单栏的 "窗口"菜单里有 "综合日志视图"选项。点击此选项将添加一个窗口到 GUI，它会把一个或多个主窗格选项卡上的信息组合并一起显示。使用日志记录对话框中综合日志[138]屏幕上的这些选项来指定将显示在该窗口里的信息。

性能计数器

MDaemon 支持 Windows 性能计数器，它允许监控软件实时跟踪 MDaemon 的状态。提供计数器用于各种协议的活动会话数、队列中的邮件数、服务器活动/闲置状态、MDaemon 正常运行时间、以及会话和邮件统计。

要使用性能计数器，通过前往 "控制面板 | 管理工具 | 性能"或通过运行 "perfmon"来启动系统监控器。这些都是 32-位计数器，因此在 64-位机器上，您必须运行 "mmc /32 perfmon.msc"。点击 "添加计数器"，选择 MDaemon 性能对象，然后选择并添加您希望查看的计数器。要从在另一台机器上运行的 MDaemon 上查看性能计数器，您必须启用 "远程注册表"服务，并能通过任何防火墙进行访问。

还请参阅：

会话窗口 69
托盘图标 68
快捷菜单 69
综合日志 138

2. .1 自动发现服务

MDaemon 支持自动发现服务，该服务允许用户通过仅提供其电子邮件地址和密码来配置其电子邮件客户端以连接到其账户，而不必知道其他配置的详细信息。大多数客户端都支持该服务，尽管少数客户对它的支持有限。自动发现服务默认处于启用状态，但您可以从 MDaemon 的主应用程序界面手动启用或禁用它。在统计窗格的**服务器**下，右键点击**自动发现服务**，并点击**启用/禁用自动服务**。

完全支持自动发现服务的客户端将使用用户电子邮件地址中的域名，对 Service Type _autodiscover._tcp 执行 DNS 服务(SRV)记录查找，并连接到该服务器以获取其他信息。因此，要支持自动发现，您必须为自动发现及其支持的服务创建 DNS SRV 记录。MDaemon 的自动发现服务实施支持：ActiveSync 349 (airsync)、IMAP、POP、SMTP、DAV 和 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.
```

注意：一些客户端将始终先查看 autodiscover.{domain}.{tld}。因此，让自动发现服务记录指向名为 autodiscover.{domain}.{tld} 的服务器会有所帮助。在以下示例中，自动发现服务器是 adsc.example.com。

示例：

域名：example.com

管理员应该为 service type _autodiscover 设置一个 _tcp service 记录

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

在本例中，它指向 adsc.example.com，其中 A 记录指向 192.168.0.101

然后，客户端将连接到该服务器，并询问某些特定协议的连接点信息：ActiveSync、IMAP、XMPP、SMTP 和 DAV 等

然后，自动发现服务将查找请求的协议，并返回这些协议的正确服务器名称。例如对于 ActiveSync，它将返回在 _tcp service record _airsync 中定义的服务器名称，在本例中，它是 eas.{domain}.{tld}

如果 Outlook 正在调用“自动发现”，它将返回 IMAP 和 SMTP 服务器，表示为 _imap 和 _msa 的 _tcp service 记录，导致服务器返回为 imap4.example.com 和 msa.example.com。

以下是正确设置自动发现服务的示例。这假设您希望为每个协议使用唯一的名称，但很容易适应使用通用名称，例如 mail.example.com。

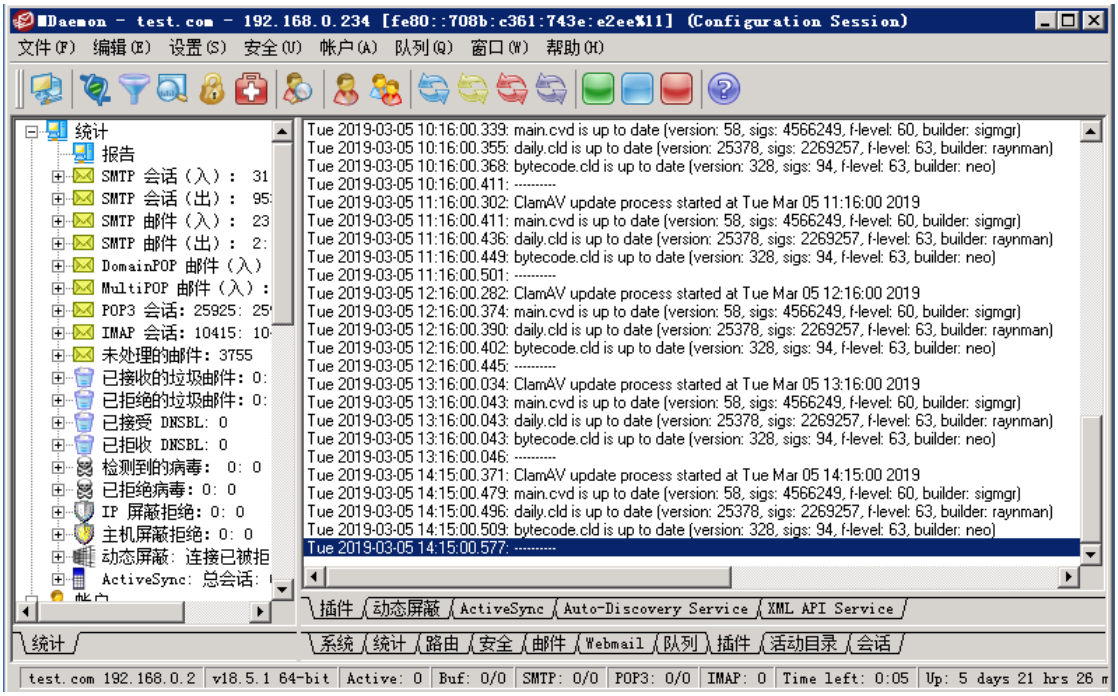
```
;
;  Database file example.com.dns for example.com zone.
;

@ IN  SOA dns.mydnsprovider.org. hostmaster.mydnsprovider.org. (
        4            ; serial number
        900          ; refresh
        600          ; retry
        86400        ; expire
        3600       ) ; default TTL

;
;  Zone NS records
;

@       NS dns.mydnsprovider.org

;
;  Zone records
;

@             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.
;
;  Service records
;

_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.
```

还请参阅：

要了解有关 AutoDiscover 的更多常规信息，请参阅 Microsoft 文档：Autodiscover for Exchange。

2.2 事件跟踪与日志记录



MDaemon 的主图形用户界面 (GUI)为您提供关于 MDaemon 的资源、统计、活动会话以及等待处理的队列邮件的重要信息。其中还提供可以轻松激活或关闭 MDaemon 各种服务器的选项。GUI 的选项卡面板帮助您查看服务器及其入站与出站连接的最新执行情况。

统计

默认情况下，统计窗口在 MDaemon 主界面的左窗格中。该窗格包含四个部分：统计、账户、队列和服务器。

"*统计*"部分含有以下统计：包括 MDaemon 收发的邮件数量、POP 和 IMAP 会话数、已接收和拒收的垃圾邮件、以及病毒等。这些统计从 MDaemon 启动时开始计数，还提供右键单击快捷菜单，帮助您清除计数器。

当您点击 "重置根节点计数"选项时，将重置所有计数器，不仅是您右键点击的那个选项。此外，在 "设置» 首选项» GUI"中有一个选项，

> 用于 *"重启后保留根节点邮件计数器。"*否则将重置计数器，不管 Windows 是否重启。

*"账户"*部分含有用于 MDaemon、MDaemon Connector 和 ActiveSync 的条目。取决于您的产品许可证，每个条目都列出已用账户数和所剩账户数。

*"队列"*部分含有针对各个邮件队列的条目，以及各个队列所含有的邮件数量（若存在）。您可以右键点击每个队列条目以打开快捷菜单，其中包含一个或多个以下选项，取决于您所选择的队列：

查看队列——该选项切换主窗口到队列选项卡并显示所选的队列。将显示队列中所有邮件的列表，您可以右键单击任何邮件以打开快捷菜单，其中包含大量选项，与那些在队列与统计管理器中的可用选项类似，例如复制、移动与编辑等等。

队列和统计管理器——打开 "队列"与 "统计管理器"以抵达 "队列页面"，其上会显示所选的队列。

立即处理——该选项 "重新排队"所有在队列中的邮件并尝试将它们处理为正常投递。如果您尝试处理包含在 "保持队列"、"坏队列"或其他类似队列中的邮件，那么这些邮件可能会遇到相同的错误，即将它们置于首位并退回至相同的队列。

冻结/解冻队列——临时停止对所选队列的处理，或如果队列当前处于停止状态那么可以继续进行处理。

释放——从保持队列释放邮件。MDaemon 将忽略遇到的错误信息，尝试投递邮件——即使这些邮件遇到导致它们被移至此队列的原始错误，也不会将它们退回到 "保持队列"。

重新排队——只对 "保持队列"有用，并和以上的 *"立即处理"*具有相同的效果。

启用/禁用队列——启用或禁用 "保持队列"。禁用时，不顾遇到的错误，不会将邮件移动到保持队列。

*"服务器"*部分包含用于 MDaemon 内每个服务器的条目，而且每个条目都列出服务器的当前状态："活动"或者 "闲置"。以下列出的每个服务器的条目用于每个域（可用时），以及该服务器或域当前正在使用的端口和 IP 地址。快捷菜单提供控件，用于切换每个服务器的活动和不活动状态。在服务器处于闲置状态时，其图标将变为红色。

事件跟踪与日志记录

主界面上默认的右边窗格包含一组标签，显示 MDaemon 其各种服务器与资源的当前活动和状态，并且它们会被持续地更新以反映当前服务器的状态。一有操作完成，每个活动会话与服务器活动就会被记录到正确的选项卡中。如果您已选择记录那些活动，显示在这些选项卡上的信息会被镜像到日志目录内的日志文件中。

MDaemon GUI 的主窗格中包含以下选项卡：

系统——在启动程序时，"系统"选项卡会显示一个初始化进程的日志，它可以提醒您 MDaemon 的配置或状态可能存在的问题。它还显示活动，例如启用/禁用 MDaemon 的各种服务器。

统计——该标签显示服务器的统计报告，对应包含在各种根节点计数器里的信息，这些根节点计数器在 "统计与工具"窗格中的 "统计"选项卡上。如果您希望更改此报告中的字体或字体大小，您可以编辑 MDaemon.ini 文件中的以下部分：

```
[ReportWindow]
```

```
DefFontFace=Courier New
DefFontHeigh=15
DefFontWidth=7
```

此外，每晚午夜，在内容过滤器的收件人[555]屏幕上列出的 Postmaster 和其他所有地址将通过邮件收到一份报告的副本。这份报告和您使用在 "常规电子邮件控制[754]"中列出的 "状态"邮件命令所生成的报告是一样的。如果您不希望发送这份报告，请禁用 *"在午夜将统计报告发送给邮件主管员"*选项，其位于 "首选项"下的其他[421]屏幕。

路由——显示通过 MDaemon 解析的每封邮件的路由信息（收件人、发件人、邮件 ID 等等）。

安全——点击此选项卡将在其上显示和安全相关的若干其他选项卡。

内容过滤器——此选项卡列出 MDaemon 的内容过滤器[540]操作。当一封邮件符合某一 "内容过滤器"的邮件规则条件时，就会在此处记录这封邮件的相关信息及操作。

AntiVirus——AntiVirus[539] 操作都列在这个选项卡上。扫描某封邮件是否存在病毒时，会在此处记录该邮件的相关信息及操作。

反垃圾邮件——显示 MDaemon 的所有垃圾邮件过滤器[564]和拦截活动。

MDSpamD——列出所有 MDaemon Spam Daemon[573] 活动。

SPF — 显示所有发件人策略框架[440]活动。

DKIM——列出所有 DomainKeys Identified Mail（域密钥标识邮件）[442] 活动。

DMARC——列出所有 DMARC[449] 活动。

VBR——该选项卡显示 VBR 证书[460]活动。

MDPGP——该选项卡显示 MDPGP[527] 活动。

屏蔽——此选项卡显示缓送[503]与动态屏蔽[472]活动。

验证失败——此选项卡（和相应的日志文件）包含每个失败的 SMTP、IMAP 和 POP 登录尝试的详细条目。该信息包括使用的协议和 SessionID，以便您可以搜索其他日志、违规者的 IP、他们尝试使用的原始登录值（有时是别名）以及与登录匹配的账户（如果没有账户匹配则使用 "无"）。您可以右键单击此选项卡中的一行，并将违规者的 IP 地址添加到阻止列表中。

MTA-STS — 显示与 SMTP MTA 严格传输安全（MTA-STS）相关的所有活动。

邮件——点击此选项卡会在其上显示若干与邮件相关的其他选项卡。

SMTP（入站）——此选项卡上显示所有使用 SMTP 协议的入站会话活动。

SMTP（出站）——此选项卡上显示所有所有使用 SMTP 协议的出站会话活动。

IMAP——在此选项卡上记录使用 IMAP 协议的邮件会话。

POP3——当用户使用 POP3 协议从 MDaemon 收集邮件时，会在此处记录该活动。

MultiPOP——此选项卡显示 MDaemon 的 MultiPOP 邮件收集活动。

DomainPOP——此选项卡显示 MDaemon 的 DomainPOP 活动。

LDAP——显示 LDAP 服务器活动。

Minger——显示 Minger[724] 服务器活动。

RAW——在此选项卡上记录 RAW 或由系统生成的邮件活动。

MDaemon Connector — 显示所有 MDaemon Connector 323 活动。

Webmail

Webmail — 显示 MDaemon Webmail 的邮件活动。

ActiveSync — 该选项卡显示 ActiveSync 的活动。

队列 — 从此选项卡可抵达其上的另一行选项卡，每个选项卡对应每个邮件队列，例如：本地、远程、保持、隔离，贝叶斯垃圾邮件等等。

插件 — 显示所有与任何 MDaemon 插件相关的活动。

活动目录 — 显示与 "活动目录"有关的所有活动。

会话 — 点击此选项卡，其上会显示若干其他选项卡。这些标签显示连接到 MDaemon 的每个活动条目。无论连接的是出站或进站的 SMTP、POP、IMAP、Webmail，或 ActiveSync，每一个启用进程的信息都会在这里显示。双击活动会话以显示会话窗口 69，它将显示 SMTP 会话在处理时的记录。

显示在这些选项卡上的信息不会对实际存储在日志文件中的数据量有任何影响。然而，MDaemon 对关于记录在那些文件中的信息类型和数量具有很强的适应性。有关日志记录选项的更多信息，请参阅日志记录 136 对话框。

事件跟踪窗口的快捷菜单

如果您右键单击任何一个事件跟踪窗格的选项卡，将打开一个快捷菜单。该菜单提供大量选项，用于选择、复制、删除或保存指定选项卡的内容。该菜单的 *"打印/复制"*选项将会在记事本中打开任何当前选中的内容，可以用来打印或保存到文件。 *"删除"*选项将删除您已选定的文本。 *"搜索"*选项将打开一个窗口，您可以在此指定一个单词或短语以在日志中进行搜索。MDaemon 将会在所有的日志文件中查找该文本字符串，接着所有包含那个字符串的会话记录将合并到一个文件并在记事本中打开以让您查看。该功能的实际应用是搜索一个特定的邮件-ID 报头，以便从包含此邮件 ID 会话记录的所有日志中提供编辑。在某些选项卡上，还有一些选项可以向 MDaemon.com 报告已被误分类为垃圾邮件或包含病毒的邮件，或者应被分类为这类 (即误报或误报)的邮件。将分析这些被报告的邮件，并将其投递给第三方供应商来采取纠正措施。

MDaemon GUI 的布局并不局限于以上描述的默认位置。您可以点击菜单栏上的 "窗口» 切换窗格"来切换它们的位置。

综合日志视图

在 MDaemon 菜单栏的 "窗口"菜单里有 "综合日志视图"选项。点击此选项将添加一个窗口到 GUI，它会把一个或多个主窗格选项卡上的信息组合并一起显示。使用日志记录对话框中综合日志 138 屏幕上的这些选项来指定将显示在该窗口里的信息。

性能计数器

MDaemon 支持 Windows 性能计数器，它允许监控软件实时跟踪 MDaemon 的状态。提供计数器用于各种协议的活动会话数、队列中的邮件数、服务器活动/闲置状态、MDaemon 正常运行时间、以及会话和邮件统计。

要使用性能计数器，通过前往 "控制面板 | 管理工具 | 性能"或通过运行 "perfmon"来启动系统监控器。这些都是 32-位计数器，因此在 64-位机器上，您必须运行 "mmc /32 perfmon.msc"。点击 "添加计数器"，选择 MDaemon 性能对象，然后选择并添加您希望查看的计数器。要从在另一台机器上运行的 MDaemon 上查看性能计数器，您必须启用 "远程注册表"服务，并能通过任何防火墙进行访问。

还请参阅：

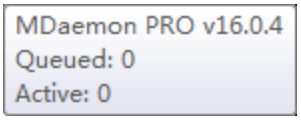
会话窗口 69
托盘图标 68
快捷菜单 69
综合日志 138

2.4 托盘图标

无论MDaemon服务器何时运行，它的图标都会显示于系统托盘中。而且，除了让您方便的知道服务是否运行以外，图标还是动态显示并根据当前服务器状态更改颜色。下面是图标显示含义的列表：

	全部正常。在本地或远程队列中没有邮件。
	全部正常。在本地或远程队列中有邮件。
	可用磁盘空间低于阈值 (请参阅设置 » 首选项 » 磁盘 415)。
	网络断开、拨号失败、或磁盘空间已满。
图标闪烁	存在更新的 MDaemon 版本。

关于可用服务器的附加信息会通过图标的工具提示显示出来。将鼠标悬停在上面就会出现工具提示，显示当前进行队列的邮件和活动的会话。



快捷菜单

鼠标右键单击 MDaemon 的托盘图标，打开快捷键菜单。该菜单帮助您快捷地访问 MDaemon 几乎全部菜单，而无需打开主用户界面。

点击"关于MDaemon..."选项（位于快捷菜单的顶部），可找到有关 MDaemon 或 MDaemon Technologies 的更多信息。

在下一部分，点击"查看MDaemon 更新..."检查是否有更新的 MDaemon 版本可下载。

在第三部分，您可用访问以下 MDaemon 菜单：设置、安全、账户和配额。这些级联菜单与主界面菜单栏的菜单相同。

第四部分含有选项可以打开账户管理器和队列及统计管理器，还有一个选项可以处理 MDaemon 的全部邮件队列。

接下来，还有命令可以锁定和解锁 MDaemon 的界面（参见下面的"锁定/解锁 MDaemon 的主界面"），请选择"启动 MDaemon..."菜单，用于当其最小化到系统托盘时打开/恢复 MDaemon 的界面。

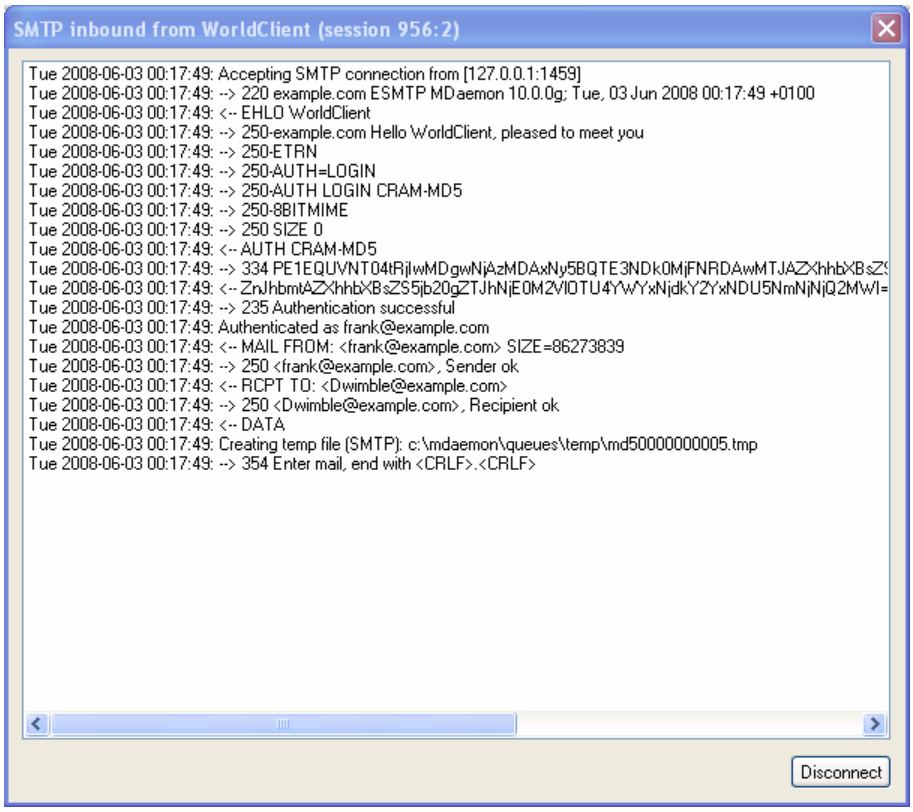
最后的选项是"关闭配置会话"，用来关闭 MDaemon 界面。关闭配置会话不会关闭 MDaemon 服务。

锁定/解锁 MDaemon 的主界面

锁定用户界面，最小化 MDaemon，点击"锁定服务器..."菜单项，之后在打开的对话框中输入一个密码。等待几秒，在确认密码之后，MDaemon 的用户界面将会被锁定。它无法被打开或者被查看，但 MDaemon 还会继续正常地工作。但是，如果您需要的话，您可以继续使用在此菜单上的"立即处理所有队列..."选项来手动处理邮件队列。要解锁 MDaemon，双击托盘图标或者右击图标，双击托盘图标选择"解锁MDaemon"对话框，或者右键单击图标然后选择"解锁服务器..."，然后输入您锁定时候时创建的密码。

2.5 会话窗口

在主 GUI 的"会话"选项卡[59]上双击某个活动的会话将打开该条目相应的会话窗口。该会话窗口将显示该会话进行过程中的 SMTP 记录。点击该窗口上的断开连接可中断正在进行的会话并断开连接。



2.6 MDaemon 的 SMTP 工作流

当创建一个入站 SMTP 连接时，MDaemon 通过一系列复杂的处理步骤来检查是否接收投递的邮件，而且如果一旦接收就继续处理下去。以下图标是对进站 SMTP 邮件工作流程的图形化表述。

执行哪些步骤取决于您的特定配置。如果在您的配置中一个功能被关闭的话，那么一个或者多个步骤将会被跳过。

章节

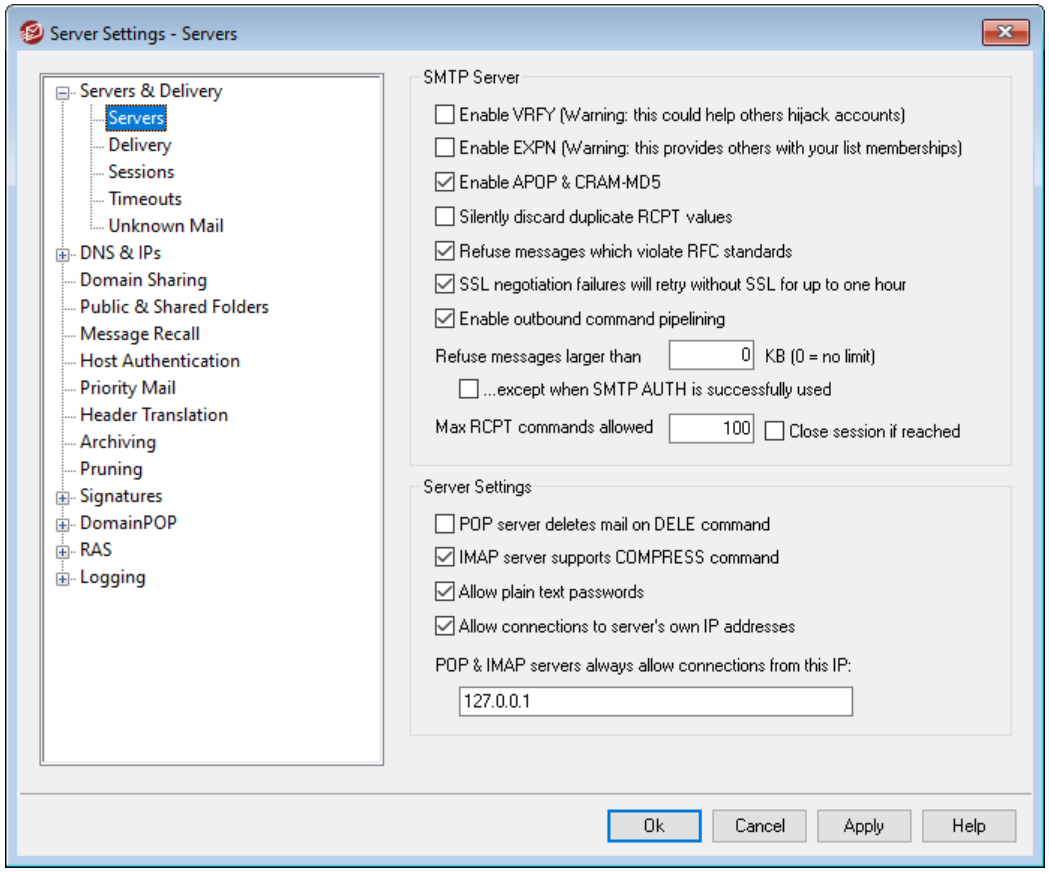
3

3 设置菜单

3.1 服务器设置

3.1.1 服务器和投递

3.1.1.1 服务器



SMTP 服务器

启用 VRFY
如果您希望响应 SMTP VRFY 命令，请点击此切换。此项命令有时候会被一些服务器使用，这些服务器使用一个 SMTP 呼叫转移或者回呼功能来试图确认您服务器上邮件地址的有效性。默认情况下，禁用该选项。

启用 EXPN
如果您希望 MDaemon 允许 EXPN 命令，点击此选择框。

启用 APOP 和 CRAM-MD5
默认情况下 MDaemon 的服务器（POP、IMAP 等）不允许 APOP 和 CRAM-MD5 认证方法。这种类型的身份验证要求使用可逆加密来存储密码，出于安全目的，我们不建议这样做。这是为了以防止 MDaemon、管理员或可能的攻击者解密密码。因此，此项不兼容密码选项 717 中 *"使用不可逆加密保存邮箱密码"*这项和 "活动目录"验证。不过如果您不

使用 SSL/TLS，则 APOP 和 CRAM-MD5 可以通过无需发送明文密码即可对用户进行身份验证来提供额外的安全性。

静默丢弃重复的 RCPT 值
如果您希望 SMTP 服务器忽略相同 SMTP 会话内重复的收件人，请启用此项。MDaemon 将接受然后丢弃重复的收件人。默认情况下，禁用该选项。

拒收违反 RFC 标准的邮件
如果您希望拒收在 SMTP 进程中不符合 RFC 因特网标准的邮件，请启用此选项。要通过依从性测试，该邮件必须：

1. 大小超过 32 字节 (最小也必须包括所有需要部分)。
2. 含有 FROM: 报头 或 SENDER: 报头 报头中的地址。
3. 含有不止一个 FROM: 报头 报头中的地址。
4. 含有不止一个 SUBJECT: 报头 即使不需要 SUBJECT 报头。

使用已验证会话或来自可信域或 IP 地址的邮件没有此项要求。

SSL 协商失败将在没有 SSL 的情况下重试一小时
此选项允许您在出站 SMTP 会话期间遇到 SSL 错误时临时重试没有 SSL 的主机 IP。这将每小时进行重置。

启用出站命令管道
默认情况下，MDaemon 支持 "SMTP Service Extension for Command Pipelining"(RFC 2920)，这就意味着它将分批而不是单独发送 MAIL、RCPT 和 DATA 命令，从而提高高延迟网络链接的性能。SMTP 管道始终用于入站连接，并且默认情况下为出站连接启用。如果您不想将其用于出站连接，请清除此复选框。

拒收大于 [xx]KB 的邮件 (0=无限制)
在此设置一个值将会阻止 MDaemon 接受或者处理超过某一大小的邮件。启用此选项后，MDaemon 将试图使用 RFC-1870 中所指定的 ESMTP SIZE 命令。若发送方支持 SMTP 扩展名，那么 MDaemon 将优先于实际投递确定邮件大小，并立即拒收邮件。如果发送方不支持此 SMTP 扩展，则 MDaemon 将不得不开始接收邮件，在传送期间，将周期性地跟踪其大小，并且一旦传输完毕，最终将拒绝投递此邮件。如果您不希望限制大小则使用 "0"。如果您希望经过验证的会话免于大小检查，请使用下方的 *"...在成功使用 SMTP 验证时例外"* 这一项。

...在成功使用 SMTP 验证时例外
如果您希望在 SMTP 会话经过验证时为邮件免除邮件大小限制，请勾选此框。

允许的最大 RCPT 命令数
如果您希望限制每封邮件可以被发送的 RCPT 命令数量，请使用此选项。如果您不希望限制设置则使用 "0"。

如果达到指定数量则关闭会话
如果到达 RCPT 命令所允许的最大值，您希望立即关闭此会话，请勾选此框。

服务器设置

POP 服务器按 DELE 命令删除邮件
如果您希望 MDaemon 在收到 DELE 命令时立即删除检索到的邮件（即使未适当完成 POP 会话），请点击此项。

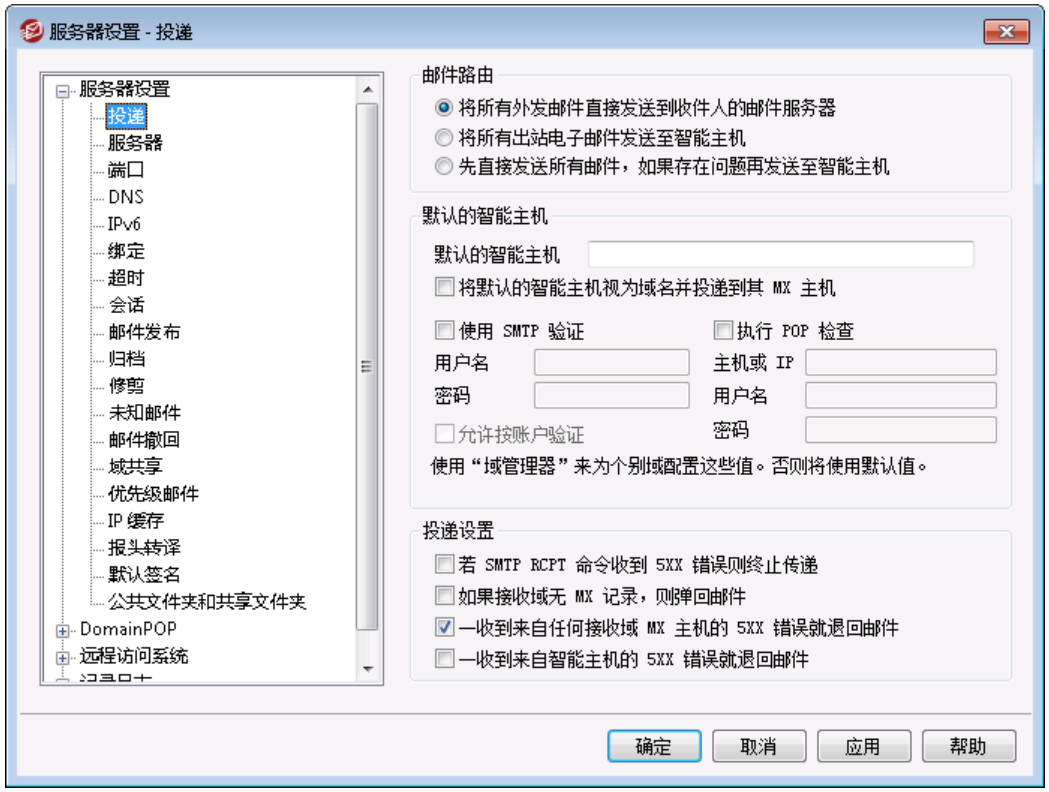
IMAP 服务器支持 COMPRESS 命令
如果您希望支持 IMAP COMPRESS 扩展（即 RFC 4978，该扩展压缩客户端间收发的所有数据），请点击此框。对于每个 IMAP 会话而言，COMPRESS 将增加 CPU 和内存使用率。

允许纯文本密码
此选项管理 MDaemon 是否允许接收发往 SMTP、IMAP、POP3 服务器的纯文本密码。如果禁用此选项，那么 POP3 用户、POP3 密码、IMAP 登录、IMAP 登录和 SMTP 验证登录命令将会返回一个错误，除非这个连接使用 SSL。

允许连接到服务器自身的 IP 地址
启用此选项后，MDaemon 可以连接到自身。

POP & IMAP 服务器始终允许来自这个 IP 的连接
POP 和 IMAP 服务器将总是接受来自在此区域输入的 IP 地址的连接，无论如何设置屏蔽和防护设置。

3.1.1.2 投递



邮件路由

将所有出站邮件直接发送到收件人的邮件服务器
选中此选项时，MDaemon 将会尝试直接投递邮件而不是将邮件转发到其他主机上。MDaemon 将把无法投递的邮件放置到其重试系统中并且根据您在邮件队列对话框重试队列 732上所设置的参数和时间间隔继续尝试投递这些邮件。

将所有出站邮件发送到智能主机
如果您想让出站邮件（无论是否在其目标域）都假脱机到另一个主机或服务器以便路由投递，请选择此选项。如果选定此项，会将出站邮件发送至下方指定的*"默认智能主机"*。通常，这一功能在直接邮件投递造成服务器资源额外压力的高流量期间是非常有用的。如果无法将一封邮件投递到指定服务器，MDaemon 就会将此邮件移至"重试"队列中，通过您在重试队列 732屏幕中（位于"邮件队列"对话框）设置的参数和时间间隔，继续尝试投递这封邮件。

先直接发送所有邮件，如果有问题再发送到智能主机
此项是前两个投递选项的组合项。首先 MDaemon 尝试将出站邮件直接投递到服务器，如果无法投递，才将此邮件发送至*下方指定的"默认智能主机"*。无法投递的邮件是由于目标地址的邮件主机无法被解析到一个实际 IP（例如转至远程网络的未注册网关）或者发送的邮件虽被主机正确处理，但却不能直接连接或拒绝直接连接造成的。该选项将会使 MDaemon 将邮件传递到一个更有力的 MTA 中，而不是将这些邮件返回到发件人。在您的本地服务器不能直接访问时，有时会通过您的 ISP 所运营的邮件系统用路由的方式投递邮件。如果无法将一封邮件投递到指定的智能主机，MDaemon 就会将此邮件移至重试系统中，通过您在重试队列 732屏幕（位于"邮件队列"对话框）中设置的参数和时间间隔，继续尝试投递这些邮件。对于每个后续投递尝试，MDaemon 将再次先尝试将此邮件直接投递到其收件人，然后是指定的智能主机。

默认智能主机

默认智能主机
在此处指定您的 ISP 或者邮件主机的名称或 IP 地址。通常为您 ISP 上的 SMTP 服务器。

> 不要在此文本框中输入 MDaemon 的默认域或 IP 地址。这里应该输入一个 ISP 或其他能够为您中继邮件的邮件服务器。

视主机为域名并投递到其 MX 主机
如果您希望 MDaemon 将*默认的智能主机*视为域名，查询其 DNS 记录并投递到其 MX 主机，请启用此项。

使用 SMTP 验证

如果*"默认智能主机"*需要验证，则点击此选框并在下方输入您的登录凭证。这些登录凭证将用于所有发送到智能主机的出站 SMTP 邮件。不过，如果您选择使用下方的*允许按每个账户验证*选项，那么 MDaemon 会使用发件账户的*智能主机访问*凭证来向您的主机分别验证每封邮件。该设置可在"账户编辑器"的邮件服务 602屏幕上指定。

用户名
在此处输入您的用户名或登录名。

密码
使用此选项指定您的智能主机登录密码。

先执行 POP 检查
如果您的智能主机需要他们的客户在通过 ISP 服务器发送邮件前先登录到一个 POP3 邮箱，请点击这个按钮，输入凭证信息。

主机或 IP
输入您希望连接的主机或 IP 地址。

用户名
这是 POP 账户的登录信息或账户名。

密码
这是 POP 账户的密码。

允许按账户验证
如果您希望对发送到上方所指定的 *"默认智能主机"*的出站 SMTP 邮件使用按账户验证，请点击此复选框。该操作并不使用在此处提供的*用户名*和*密码*凭证，而是使用各个账户的*智能主机访问*凭证（在邮件服务 602屏幕上指定。）如果已为给定账户指定智能主机凭证，则使用这些凭证。

若您希望配置*按每个账户验证*以用于每个账户的*邮件密码*而不是使用其可选的*智能主机密码*，那么您可以通过在 MDaemon.ini 文件中编辑下列键值以实现此操作：

```
[AUTH]
ISPAUTHUsePasswords=Yes（默认为 No）
```

启用 ISPAUTHUsePasswords=Yes 选项将在一段时间后将您所有账户本地邮件密码有效传达到您的智能主机。这可能对邮件的安全性造成威胁，因为它正向另一个服务器提供敏感信息。您不应该使用此选项，除非您正在使用的智能主机是您完全信赖的，而且您相信有必要这么做。另外，您应该注意到，如果您使用了此选项并且授予用户权限通过 Webmail或其他方式来改变他们的 *"邮件密码"*，那么改变 "邮件密码 *"同样可以有效地改变* 智能主机密码 *"。当本地更改了邮件密码*而没有在您的智能主机上本地更改相应的*智能主机密码*，这可能会导致对一个账户的智能主机验证失败。

若 SMTP RCPT 命令接收到一个 5xx 的错误，将中止投递
当 MDaemon 在应答 SMTP RCPT 命令时接收到一个 5xx 的致命错误，若您希望 MDaemon 终止投递邮件的尝试，请启用此选项。默认情况下，禁用该选项。

如果接收方域没有 MX 记录则退回邮件
通常在 MDaemon 检查接收域的 DNS 记录时，它将查找 MX 记录，找不到 MX 记录时将接着查找 A 记录。如果这两个记录都找不到，它会将此邮件作为无法投递的邮件退回发件人。如果您希望 MDaemon 在找不到 MX 记录时立即退回邮件，而不是允许其继续查找 A 记录，请点击此选项。默认情况下，禁用该选项。

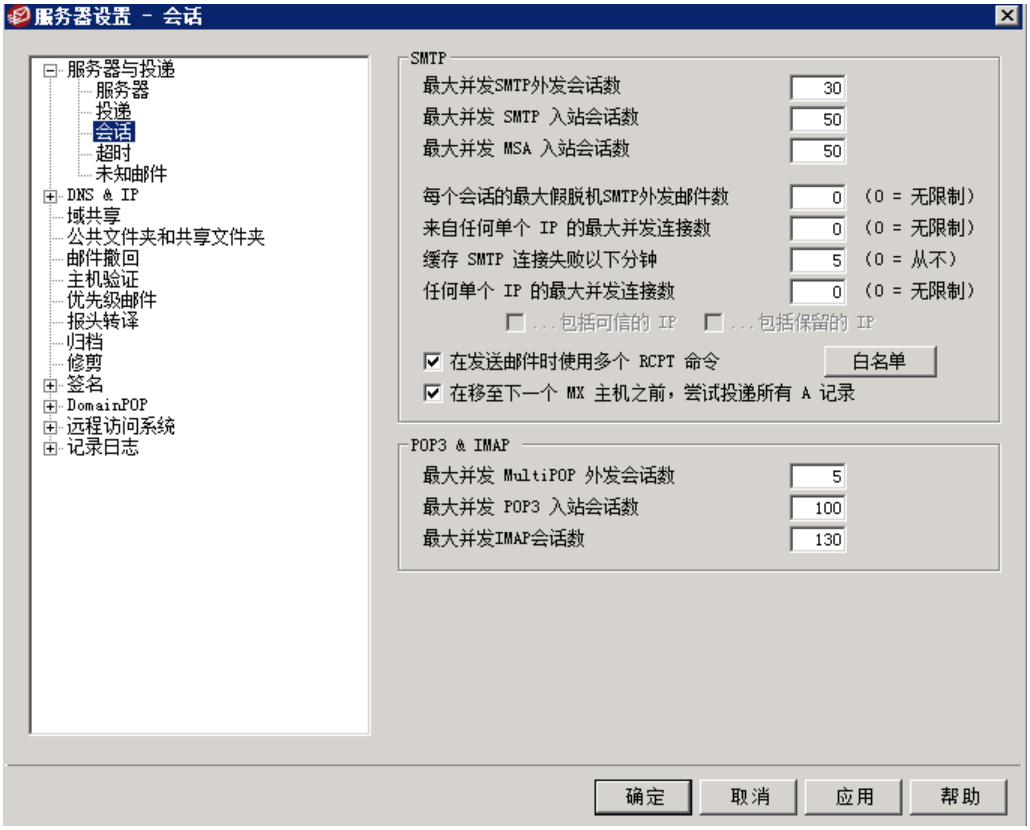
收到第一个 5XX 错误后即从接收域的任何 MX 主机退回邮件
启用此选择框后，当 MDaemon 从一个 MX 主机接收到一个 5xx 的致命错误应答时，将会返回/退回邮件。结果就是将不再尝试投递邮件到任何可能为收件人域所指定的后续 MX 主机。若禁用此选项，只要 MX 主机中的其中一个返回了 4xx 的非致命性错误应答，那么 MDaemon 将不会退回邮件。默认情况下启用此项。

遇到来自智能主机的 5xx 错误则退回邮件
如果您希望在收到来自您智能主机的 5xx 致命错误响应时返回/退回邮件，请使用此项。

还请参阅：

重试队列 732
邮件服务 602

3.1.1.3 会话



SMTP

最大并发 SMTP 出站会话数
该值将设置需要向远程系统发送邮件时，所能创建的最大远程 SMTP 会话数。每个会话都将发送出站邮件，直到任何队列中都没有邮件剩余，或者达到*每个会话的最大 SMTP 出站邮件数*所设置的值。例如，出站邮件队列中有 20 封邮件等待发送，而且该设置的值为 5，那么将同时创建 5 个会话，而每个会话会连续地发送 4 封邮件。

该选项的默认值设为 30，不过您可能希望以一定数量的会话进行试验以找到能使得您的带宽保持最佳性能的设置。指定太多的会话可能导致您的带宽超负载或者您的 Windows 机器资源耗尽，并且您将会失去投递的效率。请记住，每一个被 MDaemon 创建的 SMTP 会话都可以连续投递邮件，因此 4 个会话投递 2 封邮件要比 8 个线程各自投递 1 封邮件执行得更快更好。出色的设置是：5 - 10 个线程（使用 56k 调制解调器），20 - 30 个线程（使用宽带）。

最大并发 SMTP 入站会话数
该值控制在服务器回应"服务器太忙"邮件前，可接收并发入站 SMTP 会话的数量。默认值为 50。

最大并发 MSA 入站会话数
使用该选项来指定允许的并发邮件提交代理（MSA）入站会话最大数。

每个会话的最大 SMTP 出站邮件数
该设置对在会话停止发送邮件并从内存中释放自己之前，这些会话所发送的单独邮件数量做出了限制。通常情况下，您应该将此控件设置为零，这样可使每一个会话连续投递邮件直到队列为空。

在这些分钟内缓存 SMTP 连接失败（0=从不）
当一个到给定主机的 SMTP 连接失败时，MDaemon 在该选项所指定的分钟数内，会停止尝试连接到此主机。这样做可以防止 MDaemon 一再连接到一个有问题的主机，例如，有多个指定到该主机的邮件但是在进行首次投递尝试时，就发现该主机已关闭。默认设置是 5 分钟。如果您不希望缓存 SMTP 失败，请使用"0"。

任何单个 IP 的最大并发连接数（0=无限）
这是允许单个 IP 地址在被阻止前的最大并发连接数量。如果您不希望限制设置则使用"0"。

同时连接到任意单一 IP 的最大连接数（0=无限制）
使用此选项来限制邮件投递过程中允许同时连接到单个 IP 地址的最大连接数。如果您不希望限制并发连接，请使用"0"。

该选项有助于防止过多的连接同时连接到多个 IP 地址。投递过程中，如果邮件要求连接到的 IP 已超过其限制连接数，则该连接将被忽略并使用下一个 MX 主机（或智能主机）。如果没有其他可用主机，则邮件将在队列中等待下一轮投递。默认情况下，禁用选项以防止此类情况的发生。

...包含可信 IP
默认情况下，指向可信 IP 地址的连接不受*"同时连接到任意单一 IP 的最大连接数"*这个选项的影响。如果您希望为可信 IP 也强制执行此操作，请勾选此框。

...包含已保留 IP
默认情况下同样保留用于内网的 IP 地址也免于进行该操作。它们是 127.0.0.*、192.168.*.*、10.*.*.* 和 172.16.0.0/12。如果您希望为已保留 IP 也强制执行此操作，请勾选此框。

发送邮件时使用多个 RCPT 命令
默认情况下 MDaemon 使用智能假脱机，它在发送邮件期间将在一个会话内使用多个 RCPT 命令。如果您希望每会话仅使用一个 RCPT 命令，请取消勾选此框。

豁免列表
此按钮打开“智能假脱机豁免列表”。当 MDaemon 向此列表上的域发送邮件时，它不使用智能假脱机，而且每会话仅使用一个 RCPT 命令。

在移至下一个 MX 主机之前，尝试传递所有 A 记录
在传递错误或失败时，默认情况下，MDaemon 会尝试传递到 MX 主机的每个 A 记录，然后再移至下一个 MX 主机。如果希望 MDaemon 在遇到错误后立即在下一个 MX 主机移动，而不要先尝试所有 A 记录，请禁用此选项，

POP3 和 IMAP

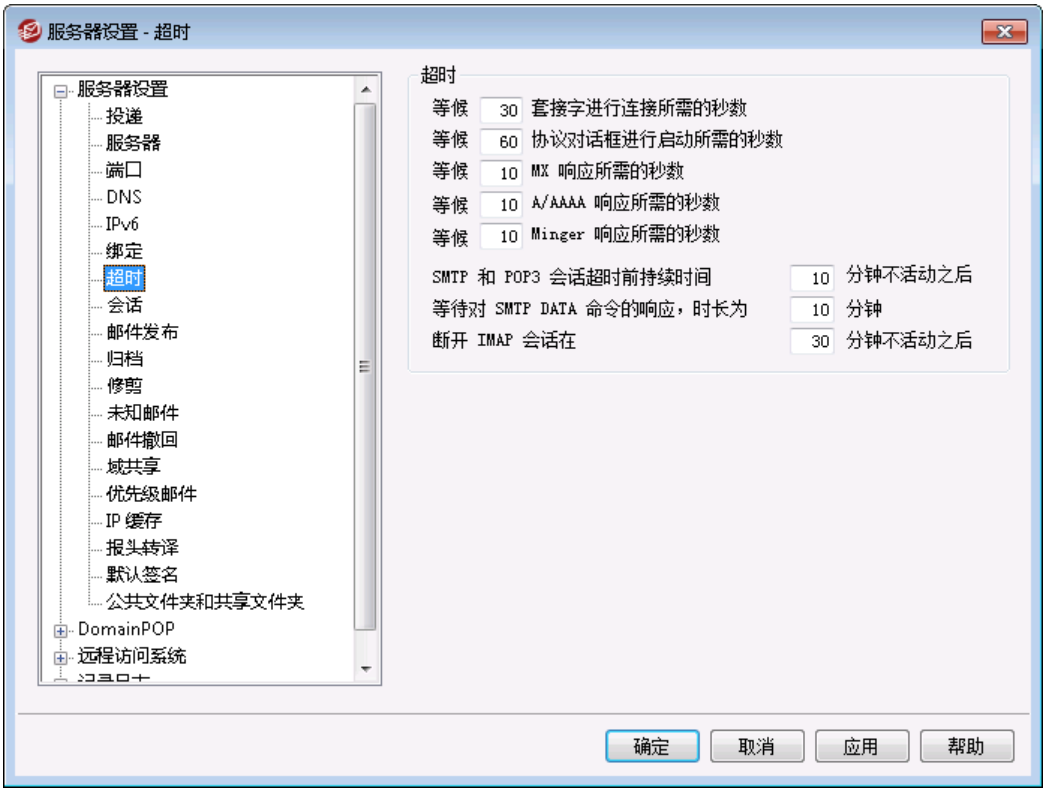
最大并发 MultiPOP 出站会话数
此处输入的值表示在收集 MultiPOP 邮件时，被创建的可能发送的最大出站 POP 会话数。每个会话都将收集此类型的邮件，直到处理完所有 MultiPOP 服务器，并且收集完所有邮件。例如，如果在您的用户中有 15 个 MultiPOP 会话，这个值设置成 3，那么之后每个会话将会从 5 个 MultiPOP 源中收集邮件。

您应该测试多少会话对您的带宽来说具有最佳性能。指定过多会话可能导致您的带宽超负载，或者您的 Windows 机器资源耗尽，并且您将会失去投递的效率。请记住，每一个被 MDaemon 创建的 POP 会话都会收集邮件直到耗尽所有资源为止。因此，4 个会话从 20 个资源里面收集邮件比 20 个会话从 1 个单独的源中收集要执行得更快更好。

最大并发 POP3 入站会话数
该值控制在服务器回应“服务器太忙”邮件前，可接收的最大并发 POP 入站邮件的数量。

最大并发 IMAP 会话数
该值控制在服务器回应“服务器太忙”邮件前，可接收的最大并发 IMAP 邮件会话的数量。

3.1.1.4 超时



超时

等候 xx 秒让套接字连接
在初始化一个连接请求后，MDaemon 将会为远程系统准许访问等待几秒钟。如果远程系统没有在时间框中设置的时间内响应，那么 MDaemon 将会发送邮件到一个指定的*智能主机*或将其放入重试系统，此操作取决于您在 "服务器设置"对话框的 "投递"屏幕上选定的选项。

等待 XX 秒让协议来启动对话框
一旦远程主机创建了一个连接，会使 MDaemon 在开始 SMTP 或 POP3 协议对话框前，等待远程主机 XX 秒。如果远程主机未在时间框中设置的时间内开始协议会话，那么 MDaemon 将会发送邮件到一个指定的*智能主机*或将其放入重试系统，此操作取决于您在 "服务器设置"对话框的 "投递"屏幕上选定的选项。

等候 XX 秒让 MX 响应
在使用 DNS 服务为远程域解析 "MX" 主机时，MDaemon 会对 "MX" 查询的响应等候这段秒数。如果 DNS 服务器未在设置的时间内响应，MDaemon 会尝试将邮件投递到远程主机的 "A" DNS 记录中所指定的 IP 地址。如果该尝试失败，MDaemon 会将邮件发送到一个指定的*智能主机*或将其放入重试系统，此操作取决于您在 "服务器设置"对话框的 "投递"屏幕上选定的选项。

等待 XX 秒 让 A/AAAA 响应
计时器控制在试图解析一个远程主机的 IP 地址时，MDaemon 将会等待多长时间。如果该尝试失败，MDaemon 会将邮件发送到一个指定的*智能主机*或将其放入重试系统，此操作取决于您在 "服务器设置"对话框的 "投递"屏幕上选定的选项。

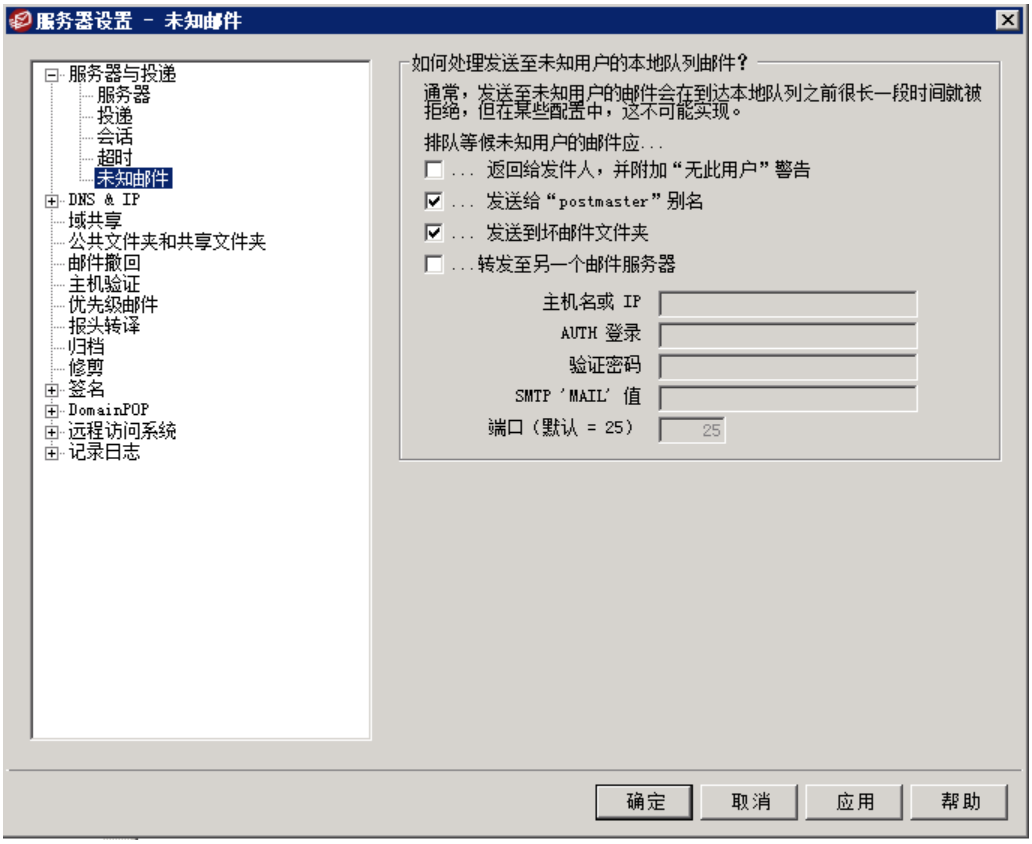
等候 XX 秒让 Minger响应
这是 MDaemon 等待来自 Minger 服务器响应所花的秒数。

在 xx 分钟内不活动时，SMTP 和 POP3 会话将超时
如果一个成功的连接和处理通话已经持续不活动了一段时间 (没有I/O)，MDaemon 将会中止这个传输处理。并在调度的下次处理间隔中，再度重试。

等待 XX分钟 SMTP DATA 命令响应
该选项管理在 SMTP 进程中在发送了 DATA 命令之后，MDaemon 等待 "250 OK"响应的时间。由于某些收件服务器在那时进行较漫长的反垃圾邮件和反病毒处理、或其他必要操作，此选项可以为服务器提供时间来完成这些任务。默认值是 10 分钟。

当有 XX 分钟不活动时，IMAP 会话超时
如果 IMAP 会话闲置一段时间，那么 MDaemon 将关闭这个会话。

3.1.1.5 未知邮件



为未知用户排队的邮件应为...

...返回给发件人，并附加“无此用户”警告
启用此选项后，到达服务器的指向未知但可能是本地用户的邮件将被返还给邮件发件人。如果您希望定制“无此类用户”的警告电子邮件的内容，您可以通过创建一个名为“NoShUser.dat”的文本文件，并将其放置在“MDaemon\app\”文件夹中来实现这点。

...发送给 "Postmaster"别名
默认情况下，无论用户是不是别名为 "邮件管理员" (Postmaster)，都会将到达服务器、且被视为指向本地未知用户的邮件返还给邮件的原始发件人。如果您不希望发送这些邮件到Postmaster，请禁用该选项。

...发送到坏邮件文件夹
默认情况下，会将到达服务器、且被视为指向本地未知用户的邮件路由至坏邮件队列。如果您不希望将这些邮件发送至坏邮件队列，清除该复选框。

...转发到另一台邮件服务器
如果您希望在将邮件发送给未知本地用户时，将其转发到另一个邮件服务器，请使用此项。

主机或 IP
指定要将邮件转发到的主机名或 IP 地址。

以下将应用到 MDaemon 的全局设置，如果您指定一个主机来进行邮件的转发，存档和发送。如果您在方括号中填入主机 (例如 [example.com])，MDaemon 将在投递到这个主机时跳过 MX 记录查询。例如，如果此项含有 "example.com"，那么将进行正常的 MX 查询。不过如果此项含有 "[example.com]"，则只进行 A-记录查询。

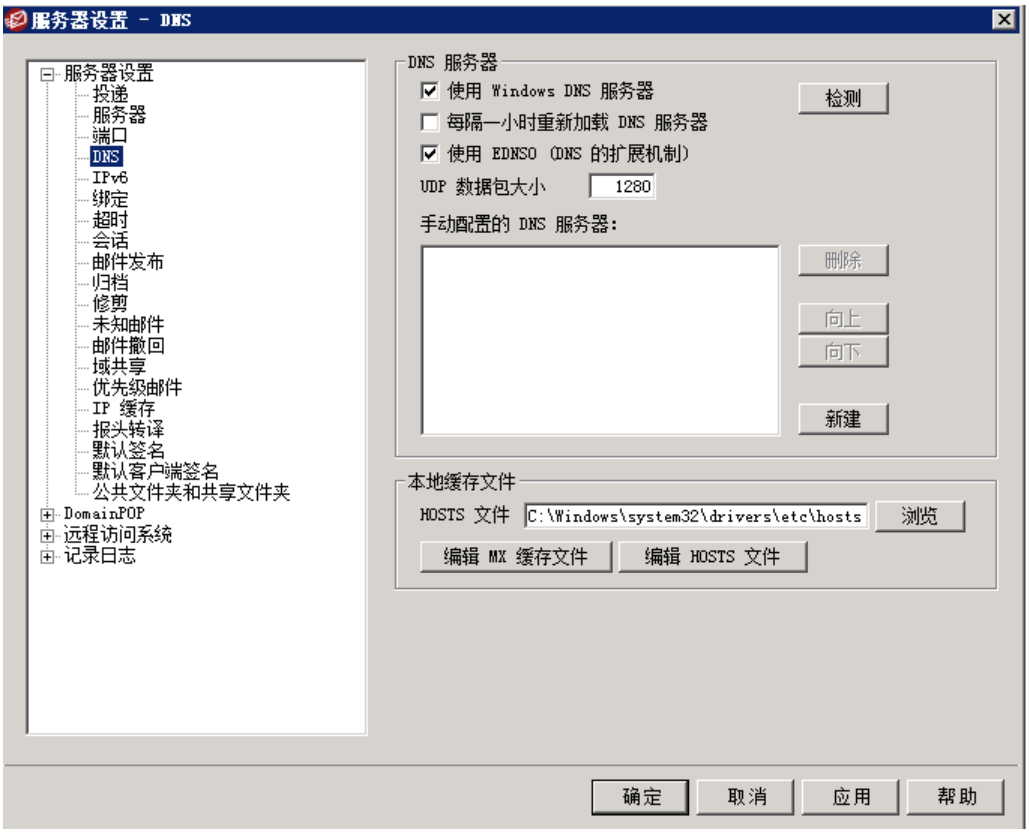
AUTH 登录/密码
输入任何必要的登录/密码凭证，用于将指向未知用户的邮件转发到的邮件服务器。

SMTP "MAIL"值
该地址将用于 SMTP "Mail From:" 语句，在与接收主机通信期间使用。通常，会将邮件的发送者用于 SMTP 信封的这个部分。如果您需要空命令 (MAIL FROM <>)，请在此控件中输入 "[trash]"。

端口 (默认 = 25)
这是 MDaemon 用来发送邮件的 TCP 端口。默认的值是 25。

3.1.2 DNS 和 IP

3.1.2.1 DNS



DNS 服务器

使用 Windows DNS 服务器
选择此项时，MDaemon 将使用在您 Windows TCP/IP 配置中找到的所有 DNS 服务器。MDaemon 会在每次查询操作中依次试验各个 DNS 服务器，直到找到完整的 DNS 服务器列表或首个能够有效工作的 DNS 服务器。如果您在下方的 *DNS 服务器*选项中包含了额外的 DNS 服务器，MDaemon 也会尝试这些服务器。最后，系统日志将在启动时显示各个 DNS 服务器，并指示其来源（例如手动配置或取自 Windows）。

每小时重新加载 DNS 服务器
如果您希望每小时重新加载 DNS 服务器，请勾选此框。默认情况下，禁用该选项。

使用 EDNS0（DNS 的扩展机制）
默认情况下 MDaemon 支持 DNS 的扩展机制（请参阅 RFC 2671）。如果您不希望支持该机制，请清除该复选框。

UDP 数据包大小
此项控制 UDP 数据包大小。默认大小是 1280 字节。

手动配置 DNS 服务器
在执行 DNS 查询时，MDaemon 将使用在此处指定的所有 DNS 服务器。MDaemon 会在每次查询操作中依次试验各个服务器，直到找到完整的 DNS 服务器列表或首个能够有效工作的 DNS 服务器。如果您启用了上方的 *"使用 Windows DNS 服务器"*选项，MDaemon 也会查询在您 Windows TCP/IP 配置中找到的所有 DNS 服务器。最后，系统日志将在启动时显示各个 DNS 服务器，并指示其来源 (例如手动配置或取自 Windows)。

本地缓存文件

Hosts 文件...
在询问 DNS 服务器之前，MDaemon 会首先通过 Windows HOSTS 文件来尝试处理一个地址。询问中如果该文件包含域 IP 地址，MDaemon 将不再询问 DNS 服务器。

您必须输入完整的路径和文件名而不仅是文件名。MDaemon 将会尝试使用以下值作为此文件的默认位置：

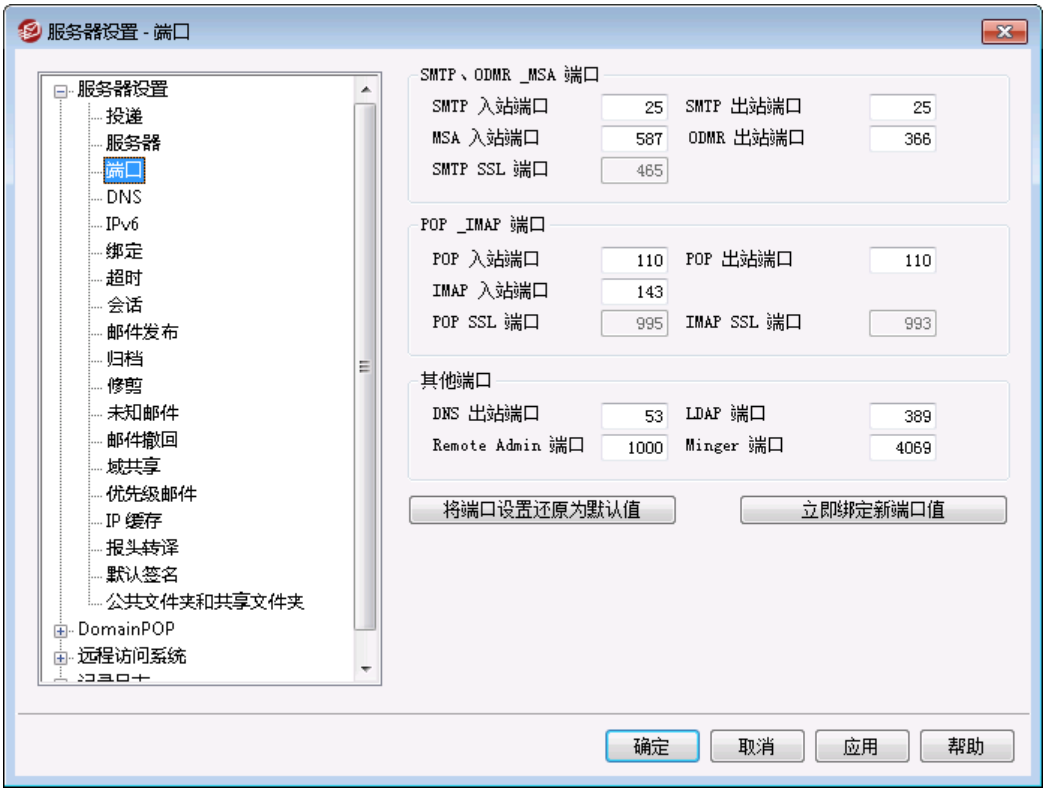
[drive]:\windows\system32\drivers\etc\hosts

HOSTS 文件是包含域名称的 A 记录或者主要 IP 地址的 Windows 文件。MDaemon 还允许您指定 MXCACHE.DAT 文件中的 MX-record IP 地址。可以在 MDaemon\APP\ 文件夹中找到该文件。请点击下方的 **编辑 MX 缓存文件**"并阅读文件顶部的注释来获取更多信息。

编辑 MX 缓存文件
点击此按钮来查看或编辑 MXCACHE.DAT 文件。

编辑 HOSTS 文件
点击此按钮来查看或编辑 HOSTS 文件。

3.1.2.2 端口



SMTP、ODMR 和 MSA 端口

SMTP 入站端口
MDaemon 将会在此端口监控从 SMTP 客户端连入的连接。第一个端口是主 SMTP 端口，在大多数情况下使用默认的 25 端口。

SMTP 出站端口
当发送邮件到其他SMTP服务器时，将使用此端口。

MSA 入站端口
这是一个邮件提交代理 (MSA)端口，您的用户可以用它来替代上述指定的 *SMTP 入站端口* 。在这个端口上个传输需要验证，因此使用这个端口发信的用户必须准确地配置他们的客户端来确保连接经过认证。另外，由于一些ISP屏蔽了25端口，远程用户可以使用MSA端口在代替。如果不希望使用指定的 MSA 端口，可以指定 "0"来禁用此功能。

> 连接到 MSA 端口将免除 PTR 和反向查询，主机和 IP 屏蔽和阻止设置。MSA 端口连接将继续利用目录攻击连接限制。

ODMR 出站端口
MDaemon 会在这个端口上监视进入的 ODMR 连接，例如来自“域网关”的 ATRN。

SMTP SSL 端口
这个端口是使用 SSL 连接专门进行 SMTP 邮件通话的。请参阅 "SSL & 证书 479"来获得更多信息。

POP 和 IMAP 端口

POP 入站端口
MDaemon 会从在此端口监听远程 POP 客户端上连入的连接。

POP 出站端口
使用此端口，从 POP 服务器上检索邮件。

IMAP 入站端口
MDaemon将会用此端口来监听进入的IMAP请求。

POP SSL 端口
这个端口是使用 SSL 连接，专门为 POP 邮件客户端所用。请参阅 "SSL & 证书 479"来获得更多信息。

IMAP SSL 端口
这个端口是使用 SSL 连接，专门为 IMAP 邮件客户端所用。请参阅 "SSL & 证书 479"来获得更多信息。

其他端口

DNS 出站端口
输入您希望 MDaemon 用来收发数据报到 DNS 服务器的端口。

LDAP 端口
MDaemon 将会使用此端口发送数据库和地址薄信息到您的 LDAP 服务器。

请参阅：LDAP 地址簿支持 696

Remote Admin 端口
这个端口将会监听 Remote Administration 293 连接。

Minger端口
这是 Minger 724 服务器用来监控连接的端口。

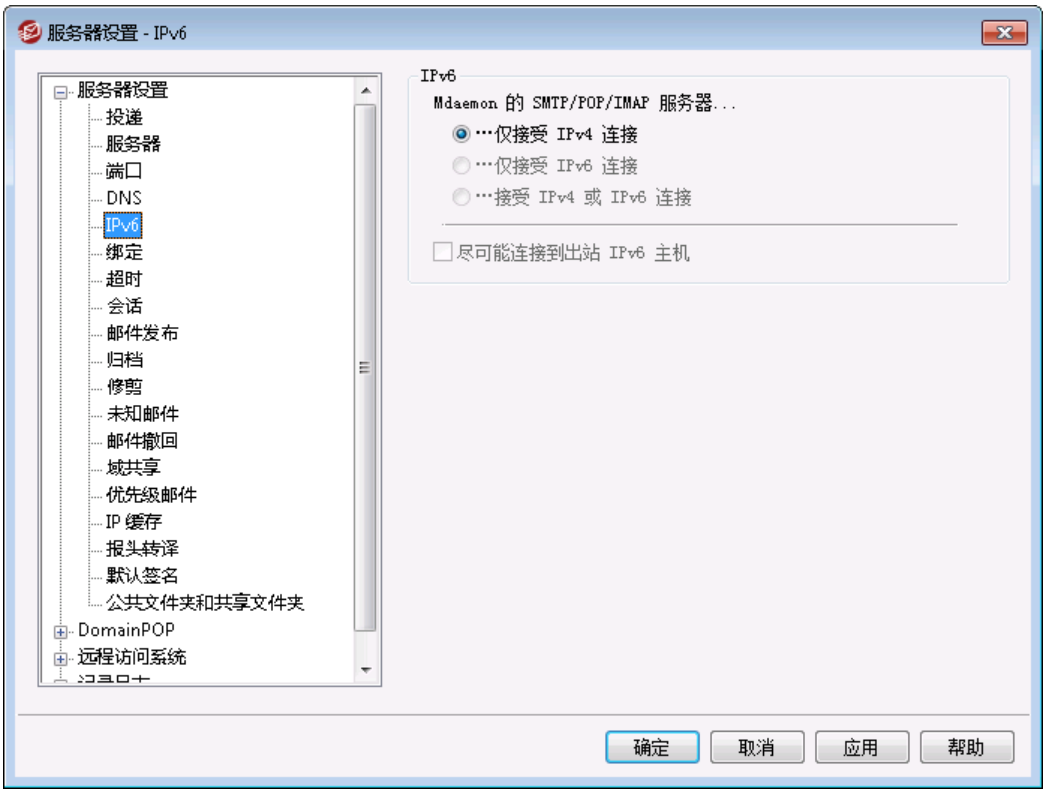
端口设置还原为默认值
这个按钮将会使端口设置变回它们的标准值。

立即绑定到新的端口值
当您对任意的端口值设置进行了改动时，您需要按此按钮使得您的更改能够立刻起效。否则，您的更改在下次服务器启动前，都不会被应用。

上述的端口设置已经是对合适的服务器操作进行了鉴定的，除非您确定您确实需要，否则就不应该更改设置。设置 MDaemon 使用的端口可以允许使用代理系统或者其他需要某些端口号的软件服务进行操作。

一个 IP 地址（一台机器）只能有一个可用的端口。如果一个程序试图连接已经在被另一个程序所使用的端口，那么一个错误信息将会提示使用者所需地址（IP:PORT）正在使用中。

3.1.2.3 IPv6



默认情况下，MDaemon 检测您系统支持的 IPv6 能力级别和可用双栈。否则 MDaemon 将单独监控 IPv4 和 IPv6。

IPv6

MDaemon 的 SMTP/POP3/IMAP 服务器...

...仅接受 IPv4 连接
如果您希望仅接受 IPv4 连接请选择此项。

...仅接受 IPv6 连接
如果您希望仅接受 IPv6 连接请选择此项。

...接受 IPv4 或 IPv6 连接
如果您希望接受 IPv4 和 IPv6 连接，请选择此项。这是默认设置，而且 MDaemon 将在可能时比 IPv4 优先考虑 IPv6。

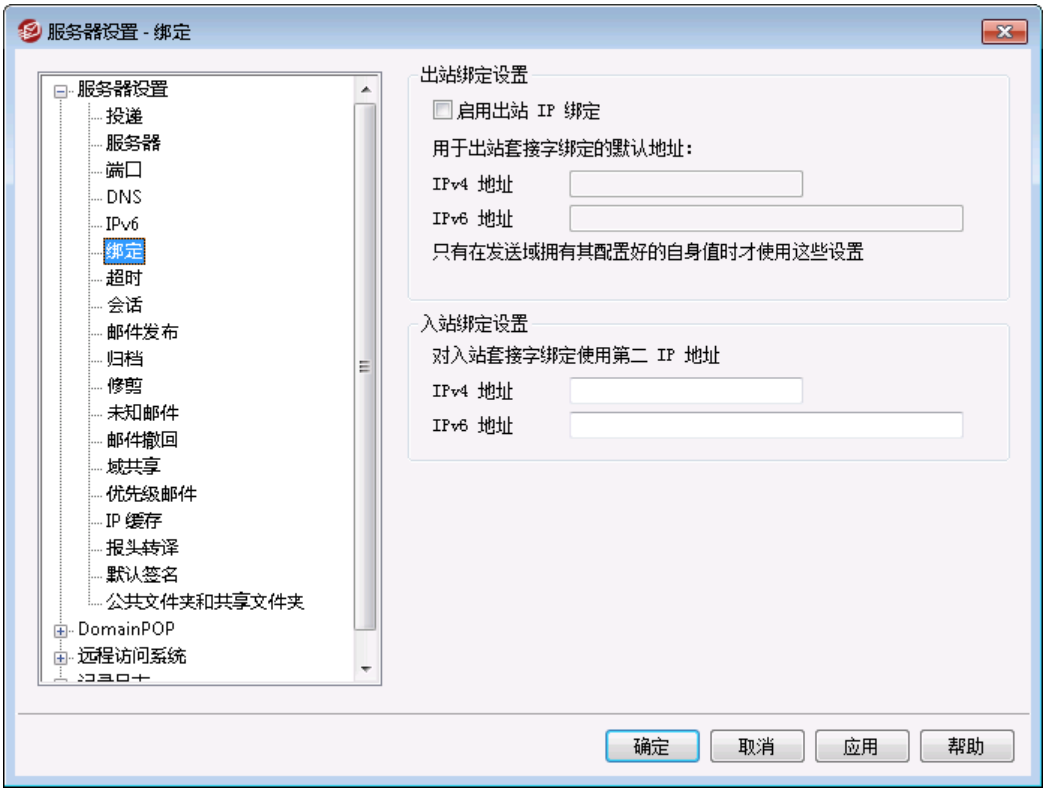
在可能时连接到出站 IPv6 主机
如果您希望 MDaemon 在可能时便连接到出站 IPv6 主机，请启用此项。

> 在 MDaemon 连接到 IPv6 主机时，它必须使用其自身的 IPv6 本地地址。IPv6 地址在 "域管理器 » 主机名称 & IP 151"屏幕上指定。必要时，可以在 "绑定 90"屏幕上指定出站套接字绑定的地址。

还请参阅：

绑定 90
域管理器 » 主机名称 & IP 151

3.1.2.4 绑定



出站绑定设置

启用出站 IP 绑定
勾选此项时，MDaemon 始终绑定出站套接字。至于勾选了 *"此域仅识别与这些 IP 建立的连接 151"*这个选项（位于 "主机名 & IP 151"屏幕）的那些域，MDaemon 将使用为该域配置的 IP。否则它将使用下方指定的 *"用于出站套接字绑定的默认地址"*。

出站套接字绑定的默认地址：IPv4/IPv6 地址
这些是将为出站套接字绑定使用的 IP 地址，用于在“域管理器”的“主机名称 & IP 151”屏幕上还未绑定到特定 IP 地址的域。

入站绑定设置

入站套接字绑定的次要 IP 地址：IPv4/IPv6 地址
如果您希望为入站套接字绑定 151 指定次要 IP 地址集，请使用此项。

还请参阅：

域管理器 » 主机名称 & IP 151
IPv6 89

3.1.2.5 IP 缓存

为了加速邮件投递和缩短邮件处理时间，MDaemon 缓存所有来自联系人的主机 IP。这些 IP 被存储下来，并且每次 MDaemon 对主机名要求进行 DNS 解析时，都将检查缓存。如果需要解析的主机名在 IP 缓存中找到，则跳过 DNS 查询，这可以节省大量的处理时间。窗口中的此设置允许您处理将运行的缓存的参数。也可以手动添加及删除条目，设置是否使用 DNSSEC，缓存的最大值，以及指定条目可以保存在缓存中的时间长短。IP 缓存可以从“设置 » 服务器设置» IP 缓存”菜单选项中获得。

IP 缓存

主机
输入您希望添加到 IP 缓存的主机。

IP
输入您希望添加到 IP 缓存的 IP 地址。

DNSSEC
为 DNSSEC 勾选此框。

添加
一旦你已经手动输入了一个主机和 IP 地址，单击此按钮以将它添加到缓存。

删除
如果您希望从列表中删除一个缓存 IP 地址，选择该条目并点击此按钮。

清除
该按钮将删除缓存中的所有条目。

无缓存
点击此按钮提出你不希望 MDaemon 添加到 IP 缓存的域名和/或 IP 地址列表。

设置

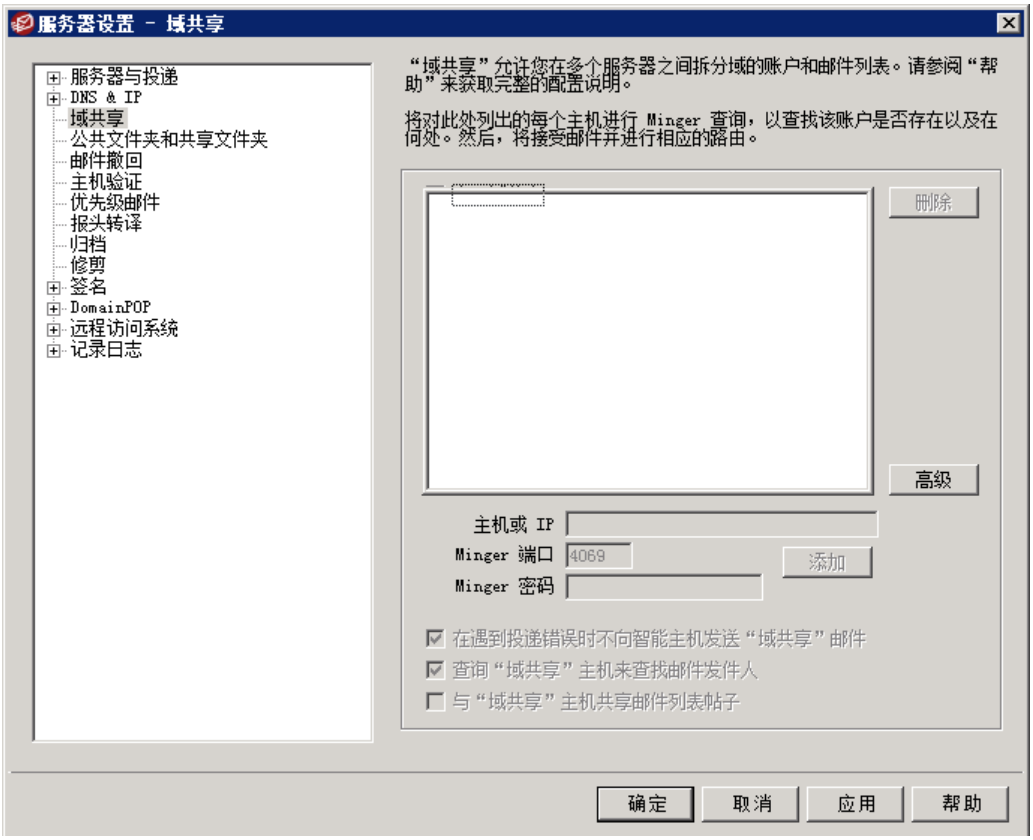
自动缓存未缓存的域
该选项控制 MDaemon 内部的自动缓存引擎。如果您希望 MDaemon 自动缓存域，则启用此选项。如果您希望自己创建 IP 缓存，则清空此复选框。

在每次处理时间间隔清除缓存
如果选中该选项，缓存的全部内容将在每次邮件会话开始时被清除掉。这允许在每次处理间隔刷新缓存。

默认生存时间（分钟）
这是条目在 IP 缓存中保留时间的默认值，以分钟计算。一旦条目在缓存中存在了这么长时间，MDaemon 将会删除它。如果您希望在 IP 缓存中设置一个永久条目，那么请将*默认生存时间*指定为 9999。

最大缓存条目
该值决定了缓存可能为多大。一旦达到了这个设置值，下一个缓存条目将会把第一个条目顶出。

3.1.3 域共享



域共享是一个新功能，允许您跨多个服务器划分一个域的用户。这帮助您在不同的位置上运行 MDaemon 服务器，不同的用户账户全部使用相同的域名。一台服务器托管您域的一部分用户账户，其余账户由一个或更多其他服务器托管。域共享对话框用于指定每个其他服务器的位置。那么，当一封发送至没有本地邮箱的本地用户的邮件抵达时，域共享将使用 Minger 询问其他服务器以找寻是否那些服务器中有一个存在该用户的账户。如果找到的地址是有效的，MDaemon 会接收邮件并将其路由至该账户位于的服务器。

比如，您在多个城市有办公室并选择使用域共享以允许每个员工的邮件地址的结尾为“example.com”。每个办公室的 MDaemon 会托管一部分 example.com 的邮件，只拥有在该办公室工作的本地员工账户。然后将每个办公室配置为使用域共享，这样每个人的邮件都会被路由到当前的办公室。

因为域共享使用 Minger 724 来验证这些地址，必须启用 Minger 并正确地配置每台服务器以便执行查询。如果在 Minger 查询期间发生错误，例如某台服务器临时不可用，MDaemon 将使用“451”临时错误代码响应，这样发件服务器可以设法在稍后再次投递该邮件。此外，一旦某一个地址已通过认证，它将被缓存五天，今后再碰到该地址发来的邮件，MDaemon 就能立即接收并开始尝试路由邮件到适当的主机。

最后，要避免在多个服务器上创建相同账户的潜在性问题，MDaemon 在创建任何一个新账户前会查询所有的域共享服务器。

有一个选项叫做 *Minger 验证查询总是触发域共享查询*”，位于“网关编辑器”的设置 222 屏幕上。每当某一网关使用了 Minger 验

证[213]，可以启用该选项让 MDaemon 同样查询您的域共享主机。

启用域共享
勾选此框来启用 "域共享"。在您启用了域共享并添加了所有的域共享主机或者 IP 地址到列表后请确保您同样启用和配置了 Minger[724]，这样在这些主机尝试验证您的本地地址时，您可以响应来自这些主机的查询。

删除
要删除您的某一域共享条目，请从列表中选中该条目然后点击此按钮。

高级
此按钮将打开一个文件，您可以在其中配置允许使用 "域共享"的域名。如果此文件中没有任何内容 (默认情况)，则所有域都可以使用 "域共享"。请参阅文件顶部的指示来获取更多信息。

主机或 IP
使用此框来输入共享您一个或多个域的主机或者 IP 地址。如果您希望在将 SMTP 邮件发送到主机时使用非默认的特定端口，您可以附加冒号与端口号 (例如：mail.example.com:2525)，这与以下的 Minger 端口不同。

Minger 端口
当查询主机时，Minger 将会使用此端口。默认的端口是 4069。

Minger 密码 (可选)
如果您添加的主机需要一个 Minger 密码，请在此输入。设置 Minger 需要密码是可选的，不过推荐使用。

添加
输入主机或 IP、端口和密码后，点击此按钮来添加新的域共享条目到此列表。

出现投递错误时不将 "域共享"邮件发送到智能主机
启用此项时，如果 MDaemon 在尝试投递域共享邮件时遇到错误 (例如域共享主机处于离线状态)，就会将该邮件保留在队列[732]中，而不是将其发送至智能主机[76]。将这些邮件发送至智能主机通常会导致邮件循环。默认情况下启用此项。

邮件发件人的 "查询域共享"主机
默认情况下，MDaemon 将接受来自其他 "域共享"主机上存在的账户的邮件。如果您不想在 SMTP MAIL 发件人上执行任何 "域共享"查找，请禁用此选项。

与 "域共享"主机共享邮件列表帖子
如果您希望与 "域共享"主机共享邮件列表，请启用此选项。当邮件抵达邮件列表时，将为每个 "域共享"主机创建一个副本，同时保留该列表的版本 (通过查询来进行检查)。这些主机收到副本后，会将邮件投递给它们所服务的所有列表成员。这样，邮件列表可以在多个服务器之间进行拆分，而不会损失功能。为此，每个 "域共享"主机必须在其可信 IP[435]配置中包含其他主机的 IP。否则，可能会因 "发件人不是列表成员"这个错误而拒绝列表邮件。

还请参阅：

Minger 724
域管理器 149

3.1.4 公共文件夹和共享文件夹

MDaemon 支持共享公共和用户 IMAP 文件夹。公共文件夹 (可以从 "公共文件夹管理器 258 "进行管理)是不属于任何特定账户、但可供多个 IMAP 用户使用的特别账户。用户文件夹是属于个别 MDaemon 账户的 IMAP 文件夹。每个共享文件夹，无论公共还是用户，都必须拥有一个与之关联的 MDaemon 用户列表，而且只有该访问列表的成员才可以通过 MDaemon Webmail 或 IMAP 电子邮件客户端访问该文件夹。

当 IMAP 用户访问其个人文件夹列表时，他们将看见被授权访问的共享的公共文件夹和共享用户文件夹。以这种方式，多个用户可共享某些邮件文件夹，但仍需要提供每个用户的个人登录凭证。不仅如此，拥有一个文件夹的访问权限并不一定意味着对此文件夹拥有完全的读/写或者管理权限。可以授予个别用户特定访问权限，因此对每一个用户，允许您设置不同的访问级别。例如，您可能允许某些用户删除邮件，但禁止他人如此操作。

一旦创建了公共或用户 IMAP 文件夹，就可使用 "内容过滤器"来设置将邮件移入此文件夹的条件。例如，制定一条过滤器规则将在 TO: 报头中包含 support@example.com 报头中的邮件移入 Support 公共文件夹可能会很有用。内容过滤器操作 542 "移动邮件到公共文件夹..."和 "复制邮件到文件夹..."使之成为可能。对于共享用户文件夹，可使用个人 IMAP 过滤器 617 将特定邮件路由到该文件夹中。除了使用内容过滤器和 IMAP 过滤器之外，可将特定账户关联到共享文件夹，使得目标为 "提交地址"的邮件被自动路由到该共享文件夹中。然而，只有那些被授予了该文件夹 "投递"权限的用户才能发送到此地址。

为了更为方便，邮件列表编辑器也包含有公共文件夹 248 屏幕，从而使您可配置用于特定列表的公共文件夹。如果启用该功能，则每个列表邮件的副本将会放置到指定公共文件夹中。所有公共文件夹都保存在 MDaemon 目录层级中的 \Public Folders\ 目录中。

Webmail文档文件夹

Webmail主题现在支持使用文档文件夹共享文档。文档文件夹完全支持访问控制列表 (ACL) 260 (就像其他共享文件夹一样)，该文件夹可以用来设置权限和共享规则，以及能够通过这个系统进行共享的任何文件类型。Webmail用户可以使用内置的工具将文件上传到其文档文件夹中。此外，在使用 LookOut 主题时，能够支持 HTML5 拖放功能的 API (例如 Chrome 和 Firefox)还可以通过将文件从桌面拖拽到浏览器窗口来上传这些文件。文件名可以进行搜索和重命名操作，还能将文件附加到正在编辑的新邮件中。

您可以通过分别编辑 \WorldClient\Domains.ini 文件和个别 \Users\..\WC\user.ini 文件来按域或按用户启用/禁用文档文件夹 (和其他共享文件夹)。您还可以配置默认设置和自定义设置来覆盖默认值。例如：

```
[Default:UserDefaults]
DocumentsFolderName=Documents
EnableDocuments=Yes

[example.com:UserDefaults]
DocumentsFolderName=Example Documents
EnableDocuments=Yes
```

```
[superControllingDomain.gov:UserDefaults]
EnableDocuments=No
EnableCalendar=No
EnableNotes=No
EnableTasks=No
```

设置文件大小最大值

您可以通过在“domains.ini”文件中添加以下项来限制被上传至文档文件夹的个别文件的大小：MaxAttachmentSize=<值的单位是 KB> 默认值是“0”，表示无限制。

阻止或允许文件类型

要阻止特定的文件类型被上传至文档文件夹，请将“BlockFileTypes=”这一项添加到“domains.ini”文件中，列出您希望阻止的文件类型，使用空格或逗号进行分隔。例如“BlockFileTypes=exe dll js”。

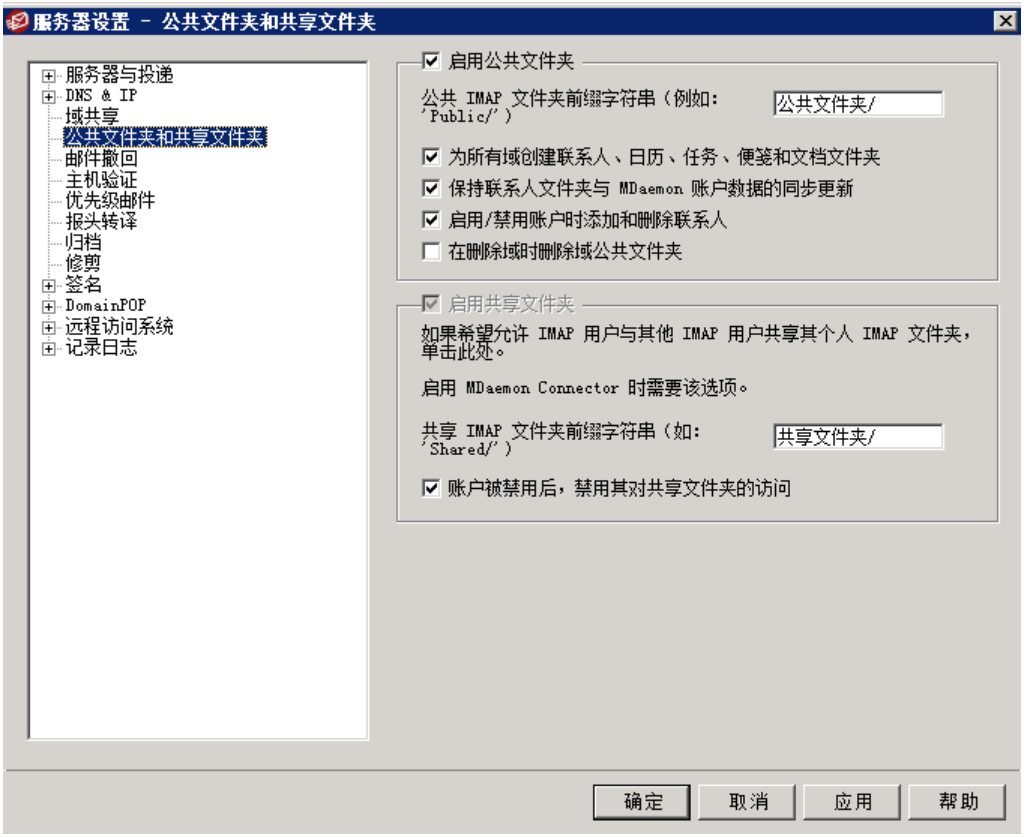
要允许特定的文件类型被上传至文档文件夹，请将“AllowFileTypes=”这一项添加到“domains.ini”文件中，列出您希望允许的文件类型，使用空格或逗号进行分隔。例如“AllowFileTypes=jpg png doc docx xls xlsx”。

同时使用这两项时，在发生冲突的情况下被阻止的文件拥有较高的优先级，如果这两个列表中同时出现了一个扩展名，将阻止这个扩展名。如果使用的项中没有值（例如未列出扩展名），则不使用该项。文件扩展名可以包含“.”（e.g. .exe .dll），但不是必需的。

还请参阅：

公共文件夹和共享文件夹 97
公共文件夹管理器 258
访问控制列表 260
账户编辑器 » 共享文件夹 623
邮件列表 » 公共文件夹 248

3.1.4.1 公共文件夹和共享文件夹



要打开“公共文件夹和共享文件夹”屏幕，请点击“设置» 服务器设置» 公共文件夹和共享文件夹”。

启用公共文件夹

如果您希望允许用户获得公共文件夹的访问权，请点击此框。在公共文件夹管理器 258 上每个文件夹下面，指定了可访问该文件夹的用户和所授予的访问级别。如果希望向所有用户隐藏公共文件夹，请清除该复选框。

公共 IMAP 文件夹前缀字符串（例如：“Public/”）

公共文件夹的前缀字符串最多可达 20 个字符，例如“#”或“Public Folders/”。这是为了帮助用户在其邮件客户端内轻松区分公共文件夹和私人文件夹。使用该文本框可以指定用来表示公共文件夹的一系列字符。

为所有域创建联系人、日历、任务、日志和便签文件夹

如果希望确保所有域都存在这些文件夹，请点击该复选框。每当向 MDaemon 添加了域 149，就会创建这些文件夹。

保持联系人文件夹与 MDaemon 账户数据同步更新

如果启用该选项，MDaemon 将使联系人文件夹与其账户列表保持同步。

启用/禁用账户时添加和删除联系人
默认情况下，禁用账户后，该账户将从域的公共联系人文件夹中删除。然后，如果您重新启用该账户，它将再次被添加到联系人中。默认情况下启用此项，以防止被禁用的账户显示在 Webmail的自动完成系统中。

在删除域时删除域公共文件夹
如果您希望在删除域时，删除这个域的公共文件夹，请点击此勾选框。

启用共享文件夹

如果您希望允许 IMAP 用户共享其 IMAP 文件夹，请点击此选框。在 "账户编辑器"的 "共享文件夹[623]"屏幕上（"账户» 账户管理器» [用户账户] » 共享文件夹"）每个文件夹下面指定了可访问该文件夹的用户和所授予的访问级别。如果希望使用户无法共享其文件夹的访问权限，并阻止上述 "共享文件夹"屏幕出现在 "账户编辑器"上，请清除该复选框。

> 在使用 MDaemon Connector[323]时，此项不可用。您无法撤销该选项，因为必须共享用户文件夹才能使 MDaemon Connector 正常运行。

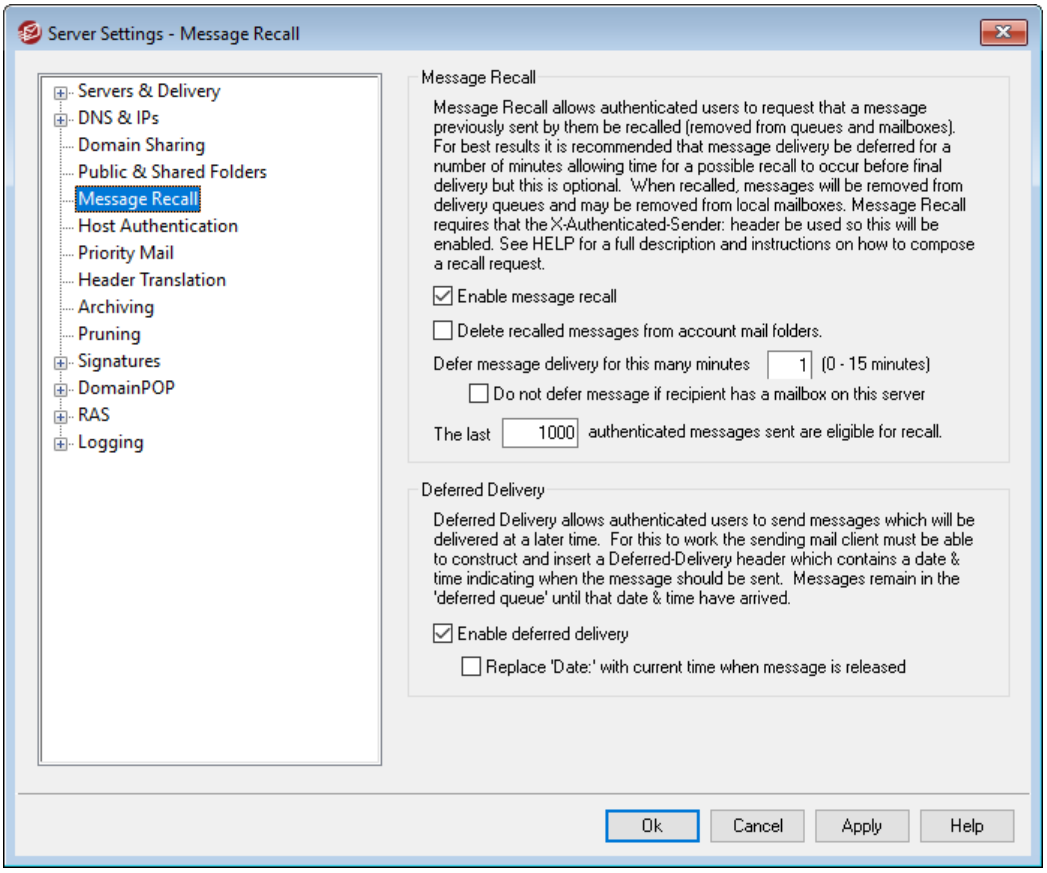
共享的 IMAP 文件夹前缀字符串 (如："Shared/")
共享用户文件夹的前缀字符串最多可达 20 个字符，例如 "Shared Folders/"。这是为了帮助用户在其邮件客户端内轻松区分共享文件夹和私人文件夹。使用该文本框可以指定用来表示共享文件夹的一系列字符。

禁用账户后，无法访问共享文件夹
默认情况下，MDaemon 的 IMAP、WebMail和 ActiveSync 服务器不允许对已禁用账户的共享文件夹的访问。如果您希望即使在禁用账户的情况下也允许访问账户共享文件夹，请清除此复选框。

还请参阅：

公共文件夹概述[95]
公共文件夹管理器[258]
访问控制列表[260]
账户编辑器 » 共享文件夹[623]
邮件列表 » 公共文件夹[248]

3.1.5 邮件撤回



邮件撤回系统

MDaemon 具有邮件撤销系统，您可以使用该系统将经过身份验证的本地用户发送的入站邮件延迟0到15分钟，从而为用户提供了一段较短的时间，使他们可以尝试阻止投递邮件。在这段延迟期间，邮件将放置在专用的延迟队列中，而不是直接进入入站邮件队列——延迟队列中的邮件具有设置为将队列编码为文件名的日期。MDaemon 每分钟检查一次队列，当邮件离开队列时，它将移至入站队列，并接受常规的邮件处理和投递。活动将被记录到 "路由"选项卡和日志文件中。

您可以根据需要将延迟时间设置为 "0"，但这增加了用户希望撤回的邮件可能已被投递的可能性。因此，建议至少延迟1或2分钟，以使您的用户有时间意识到他们想要撤回邮件，发送撤回请求，并留出时间让 MDaemon 处理该请求。不过，由于 MDaemon 能够从可能已经存在延迟的 "远程"队列中删除撤回的邮件，因此某些管理员可能会发现这个延迟投递计时器不是非常必要。

撤回邮件

用户可以通过多种方式来撤回一封邮件。

1. 在 MDaemon Webmail中，点击 "撤回"按钮，在 "已发送项目"文件夹中查看最近发送的邮件时显示该按钮。如果在撤回时间限制过期前点击此按钮，Webmail将向 MDaemon 发送一封 RECALL (撤回)邮件。

2. 将邮件发送到 mdaemon@example.com 系统账户，并以单词 "RECALL"（不带引号）作为邮件的主题。这将撤回您发送的上一封邮件。该功能只撤回上一封邮件。
3. 在 "已发送项目"文件夹中，找到您要撤回的邮件，选择 "转发为附件"选项，然后使用 "RECALL"作为邮件的主题，将邮件发送到 mdaemon@example.com 系统账户。
4. 查看邮件的报头，复制 "Message-ID：<message-ID value>"报头，并在主题中使用 "RECALL Message-ID：<message-ID value>"（无引号）新建一封邮件。

无论选择哪种撤回方式，MDaemon 都会向这名用户回发一封邮件，说明撤回操作是否成功。成功撤回邮件时，MDaemon 会删除队列中的指定邮件，就好像从未发送过这封邮件一样。此外如果启用了 *"删除账户邮件文件夹中的已撤回邮件"*这个选项，MDaemon 还将尝试从可能已投递该邮件的任何本地用户的邮件文件夹中删除这封被撤回的邮件。发送到多个收件人的邮件都将通过单个请求被撤回。最后，要是没有 "X-Authenticated-Sender"报头提供安全性，并防止其他人撤回不属于他们的邮件，"邮件撤回"系统将不起作用。因此，如果启用了 "邮件撤销"，将覆盖要禁用这个报头的选项 418。

邮件撤回

启用邮件撤回
点击该复选框来激活邮件撤回系统。默认情况下，禁用该选项。

删除账户邮件文件夹中已撤回的邮件
如果您还希望从本地 MDaemon 账户的邮件文件夹中删除已撤回的邮件（如果在撤回该邮件之前已经发送过这些邮件），请选中此框。这可能导致邮件从本地用户邮件客户端和电话中消失。默认情况下，禁用该选项。

延迟邮件投递长达这些分钟 XX（0-15 分钟）
这是 MDaemon 将为经过验证的本地用户保留入站邮件的分钟数。如果在延迟期间收到一封 RECALL（撤回）邮件，那么 MDaemon 将在做出任何投递尝试之前删除指定的邮件。可以将此项设置成 0-15 分钟。1 分钟是默认设置。

如果收件人在此服务器上有邮箱，则不延迟邮件
如果收件人的邮箱与发件人位于同一 MDaemon 服务器上时，您不希望延迟邮件，请选中此框。请注意：在使用上方的 *"删除账户邮件文件夹中的已撤回邮件"*这个选项时，即使是已投递的邮件，也能从用户的邮箱中撤回和删除。

上 [xx]封经过验证的已发邮件有资格撤回
MDaemon 会记住经过身份验证的用户发送的指定数量的最新电子邮件的邮件 ID 和位置。如果要撤回的邮件不在该组邮件中，则撤回尝试将失败。因此在使用上方的 *"删除账户邮件文件夹中的已撤回邮件"*这个选项时，即使邮件已经投递，也可以立即将其从用户邮箱中撤回。默认情况下，此选项设置为 1000 封邮件。

延迟投递

"延迟投递"选项允许经过身份验证的客户端发送要在预定日期和时间发送的消息。Webmail 包括此项，允许用户点击 "稍后发送"，并指定发送邮件的日期和时间。该邮件包含的 "延迟投递"邮件报头包含要投递邮件的日期和时间。如果 "邮件撤销"选项被启用，并且收到针对计划延迟投递邮件的撤销请求，MDaemon 将尝试删除已撤销的邮件。

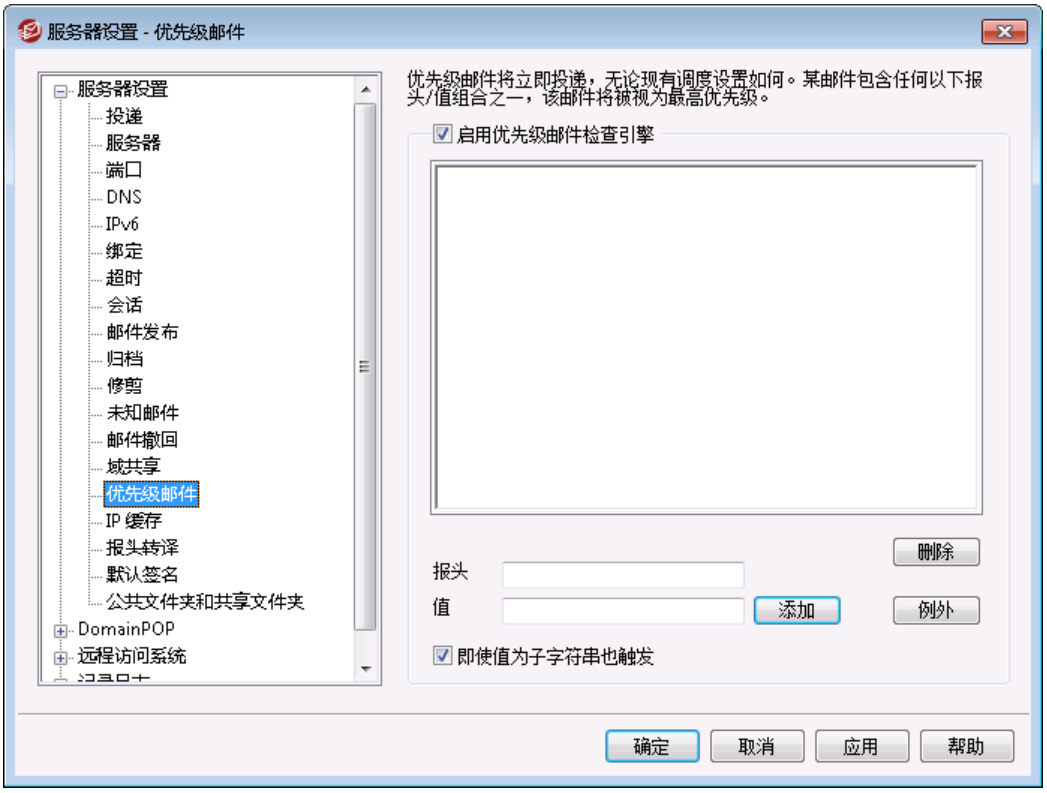
启用延迟投递
如果您希望允许通过验证的客户端使用 "延迟投递"报头来为邮件调度延迟投递，请启用此项。启用此项时，Webmail用户将能在 WorldClient 和 Lookout 主题中使用 **稍后发送**"选项。默认情况下，禁用该选项。

在释放邮件时将 "日期:"替换为当前时间
如果您希望在从 "延迟队列"释放邮件时，将 "日期:"报头 替换为当前日期和时间，请启用此项。默认情况下，禁用该选项。

3.1.6 主机验证

主机验证
使用此屏幕可配置任何主机的登录、密码和端口值。当 MDaemon 将 SMTP 邮件发送到该主机时，将使用此处找到的关联凭证。请注意，这些凭证属于后备之需，仅在其他针对特定任务的凭证不可用时才使用。例如，如果您为 "账户编辑器"的转发选项或 "网关管理器"的出队选项或许多其他任务特定设置中的任何一个配置登录和密码设置，则将使用这些凭证，并取代此处配置的任何凭证。此功能仅适用于主机名（不适用于 IP 地址）。

3.1.7 优先级邮件



"优先级邮件"屏幕可以从"设置» 服务器设置» 优先级邮件"菜单选项抵达。用它来指定您系统上组成优先级邮件的部分。优先级邮件将通过 MDaemon 立即进行投递，无论如何安排邮件处理间隔。当一封新邮件抵达时，MDaemon 将会检查其报头，以寻找您在此对话框上指定的一组报头/值组合。如果 MDaemon 发现了它们，它会认为此邮件具有高优先级，并且尝试立即投递它。

优先级邮件引擎

启用优先级邮件检查引擎
点击此框以启用优先级邮件功能。MDaemon 将检查入站邮件寻找优先级状态。

页眉
在字段输入邮件报头。不要包括结尾的冒号字符。

值
输入的值必须能够在指定的报头中找到，这是为了邮件可以被视作高优先级。

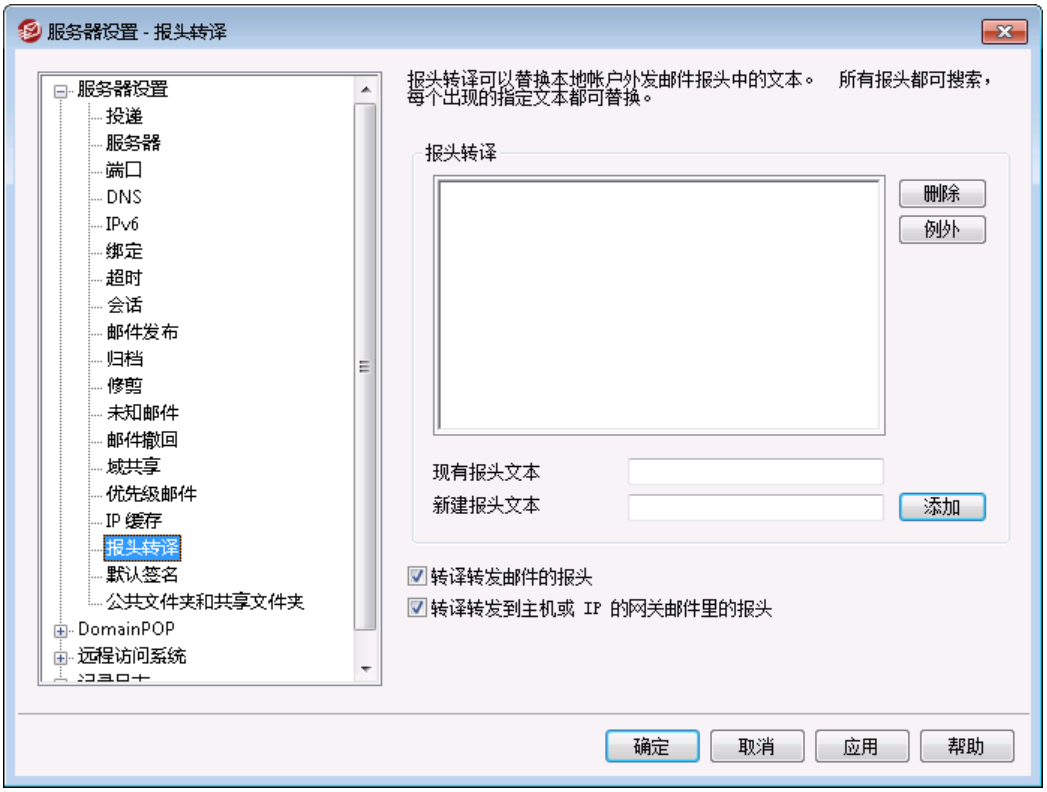
即使值为子字符串也触发
当输入一个新的优先级邮件设置时，您可以选择此功能以启用报头值一部分（或子字符串）的优先级匹配。比如，您可以为带有值"Boss"的"To"报头创建优先级邮件设置。那么，任何报头中包含"Boss@anything"的邮件将被视作优先级邮件。如果创建的条目没有启用这项功能，则报头值必须精确匹配条目；只匹配一部分是不够的。

添加
当在指定的文本框中输入报头/值信息后，并且指定是否此条目将会应用到子字符串，点击*添加*按钮来创建新的优先级邮件条目。

删除
点击此按钮以从 *"当前优先级邮件设置"*窗口中删除所选的条目。

例外
这允许您定义字段/值组合，使邮件被视作优先级邮件设置的例外。这将在此功能基础上赋予您更多的灵活性。

3.1.8 报头转译



只要邮件必须包含您指向远程服务器的域名，就可以使用报头转换功能替换报头中文本的任何部分。你可以指定邮件中的想要被替换的文本和相应的替换值。Mdaemon 将查找邮件中所有的报头，然后替换。您还可以指定 MDaemon **无法**修改的报头 (比如 "Subject:" 或 "Received:" 报头)，只要点击该对话框上的 *"例外"*按钮即可。

这个功能对于一些本地域名是伪造或不合法的或和外发邮件显示的域名不一样的 Mdaemon 设置是非常必要的。在这种情况下，可以使用报头转换将每一个 "localdomain"更改为 "RemoteDomain"。

报头转译
此列表包含一些文本信息，MDaemon 将会检查外发邮件报头并在发现匹配时，用该文本替换。

删除
在当前报头转译列表中选择一个条目，然后点击此按钮从列表中删除它。

例外
点击此按钮以打开报头转译例外 104 对话框。该对话框用来指定任何您希望从报头转译过程中忽略的报头。

现有报头文本
输入当在任何外发的邮件中存在并希望替换的文本。

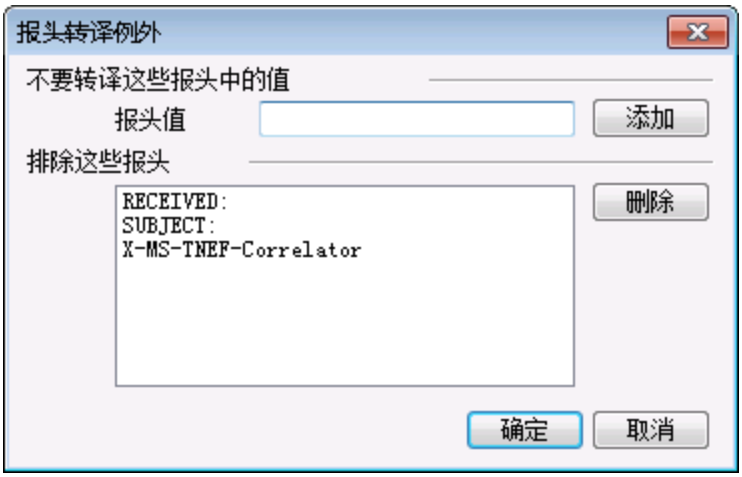
新建报头文本
该文本将会被用来替换您在*现有报头文本*区域中指定的那个。

添加
点击此按钮以添加以上文本参数到*报头转译*列表。

转译转发邮件的报头
点击此复选框以将报头转译也应用到从一个本地域自动转发到一个非本地域的邮件中。

转译转发到主机或 IP 的网关邮件里的报头
如果您希望报头在转发的域网关邮件中被转译，点击此复选框。要了解更多详情，请参见网关编辑器的转发 217 屏幕。

3.1.8.1 报头转译例外



不转译这些报头中的值

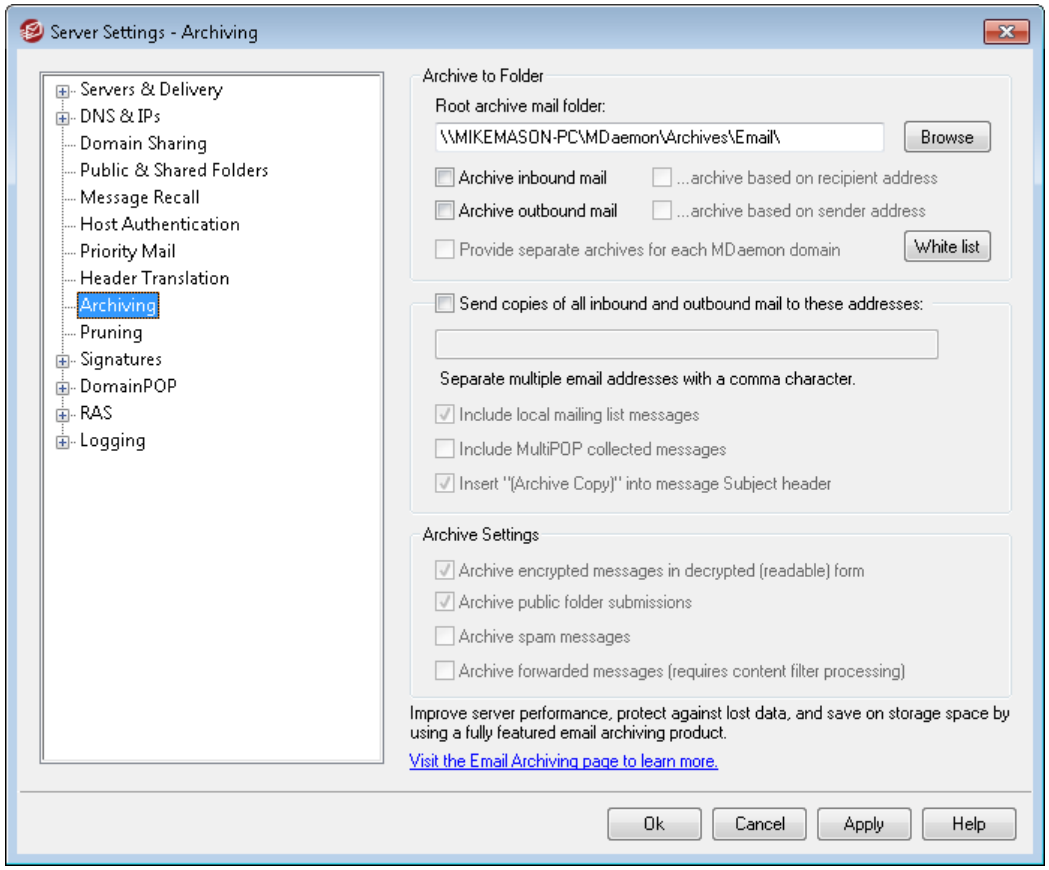
报头值
输入您希望从报头转译 103 过程中忽略的任何报头。

添加
点击此按钮以添加一个新报头到列表。

排除这些报头
当替换报头文本时，MDaemon 将不会扫描这些报头。

删除
在列表中选择一个报头，然后点击此按钮以删除它。

3.1.9 归档



使用此功能来将所有入站或出站邮件归档到一个文件夹。此文件夹的默认位置是 C:\MDaemon\Archives\Email\，不过您可以按需将其设置成任何文件夹。您可以选择归档指向您本地用户的入站邮件，来自您本地用户的出站邮件，或同时归档两者。邮件列表流量、正在中继的邮件、系统级邮件和自动应答器绝不会被归档。垃圾邮件或含有病毒的邮件也是如此。

会将入站和出站邮件分别保存在 \In\ 和 \Out\ 子文件夹中。可以使用下方的 *"..基于收件人地址归档"*和 *"..基于发件人地址归档"*选项进一步细分。此外，可以使用 *"为各个 MDaemon 域提供独立归档"*选项保留单独的归档。

会以邮件在本地用户的邮件文件夹中出现的最后状态保存归档邮件，或将出站邮件以 "准备投递"状态进行归档。这就意味着如果您使用内容过滤器对邮件做出变更，例如向其添加报头，则归档的邮件不会含有这种变更。

要浏览归档文件夹，使用您的一个邮件账户（或新建一个），并将其邮件文件夹[601]指向用于归档的相同文件夹。如果多人需要访问这个归档，则登录到归档账户并共享[623]所需文件夹（使用其访问控制列表[260]）。

有一个隐藏的系统队列位于："\MDaemon\Queues\ToArchive\"。将定期检查此队列中是否有通过插件或其他方式手动放置在其中的邮件。在此找到邮件后，将立即将其归档并删除。如果发现不符合归档条件的邮件，则将其删除。邮件成功归档后，"路由"屏幕/日志将显示详细信息。

归档到文件夹

请在此处指定您的归档邮件文件夹。此文件夹的默认位置是 C:\MDaemon\Archives\Email\，不过您可以按需将其设置成任何文件夹。

归档入站邮件

点击此复选框来保存将发送给本地用户的所有邮件的副本。不归档邮件列表邮件和含有病毒的邮件。

...基于收件人地址归档

如果您希望根据收件人电子邮件地址来分类入站邮件归档，请点击此选项。

归档出站邮件

点击此复选框来保存将发送给本地用户的所有邮件的副本。不归档邮件列表邮件和含有病毒的邮件。

...基于发件人地址归档

如果您希望根据发件人电子邮件地址来分类入站邮件归档，请点击此选项。

给每个 MDaemon 域提供各自的归档

如果您希望每一个域都有用单独的归档，请点击此对话框。

豁免列表

点击该按钮可打开"归档豁免列表"。您可以在此处列出希望免于归档的"收件人"和"发件人"地址。

发送所有入站和出站邮件的副本到这些地址。

输入一个或多个您希望发送归档邮件的地址。多地址时需要用逗号隔开。您可以指定本地和远程地址以及地址别名。

包含本地邮件列表的邮件

启用此项时，也将本地邮件列表邮件的副本发送到那些地址。

包含 MultiPOP 已收集的邮件

如果您希望通过 MDaemon 的MultiPOP[620]功能来发送邮件，请使用此选项。

插入“(归档副本)”到邮件主题报头
启用此选项后“(归档副本)”将插入到已发送邮件的主题：报头。报头里显示线索数量。

归档设置

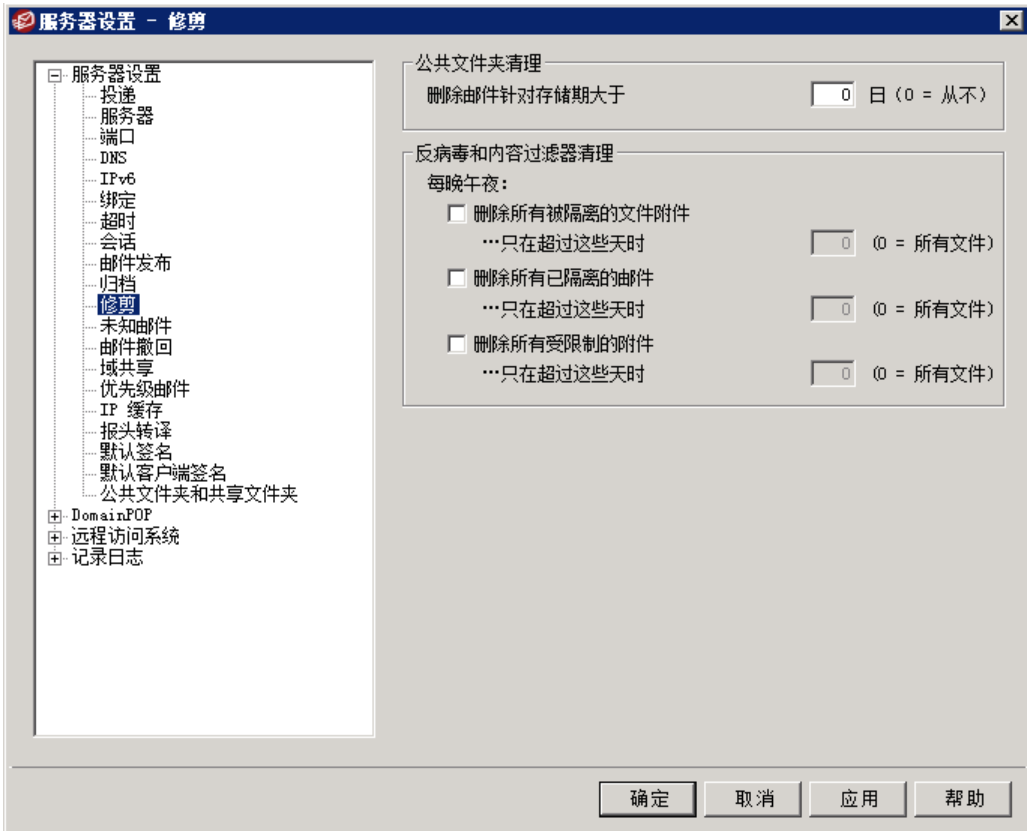
以解密(可读)形式归档加密邮件
默认情况下，加密邮件的未加密副本将存储在归档中。但是，如果无法解密邮件，则将存储加密的表单。如果您宁愿存储加密版本(即使可以解密)，也请禁用此选项。

归档公共文件夹提交
默认情况下，发送到公共文件夹提交地址的邮件将被归档。如果您不希望归档那些邮件，请禁用该选项。

归档垃圾邮件
如果您希望在归档和已发送副本中包含被标记成垃圾邮件的邮件，请启用此项。

归档转发的邮件(需要内容过滤处理)
如果您希望在归档和已发送副本中包含转发的邮件，请启用此选项。默认情况下不归档这些邮件。

3.1.10 清理



公共文件夹清理

删除旧于 XX 天的邮件 (0=永不)
如果您想从公共文件夹[95]中删除旧邮件，请在此选项中指定天数。

反病毒/内容过滤器清理

删除所有隔离文件
如果您希望每晚删除所有被隔离的文件附件，请点击此选项。

...仅在存在时间大于这些天时 [xx] (0 = 所有文件)
默认情况下将删除所有被隔离的文件。如果只希望删除早于该值的文件，则在此选项中指定天数。

删除所有被隔离的邮件
如果您希望每晚删除所有被隔离的邮件，请点击此选项。

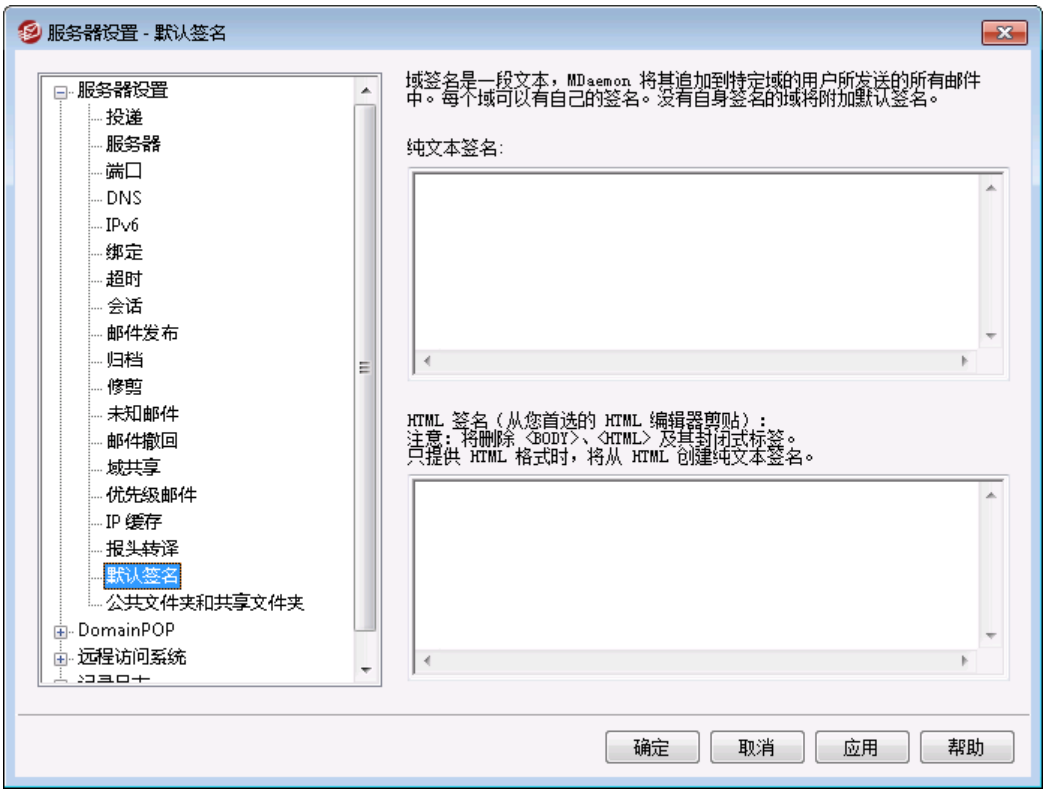
...仅在存在时间大于这些天时 [xx] (0 = 所有文件)
默认情况下将删除所有被隔离的邮件。如果只希望删除早于该值的邮件，则在此选项中指定天数。

删除所有受限附件
如果您想每晚删除所有受限的附件，请点击此选项。

...仅在存在时间大于这些天时 [xx] (0 = 所有文件)
默认情况下将删除所有受限制的附件。如果只希望删除早于该值的受限附件，则在此选项中指定天数。

3.1.11 签名

3.1.11.1 默认签名



使用此屏幕来将签名附加到由您 MDaemon 用户发送的所有邮件。如果您希望为特定域的用户使用不同的签名，请使用 "域管理器"上的签名[166]屏幕——存在视域而定的签名时，将使用这个签名来替代默认签名。签名被添加到邮件底部，除非邮件列表邮件已使用脚注，会将脚注[246]添加到 "域签名"之下。您还可使用 "账户编辑器"的签名[632]功能为每个账户添加个人签名。将在默认或域签名前添加账户签名。

纯文本签名

此区域用于插入纯文本签名。如果您希望在多部分邮件 (multipart message)的文本/html 部分中使用指定且相应的 html签名，请使用下方的*HTML 签名*屏幕。如果一个签名同时存在于这两个位置，MDaemon 将为多部分邮件的各个部分使用正确的签名。如果未指定 html签名，就会在两个部分中都使用纯文本签名。

HTML 签名 (剪贴自您首选的 HTML 编辑器)

此区域用于插入 HTML 签名，将在多部分邮件的文本/html部分使用。如果此处和上方的*纯文本签名*区域都包括同一个签名，MDaemon 将为多部分邮件的各个部分使用正确的签名。如果未指定纯本文签名，就会使用 html格式来创建一个签名。

要创建您的 html签名，可以在此处手动输入 html代码，也可直接从您首选的 HTML 编辑器对签名进行剪切和粘贴操作。如果您希望在您的 HTML 签名中包含内嵌图像，您可以使用 $ATTACH_INLINE:path_to_image_file$ 宏来实现这点。

例如：

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

还有多种将内嵌图像插入签名的方式，您可以从 MDaemon 的 Remote Administration 293 web 界面执行操作：

- 在 Remote Administration 的 "默认签名"屏幕上，点击 HTML 编辑器中的 "图像"工具栏按钮并选择上传选项卡。
- 在 Remote Administration 的 "默认签名"屏幕上，点击 HTML 编辑器中的 "添加图像"工具栏按钮。
- 借助 Chrome、FireFox、Safari 或 MSIE 10+，拖放图像到 "默认签名"屏幕的 HTML 编辑器
- 借助 Chrome、FireFox 或 MSIE 11+，将剪贴板中的图像复制粘贴到 "默认签名"屏幕的 HTML 编辑器

签名中不允许 <body></body> 和 <html></html> 标签，而且在找到这些标签时会将它们删除。

签名宏

MDaemon 签名支持将发件人的联系信息插入签名的宏，该签名取自位于其域的公共联系人文件夹中的发件人联系人。这允许使用发件人的信息对默认和域签名进行个性化。例如 $CONTACTFULLNAME$ 插入发件人的全名，$CONTACTEMAILADDRESS$ 插入发件人的邮件地址。使用 Webmail、MDaemon Connector 或 ActiveSync 来编辑公共联系人。如果发件人不存在联系人，则使用空值。可用的宏如下所示。

用户可以通过使用 $SYSTEMSIGNATURE$ 宏放置默认/域签名，并使用 $ACCOUNTSIGNATURE$ 放置账户签名来控制 MDaemon 签名在其邮件中的位置。

Signature Selector	
$SYSTEMSIGNATURE$	Places the Default Signature 109 or Domain Signature 166 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 113 or Domain Client Signature 170 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 632 in the message.
姓名和 ID	
全名	**$CONTACTFULLNAME$**
名	**$CONTACTFIRSTNAME$**

中间名	**$CONTACTMIDDLENAME$,**
姓	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
后缀	**$CONTACTSUFFIX$**
昵称	**$CONTACTNICKNAME$**
Yomi名	**$CONTACTYOMIFIRSTNAME$**
Yomi姓	**$CONTACTYOMILASTNAME$**
账户名称	**$CONTACTACCOUNTNAME$**
客户 ID	**$CONTACTCUSTOMERID$**
政府 ID	**$CONTACTGOVERNMENTID$**
文件作为	**$CONTACTFILEAS$**
电子邮件地址	
电子邮件地址	**$CONTACTEMAILADDRESS$**
电子邮件地址 2	**$CONTACTEMAILADDRESS2$**
电子邮件地址 3	**$CONTACTEMAILADDRESS3$**
电话和传真号码	
手机号码	**$CONTACTHOMEMOBILE$**
手机 2	**$CONTACTMOBILE2$**
车载电话	**$CONTACTCARPHONENUMBER$**
家庭电话	**$CONTACTHOMEPHONE$**
家庭电话 2	**$CONTACTHOMEPHONE2$**
家庭传真	**$CONTACTHOMEFAX$**
其他电话	**$CONTACTOTHERPHONE$**
即时通讯和 Web	
IM 地址	**$CONTACTIMADDRESS$**
IM 地址 2	**$CONTACTIMADDRESS2$**
IM 地址 3	**$CONTACTIMADDRESS3$**
MMD 地址	**$CONTACTMMSADDRESS$**
家庭网址	**$CONTACTHOMEWEBADDRESS$**
地址	

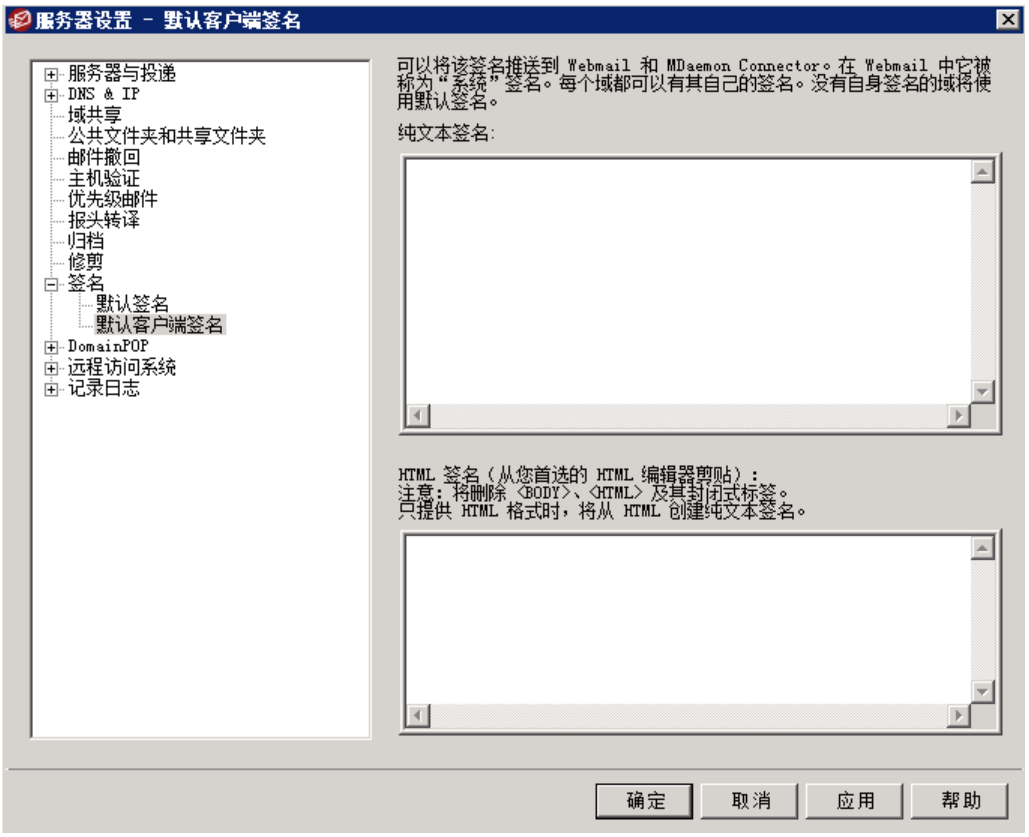
家庭地址	**$CONTACTHOMEADDRESS$**
家乡城市	**$CONTACTHOMECITY$**
家乡州	**$CONTACTHOMESTATE$**
家乡邮政编码	**$CONTACTHOMEZIPCODE$**
家乡国家	**$CONTACTHOMECOUNTRY$**
其他地址	**$CONTACTOTHERADDRESS$**
其他城市	**$CONTACTOTHERCITY$**
其他州	**$CONTACTOTHERSTATE$**
其他邮政编码	**$CONTACTOTHERZIPCODE$**
其他国家	**$CONTACTOTHERCOUNTRY$**
公司相关	
公司名称	**$CONTACTBUSINESSCOMPANY$**
Yomi公司名称	**$CONTACTYOMICOMPANYNAME$**
公司职位	**$CONTACTBUSINESSTITLE$**
公司办公室	**$CONTACTBUSINESSOFFICE$**
公司部门	**$CONTACTBUSINESSDEPARTMENT$**
公司经理	**$CONTACTBUSINESSMANAGER$**
公司助理	**$CONTACTBUSINESSASSISTANT$**
公司助理电话	**$CONTACTBUSINESSASSISTANTPHONE$**
公司总机	**$CONTACTBUSINESSMAINPHONE$**
公司电话	**$CONTACTBUSINESSPHONE$**
公司电话 2	**$CONTACTBUSINESSPHONE2$**
公司 IP 电话	**$CONTACTBUSINESSIPPHONE$**
公司传真	**$CONTACTBUSINESSFAX$**
公司寻呼机	**$CONTACTBUSINESSPAGER$**
公司无线电	**$CONTACTBUSINESSRADIO$**
公司地址	**$CONTACTBUSINESSADDRESS$**
公司所在城市	**$CONTACTBUSINESSCITY$**
公司所在州	**$CONTACTBUSINESSSTATE$**
公司邮政编码	**$CONTACTBUSINESSZIPCODE$**
公司所在城市	**$CONTACTBUSINESSCOUNTRY$**

公司网址	**$CONTACTBUSINESSWEBADDRESS$**
其他	
配偶	**$CONTACTSPOUSE$**
孩童	**$CONTACTCHILDREN$**
类别	**$CONTACTCATEGORIES$**
备注	**$CONTACTCOMMENT$**

还请参阅：

域管理器 » 签名 166
账户编辑器 » 签名 632

3.1.11.2 默认客户端签名



使用此屏幕来创建默认的客户端签名，您可以将其推送至 MDaemon Webmail 289 和 MDaemon Connector 339，供您的用户在编写邮件时使用。您可以使用下方列出的宏 114 来个性化签名，这样签名对于每个用户都是唯一的，包括用户名、电子邮件地址和电话号码等元素。如果您希望为特定域的用户使用其他签名，请使用“域管理器”中的“客户端签名 170”屏幕。存在针对一个域的特定签名时，将使用这个签名来取代“默认客户端签名”。如果您希望将客户端签名推送至 Webmail，请使用“*推送客户端签名* 289”选项，如果您希望将其推送到 MDaemon Connector，请使用“*推送客户端签名至 Outlook* 339”选项。在 Webmail

的 "编写"选项中，推送的客户端签名被称为 "系统"。对于 MDaemon Connector，您可以为 Outlook 中将显示的签名指定名称。

纯文本签名

此区域用于插入纯文本签名。如果您希望在多部分邮件 (multipart message)的文本/html 部分中使用指定且相应的 html签名，请使用下方的 *"HTML 签名"*屏幕。如果一个签名同时存在于这两个位置，MDaemon 将为多部分邮件的各个部分使用正确的签名。如果未指定 html签名，就会在两个部分中都使用纯文本签名。

HTML 签名 (剪贴自您首选的 HTML 编辑器)

此区域用于插入 HTML 签名，将在多部分邮件的文本/html部分使用。如果此处和上方的 *"纯文本签名"*区域都包括同一个签名，MDaemon 将为多部分邮件的各个部分使用正确的签名。如果未指定纯本文签名，就会使用 html格式来创建一个签名。

要创建您的 html签名，可以在此处手动输入 html代码，也可直接从您首选的 HTML 编辑器对签名进行剪切和粘贴操作。如果您希望在您的 HTML 签名中包含内嵌图像，您可以使用 $ATTACH_INLINE:path_to_image_file$ 宏来实现这点。

例如：

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

还有多种从 MDaemon 的Remote Administration 293 web 界面，将内嵌图像插入签名的方法：

- 在 Remote Administration 的 "默认客户端签名"屏幕上，点击 HTML 编辑器中的 "图像"工具栏按钮并选择上传选项卡。
- 在 Remote Administration 的 "默认客户端签名"屏幕上，点击 HTML 编辑器中的 "添加图像"工具栏按钮。
- 将一个图像拖放到 "默认客户端签名"屏幕的 HTML 编辑器 (使用 Chrome、FireFox、Safari或 MSIE 10+)
- 借助 Chrome、FireFox 或 MSIE 11+，将剪贴板中的图像复制粘贴到 "默认客户端签名"屏幕的 HTML 编辑器

签名中不允许 <body></body> 和 <html></html> 标签，而且在找到这些标签时会将它们删除。

签名宏

MDaemon 签名支持将发件人的联系信息插入签名的宏，该签名取自位于其域的公共联系人文件夹中的发件人联系人。这允许使用发件人的信息对默认和域签名进行个性化。例如 $CONTACTFULLNAME$ 插入发件人的全名，$CONTACTEMAILADDRESS$ 插入发件人的邮件地址。使用 Webmail、MDaemon Connector 或 ActiveSync 来编辑公共联系人。如果发件人不存在联系人，则使用空值。可用的宏如下所示。

用户可以通过使用 $SYSTEMSIGNATURE$ 宏放置默认/域签名，并使用 $ACCOUNTSIGNATURE$ 放置账户签名来控制 MDaemon 签名在其邮件中的位置。

Signature Selector	
$SYSTEMSIGNATURE$	Places the Default Signature 109 or Domain Signature 166 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 113 or Domain Client Signature 170 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 632 in the message.
姓名和 ID	
全名	**$CONTACTFULLNAME$**
名	**$CONTACTFIRSTNAME$**
中间名	**$CONTACTMIDDLENAME$,**
姓	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
后缀	**$CONTACTSUFFIX$**
昵称	**$CONTACTNICKNAME$**
Yomi名	**$CONTACTYOMIFIRSTNAME$**
Yomi姓	**$CONTACTYOMILASTNAME$**
账户名称	**$CONTACTACCOUNTNAME$**
客户 ID	**$CONTACTCUSTOMERID$**
政府 ID	**$CONTACTGOVERNMENTID$**
文件作为	**$CONTACTFILEAS$**
电子邮件地址	
电子邮件地址	**$CONTACTEMAILADDRESS$**
电子邮件地址 2	**$CONTACTEMAILADDRESS2$**
电子邮件地址 3	**$CONTACTEMAILADDRESS3$**
电话和传真号码	
手机号码	**$CONTACTHOMEMOBILE$**
手机 2	**$CONTACTMOBILE2$**
车载电话	**$CONTACTCARPHONENUMBER$**

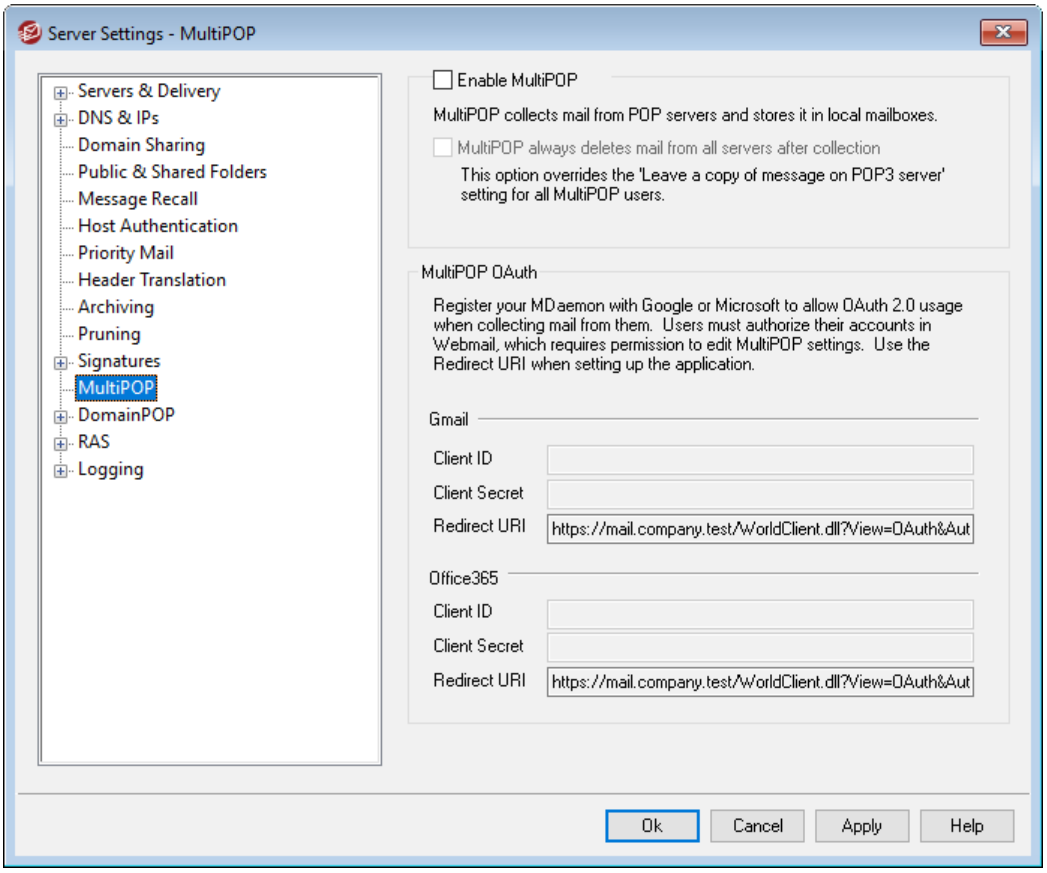
家庭电话	**$CONTACTHOMEPHONE$**
家庭电话 2	**$CONTACTHOMEPHONE2$**
家庭传真	**$CONTACTHOMEFAX$**
其他电话	**$CONTACTOTHERPHONE$**
即时通讯和 Web	
IM 地址	**$CONTACTIMADDRESS$**
IM 地址 2	**$CONTACTIMADDRESS2$**
IM 地址 3	**$CONTACTIMADDRESS3$**
MMD 地址	**$CONTACTMMSADDRESS$**
家庭网址	**$CONTACTHOMEWEBADDRESS$**
地址	
家庭地址	**$CONTACTHOMEADDRESS$**
家乡城市	**$CONTACTHOMECITY$**
家乡州	**$CONTACTHOMESTATE$**
家乡邮政编码	**$CONTACTHOMEZIPCODE$**
家乡国家	**$CONTACTHOMECOUNTRY$**
其他地址	**$CONTACTOTHERADDRESS$**
其他城市	**$CONTACTOTHERCITY$**
其他州	**$CONTACTOTHERSTATE$**
其他邮政编码	**$CONTACTOTHERZIPCODE$**
其他国家	**$CONTACTOTHERCOUNTRY$**
公司相关	
公司名称	**$CONTACTBUSINESSCOMPANY$**
Yomi公司名称	**$CONTACTYOMICOMPANYNAME$**
公司职位	**$CONTACTBUSINESSTITLE$**
公司办公室	**$CONTACTBUSINESSOFFICE$**
公司部门	**$CONTACTBUSINESSDEPARTMENT$**
公司经理	**$CONTACTBUSINESSMANAGER$**
公司助理	**$CONTACTBUSINESSASSISTANT$**
公司助理电话	**$CONTACTBUSINESSASSISTANTPHONE$**

公司总机	**$CONTACTBUSINESSMAINPHONE$**
公司电话	**$CONTACTBUSINESSPHONE$**
公司电话 2	**$CONTACTBUSINESSPHONE2$**
公司 IP 电话	**$CONTACTBUSINESSIPPHONE$**
公司传真	**$CONTACTBUSINESSFAX$**
公司寻呼机	**$CONTACTBUSINESSPAGER$**
公司无线电	**$CONTACTBUSINESSRADIO$**
公司地址	**$CONTACTBUSINESSADDRESS$**
公司所在城市	**$CONTACTBUSINESSCITY$**
公司所在州	**$CONTACTBUSINESSSTATE$**
公司邮政编码	**$CONTACTBUSINESSZIPCODE$**
公司所在城市	**$CONTACTBUSINESSCOUNTRY$**
公司网址	**$CONTACTBUSINESSWEBADDRESS$**
其他	
配偶	**$CONTACTSPOUSE$**
孩童	**$CONTACTCHILDREN$**
类别	**$CONTACTCATEGORIES$**
备注	**$CONTACTCOMMENT$**

还请参阅：

默认签名 109
域管理器 » 签名 166
域管理器 » 客户端签名 170
账户编辑器 » 签名 632
Webmail设置 289
MC客户端设置 » 签名 339

3.1.12 MultiPOP



启用 MultiPOP

勾选此框来启用 MultiPOP 服务器。MultiPOP 代表您的用户从 POP 服务器收集邮件，并将其存储在其本地邮箱中。MultiPOP 功能帮助您为多种来源的邮件集创建无限数量的 POP3 主机/用户/密码组合。这对那些在多个服务器上拥有邮件账户，而又希望将邮件收集并保存在一个地方的用户来说，非常有用。邮件在被放置到用户的邮箱之前，MultiPOP 所收集的邮件首先放置到本地队列中，以使它能像其他拥有自动应答器和内容过滤器的邮件一样被处理。MultiPOP 的调度选项位于：设置» 事件调度» 邮件调度选项» MultiPOP 收集[320]。

MultiPOP 在收集后始终删除所有服务器中的邮件

如果希望覆盖所有用户的 *"在 POP 服务器上保留邮件副本"*选项（位于"账户编辑器"的 MultiPOP[620]"屏幕上），请点击该复选框。所有邮件在收集后将从每个 MultiPOP 服务器上删除掉。

Send notification email after this many failures

By default, MDaemon sends a notification email after multiple failures when checking a MultiPOP account. Since temporary failures can be common, this option allows you to specify how many consecutive failures it takes to trigger the notification, and the option below allows you to choose how many days to wait between those notifications. The content and recipients of the notification emails can be customized by editing `\MDaemon\App\MPOPFailureNotice.dat`. By default the

notifications are sent to the MultiPOP account owner after 5 failures, no more than once every 7 days.

Do not notify again for this many days
By default MultiPOP failure notifications are sent no more than once every seven days. Use this option if you wish to adjust that interval.

MultiPOP OAuth

OAuth2.0 是 Gmail和 Microsoft Office)365 现在需要 (或即将需要)的现代身份验证方法，因为它们禁用了对传统/基本身份验证的支持。为了让 MDaemon 的 MultiPOP 功能使用 OAuth2.0 来代表用户从 Gmail或 Office365 收集邮件，您必须分别向 Google 或 Microsoft 注册 MDaemon 服务器，使用 Google API控制台或 Microsoft 的 Azure Active Directory 来创建 OAuth2.0 应用程序。这与为您的 Webmail用户使用 MDaemon 的 Dropbox 集成 282所需的流程类似。

要设置 MultiPOP 为您的用户从 Gmail或 Microsoft (Office) 365 收集邮件：

1. 启用上方的 "**启用 MultiPOP**"选项。
2. 按照以下指示来为 Gmail或 Office 365 创建并链接您的 MultiPOP OAuth 应用 120。
3. 在账户编辑器的 MultiPOP 页面 620上，为您希望允许使用 MultiPOP 来从 Gmail或 Office 365 检索邮件的每名用户**启用 MultiPOP**。
4. 为每名用户添加 Gmail(pop.gmail.com:995) 或 Office 365 (outlook.office365.com:995) 账户，并启用 "**使用 OAuth**"选项。此外，您可以让您的用户在 Webmail 266中亲自完成这一步。**请注意：**对于 Gmail账户，必须将每个 Gmail账户添加到您 GmailOAuth 应用中的 "测试用户"中(还请参阅**发布状态**注释，位于下方的*创建并链接您的 MultiPOP OAuth 应用* 120指南中)。
5. 在账户编辑器的 Web 服务 603页面上，为这些用户的每一个人启用 "...**编辑 MultiPOP 设置**"。
6. 每名用户必须登录其 Webmail，前往其 "选项"下方的 "**邮箱**"页面，添加其 Gmail或 Office 365 账户 (如果您没有为他们添加)，然后点击 "**授权**"来登录到其 Gmail或 Office 365 账户，并继续执行步骤来授权MDaemon 从该位置收集其邮件。

Gmail/Office 365

Client ID
这是在 Google API控制台或 Microsoft Azure Active Directory 门户中创建 MultiPOP OAuth2.0 应用时，分配的唯一客户端 ID。创建完应用程序后，复制其客户端 ID，并将其粘贴到此处。

Client Secret
这是在 Google API控制台或 Microsoft Azure Active Directory 门户中创建 MultiPOP OAuth2.0 应用时，分配的唯一客户端 Secret。创建完应用程序后，复制其 Client Secret，并将其粘贴到此处。**请注意：**在为 Azure 应用程序创建 Client Secret 时，必须在创建应用程序时复制它，因为之后它将不再可见。如果您当时未能复制它，那么您必须删除这个 Secret 并创建一个新的 Secret。

Redirect URI
在为 Gmail或 Office365 创建 OAuth2.0 应用程序时，必须指定 Redirect URI。这个显示在 MultiPOP 屏幕上的重定向 URI 是从您默认域的[149] SMTP 主机名称[151]创建而成的，在登录 Webmail时，它应该适用于该域的用户。您应该在用户登录 Webmail时，为他们前往的任何其他 MDaemon 域，将额外的重定向 URI 添加到您的应用程序。例如，"https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Office365"将适用于在登录 Webmail时，前往 mail.example.com 的任何用户。还请参阅：下方的**创建并链接您的 MultiPOP OAuth App**来获取更多信息。

Redirect URI 示例：

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

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

创建并链接您的 MultiPOP OAuth 应用

创建 MultiPOP OAuth 2.0 应用的按步指南。

对于 Google Gmail

按照以下步骤创建 Google 应用程序，以便在为用户从 Gmail收集邮件时，允许 MultiPOP 使用 OAuth2.0 进行身份验证。

1. 在您的浏览器中，前往 Google API 控制台.
2. 如果位于"项目列表"上，请点击 **"NEW PROJECT"**，如果位于管理资源页面，请点击 **(+) CREATE PROJECT**。
3. 输入**项目名称**，如果您希望编辑项目 ID 或使其保留默认值，请点击 **"编辑"**。**请注意：**在创建项目后无法更改项目 ID。
4. 在左窗格中，前往APIs & Services | OAuth consent屏幕。
5. 选择 **"External"**并点击 **"Create"**。
6. 输入**应用名称**（例如 MultiPOP OAuth 2.0 for Gmail）、供用户联系的**技术支持邮件地址**、供 Google 对于项目变更可以联系到的**开发人员邮件地址**。这就是该页面上需要完成的全部设置，不过取决于您特定的组织或验证要求，您还能输入公司徽标并链接到您的服务条款[304]和隐私策略。会为您自动填写 **"Authorized domains"**字段，在您稍后添加 *"Redirect URIs"*这一步时。**请注意：**此信息用于 Consent 屏幕，该屏幕将呈现给用户，以授权 MultiPOP 从 Gmail收集。
7. 点击 **"Save and Continue"**。
8. 点击 **"ADD OR REMOVE SCOPES"**，然后在 "Manually add scopes"下输入 **"https://mail.google.com/"**。点击 **"ADD TO TABLE"** 并点击 **"Update"**。
9. 点击 **"Save and Continue"**。
10. 在 "Test Users"下，请点击 **"ADD USERS"**，输入您将从中收集邮件的每个 Gmail账户，然后点击 **"ADD"**（请参阅下方有关您应用的发布状态[121]的注释）。
11. 点击 **"Save and Continue"**。

12. 在 Summary 上，点击位于页面底部的 "**BACK TO DASHBOARD**"。
13. 点击左窗格中的 "**Credentials**"，点击 **(+) Create Credentials** 并选择 **OAuth client ID**。
14. 在 "Application type"下拉框中选择 "**Web application**"，在 "Authorized redirect URIs"下点击 "**+ ADD URIs**"。输入重定向 URI。在 MultiPOP 屏幕上显示的 "重定向 URI"是从您默认域的[149] SMTP 主机名称[151]构建而成的示例，在登录到 Webmail 时应能适用于该域的用户。您应该在用户登录 Webmail 时，为他们前往的任何其他 MDaemon 域，将额外的重定向 URI 添加到您的应用程序。例如，"https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Gmail"将适用于在登录 Webmail 时，前往 mail.example.com 的任何用户。
15. 点击 "**CREATE**"。
16. 将 "**Your Client ID**"和 "**Your Client Secret**"中的值复制到 MultiPOP 页面上的 Gmail Client ID 和 Client Secret 框。

> **发布状态** — 这些指示用于通过 发布状态 (被设置成 "**Testing**")来创建 Google 应用。这需要您添加每个特定的 Google 账户，这些账户将使用该应用程序从 Gmail 收集他们的邮件，并且仅限于 100 个用户。此外，在 Webmail 中，当你的用户被要求授权 MDaemon 从 Gmail 收集邮件时，会显示一条警告信息："确认用户对你的项目有测试访问权限，但应考虑向未验证的应用程序授予对其数据的访问权限所存在的相关风险。"此外，授权在七天后到期，因此每个用户都需要每周从 Gmail 重新授权收集。
>
> 如果您希望删除这些要求和限制，那么您必须将您的状态更改为 "**In Production**"，这可能需要也可能不需要你进行验证过程。有关应用程序验证和发布状态的更多信息，请参阅以下 Google 文章：设置您的 OAuth 同意屏幕和 OAuth API 验证常见问题解答.

对于 Microsoft (Office) 365

按照以下步骤创建 Microsoft Azure 应用程序，以便在为用户收集 Office 365 邮件时，允许 MultiPOP 使用 OAuth2.0 进行身份验证。

1. 前往 Microsoft Azure Active Directory 页面，它位于 Azure 门户，并点击左窗格中的 "**App Registrations**"(如果您没有账户，您必须注册一个免费或付费的 Azure 账户)。
2. 点击 "**+ New Registration**"。
3. 请在 "**Name**"字段输入应用程序名称 (例如 "Mailbox OAuth for Office 365")。
4. 对于 "Supported account types"，请选择**Accounts in any organizational directory (Any Azure AD directory - Multitenant)**。
5. 对于 "Redirect URI"，请选择 "**web**"并输入您的 Office 365 **Redirect URI**。在 MultiPOP 屏幕上显示的 "重定向 URI"是从您默认域的[149] SMTP 主机名称[151]构建而成的示例，在登录到 Webmail 时应能适用于该域的用户。您应该在用户登录 Webmail 时，为他们前往的任何其他 MDaemon 域，将额外的重定向 URI 添加到您

的应用程序。例如，"https://mailexample.com/WorldClient.dll?View=OAuth&AuthRequest=Office365"将适用于在登录 Webmail 时，前往 mailexample.com 的任何用户。

6. 点击 **"Register"**。
7. 记录 **"Application (client) ID"**(附近有一个复制到剪贴板按钮)。您可以通过点击左窗格中的 **"Overview"**来找到此 ID。
8. 如果您需要添加额外的 Redirect URI，请点击右侧的 **"Redirect URIs: 1 web"**链接。点击 **"Add URI"**并输入 URI，重复是必要的，然后点击 **"Save"**。
9. 点击左窗格中的 **"API 权限"**。
10. 点击 **"+ Add a permission"**。
11. 点击 **"Microsoft Graph"**。
12. 点击 **"Delegated Permissions"**。
13. 向下滚动至 **"POP"**并选择 **"POP.AccessAsUser.All"**，然后在 **"User"**下选择 **"User.Read"**(默认情况下已选定 User.Read)。
14. 点击 **"Add permissions"**。
15. 在左窗格中，点击 **"Certificates & Secrets"**。
16. 点击 **"+ New Client Secret"**。
17. 输入描述 (例如 "Client secret for Office 365 MultiPOP OAuth app")。
18. 选择 Client Secret 多久过期。
19. 点击 **"添加"**。
20. 记录在 **"Value"**字段中生成的 Client Secret (附近有一个复制到剪贴板按钮)。**注意：**此页面上无法再次查看 Client Secret——条目旁有一个 **"Delete"**图标，这样您便能在必要时将其删除，并创建一个新的 Client Secret。
21. 请在 "服务器设置"下方 MDaemon 的 MultiPOP 页面的 Office 365 部分下的 **"Client ID"**和 **"Client Secret"**字段中输入 Application (Client) ID 和 Client Secret 的值。

还请参阅：

账户编辑器 | MultiPOP 620
邮件调度 | MultiPOP 收集 320

3.1.13 DomainPOP

使用 DomainPOP 邮件收集（"设置» 服务器设置» DomainPOP"）来配置 MDaemon 从远程 POP 邮箱下载邮件再分发到你的用户。此功能可以使用 POP3 协议来下载与指定登录信息相关联的 ISP 的 POP 邮箱中找到的所有邮件。一旦下载完成，将根据此对话框上提供的设置来解析邮件，然后分发到用户的邮箱或 MDaemon 的远程队列来投递，就好象邮件是使用了传统的 SMTP 处理来抵达服务器的。

值得注意的是，存储在邮箱中并且使用 POP3 协议进行检索的邮件将缺少重要的路由信息（有时被称为邮件的“信封”）。如果这些邮件是使用了更加强大的 SMTP 协议来投递，则将照常提供这些信息。没有这些信息，Mdaemon 会强制“读取”邮件并且检查这些报头来确定邮件的来源。至少说来这并非精确的科学。邮件报头由于缺乏必要的信息，有时很难确定邮件的目标收件人。这种缺乏的信息似乎是正常邮件的必要信息-收件人-但是必须知道，如果使用POP协议，邮件是不会被发送到收件人的。使用 SMTP，由于协议本身在传递会话中和服务器使用命令交互，所以邮件内容和收件人是不相关的。

为了让 POP 检索邮件和传递邮件更加可靠和协调，MDaemon 使用了一套强大的报头处理选项。当Mdaemon从远程POP下载邮件，立即会处理邮件中相关的邮件头，然后创建相关的收件人。在 MDaemon 检查的报头中找到的各个邮件地址都会包含在这个集合中。

当进程结束的时候，MDaemon 的收件人收集将被分为本地组和远程组。此外，所有被解析并被放入潜在收件人集合的所有地址，在被分为本地集合和远程集合之前都将经过“别名 699”转换程序的处理。本地集合的各个成员（地址使用匹配 MDaemon 本地域的域）将收到邮件的一个副本。对于远程集合地址，在这个对话框中设置。你可以选择简单地忽略这些地址，转发概要列表到邮件管理员—或 MDaemon 将真实传递邮件到远程收件人。只有在少数情况下，才需要保证把邮件传递到远程收件人。

必须要注意防止产生重复邮件或无限制的邮件传递循环。一个常见的问题就是邮件列表的邮件丢失标识自己的SMTP信封。典型的，由邮件列表分发的邮件通常在邮件体中不包含任何和收件人相关的地址。而是，邮件列表引擎仅会将邮件列表名称插入到“收件人：”这导致接下来的问题：如果“收件人：”字段中包含了邮件列表的名称，那么就有可能让 MDaemon 来下载该邮件，解析此“收件人：”字段（将会生成邮件列表的名称），然后将这封邮件发回相同的列表中。这将导致投递该邮件的备份到 MDaemon 下载该封初始邮件的 POP 邮箱—从而又导致了整个循环。为了解决这个问题，邮件管理员必须小心使用Mdaemon提供的工具来删除邮件列表邮件，或使用别名来把信件投递到相应的邮箱。您也可以使用“路由规则”或“内容过滤器”来将邮件投递到正确的收件人。

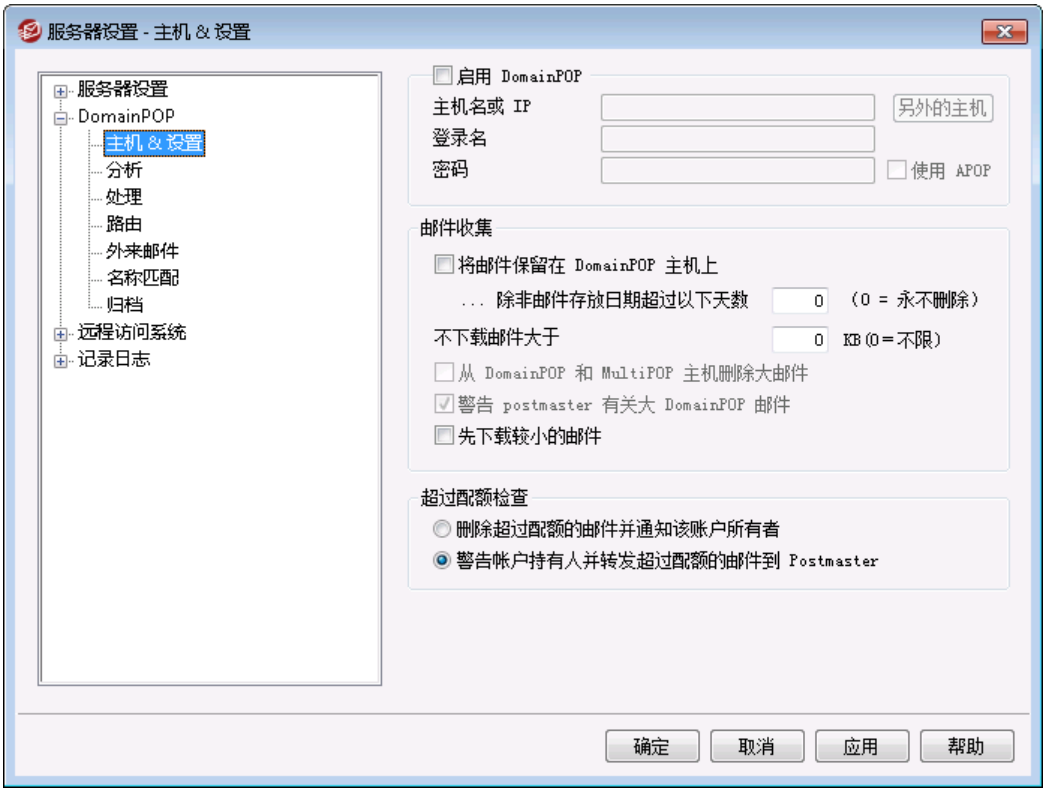
另外一个顾虑就是当使用这种邮件收集方法会产生意想不到的邮件副本问题。一旦使用 DomainPOP 来收集邮件，对于使用 SMTP 投递到 ISP 的 POP 邮箱的邮件来说很容易就会产生不想要的邮件副本。假设一封邮件发送给你域中的某个人，抄送给该域的另外一个人。在这种情况下，SMTP 将投递该邮件的两个副本到您的 ISP 邮箱—每个收件人有一份。两个邮件文件都会包含两个收件人的参考—有一个在收件人：字段而另一个在抄送：Mdaemon会收集这两封相同的邮件而后会处理每个邮件的地址。这将会导致每个收件人都会收到两封相同的邮件。为了避免这种情况，Mdaemon设置将检查指定一个邮件头来看看是否被复制。邮件 ID 字段就是个好主意。在上述例子中，两个相同的邮件包含相同的邮件 ID 字段值。MDaemon 可以使用这个值，在地址信息能够被解析之前的下载阶段来识别并删除第二封邮件。

作为一个解决复制邮件和终止邮件传递循环的终极解决方案，MDaemon 使用一种方法来检测在邮件传输系统中邮件经过多少跳转。当 SMTP 邮件服务器每次处理一封邮件时，都会为邮件加上一个“已接收”报头。当Mdaemon第一次接收到该邮件时，计算所有这样的邮件头。如果总的数量超过一个指定的值，很有可能该邮件进入一个传递循环了而应该被放到一个坏的队列里去。此值可以在重试队列 732”下配置。

还请参阅：

内容过滤器 539
邮件列表 223

3.1.13.1 主机 & 设置



DomainPOP 主机属性

启用 DomainPOP 邮件收集引擎
如果选择，MDaemon 将会使用在此屏幕上提供的设置来从 DomainPOP 邮件主机收集邮件，然后再分发给本地用户。

主机名或 IP
在此输入您 DomainPOP 主机的域名或 IP 地址。

额外域
点击此按钮打开 DpopXtra.dat 文件，可以在此指定收集 DomainPOP 邮件的额外主机。参见该文件的内容以获得更多信息。

登录名
输入 DomainPOP 使用 POP 账户的登录名。

密码
在此输入 POP 或 APOP 账户的密码。

使用 APOP
如果你希望在收集你的邮件时，使用 APOP 命令和 CRAM-MD5 认证，点击此框。这将使你不必再发送明文密码来认证。

邮件收集

将邮件保留在 DomainPOP 主机上
如果选中，MDaemon 将不会从你的 DomainPOP 邮件主机删除收集的邮件。

...除非邮件存放日期超过以下天数 (0=从不删除)
这是邮件在删除以前可以保留在 MultiPOP 主机上的天数。若您不希望删除旧的邮件，请使用 "0"。

有些主机可以限制在您的邮箱中存储邮件所允许的时间。

不下载大于 [XX] KB 的邮件 (0=不限)
大于等于此大小的邮件将不会从你的 DomainPOP 邮件主机上下载。如果你希望 MDaemon 不考虑大小下载邮件，则输入 "0"。

从 DomainPOP 和 MultiPOP 主机删除大的邮件
启用此选项，然后 MDaemon 将删除超出上述指定大小的邮件。邮件可以方便的从 DomainPOP 和 MultiPOP 邮件主机中删除，并且将不再下载。

警告管理员 "Postmaster"有较大的 DomainPOP 邮件
勾选此项时，每当在 DomainPOP 邮箱中发现一封较大的邮件，MDaemon 将会发送一个警告给邮件管理员。

先下载较小的邮件
如果你希望邮件根据邮件的大小下载顺序，点击此复选框——从最小的开始，一直处理到最大的。

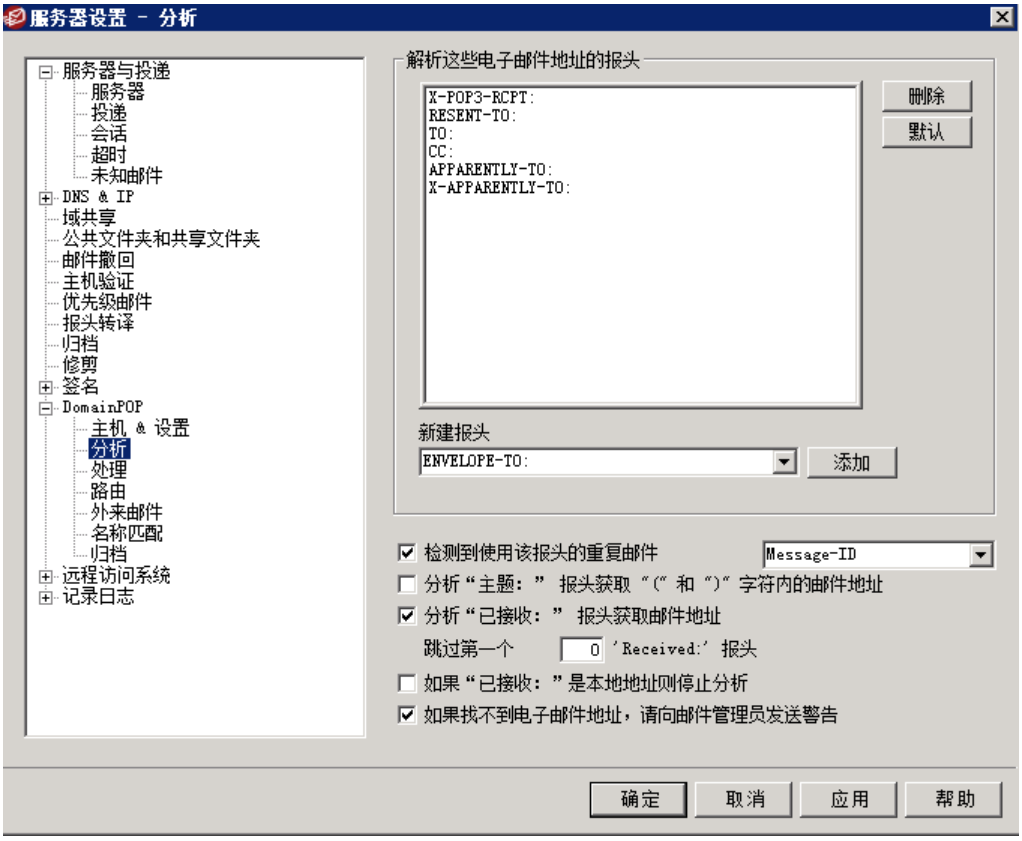
此选项可以更快的找回更小的邮件，但是要求大量的排序和处理。

超过配额检查

警告账户持有人，并删除超过限额的邮件
当选择此选项并且为一个超过它配额的账户收集邮件时 (在帐号编辑器的配额 613 屏幕上指定)，MDaemon 将会删除邮件，并发送一个警告到用户，使他们知道其账户超过了它的限制。

警告账户持有人，并转发超过限额邮件给邮件管理员
当选择此选项并且为一个超过它配额的账户收集邮件时，MDaemon 将会转发邮件给邮件管理员，并发送一个警告到用户，使他们知道他们的账户超过了它的限制。

3.1.13.2 解析



分析这些报头的电子邮件地址

该区域列出了 MDaemon 将会尝试解析提取地址的报头。会检查此处列出的每个报头来获取地址。

删除
此按钮将从报头列表中删除所选条目。

默认
此按钮将会清除当前报头列表的内容，并且添加 MDaemon 的报头默认列表。默认报头足以用来提取邮件中的所有地址。

新建报头
输入您希望添加到报头列表的报头

添加
在*新建报头*选项中指定了一个报头后，点击此按钮将其添加到列表。

检测到使用该报头的重复邮件
如果选择了此项，MDaemon 将会记住报头中指定的值，不会对在同一处理循环中所收集的包含相同值的额外邮件进行处理。Message-ID 报头是该选项所使用的默认报头。

解析 "Subject:"报头获取 "(and)"字符内的邮件地址
当选中此选项时，MDaemon 在邮件的 "Subject:"报头中找到了一个包含在 "()"中的地址，将该地址连同任何其他已解析的地址一起，添加到邮件的收件人列表中。

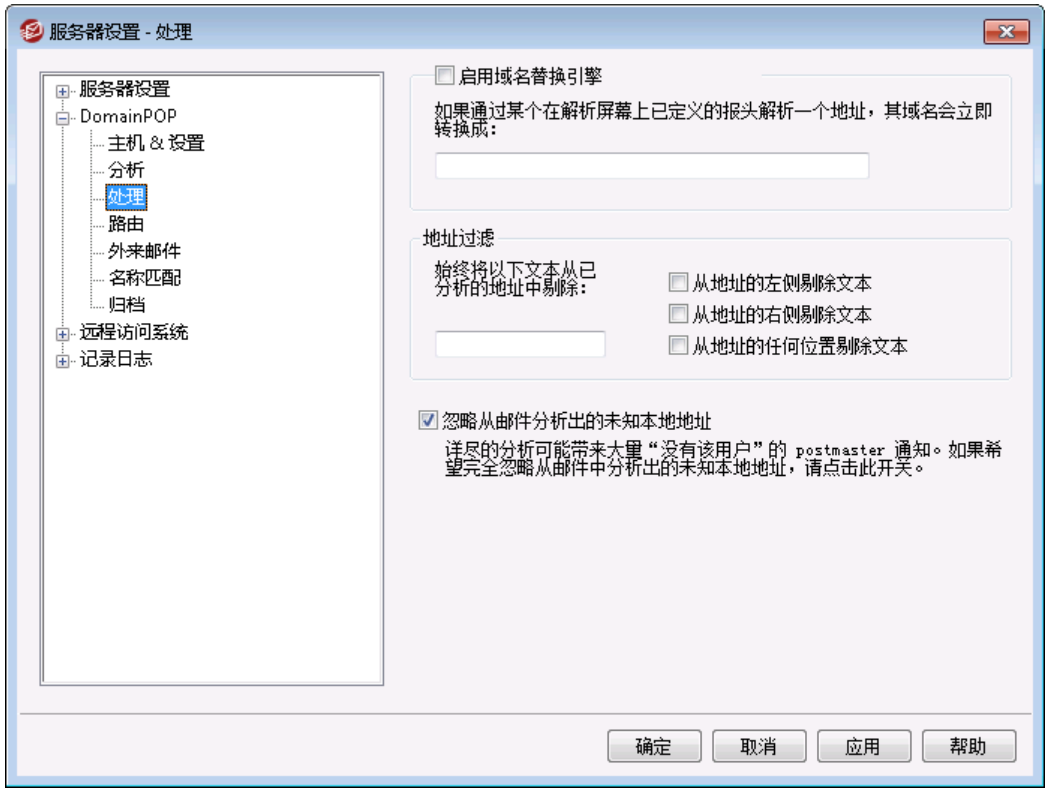
为邮件地址解析 "Received"报头
可以存储收件人的信息，此类信息通常只能在 "Received"邮件报头的信封上找到。这就使得邮件的解析程序只需稍后检查 Received 报头即可获取真实收件人地址。如果您希望解析来自于在邮件中所找到的所有 "Received"报头的有效地址，请点击此选框。

跳过最初的 xx "Received"报头
在一些服务器配置中，您可能希望解析 Received 报头不过需要跳过最初的几项。此设置允许你输入 MD 将会在开始解析前跳过 "Received"报头的数量。

如果 "Received"字段生成了一个有效本地地址，则停止解析
当解析一个 "Received"报头时，MDaemon 检查到一个合法的本地地址，此开关将导致停止所有高级解析，并且 MDaemon 不会搜索邮件来查找更合适的投递地址。

在找不到邮件地址时向邮件管理员发送警告
默认情况下，解析进程未找到地址时，MDaemon 会向邮件管理员发送警告邮件。如果您不希望发送警告，请清除该复选框。

3.1.13.3 处理



域名替换

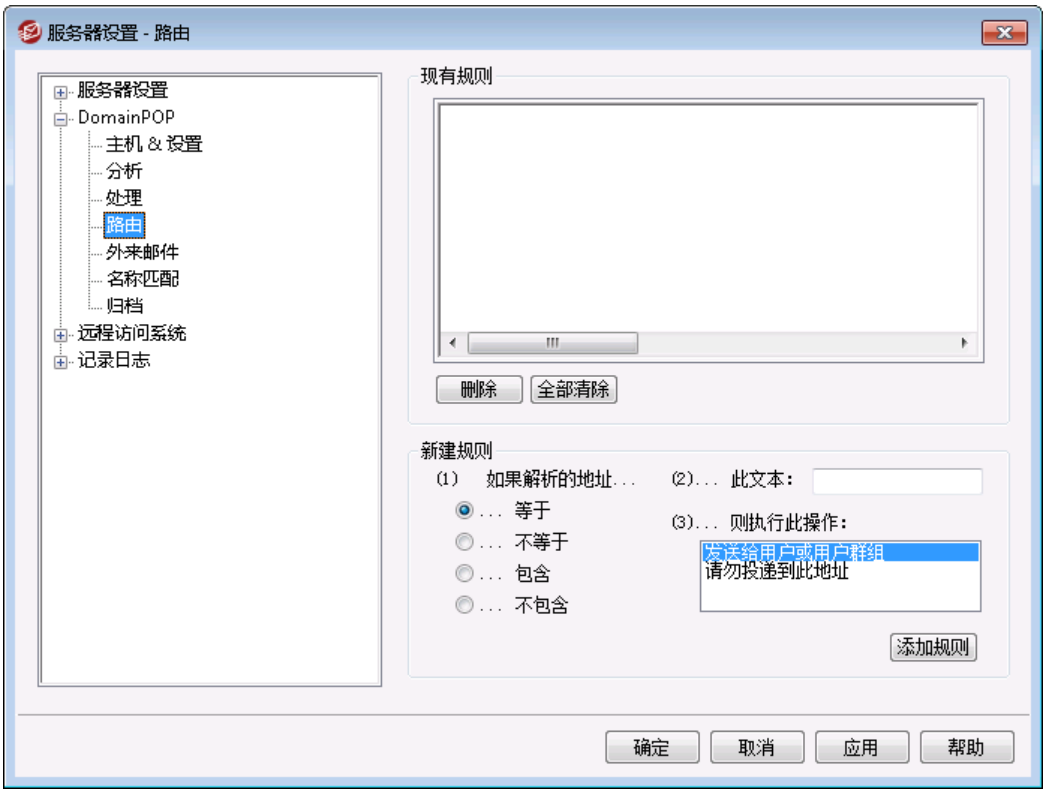
启用域名替换引擎
该选项用来减少您站点上可能需要的别名数量。当下载了一封邮件后，该邮件中所解析的所有地址中的所有域名都将转换成这里指定的域名。

地址过滤

始终从所有解析的地址中剔除以下文本
一些主机将会标记每封邮件，以一条线来表示消息的收件人，并在左侧或者右侧添加一点附加地址的路由信息。此标记对于解析收件人地址是为非常完美的，除了没有大量账户别名的附加信息使其变得不可能。无需做上述所有的事，你可以简单地指定与此功能关联的编辑框中的值，并且 MDaemon 将从所有它解析过的地址中除去此文本。

忽略从邮件解析的未知本地地址
如上所述，域名替换功能将会为所有从邮件中解析的邮件地址中更改域名，转换它到一个你在此屏幕上指定的域名。这样可以创建一些在您的服务器没有对应账户的地址。于域名是有效的，而不是邮件箱是有效的，MDaemon 将考虑这些地址为未知本地用户。这类邮件将典型地生成一个"无此用户"邮件。如果您希望防止域名替换引擎生成此类邮件，请点击此框。

3.1.13.4 路由



现有规则

此列表向您显示了您已经创建的，并将应用到您邮件的规则。

删除

选择一个在此列表中的规则，然后点击此按钮删除这个规则。

全部删除

此按钮删除所有现有规则。

新建规则

⑴如果已分析的地址...

相于、不等于、包含、不包含

当一个地址同此路由规则比较时，将会生成这种类型的比较。MDaemon 将为下方 *"...此文本"* 选项中包含的文本搜索每一个地址，然后根据此选项的设置继续处理 - 该地址的全部文本是否精确匹配，不精确匹配，包含此文本还是根本不包含？

⑵...该文本：

输入您希望 MDaemon 在检查地址时搜索的文本。

⑶...然后执行：

如果规则的结果为真实的，此控件列出可用的可执行操作。您可从下列操作中进行选择：

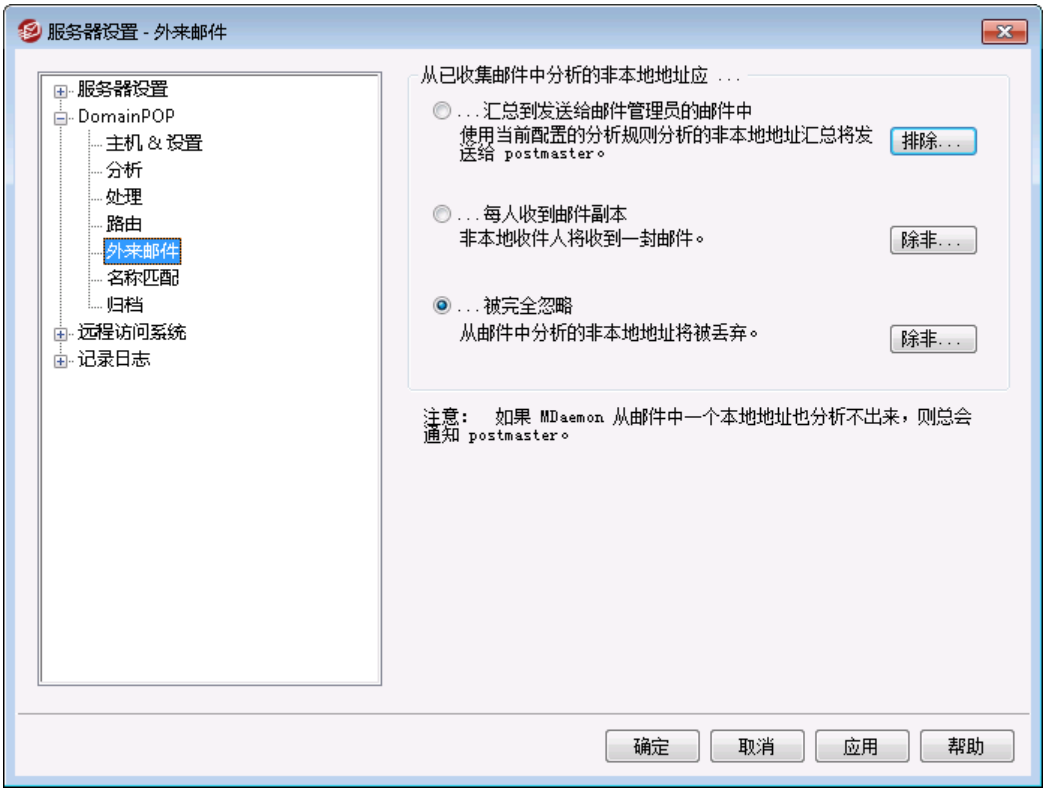
使用投递到此地址 - 选择此规则将会阻止消息发送到指定地址。

发送到用户或用户组—选择此操作将会打开一个对话框，您可以在此指定一个邮件地址列表来接收正在处理邮件的副本。

添加规则

设置了新规则参数后，点击 *"添加规则"* 将其添加到规则列表中。

3.1.13.5 外来邮件



从已收集邮件中分析的非本地地址应 ...

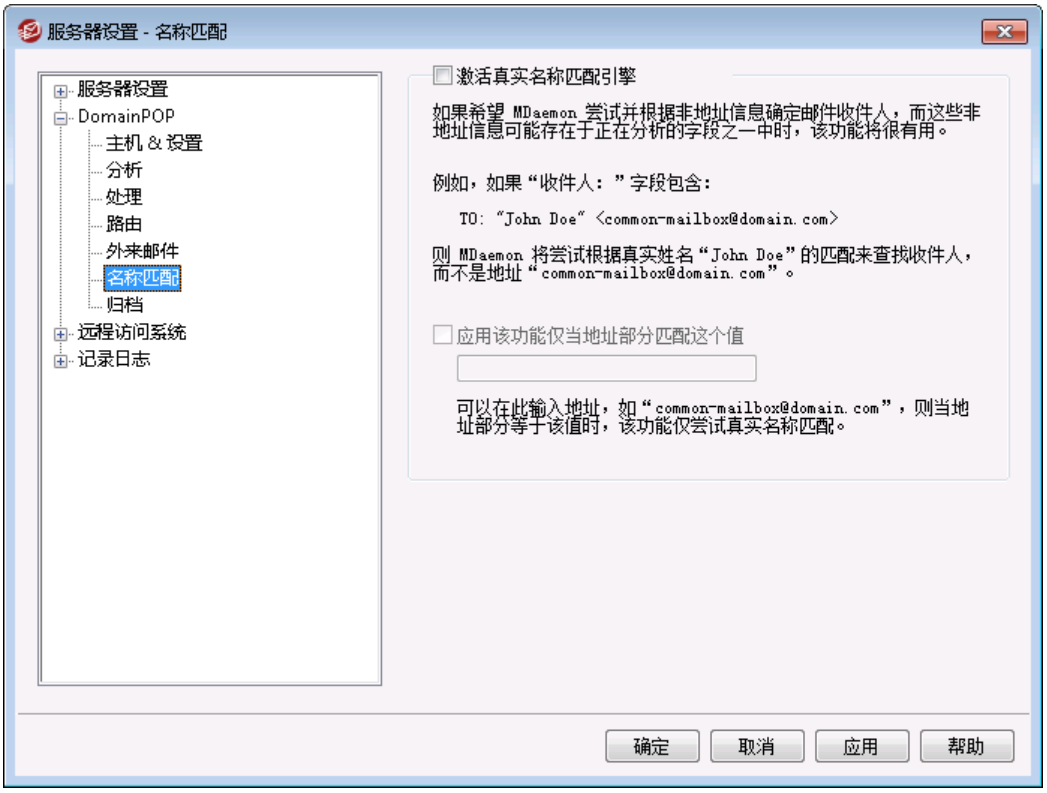
...汇总到发送给邮件管理员的邮件中
如果选择了此选项，MDaemon 将向邮件管理员发送一封邮件的副本，其中含有使用当前报头设置和解析规则的解析引擎提取出的非本地地址的摘要。

...每人收到邮件副本
如果选择选项，MDaemon 将会递送邮件的副本给任何在检查的报头中找到的非本地收件人。

...被完全忽略
如果选择此选项，MDaemon 将会从收件人列表中删除任何非本地的地址。它就像 MDaemon 从未从原始下载的邮件中解析过远程地址。

"*排除...*"和 "*除非...*"按钮允许您定义将被视为所选项例外的地址。

3.1.13.6 名称匹配



名称匹配功能只有在和 DomainPOP 邮件收集引擎合作的时候才能激活。如果您希望使用此功能，您必须确保已启用 DomainPOP。可以从"设置» 服务器设置» DomainPOP"菜单选项抵达 DomainPOP。

真实名称匹配引擎

激活真实名称匹配引擎
该功能允许 MDaemon 决定谁应该基于地◆◆◆中所含文本而不是已解析的邮件地址，来接收 DomainPOP 收集的邮件。这是典型的收件人真实姓名。

例如，一个邮件的收件人报头可以读成：

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

或者

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

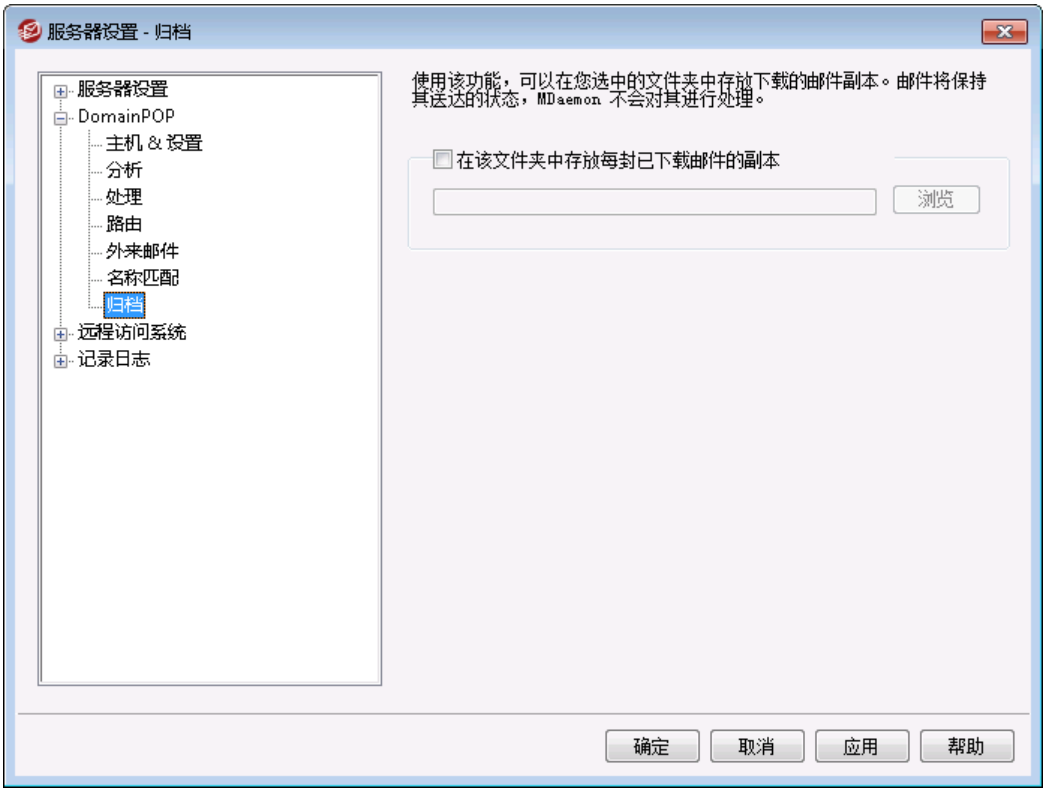
"名称匹配"忽略此地址的"user01@example.com"部分。而是提取了"MichaelMason"部分并且检查这是不是 MDaemon 用户。如果在一个账户的全名区域发现匹配，则此账户的本地邮件地址将会用于投递目的。如果没有匹配，MDaemon 恢复成将邮件投递到从数据中解析的邮件地址（此例中的 user01@example.com）。

地址的真实姓名部分不能包含逗号、分号或者冒号字符。

如果地址部分匹配此值才应用此功能
该选项允许你指定一个必须在提取出的数据中显示的邮件地址，这是为了全名匹配过程能够继续。这为您提供一种在使用实名匹配功能时的控制方法。例如：您可以指定一个地址 "user01@example.com"，只有匹配此值的地址才能成为 "名称匹配"的候选。

假设您在此选项中指定 "user01@example.com"。这意味着 "TO: 'Michael Mason' <user01@example.com>"将成为 "名称匹配"的候选，而不是 TO: 'Michael Mason' <user02@example.com>。

3.1.13.7 归档

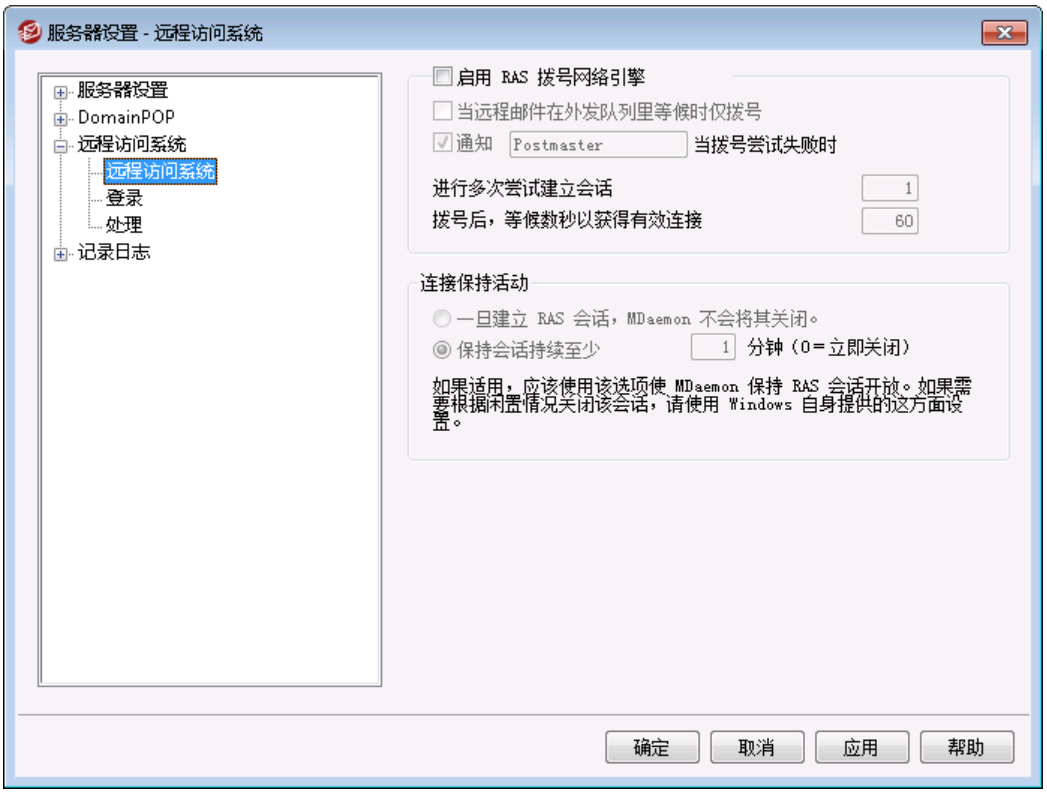


归档

在该文件夹中存放每封已下载邮件的副本
此安全功能保证你不会因为不可预知的解析或者其它可能在垃圾邮件隔离中下载邮件时发生的错误，丢失任何邮件。如果您希望保存每封已下载邮件的副本到您指定的文件夹，请勾选此框。邮件将完全保持其送达的状态，MDaemon 不会对其进行处理。

3.1.14 远程访问系统

3.1.14.1 远程访问系统



点击"设置» 服务器设置» RAS"菜单选项来配置您的 RAS 拨号设置。只有在系统上安装有远程访问服务时该对话框才可用。当您恰恰在远程邮件处理事件之前需要拨号连接 ISP 时，MDaemon 将使用该设置。

启用 RAS 拨号/挂断引擎
启用该选项时，MDaemon 将在收发远程邮件之前使用在此指定的设置来连接远程主机。

仅当远程邮件在出站队列中等候时才拨号
选中该复选框时，MDaemon 不会拨号连接 ISP，除非在远程队列中有正在等候的远程邮件。在某些情况下，这可能会有用，但请注意如果 MDaemon 不拨号，它也无法收集任何邮件（除非是通过本地局域网投递的邮件）。

当拨号尝试失败时通知[地址]
选中后，当因为某个错误致使拨号失败时，MDaemon 将发送邮件到指定地址。

进行多次尝试建立会话
在放弃前，MDaemon 将会尝试连接远程主机这么多次。

拨号后，等候数秒以获得有效连接
该值确定了 MDaemon 将等待远程计算机多长时间来应答并完成 RAS 连接。

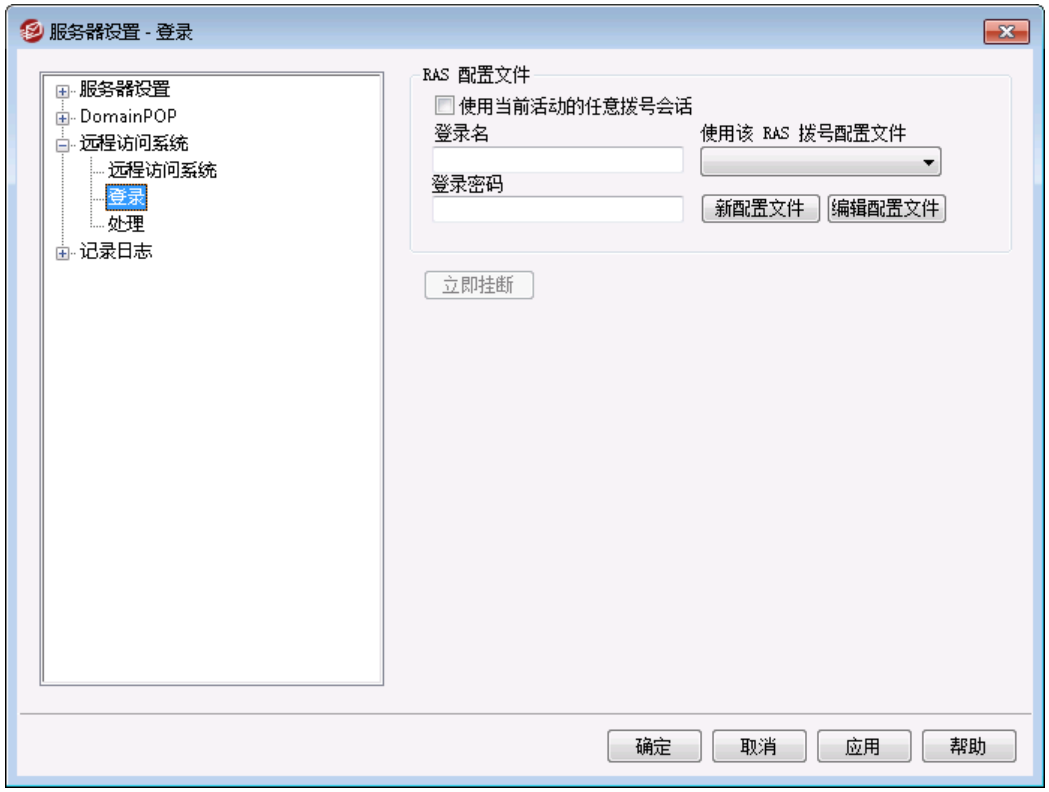
连接保持活动

一旦建立，MDaemon 不会关闭 RAS 会话
默认情况下，在完成所有邮件传输且不再使用会话后，MDaemon 将立即关闭已创建的连接。选择该选项将导致连接在所有传输都已完成后仍保持开放。

MDaemon 不会关闭一个没有创建的连接。

保持会话持续至少 xx 分钟
如果启用，该选项将会使由 MDaemon 创建的 RAS 会话保持开放至少达到指定的分钟数，或者直到所有的邮件传输都已完成（以较大值为准）。

3.1.14.2 登录



RAS 配置文件

使用任何当前活动拨号会话
如果希望 MDaemon 在检测到有其他活动连接时，能利用其连接配置文件，请点击该复选框。每当需要拨号时，MDaemon 将首先查看是否有可以使用的活动连接，而不是先拨号。

登录名
在此指定的值是身份验证过程中将传递给远程主机的用户标识或登录名。

登录密码
在此指定的值是身份验证过程中将传递给远程主机的密码。

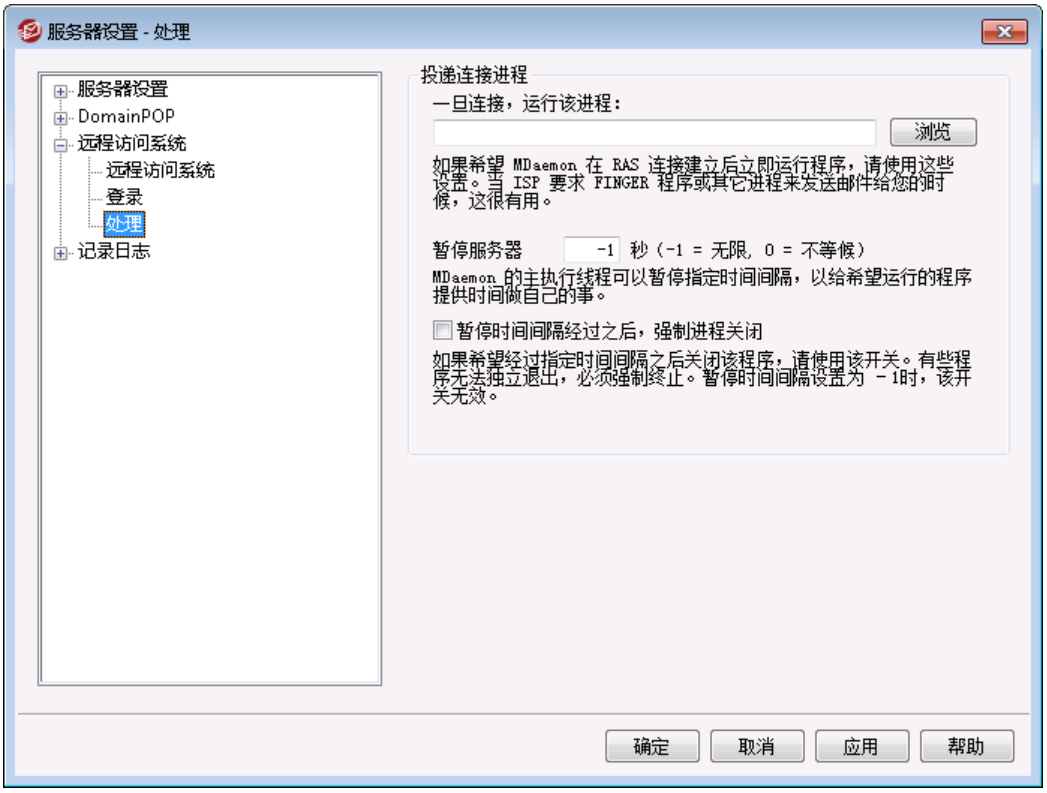
使用该 RAS 拨号配置文件
此下拉列表框允许您选择一个会话配置文件，该文件已通过 Windows 拨号网络或者远程访问服务设置预先作了定义。

新建配置文件
点击该按钮创建新的拨号网络或者远程访问服务配置文件。

编辑配置文件
点击该按钮编辑当前选定的拨号网络或者远程访问服务配置文件。

立即挂断
该按钮将关闭与 ISP 的连接。只有当 MDaemon 发起了 RAS 会话时，该按钮才有效。

3.1.14.3 处理



投递连接进程

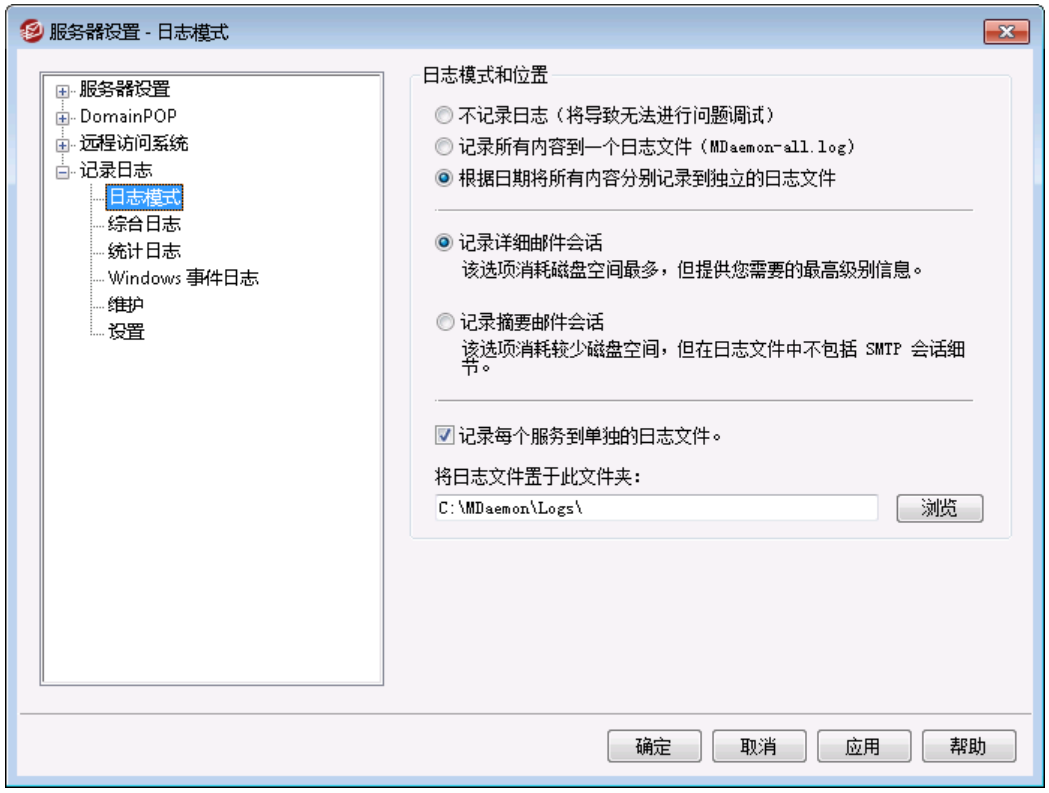
一旦连接，运行该进程
如果在此指定程序，MDaemon 将生成一个线程来执行该程序。如果需要 Finger 或其他程序来解锁 ISP 的邮箱，这会非常有用。

暂停服务器 xx 秒（-1 = 无限，0 = 不等候）
如果*一旦连接，运行该进程*控件包含有效条目，则在服务器等待执行进程返回时，将暂停其操作达此处指定的时间。输入“1”会导致服务器无限期地等待进程返回。

暂停间隔过后强制关闭进程
有时，您需要运行的程序一旦运行后将无法自动退出；有些程序需要用户干预才能将其关闭。当软件必须在无人照看的情况下运行时，这是无法接受的。如果选择了该选项，一旦在*暂停服务器 xx 秒*中指定的秒数流逝后，MDaemon 将强制终止进程线程。当服务器配置为无限期地等待进程返回时，该功能无效。

3.1.15 日志

3.1.15.1 日志模式



点击“设置 » 服务器设置 » 记录日志”菜单选项来配置您的记录日志设置。记录日志对诊断问题以及查看服务器在未被照看时，都作了哪些工作，是非常有用的。

在首选项对话框上管理日志数据量的几个选项可以显示在 MDaemon 主界面的事件跟踪窗口中。要了解更多详情，请参阅首选项 » UI[411]。

日志模式和位置

不记录日志

使用这个选项将会使所有的日志都无效。日志文件仍然会创建，但是不会有日志数据写入里面。

我们不推荐使用这个选项。如果没有日志，要诊断或调试任何您所遇到的与邮件相关的潜在性问题是极其困难的。

记录所有内容到一个日志文件 (MDaemon-all.log)

如果您希望记录所有事件到一个单一文件中，请选中该选项，这个日志文件会以 MDaemon-all.log 命名。

按日期将所有内容分别记录到独立的日志文件

如果选择了此选项，则每天都将创建独立的日志文件。文件名将与创建的日期对应。

记录详细的邮件会话

启用该选项时，每一个邮件处理会话的完整记录将会被复制到日志文件中。

记录摘要邮件会话

此选项将复制每一个邮件处理会话的摘要记录到日志文件。

记录每个服务到单独的日志文件

点击此复选框，使得 Mdaemon 基于服务生成几个单独的日志，而不是在一个文件中。例如，使用此开关设置 MDaemon 将在 MDaemon-SMTP.log 文件中记录 SMTP 活动，以及在 MDaemon-IMAP.log 文件中记录 IMAP 活动。当运行一个 MDaemon 界面的配置会话或终端服务时，必须选中该选项以让界面上的标签显示记录下的信息。

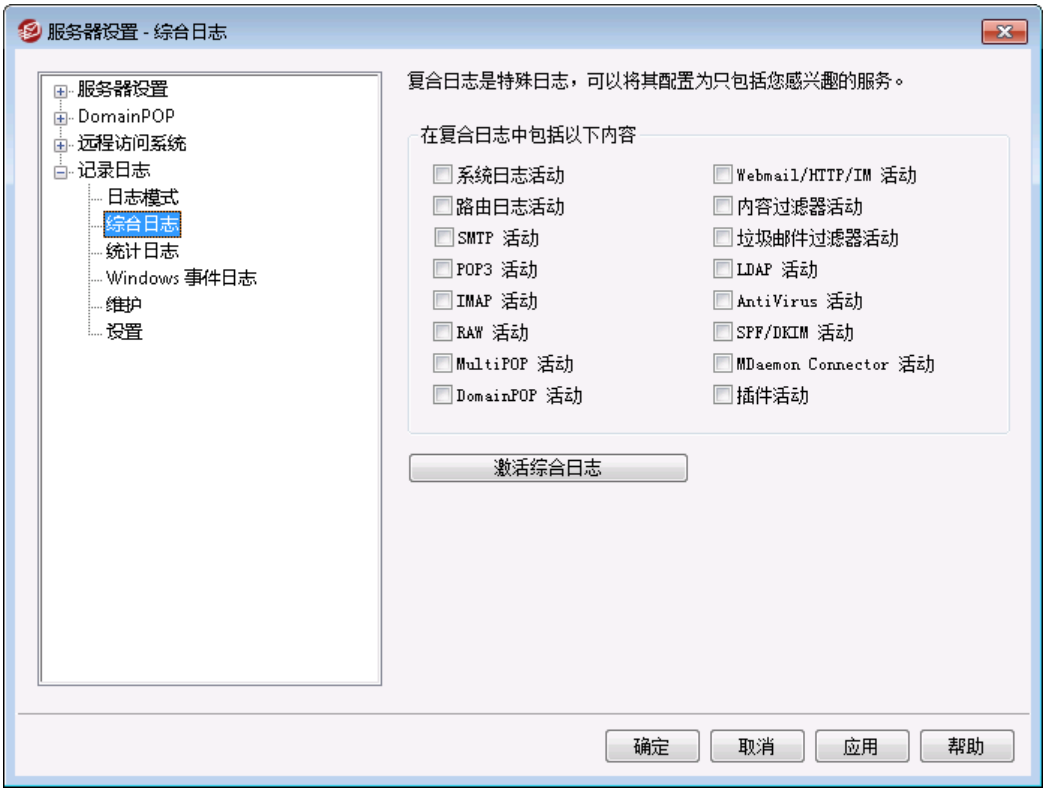
将日志文件置于此文件夹：

如果您希望为您的日志文件指定一个特定的文件夹，请使用该选项。

BadAddress.txt 文件

除了日志文件以外，MDaemon 还在日志文件夹中保留 BadAddress.txt 文件。在投递到一个地址导致 5xx 错误时，会将该地址附加到文件中。这可以帮助您比搜索出站 SMTP 日志这种方式更快地识别您邮件列表中的坏地址。每晚午夜将自动删除这个文件来防止其越变越大。

3.1.15.2 综合日志



综合日志

在“综合日志”中包括以下内容

“综合日志查看”选项位于 MDaemon 菜单栏的“窗口”菜单。点击此选项将添加一个窗口到 MDaemon 的主界面，该窗口会把在一个或者多个“事件跟踪器”选项卡上显示的信息组合起来。使用此部分中的这些控件来指定哪些选项卡的信息将会组合到该窗口中。可以组合以下选项卡中包含的信息：

系统日志活动——显示 MDaemon 的系统活动，例如初始化服务以及启用/禁用任何 MDaemon 的各种服务器。

路由日志活动——显示 MDaemon 解析的每一封邮件的路由信息（收件人、发件人、邮件 ID 等）。

SMTP 活动——显示所有使用 SMTP 协议的发送/接受会话活动。

POP3 活动——当用户从使用 POP3 协议的 MDaemon 中收集邮件时，记录此活动。

IMAP 活动——记录使用 IMAP 协议的邮件会话。

RAW 活动——记录 RAW 或者系统生成的邮件活动。

MultiPOP 活动——显示 MDaemon 的 MultiPOP 邮件收集活动。

DomainPOP 活动——显示 MDaemon 的 DomainPOP 活动。

Webmail/HTTP/IM—显示所有 Webmail 和实时通讯活动

内容过滤器活动——列出 MDaemon 的内容过滤器操作。

垃圾邮件过滤器活动——显示所有的垃圾邮件过滤器活动。

LDAP 活动——显示 LDAP 活动。

反病毒活动——在综合视图中显示反病毒操作。

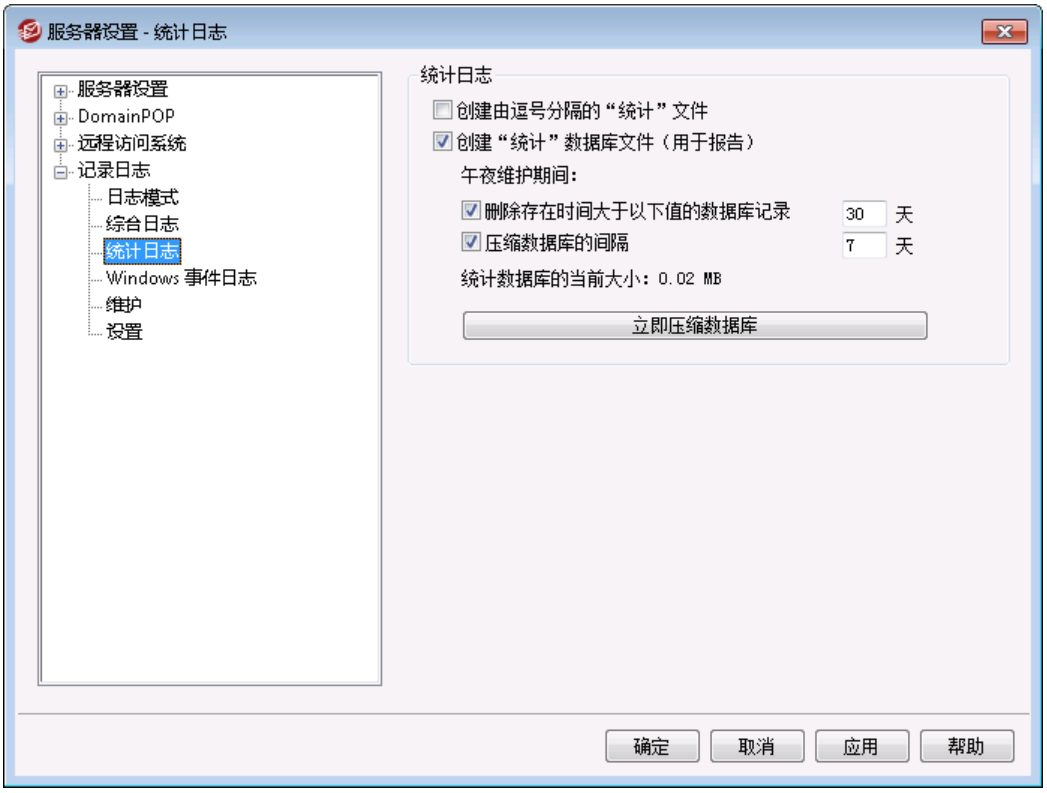
SPF/DKIM——显示所有发件人策略框架与 DKIM 活动。

MDaemon Connector—显示所有 MDaemon Connector 活动。

插件活动——在综合日志中记录 MDaemon 插件活动。

激活综合日志
点击此按钮以在 MDaemon 的主界面启用综合日志窗口。还可以从 MDaemon 菜单栏的"窗口"菜单上启用它。

3.1.15.3 统计日志



统计日志

创建由逗号分隔的"统计"文件
如果您希望保留一份由逗号分隔的统计文件（其中包含有关已处理入站和出站邮件数量的数据、垃圾邮件统计和反病毒统计数据等），则使用此项。默认情况下，禁用该选项。

创建“统计”数据库文件（用于报告）
如果您希望将有关 MDaemon 活动的统计信息记录到 SQLite 数据库文件，则勾选此框。数据库所含数据包括 MDaemon 的带宽使用、入站和出站邮件的数量、以及垃圾邮件统计等。默认情况下，会将这个数据库存储在“MDaemon\StatsDB”文件夹中，并保留30天数据。不过如果您希望缩短或延长默认的30天保留期，您可以调整保留期。将在夜间维护时删除存在时间超过指定限制的数据。您也可以指定 MDaemon 通过精简数据库来节约空间的频率。

MDaemon Remote Administration 的 web 界面中的“报告”页面使用这个数据库来生成供全局管理员使用的各种报告。对于各个报告，可以生成针对几个预定义日期范围的数据，也能由管理员指定自定义日期范围。管理员可以选择以下报告：

- 增强的带宽报告
- 入站邮件对比出站邮件
- 合法邮件对比垃圾邮件（显示垃圾邮件或病毒的百分比）
- 已处理的入站邮件
- 按邮件数量排序的收件人排行榜
- 按邮件大小排序的收件人排行榜
- 已处理的出站邮件
- 垃圾邮件源（域）排行榜
- 垃圾邮件收件人排行榜
- 已阻止的病毒，按时间排序
- 已阻止的病毒，按名称排序

夜间维护期间：
下方这些选项控制 MDaemon 将在夜间维护时执行哪些与数据库相关的任务。

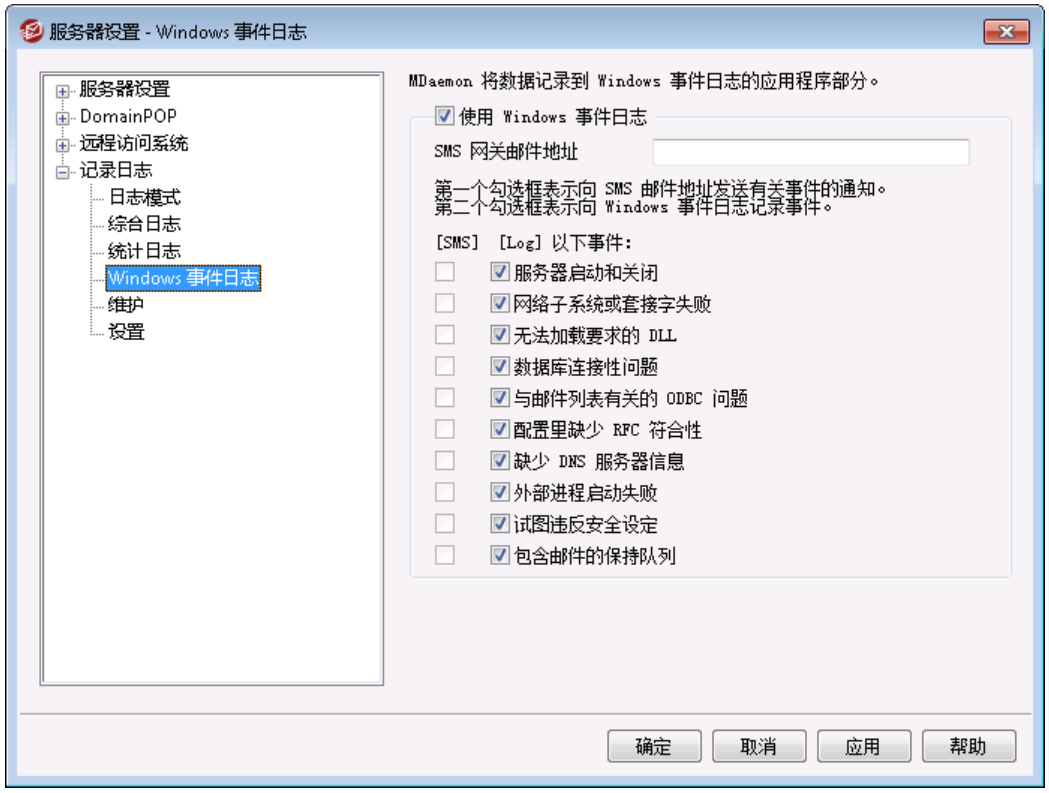
删除存在时间大于 [xx] 天的数据库记录
使用此项来指定您希望将统计数据库记录保留几天。默认情况下启用此项并设置成 30 天。

每隔 [xx] 天精简数据库
如果您希望定期精简数据库来节约空间，则使用此项。默认情况下启用此项并设置成每隔 7 天精简数据库。

统计数据库的当前大小：
在此处列出了您统计数据库的当前大小。

立即精简数据库
点击这个按钮来立即精简数据库。

3.1.15.4 Windows 事件日志



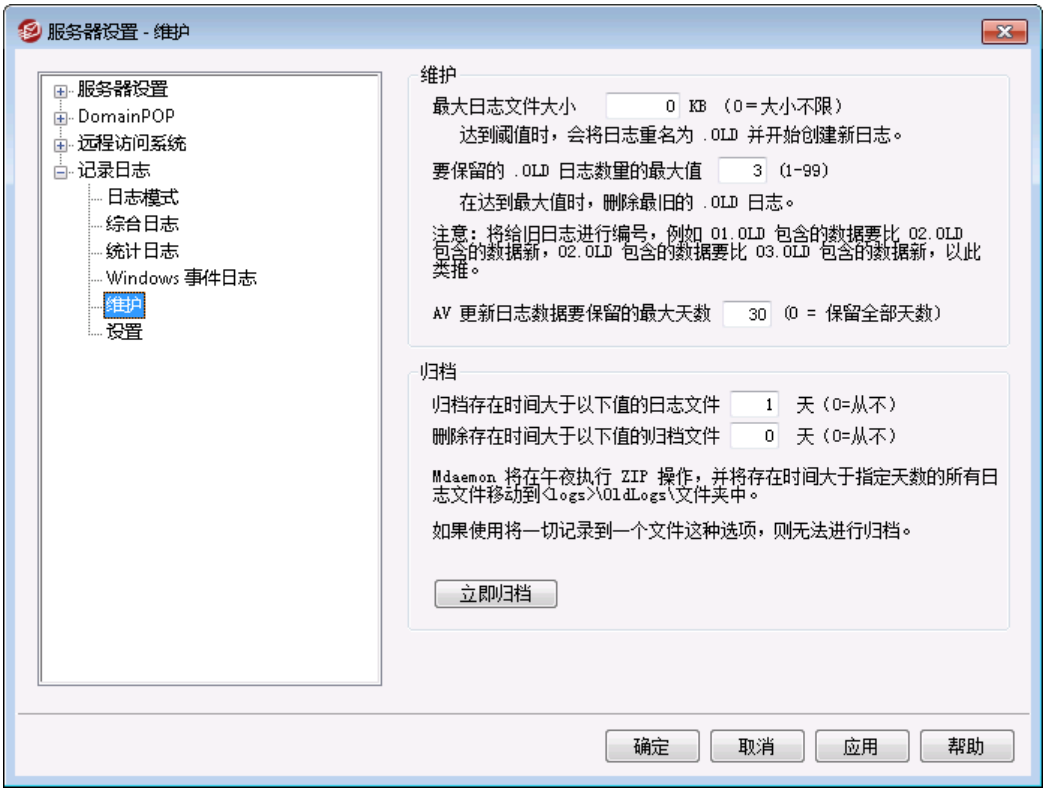
使用 Windows 事件日志
如果您希望记录危急的系统错误，警告和包含其他的事件到 Windows 事件日志的应用程序部分，点击此复选框。

SMS 网关邮件地址
如果您希望以 SMS (文本)消息格式将以下指定的任何事件的事件数据发送到设备，请使用此项。要执行该操作，请指定您电话运营商的邮件至消息 (例如文本消息)网关的邮件地址，例如 Verizon 的便是 PhoneNumber@vtext.com (例如 8175551212@vtext.com)。然后使用以下 SMS 栏内的勾选框来指定您希望发送到设备的事件。

SMS |记录以下事件：
使用这个 SMS 选项来指定您希望通过文本消息发送到设备的事件。使用 "日志记录"选项来指定您希望记录到 Windows 事件"日志的 "应用程序"部分内的事件。要发送 SMS 消息，您必须在上方选项中指定您电话运营商的邮件至消息网关的邮件地址。此外，向 SMS 网关触发通知消息的任何事件将启动远程队列的处理，会将通知视为 "紧急"邮件。

用于*服务器开机和关机*事件的 SMS 选项仅为开机事件 (非关机)发送邮件至 SMS 消息。

3.1.15.5 维护



维护

最大日志文件大小 [xx]KB
这是日志文件可以达到的最大文件大小，以 KB 为单位。一旦达到了此大小，日志文件将被复制到 "LOGFILENAME.01.OLD"，并且开始一个新日志。如果 LOGFILENAME.01.OLD 已存在，就会删除这个旧文件，或将其重命名成 "LOGFILENAME.02.OLD"，这取决于在下方的 "*OLD 日志保留数量的最大值*"中设置的值。如果您不希望限制文件大小，请在此项中使用 "0"。默认情况下将此项设置成 "0"。

.OLD 日志保留数量的最大值 (1-99)
在使用上方的这个选项限制日志文件大小时，此项控制在删除最旧日志前，要保留多少指定的 .OLD 日志文件的迭代文件。将以如下方式命名备份文件："LOGFILENAME.01.OLD"和 "LOGFILENAME.02.OLD"等，始终先列出最新的文件。例如，SMTP(out).log.01.old 所含数据要比 SMTP(out).log.02.old 这些文件所含的数据新。在达到最大值时，将删除最旧的文件并新建一个文件。

AV 更新日志数据的天数最大值 (0=无限制)
此项控制 Antivirus 更新日志 (例如 avupdate.log)保留数据长达几天的最大值。每晚午夜，以及每次 MDaemon 在升级后启动时，都将从该文件删除较旧的数据。如果您不希望设置时间限制，则在此项中使用 "0"。默认情况下将保留前 30 天的数据。

默认情况下保留 AV 更新日志，并将其大小限制为 5120 KB。如果您希望更改其大小或禁用 AV 更新日志，AV 更新程序配置 564 对

话框上的选项可以为您实现这一点，该对话框位于：安全 » AntiVirus » AV 更新程序 » 配置更新程序 » 其他。

归档

归档日志文件存在时间大于 [XX]天 (0=从不)
如果您希望 MDaemon 归档每一个超过指定天数的日志文件，请点击此选项。每晚午夜，MDaemon 将压缩旧的 *.log 与 *.old 文件并将它们移动到 \Logs\OldLogs\ 子文件夹中 (删除处理过程中的原始文件)。此处理过程将不会归档或者删除正在使用的文件，当选择 *"将一切记录到独立的日志文件 (MDaemon-all.log)"* 选项 (其位于 "日志模式 136 "屏幕。

删除存在时间大于 [XX]天的归档 (0=从不)
如果您希望 MDaemon 自动删除存在时间超过指定天数的已归档日志文件，请使用此项。如果您不希望自动删除归档，则在此项中使用 "0"。将在每天的午夜清理事件中删除归档。

立即归档
点击此按钮立即归档旧的日志文件，而不是等待 MDaemon 在午夜自动归档它们。

3.1.15.6 设置

选择要记录的数据

创建“全部”日志
如果您希望产生 *-all.log”文件，它会包含所有被记录的活动，请点击此选项。

记录 SMTP 活动
如果您希望记录所有 MDaemon 发送/接受的 SMTP 活动，点击此选项。

记录 POP3 活动
点击此复选框以记录所有的 POP 邮件活动。这将从 MDaemon 记录您用户的 POP 邮件收集会话。

记录 DomainPOP 活动
点击此复选框以记录所有 DomainPOP 活动。

记录 MultiPOP 活动
单击此复选框以记录所有您用户的 MultiPOP 邮件收集活动。

记录 IMAP 活动
启用此选项将会使得 MDaemon 的日志文件中包括所有您用户的 IMAP 会话。

记录插件活动
该选项记录与插件相关的所有活动。

记录 RAS 活动
如果您希望 MDaemon 复制 RAS 拨号/挂断活动到日志文件中，点击此复选框。此信息对于诊断拨号问题是非常有用的。

记录屏蔽活动
如果您希望 MDaemon 的日志文件中包括 MDaemon 的屏蔽活动，请点击此复选框。

记录 Minger 活动
点击此复选框以记录 Minger 服务器活动。

记录系统活动
该选项记录系统活动。

记录路由活动
此选项记录所有入站、本地和远程队列解析活动。

记录活动目录活动
此选项用于记录与 MDaemon 相关的活动目录活动。

记录 MTA-STS/TLS 报告活动
记录与 SMTP MTA 严格传输安全 (MTA-STS) 相关的所有活动。

记录调度程序活动
如果您希望记录所有事件调度程序的 318 活动，请启用此复选框。

记录完整的 Webmail/HTTP/IM 活动
如果您希望记录所有的 Webmail，HTTP 和 MDaemon Instant Messenger 活动，请点击此复选框。禁用该选项时，将仍然创建 Webmail 与 HTTP 日志并显示 MDaemon Webmail 的启用和关闭记录，但是将不再记录其他的 WC/HTTP/IM 活动。

记录 AntiVirus 活动
该选项记录 AntiVirus 活动。

记录垃圾邮件过滤器活动
记录所有垃圾邮件过滤器活动。

记录 DNS 阻止列表活动
此选项会使 MDaemon 记录 DNS 阻止列表活动。使用此选项会提供给您一个针对被记录为阻止站点的简单参考。

记录邮件分析活动
当确定一封邮件投递的目标时，MDaemon 会周期性地执行大量的邮件分析活动。如果您希望在日志文件中包含此信息，请点击此选项。

记录内容过滤器活动
如果您希望在日志文件中包含内容过滤器活动，点击此复选框。

记录 MDaemon Connector 活动
此选项管理是否记录 MDaemon Connector 活动。

记录 SMTP “探测”
点击该选项以记录发件服务器没有传输邮件数据时的 SMTP 会话 (如：发件服务器没有使用 DATA 命令)。

记录验证失败
使用此项来记录验证失败。

记录 RAW 活动
记录 MDaemon 的 RAW 邮件活动。

记录 MDaemon 邮件任务
记录邮件任务。

记录 LDAP 活动
记录所有 LDAP 活动。

记录 SPF 活动
如果您希望记录所有 SPF 查找活动，点击此复选框。

> **……但仅当找到 DNS 数据时**
> 如果您在记录 SPF 活动，当您希望只记录在 DNS 查询中发现的记录，而不是记录所有 SPF 查找时，点击此复选框。

记录 DKIM 活动
如果您希望记录 DomainKeys Identified Mail (DKIM)活动，请点击此选项。

……但仅当找到 DNS 数据时
如果您记录 DKIM 活动，当您希望只记录在 DNS 查询中发现的记录，而不是记录所有活动时，点击此复选框。

记录 DMARC 活动
使用这个选项将记录 DMARC 活动。

……但仅当找到 DNS 数据时
如果您记录 DMARC 活动，当您希望只记录在 DNS 查询中发现的记录，而不是记录所有活动时，点击此复选框。

记录 VBR 活动
如果您希望记录邮件证书 460，请使用此项。

…但仅当找到 DNS 数据时
如果您在记录邮件证书活动，在您希望只记录在 DNS 查询中发现的实际证书数据时，请点击此复选框。

3.1.15.7 更多设置

选择要记录的数据

记录所有本地 MDSpamD 活动（调试记录——性能耗尽）
如果您希望记录所有本地 MDSpamD 活动，使用此选项（请参阅以下的警告）。

实时记录会话（调试记录——性能耗尽）
通常，会话信息将在会话完成后被记录，这是为了保存资源。如果您希望会话信息在它发生中被记录，点击此选项。

当使用以上任何一个或全部两个记录选项时，可能会降低邮件系统的性能，这取决于您的系统与活动的级别。根据你的系统和活动情况，一般此两个选项只作为调试时使用。

记录多行协议响应（如 UIDL 和 LIST）
有时，对协议请求的回应要求不止一行信息。如果您希望记录这些附加行，点击此复选框。

启用此控件可能会潜在地大量增加记录信息。由于在回应中的行数不能预先确定，并且由于一些回应会潜在地使用可能不重要的信息"填满"您的日志文件（例如，那些列出邮件真实内容的 POP TOP），因此如果您在意冗长的日志文件大小，那么我们不推荐使用此功能。

在邮件会话日志里记录 ID 字符串
如果您希望在会话记录中包括 [%d:%d] ID 字符串，点击此选项。

在显示邮件会话日志时使用颜色（需要重启 MDaemon）
如果您希望使 MDaemon 用户界面中若干事件跟踪和日志记录[59]选项卡上显示的文本成为彩色文本，请启用此项。默认情况下启用此项，而且对该选项的启用/禁用需要在重启 MDaemon 之后才能使更改生效。还请参阅：下方的"着色会话日志"来获得更多信息。

始终记录到屏幕
如果希望将日志数据复制到 MDaemon GUI，即使它已最小化或在通知栏运行，请点击该选项。

当清空此控件时，日志数据将不能在 MDaemon 以系统托盘方式运行的时候，复制到事件跟踪窗口。因此，首次打开 MDaemon 时，大多数最近的活动将不会被列到任何事件跟踪窗口的标签上。将从那一点向前，开始显示新的记录信息。

着色会话日志

在 MDaemon 的用户界面上[59]，可以着色显示路由、SMTP-入站、SMTP-出站、IMAP、POP、MultiPOP 和 DomainPOP 活动的选项卡，来帮助用户更直观地区别会话中的事件。默认情况下禁用此功能，不过可以通过*"在显示邮件会话日志时使用颜色"*选项来启用此功能，该选项位于 日志 » 更多设置[146]和首选项 » 用户界面[411]。可以通过编辑 [Colors] 会话（位

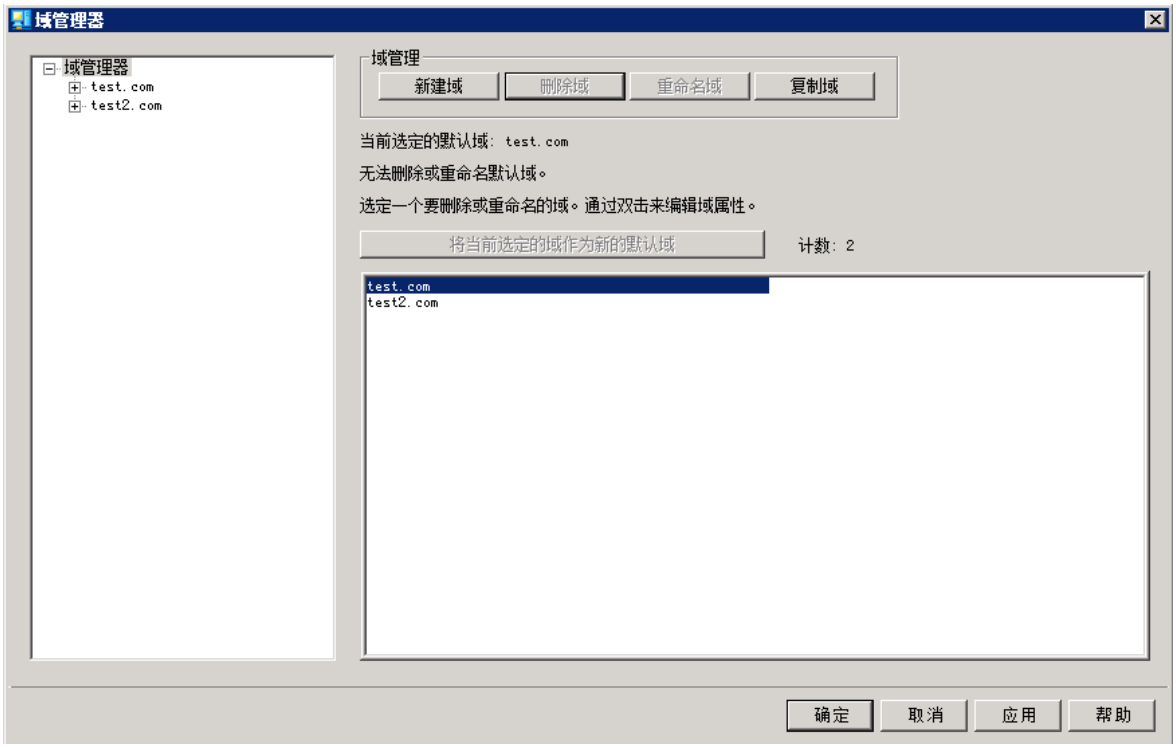
于 LogColors.dat 文件)来更改默认的文本颜色。请参阅以下图表来了解默认的颜色列表。

如果您希望使用颜色，但是不希望着色所列出的一个或多个要素，请将各个要素值设置成零 (例如SpamFilter=0)。这将使选定的要素使用默认颜色。不过对于 Background 和 SelectedBackground 而言，将其值设置成零则无法正常工作。如果您希望更改上述要素，您必须提供一个新的颜色值。使用以下格式以十六进制指定颜色值："0xbbggrr"，其中 "bb"指蓝色的相对强度，"gg"用于绿色，而 "rr"用于红色。例如 "Error=0x0000ff"将错误文本设置成红色。**请注意：**这颠倒了常规颜色代码的顺序，通常的顺序是 "rrggbb"。如果您更改了颜色，您必须重启 MDaemon 或创建一个名为 COLORS.SEM 的文件，并将其放置在 MDaemon 的 \APP\ 文件夹中。

默认的日志颜色

Background=0x000000	背景颜色；黑色
SelectedBackground=0xff0000	选定的背景颜色；蓝色
Default=0xffffff	默认的文本颜色；白色
Processing=0x00ffff	内部处理和解析活动；默认值是黄色
DataIn=0x008040	来自其他服务器的入站数据；默认值是深绿色
DataOut=0x00ff00	发送至其他服务器的出站数据；默认值是浅绿色
Error=0x0000ff	错误消息；默认值是红色
TCPIP=0xff8000	TCP/UDP/DNS/PTR 相关活动；默认值是浅蓝色
SpamFilter=0x0080ff	垃圾邮件过滤；默认值是橙色
AntiVirus=0xdda0dd	反病毒处理；默认值是深紫色
DKIM=0xff00ff	DKIM 活动；默认值是 fuchsia
VBR=0x40c0ff	Vouch by Reference 活动；默认值是浅橙色
SPF=0x808080	发件人策略框架活动；默认值是灰色
Plugins=0x0080c0	从插件发送的任何邮件；默认值是棕色
Localq=0x00ffff	本地队列路由；默认值是黄色
Spam=0x0080ff	垃圾邮件路由；默认值是橙色
Restricted=0x40c0ff	受限邮件路由；默认值是浅橙色
BlackList=0x808080	列入阻止列表的邮件路由；默认值是灰色
Gateway=0x00ff00	网关邮件路由；默认值是浅绿色
Inboundq=0xff8000	入站邮件路由；默认值是浅蓝色
PublicFolder=0xdda0dd	公共文件夹邮件路由；默认值是深紫色

3.2 域管理器



MDaemon Pro 包含针对多个域的完全支持，通过域管理器进行管理。您可以在此处，为您的域管理其域名、IP 地址、账户、邮件清理设置、Webmail和其他视域而定的选项。

MDaemon 支持单个 IP 地址和多个 IP 地址，而且这些 IP 地址对于个别域来说可以是唯一的，也能在这些域间进行共享。此外，几个关键功能（例如账户、邮件列表和安全设置）都是基于域的功能。举例来说，在您创建一个账户时，您必须指定新账户所属的域。对邮件列表也是一样。这意味着 IP 屏蔽 468 和 IP 防护 436 这些功能将分别受到域的约束。

但是一些功能，例如“名称匹配 131”（位于“DomainPOP 122”之下，仅受限于“默认域”。“默认域”还是各种选项中默认显示的域，例如在新建账户或邮件列表的时候。此外，为了支持 MDaemon 对系统邮件的处理，以下“别名 699”的默认设置将一些保留的邮箱名指向 MDaemon 的默认域，而不是指向它的其他域：

```
MDaemon@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserver@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
list-serv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
```

最后要支持多个域，默认情况下 MDaemon 要求用户使用其完整的电子邮件地址（例如“user01@example.com”）作为其登录值，而不是只使用其地址的邮箱部分（例如“user01”）。不过某些非常旧的邮件客户端不支持在登录字段中使用“@”。因此要适应这些客户端，您可以在“首选项”下的“系统 414”屏幕上指定备用字符。此值至多可以设置到 10 个字符，使得它可以提供字符串作为分隔符来替换单独字符，例如“$”。例如，使“.at.”将允许您使用“user02.at.example.com”作为登录值。您也可以禁用完整的电子

邮件地址要求，允许用户只使用邮件地址的邮箱部分作为登录值，不过我们不建议这样做，因为当您拥有多个域时，这会引起问题。

域列表

这个对话框左侧的区域含有您的域列表，其中提供链接转至用于配置各种特定域设置的屏幕。首先列出的是 "默认域"，所有其他域按字母顺序排列。右侧的列表用于删除和重命名域，以及指定默认域。您可以双击此列表中的一个域来切换至此域，并配置其设置。

域管理

新建域

要新建域：请点击 *"新建域"*，然后在 "创建/更新域"对话框中输入域名，并点击 *"确定"*。

通常，这里输入的值将是已经被注册过为网络域名并且可以让 DNS 服务器解析到本地运行服务器的 IP 地址或者此名称的一个有资格的别名。或者，您可以为您的域名选择使用一个仅限于内部或者非有效，非公共域名 (例如 "company.mail")。当以这种方式配置您的服务器时，有必要使用报头转译 103 功能，和/或域名替换引擎 127 来启用正确的邮件分发。

删除域

要删除域：从以下列表选择一个域，点击 *"删除域"*，然后通过点击 *"是"*确认您要删除此域的决定。

您不能删除或重命名默认域。如果您希望删除或重命名默认域，您必须先将一个不同的域指定为默认域。

重命名域

要更改域名：从以下列表选择一个域，点击 *"重命名域"*，然后在 "创建/更新域"对话框中输入新域名，并点击 *"确定"*。

复制域

如果您要创建具有与另一个域匹配设置的新域，请从列表中选择一个域，点击此按钮，然后指定新域的名称。账户和列表等将不会复制到新域。

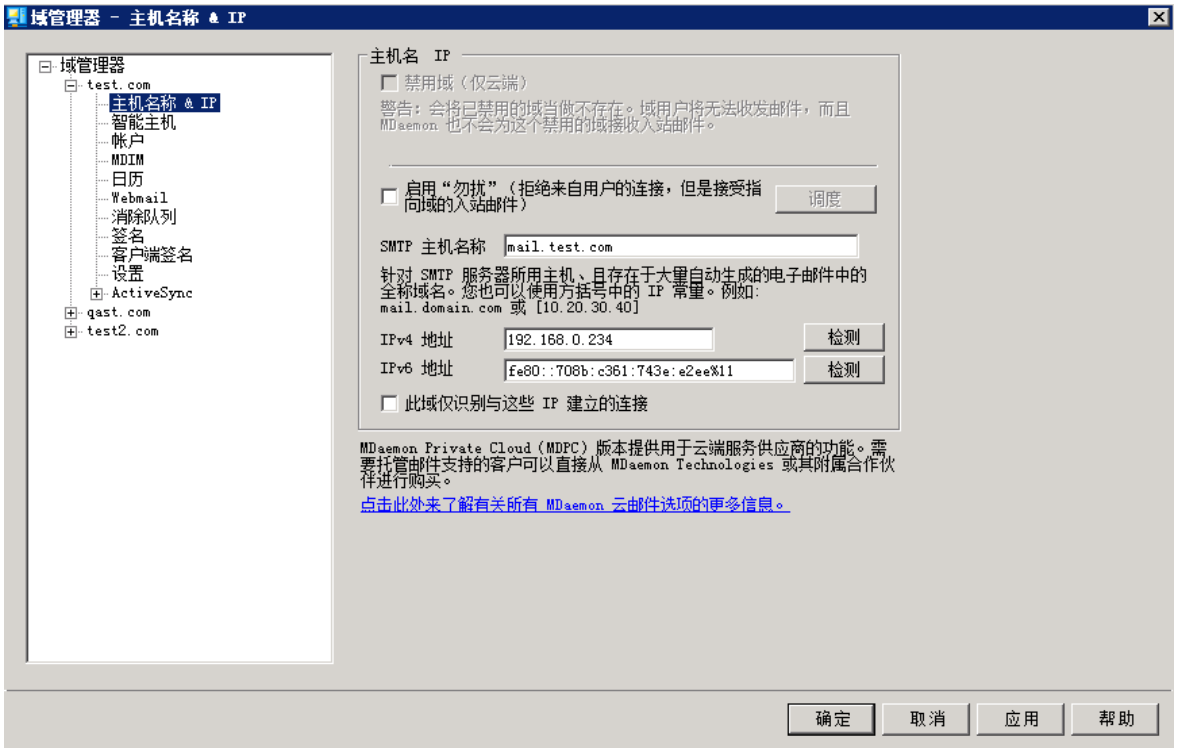
将当前选定的域作为新的默认域。

如果您希望更改 MDaemon 的默认域，请从以下列表选择所需域并点击这个按钮。

还请参阅：

首选项 » 系统 414

3.2.1 主机名称 & IP



主机名 & IP

禁用域（仅云）
如果您希望禁用这个域，可点击此复选框。MDaemon 会将禁用的域视为不存在。域用户无法收发邮件，MDaemon 也不接受此域的入站邮件。此项仅适用于 MDaemon Private Cloud。

启用勿扰
使用此选项可以为域激活“勿扰”。启用后，域将拒绝所有用户的所有服务连接，但仍会接受来自外部世界的邮件。

调度
点击此按钮可以调度“勿扰”的开始和停止的时间。例如，如果您配置2020年5月1日到2020年6月30日，时间是星期一至星期五的下午5:00到早上7:00，那么这意味着从下午5:00开始，该天的用户将无法使用该邮件服务，并且只要当前日期是2020年5月

1日至2020年6月30日之间，就在上午7:01恢复。删除调度的开始日期会取消这次调度，而且有*永久将域置于"勿扰"模式*"的效果。

SMTP 主机名称
当向该域发送邮件时，该值是在 SMTP HELO/EHLO 指令中所用的全称域名 (FQDN)。至于入站连接，如果使用了下方*"此域只识别与主机 IP 地址建立的连接"*这一选项，会将此域绑定到其自己的 IP 地址，并为与这个域建立的连接使用正确的 FQDN。然而，这并不一定要求使用该选项。如果有两个或多个域使用相同的未绑定 IP 地址，那么所用的 FQDN 将与按字母顺序排在首位的域相关联。

大多数情况下，FQDN 是*"域名"*或其子域 (例如 "mail.example.com")，但也可使用 [192.0.2.0]之类的 IP 原址语法。未指定 FQDN 值时，MDaemon 将使用默认域的 FQDN。

IPv4/IPv6 地址
输入与这个域相关联的 IPv4 和 IPv6 地址。如果缺少 IP 地址，MDaemon 将自动尝试检测一个合适的地址进行使用。

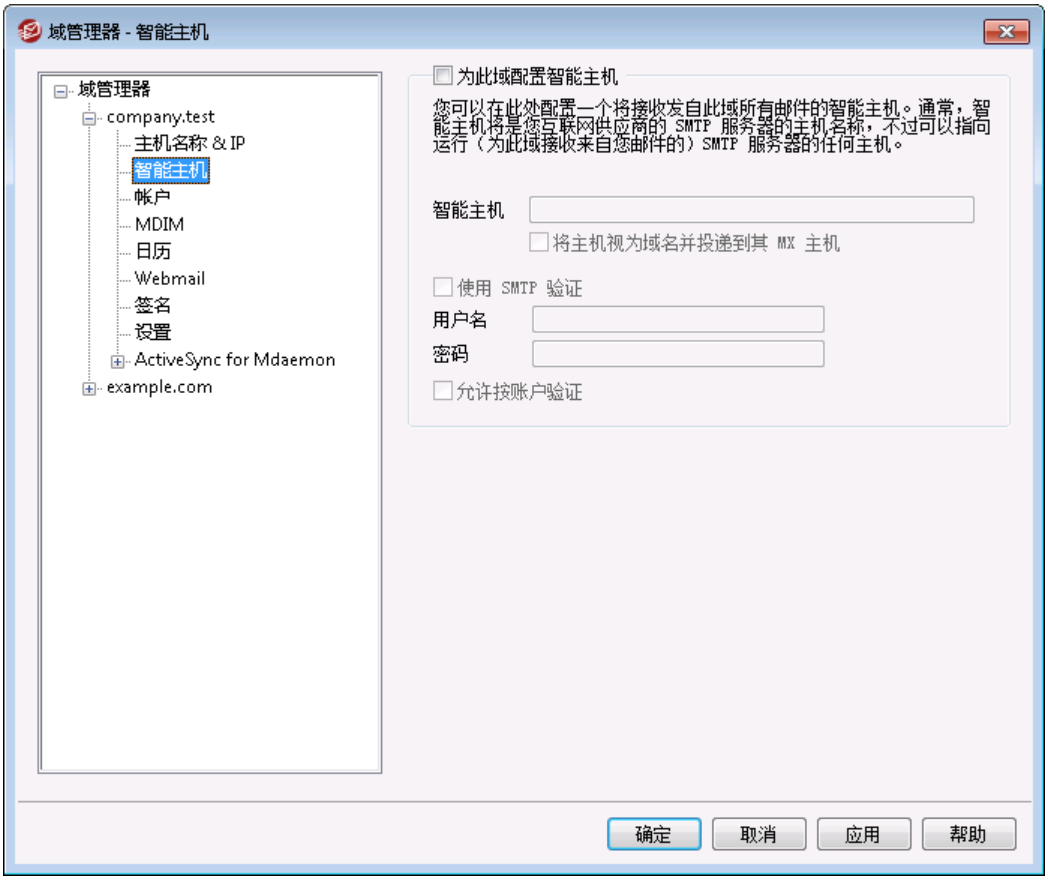
检测
使用这些按钮来检测适用于相应 IP 地址选项的 IPv4 和 IPv6 IP 地址。然后您可以从列出的 IP 地址进行选择。

此域仅识别与这些 IP 建立的连接
如果您希望限制这个域与上方指定的 IP 地址建立的入站连接，请点击此勾选框。默认情况下，这只适用于入站连接。通过"服务器设置» 绑定 90"下的某个选项管理出站套接字绑定。

还请参阅：

域管理器 149
首选项 » 系统 414
绑定 90
IPv6 89

3.2.2 智能主机



为此域配置智能主机

如果您希望通过特定的 "智能主机"而不是使用 MDaemon 默认的 投递 76 "选项来路由这个域的出站邮件，则启用此选框，并在下方指定智能主机。会将此域的所有出站邮件路由到这个主机。

智能主机

在此处指定您的 ISP 或者邮件主机的名称或 IP 地址。这通常是您 ISP 的 SMTP 服务器。

不要在此文本框中输入 MDaemon 的默认域或 IP 地址。这里应该输入一个 ISP 或其他能够为您中继邮件的邮件服务器。

视主机为域名并投递到其 MX 主机

如果您希望将主机视为域名而不是特定的服务器，请勾选此框，这样将使 MDaemon 检索与此域相关联的任何 MX 主机并与其建立连接。

使用 SMTP 验证

如果 *"智能主机"*需要验证，则点击此选框并在下方输入您的登录凭证。这些登录凭证将用于所有发送到智能主机的出站 SMTP 邮件。不过，如果您选择使用下方的*允许按每个*

*账户验证*选项，那么 MDaemon 会使用发件账户的*智能主机访问*凭证来向您的主机分别验证每封邮件。该设置可在 "账户编辑器"的邮件服务[602]屏幕上指定。

用户名
在此处输入您的用户名或登录名。

密码
使用此选项指定您的智能主机登录密码。

允许按账户验证
如果您希望对发送到上方所指定的*"智能主机"*的出站 SMTP 邮件使用按账户验证，请点击此复选框。该操作并不使用在此处提供的*用户名*和*密码*凭证，而是使用各个账户的*智能主机访问*凭证（在邮件服务[602]屏幕上指定。）如果已为给定账户指定智能主机凭证，则使用这些凭证。

若您希望配置*按每个账户验证*以用于每个账户的*邮件密码*而不是使用其可选的*智能主机密码*，那么您可以通过在 MDaemon.ini 文件中编辑下列键值以实现此操作：

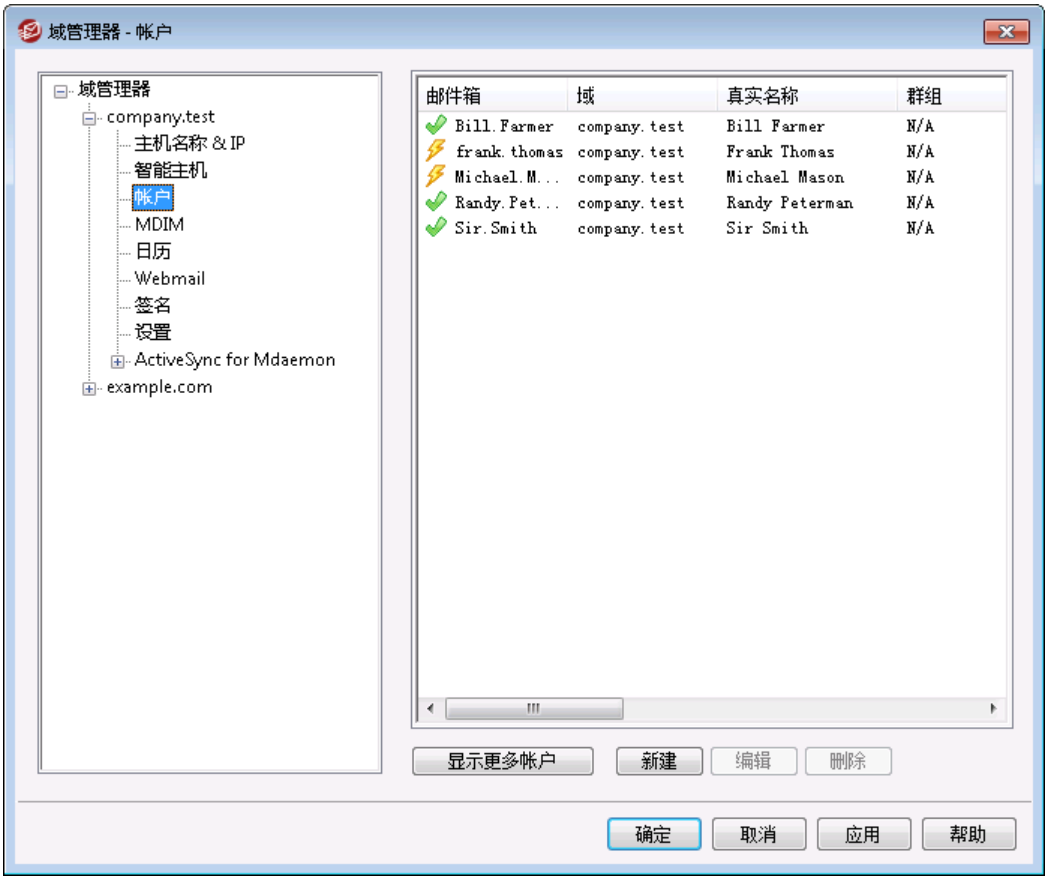
```
[AUTH]
ISPAUTHUsePasswords=Yes（默认为 No）
```

启用 ISPAUTHUsePasswords=Yes 选项将在一段时间后将您所有账户本地邮件密码有效传达到您的智能主机。这可能对邮件的安全性造成威胁，因为它正向另一个服务器提供敏感信息。您不应该使用此选项，除非您正在使用的智能主机是您完全信赖的，而且您相信有必要这么做。另外，您应该注意到，若您使用了此选项并且授予用户权限通过 Webmail或者其他方式来改变他们的*邮件密码*，那么改变*邮件密码*同样可以有效地改变*智能主机密码*。当本地更改了*邮件密码*而没有在您的智能主机上本地更改相应的*智能主机密码*，这可能会导致对一个账户的智能主机验证失败。

还请参阅：

域管理器[149]
服务器设置 » 投递[76]
账户编辑器 » 邮件服务[602]

3.2.3 账户



该 "账户"页面显示此域所有 MDaemon 账户的列表。列表中的每个条目都包含了一个 "账户状态图标"(见下),邮箱、账户持有人的 "实际姓名",账户所属的任何群组、邮件计数、已用磁盘空间 (单位是 MB)。此列表可以按照您的需要升序和降序排列。点击任何栏目的标题来以升序排列列表。再次点击该列,对其进行降序排列。

账户状态图标

账户为全局或域管理员。

完全访问账户。同时启用 POP 和 IMAP 访问。

受限访问账户。禁用 POP、IMAP 或同时禁用两者。

账户被冻结。MDaemon 仍将接收该账户的邮件,不过该用户无法发送或检查邮件。

禁用账户。禁用该账户的所有访问。

新建

点击此按钮打开 "账户编辑器"[598]来创建一个新账户。

编辑
从列表中选择一个账户然后点击此按钮，在“账户编辑器[598]”中将其打开。您还可以双击此账户来将其打开。

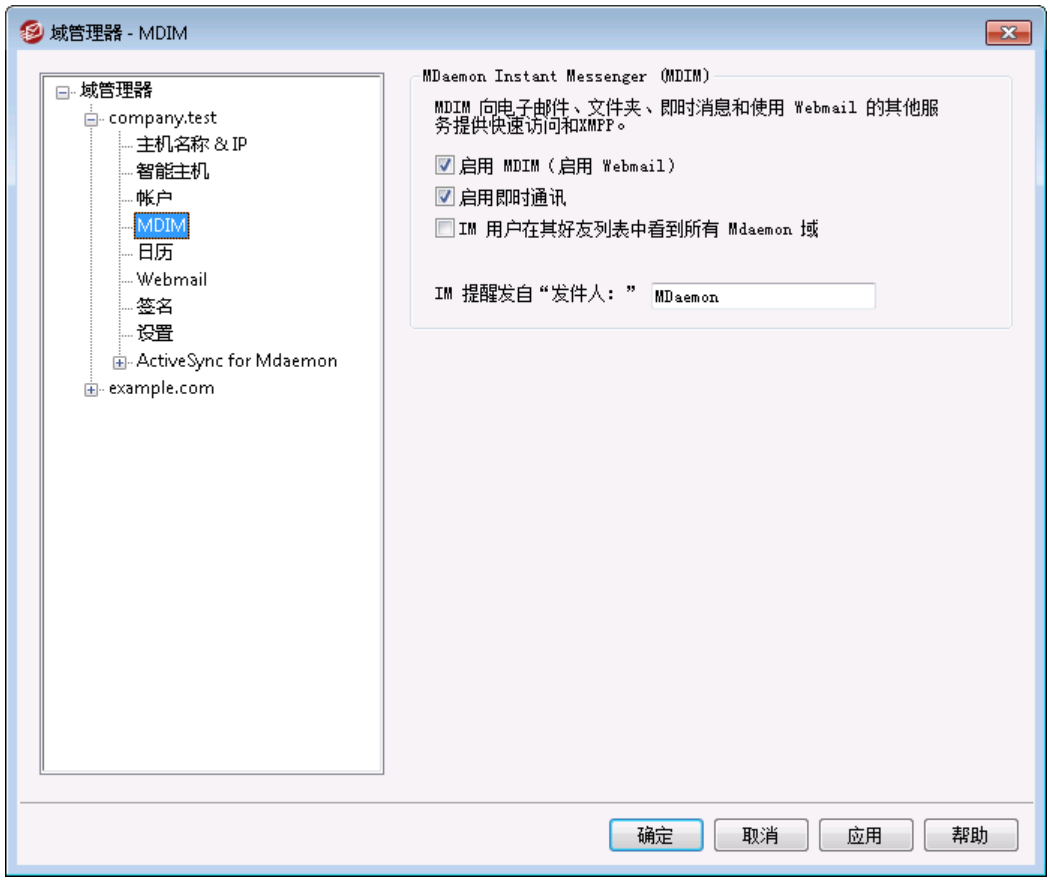
删除
从列表中选择一个账户然后点击此按钮将其删除。在 MDaemon 执行删除账户的操作中，将要求您确认此决定。

显示更多账户
该账户列表一次只能显示 500 个账户。如果在你选择的域中有多于500个帐号，则点击此按钮来显示下500个。

还请参阅：

账户管理器[596]
账户编辑器[598]
新建账户模板[667]

3.2.4 MDIM



该屏幕为域控制 MDaemon Instant Messenger (MDIM)[267] 的各方各面。此屏幕上的初始设置由 "Web & IM 服务"对话框上的默认 MDaemon Instant Messenger[278] 设置确定。可以通过 Web 服务[603]和群组属性[658]屏幕分别为特定账户或群组启用或禁用 MDIM 服务。

MDaemon Instant Messenger (MDIM)

启用 MDIM (启用 Webmail)
如果您希望在默认情况下，域的用户可以从 Webmail 内下载 MDaemon Instant Messenger，请启用此项。他们可以从 *"选项 » MDaemon Instant Messenger"* 页面下载这个部件。下载好的安装文件将自动定制每一个用户的账户，便于安装和设置。此选项还使 MDIM 可以使用 "我的邮件文件夹"功能，允许用户检查新的电子邮件，并直接从 WCIM 的快捷菜单打开 Webmail。默认启用 MDIM。

启用即时通讯
默认情况下，账户可以使用 MDIM 和第三方 XMPP[312] 客户端来与其域的其他成员进行即时通讯。如果您不希望允许此域用户使用即时消息，请清除此复选框。

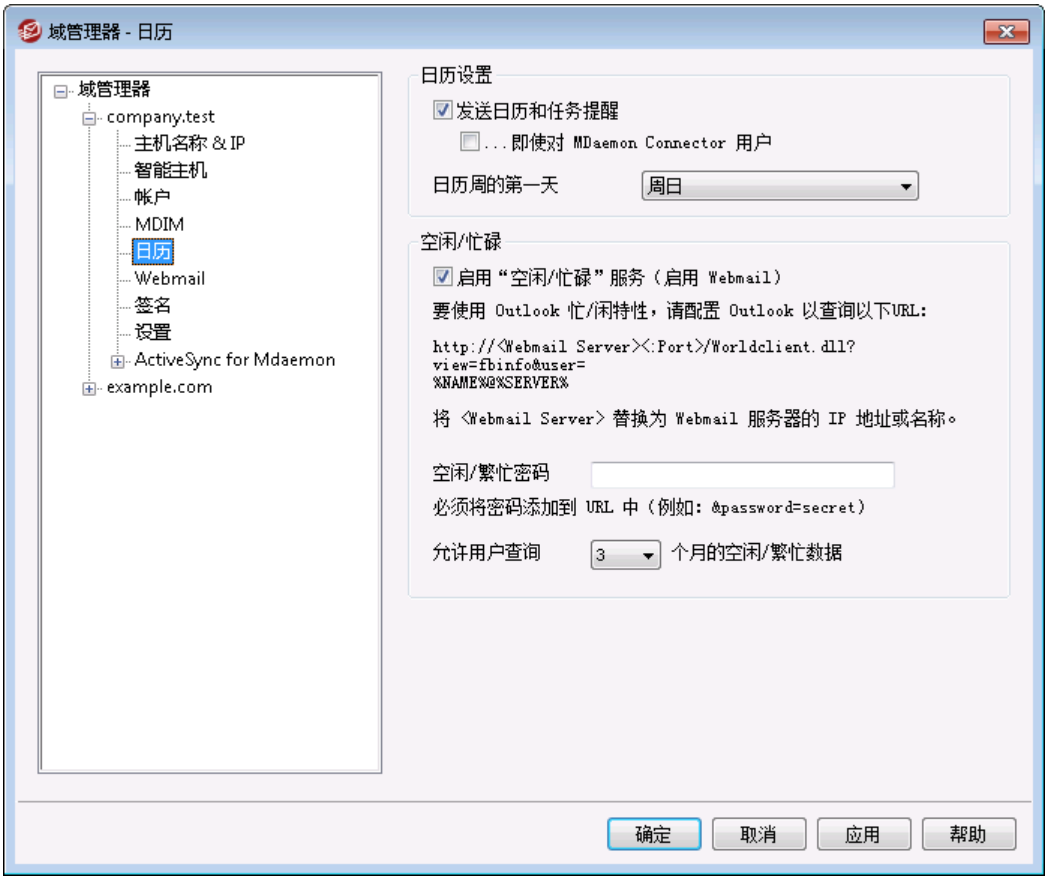
IM 用户在其好友列表中看见所有 MDaemon 域
如果您希望此域的用户在默认情况下能够将联系人添加到所有 MDaemon 域的好友列表，请点击此选项。当禁用此项时，联系人必须位于同一个域。例如，如果您的 MDaemon 正在为 example.com 和 example.org 托管邮件，则为 example.com 激活此项就意味着 example.com 用户可以从这两个域添加即时通讯联系人。禁用此项就意味着 example.com 用户只能添加其他 example.com 用户。默认情况下，禁用该选项。

IM 提醒发送 "发件人:" [文本]
当一个约会被安排到用户的 Webmail 日历中时，可以设置事件在指定时间向用户发送一个提示。如果对于每个用户的域，IM 系统都是激活的，则在即时消息中向该用户发送提醒。使用此文本框来指定您希望在消息中显示的 "From:" 名称。

还请参阅：

域管理器[149]
Webmail » MDIM[278]
账户编辑器 » Web 服务[603]
群组属性[658]

3.2.5 日历



该屏幕为此域控制 MDaemon 的“日历”功能。此屏幕上的初始设置由“Web & IM 服务”对话框上的日历 279 屏幕确定。

日历设置

发送日历和任务提醒

如果您希望允许 Webmail 的日历和任务提醒通过电子邮件和 MDaemon Instant Messenger 发送给您的用户，请点击此勾选框。

...也发送至 MDaemon Connector 用户

如果您已启用以上的 *“发送日历和任务提醒”*选项，如果您还希望为 MDaemon Connector 323 用户启用提醒，请点击此选项。

每周第一天

从下拉菜单中选择一天。选中的那天将出现在日历中，作为每周的第一天。

空闲/忙碌

MDaemon 包含了空闲/忙碌服务器，使得会议组织者可以查看潜在出席者能否参加。要访问此功能，请在创建新的日程时在 Webmail 中点击**调度**。这将打开调度窗口，其中包含出席者列表和针对每位出席者的一行用颜色区分的日历网格。每位出席者所在的行都用颜色区分标识出其有空参加会议的时间。有可以表示忙碌、不确定、外出和无信息的

颜色。**自动选择下一个**按钮可以用来在服务器上查询下一个所有出席者都有空的时间空挡。当您创建完预约后，它向所有出席者发送邀请，出席者可以接受或拒绝邀请。

Webmail的空闲/忙碌服务器同样可以与 Microsoft Outlook 兼容。要使用该功能，只需配置 Outlook 来查询以下列出的 "空闲/忙碌"数据的 URL。例如在 Outlook 2002 中，空闲/忙碌选项位于 "工具» 选项» 日历选项.. » 空闲/忙碌选项.."

用于 Outlook 空闲/忙碌服务器的 URL：

```
http://<Webmail><:Port>/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

使用 Webmail服务器的 IP 或域名替换 "<Webmail>"，并且用端口号替换 "<:Port>"（如果没有使用默认的 Web 端口）。例如：

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

有关如何使用 Webmail的空闲/繁忙功能调度预约的更多信息，请参考 Webmail的在线帮助系统。

启用空闲/忙碌服务 (已启用 Webmail)
如果您要为用户启用空闲/忙碌服务器功能，则点击该选项。

空闲/忙碌密码
如果您希望在用户试图通过 Outlook 访问 "空闲/忙碌"服务器功能时要求他们提供密码，请在此处输入密码。当用户在 Outlook 中配置其空闲/忙碌设置时，密码必须追加在以上列出的 URL 后（格式："&password=FBServerPass"）。例如：

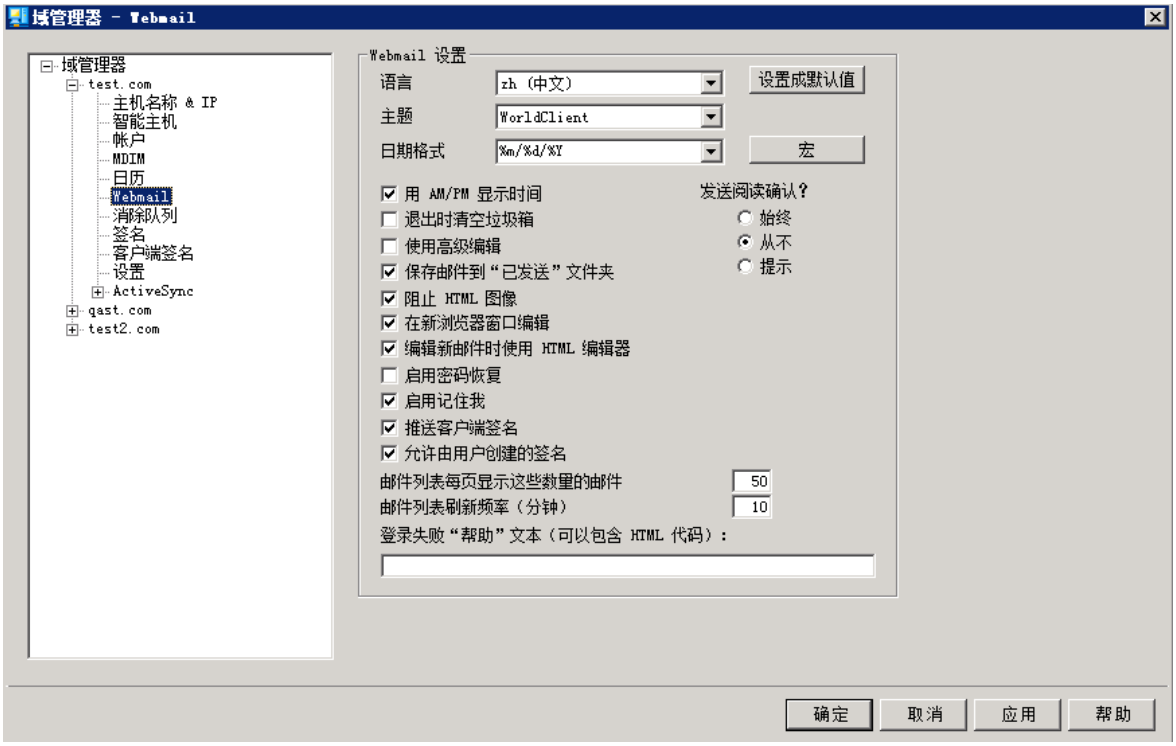
```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%&password=MyFBServerPassword
```

允许用户查询 X 月的空闲/忙碌数据
使用该选项指定您的用户可以查询空闲/忙碌数据的月份数目。

还请参阅：

Webmail» 日历 279

3.2.6 Webmail



此屏幕管理此域的 Webmail的各种客户端级别的选项。在用户登录 Webmail时，这些选项控制 Webmail初次为用户提供的服务和工作方式。用户可以稍后通过 Webmail内的 "选项"页面定制其中的大量设置。此屏幕上的默认设置由 "Web & IM 服务"对话框上的 "Webmail» 设置 289"屏幕确定。

Webmail设置

设置为默认值
此按钮将域重置为 "默认的 Webmail设置 289"。

语言
当您的用户初次登录到所选域时，使用下拉列表框来选择 Webmail界面中的默认语言。用户可以在 Webmail登录页面更改他们的个人语言设置，该选项位于 Webmail中的 "选项» 个性化"中。

主题
当所选域的用户第一次登录时，使用下拉列表框来指定用于他们的默认 Webmail主题。用户可以从 Webmail中的 "选项» 个性化"来自定义主题设置。

日期格式
使用此文本框指定所选域中的日期将以何种格式显示。点击 "宏"按钮以显示可以在此文本框中使用的宏代码列表。您可以在此控件中使用以下宏：

%A——完整的平日名称

%B——完整的月份名

%d——日（显示为“01-31”）

%d——月（显示为“01-12”）

%y——2 位数字年

%Y——4 位数字年

例如，“%m/%d/%Y”在 Webmail中显示为“12/25/2011”。

宏
点击此按钮以显示可以在*“日期格式”*中使用的宏代码列表。

发送已读确认？
该选项控制 Webmail如何答复包含已读确认请求的入站邮件。

始终
如果选定此项，MDaemon 将向发件人发送通知，告之邮件已读。收到邮件的 Webmail用户将不会看到任何关于已请求或已回复已读确认的提示。

从不
如果您希望 Webmail忽略已读确认请求，请选择此选项。

提示
如果您希望每次打开邮件收到此请求时，都询问 Webmail用户是否发送已读确认，请选择此选项。

使用 AM/PM 显示时间
如果您希望在 Webmail中使用带 AM/PM 的 12 小时时钟作为此域的显示时间，请点击此选项。如果您希望为这个域使用 24 小时时钟，请清空此复选框。个人用户可以通过 Webmail中位于*“选项 » 日历”*页面的“以AM/PM 格式显示我的时间”选项修改这项设置。

退出时清空垃圾箱
用户注销 Webmail时，此选项可以清空用户的垃圾站。个人用户可以从 Webmail中的“选项» 个性化”页面修改这项设置。

使用高级编写
如果您希望域用户在 Webmail中看到高级编写屏幕而不是默认情况下的常规编写屏幕，请勾选此选框。个人用户可以从 Webmail中的“选项» 编写”修改这项设置。

保存邮件到“已发送”文件夹
如果您希望发送的每封邮件副本都被保存到您邮箱中的*“已发送”*文件夹，请点击该选项。个人用户可以从 Webmail中的“选项» 编写”页面修改这项设置。

阻止 HTML 图像
如果您希望在 Webmail中查看 HTML 电子邮件时阻止远程图像自动显示，请启用此选框。用户必须点击浏览器窗口中邮件上方的一栏，才能查看图像。这是垃圾邮件防范功能，因为大量垃圾邮件包含带有特殊 URL 的图像，这些 URL识别查看此图像的用户的邮件地址，以向垃圾邮件制造者确保这是有效地址。默认情况下启用此项。

在新浏览器窗口编写
如果您希望打开一个单独的浏览器窗口来编写邮件而不是简单地将主窗口切换到编写屏幕，请点击此选项。如果您不希望打开单独的窗口，清空此框。个人用户可以从 Webmail中的 "选项» 编写"页面修改这项设置。

编辑新邮件时使用 HTML 编辑器
如果您希望 Webmail在默认情况下能让域的用户看见 HTML 编写编辑器，请勾选此框。他们可以从 "选项» 编写" (位于**Webmail**内)为他们自己控制这项设置。

启用密码恢复
若启用此项，有权编辑其密码[603]的域用户将能在 Webmail中输入备选的电子邮件地址，可以向其发送链接，以便在用户忘记密码时重置其密码。要设置此功能，用户必须在 Webmail中的 "选项 » 安全"页面上输入密码恢复邮件地址及当前密码。一旦设置完毕，如果用户尝试使用不正确的密码登录 Webmail，将显示 "忘记密码？"这个链接。该链接将他们带往一个页面，让其确认密码恢复邮件地址。如果输入正确，将发送一封电子邮件，其中提供一个转至更改密码页面的链接。默认情况下禁用此功能。

您可以通过向 Webmail用户的 user.ini 文件 (例如 \Users\example.com\frank\WC\user.ini)添加以下键来按用户启用或禁用此项：

```
[User]
EnablePasswordRecovery=Yes (或 "=No"来为用户禁用此项)
```

允许双重验证记住我 (也适用于 Remote Admin)
当某人在登录 Webmail或 Remote Admin 时使用 "双重验证 (2FA)"时，通常在 2FA 验证页面上有一个可供用户使用的 "记住我"选项，这将阻止服务器再次要求该用户设置 2FA 天数 (请参阅下方的 *"启用记住我"*选项)。如果您不希望显示 "2FA 记住我"选项，请清除此复选框，这意味着所有启用 2FA 的用户每次登录时都必须输入 2FA 代码。**注意：**此项仅在 MDaemon Remote Administration (MDRA)[293] web 界面中可用。

启用 "记住我"
如果您希望 MDaemon Webmail的登录页面上存在 *"记住我"*勾选框，(在域的用户通过 https[274] 端口进行连接时)，请勾选此框。如果用户在登录时勾选此框，则将为该设备记住其凭证。然后，无论他们何时使用该设备连接到 Webmail，他们都将自动登录，直至他们手动注销其账户或其 "记住我"令牌过期。

默认情况下，在用户被强制重新登录之前，最多可以记住30天的用户凭证。如果您希望延长过期时间，可以通过更改 *"这些天后过期记住我令牌"*这个选项的值 (位于 MDaemon Remote Administration (MDRA)[293] web 界面)来实现这点。您也可以通过编辑 RememberUserExpiration=30 键值 (Domains.ini 文件，位于 \MDaemon\WorldClient\ 文件夹)来进行更改。过期值的最大值可以设置成 365 天。**请注意：**双重验证[603] (2FA) 拥有其自身的 "记住我"键值 (TwoFactorAuthRememberUserExpiration=30)，位于 [Default:Settings] 部分，Domains.ini 文件，位于 \MDaemon\WorldClient\ 文件夹。因此，当 2FA 记住我令牌过期时，即使常规令牌仍然有效，登录时也需要 2FA。

默认禁用 *"记住我"*选项，而且仅适用于此域。这个全局选项位于 Webmail设置[289]屏幕。

因为 *"记住我"*允许用户在多台设备上进行永久登录，因此用户不应该在公共网络上使用它。此外，如果您怀疑某个账户可能存在

> 安全漏洞时，MDRA 中有一个 *"重置记住我"*选项，帮助您为所有用户重置 "记住我"令牌。这将要求所有用户再次登录。

推送客户端签名
如果您将客户端签名[170]推送至域的 Webmail用户，请勾选此框。在 Webmail中，这将在以下签名选项下创建一个名为 "系统"的签名：**选项 » 编写**。然后，用户可以选择在编写新邮件时，将此签名自动插入到编写视图中。如果启用了此选项，但尚未在 "域管理器"的 "客户端签名"屏幕上创建客户端签名，将使用默认客户端签名[113]选项。如果也没有默认的客户端签名，则 Webmail中将没有系统签名选项。

允许用户创建的签名
如果您希望允许该域的用户在 Webmail中创建自己的自定义签名，请选中此框。然后用户可以选择在编写邮件时希望将哪些签名自动插入到编写视图中。在您不允许用户创建的签名，但启用了上方的 *"推送客户端签名"*选项时，只会自动插入客户端签名[113]（例如 Webmail中的 "系统"签名）。在 Webmail中，签名选项位于：**选项 » 编写**。

邮件列表每页显示这些数量的邮件
这是在您的每一个邮件文件夹中，每一页邮件列表显示的邮件数。如果一个文件夹中包含超出这个数量的邮件，那么将会在列表的上方和下方出现几个控件，帮助您过渡到其他页。个人用户可以从 Webmail中的 "选项» 个性化"修改这项设置。

邮件列表刷新频率（分钟）
这是 Webmail在自动刷新邮件列表前等待的分钟数。个人用户可以从 Webmail中的 "选项» 个性化"修改这项设置。

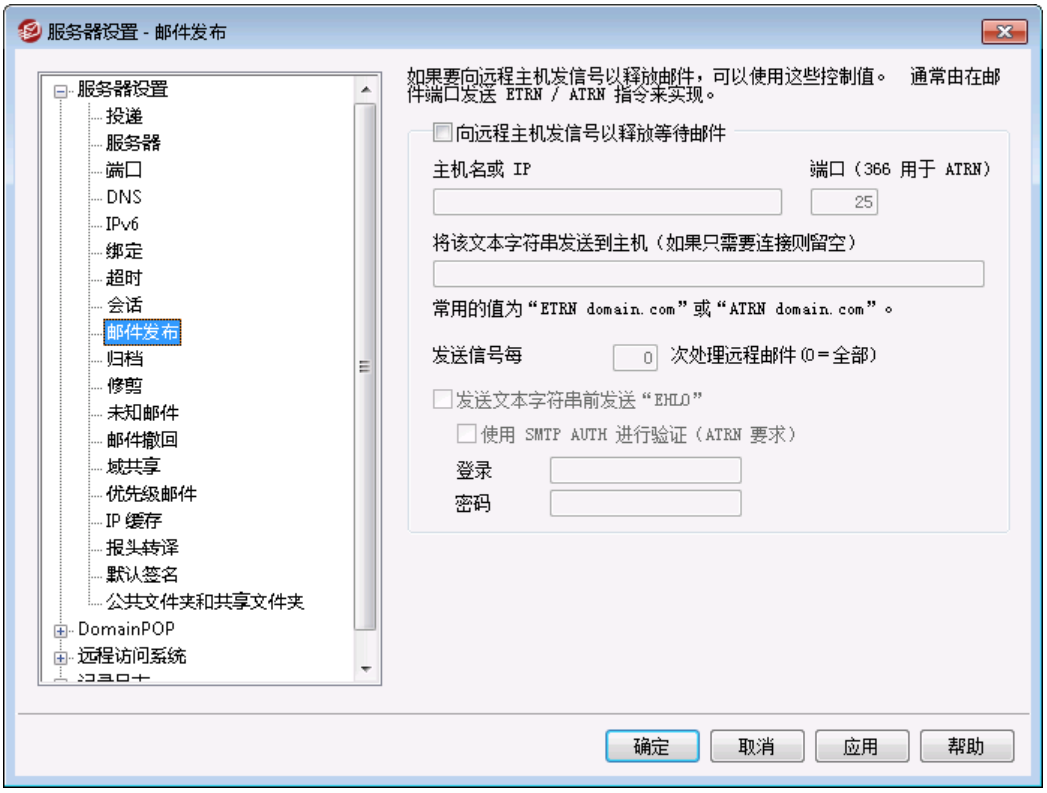
登录失败 "帮助"文本（可包含 HTML 代码）
您可以使用此选项指定在用户遇到登录问题时，显示在 Webmail登录页面上的文本句（纯文本或 HTML 格式）。该文本在以下默认文本下方显示：*"错误登录，请重试。如果您需要帮助，请联系您的邮件管理员。"*可使用此文本引导用户到有关登录 Webmail的帮助页面或联系信息。

> 为了使此功能可以在多个域中正常使用，每个域都需要有效的 SMTP 主机名称[151]设置，否则将使用默认域[149]的文本。因此，如果您有多个域，但将所有 Webmail用户定向到单个主机名进行登录，可能将不显示视域而定的*登录失败 "帮助"的正确文本*。

还请参阅：

Webmail» 设置[289]

3.2.7 出队



出队（邮件释放/ETRN/ODMR/ATRN）

启用出队
处理远程邮件时，MDaemon 可以从任何端口连接到任何服务器，并发送您希望发送的任何字符串。当您需要通过发送一些字符串到服务器，来用信号通知远程服务器发布您的邮件，这是非常有用的。例如：ATRN、ETRN 或 QSND。您也可以在暂时需要 FINGER 或 TELNET 会话时，使用此功能，以便您的远程主机或 ISP 确定您是否在线。

主机名或 IP
这是将接收信号并发布您邮件的主机。

端口
输入您希望连接的端口。默认值为 25（SMTP 端口），适用于 ETRN 或 QSND 信号发送方法。366 端口专用于 ATRN，79 端口用于 FINGER。

发送文本字符串前发送“EHLO”
如果您启用此选择框，您应该连接到 SMTP 服务器以发送释放您邮件的信号。该选项将使用指定的主机初始化 SMTP 会话，并允许此会话在发送解锁字符串之前只进行到 SMTP“EHLO”阶段。

发送文本字符串前先验证（需要 ATRN）
作为一项安全措施，某些主机或服务器要求客户端在发布等待邮件前使用 ESMTP AUTH 进行验证。如果您的邮件主机也是这种情况，请点击此检查框并在以下输入需要的验证凭证。

使用 ATRN 命令出列您的邮件时，需要验证。

AUTH 登录
请在此处输入您主机要求的 AUTH 登录参数。

AUTH 密码
请在此处输入 AUTH 密码。

发送此命令到主机（如果仅连接就足够的话请留空）
此控件用于指定需要发送的文本字符串，以便发布您的邮件。例如，ETRN 方法需要在排队站点的域名后跟着 "ETRN"文本。其他方法需要发送不同的文本。有关发送何文本以解锁您邮件队列的更多信息，请向您的 ISP 咨询。如果您可以选择使用方法，我们推荐您使用按需邮件中继（ODMR）165。在该选项中，ODMR 需要使用 ATRN 命令。

每 [xx]次处理远程邮件都会发生出队（0=每次）
默认情况下，每次处理远程邮件时发送出列信号。在该控件中输入数字将阻止每次被发送的出队信号。将通过指定的每 x 次发送它。例如，将该值设置为 "3"则在每 3 次处理远程邮件后发送一次信号。

这是全局设置，将应用到所有域。

3.2.7.1 按需邮件中继（ODMR）

当您要求使用队列/消除队列方法来托管与发布您的邮件时，我们推荐您使用按需邮件中继（ODMR）。此方法胜于 ETRN 和其他方法的原因是它在发布邮件前需要验证。此外，它利用一种 ESMTP 命令叫做 ATRN，无需客户端有一个静态 IP 地址，因为它能迅速反向客户端和服务器端之间的数据流，不必创建新连接即可发布邮件。（不像 ETRN）。

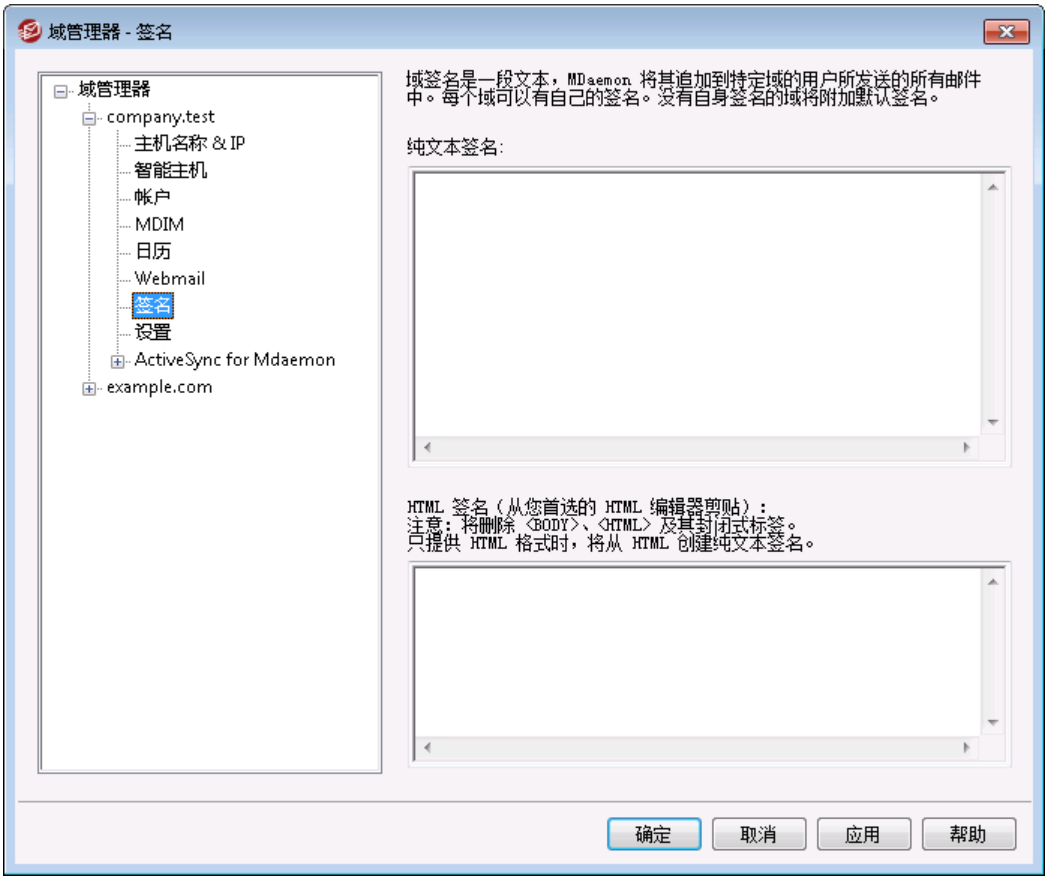
MDaemon 完全支持客户端上的 ODMR，通过使用 ATRN 命令、位于邮件发布164屏幕上的验证控制，以及在服务器端使用位于 "网关编辑器"消除队列218屏幕上的 "域网关"功能来实现这点。

某些邮件服务器不支持 ODMR，因此您应该在尝试前向您的供应商查询此事。

还请参阅：

网关编辑器 » 消除队列218

3.2.8 签名



使用此屏幕来将签名附加到由这个域的用户发送的所有邮件。如果未在此处指定签名则附加默认签名[109]。签名被添加到邮件底部，除非邮件列表邮件已使用脚注，会将脚注[246]添加到 *"域签名"*之下。您还可使用 *"账户编辑器"*的签名[632]功能为每个账户添加个人签名。将在默认或域签名前添加账户签名。

纯文本签名

此区域用于插入纯文本签名。如果您希望在多部分邮件 (multipart message)的文本/html 部分中使用指定且相应的 html签名，请使用下方的 *"HTML 签名"*屏幕。如果一个签名同时存在于这两个位置，MDaemon 将为多部分邮件的各个部分使用正确的签名。如果未指定 html签名，就会在两个部分中都使用纯文本签名。

HTML 签名 (剪贴自您首选的 HTML 编辑器)

此区域用于插入 HTML 签名，将在多部分邮件的文本/html部分使用。如果此处和上方的 *"纯文本签名"*区域都包括同一个签名，MDaemon 将为多部分邮件的各个部分使用正确的签名。如果未指定纯本文签名，就会使用 html格式来创建一个签名。

要创建您的 html签名，可以在此处手动输入 html代码，也可直接从您首选的 HTML 编辑器对签名进行剪切和粘贴操作。如果您希望在您的 HTML 签名中包含内嵌图像，您可以使用 `$ATTACH_INLINE:path_to_image_file$` 宏来实现这点。

例如：

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

还有多种将内嵌图像插入签名的方式，您可以从 MDaemon 的 Remote Administration 293 web 界面执行操作：

- 在 Remote Administration 的 "签名"屏幕上，点击 HTML 编辑器中的 "图像"工具栏按钮并选择上传选项卡。
- 在 Remote Administration 的 "签名"屏幕上，点击 HTML 编辑器中的 "添加图像"工具栏按钮。
- 将一个图像拖放到 "签名"屏幕的 HTML 编辑器 (使用 Chrome、FireFox、Safari 或 MSIE 10+)
- 将剪贴板中的图像复制粘贴到 "签名"屏幕的 HTML 编辑器 (使用 Chrome、FireFox 或 MSIE 11+)

签名中不允许 <body></body> 和 <html></html> 标签，而且在找到这些标签时会将它们删除。

签名宏

MDaemon 签名支持将发件人的联系信息插入签名的宏，该签名取自位于其域的公共联系人文件夹中的发件人联系人。这允许使用发件人的信息对默认和域签名进行个性化。例如 $CONTACTFULLNAME$ 插入发件人的全名，$CONTACTEMAILADDRESS$ 插入发件人的邮件地址。使用 Webmail、MDaemon Connector 或 ActiveSync 来编辑公共联系人。如果发件人不存在联系人，则使用空值。可用的宏如下所示。

用户可以通过使用 $SYSTEMSIGNATURE$ 宏放置默认/域签名，并使用 $ACCOUNTSIGNATURE$ 放置账户签名来控制 MDaemon 签名在其邮件中的位置。

Signature Selector	
$SYSTEMSIGNATURE$	Places the Default Signature 109 or Domain Signature 166 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 113 or Domain Client Signature 170 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 632 in the message.
姓名和 ID	
全名	**$CONTACTFULLNAME$**
名	**$CONTACTFIRSTNAME$**

中间名	**$CONTACTMIDDLENAME$,**
姓	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
后缀	**$CONTACTSUFFIX$**
昵称	**$CONTACTNICKNAME$**
Yomi名	**$CONTACTYOMIFIRSTNAME$**
Yomi姓	**$CONTACTYOMILASTNAME$**
账户名称	**$CONTACTACCOUNTNAME$**
客户 ID	**$CONTACTCUSTOMERID$**
政府 ID	**$CONTACTGOVERNMENTID$**
文件作为	**$CONTACTFILEAS$**
电子邮件地址	
电子邮件地址	**$CONTACTEMAILADDRESS$**
电子邮件地址 2	**$CONTACTEMAILADDRESS2$**
电子邮件地址 3	**$CONTACTEMAILADDRESS3$**
电话和传真号码	
手机号码	**$CONTACTHOMEMOBILE$**
手机 2	**$CONTACTMOBILE2$**
车载电话	**$CONTACTCARPHONENUMBER$**
家庭电话	**$CONTACTHOMEPHONE$**
家庭电话 2	**$CONTACTHOMEPHONE2$**
家庭传真	**$CONTACTHOMEFAX$**
其他电话	**$CONTACTOTHERPHONE$**
即时通讯和 Web	
IM 地址	**$CONTACTIMADDRESS$**
IM 地址 2	**$CONTACTIMADDRESS2$**
IM 地址 3	**$CONTACTIMADDRESS3$**
MMD 地址	**$CONTACTMMSADDRESS$**
家庭网址	**$CONTACTHOMEWEBADDRESS$**
地址	

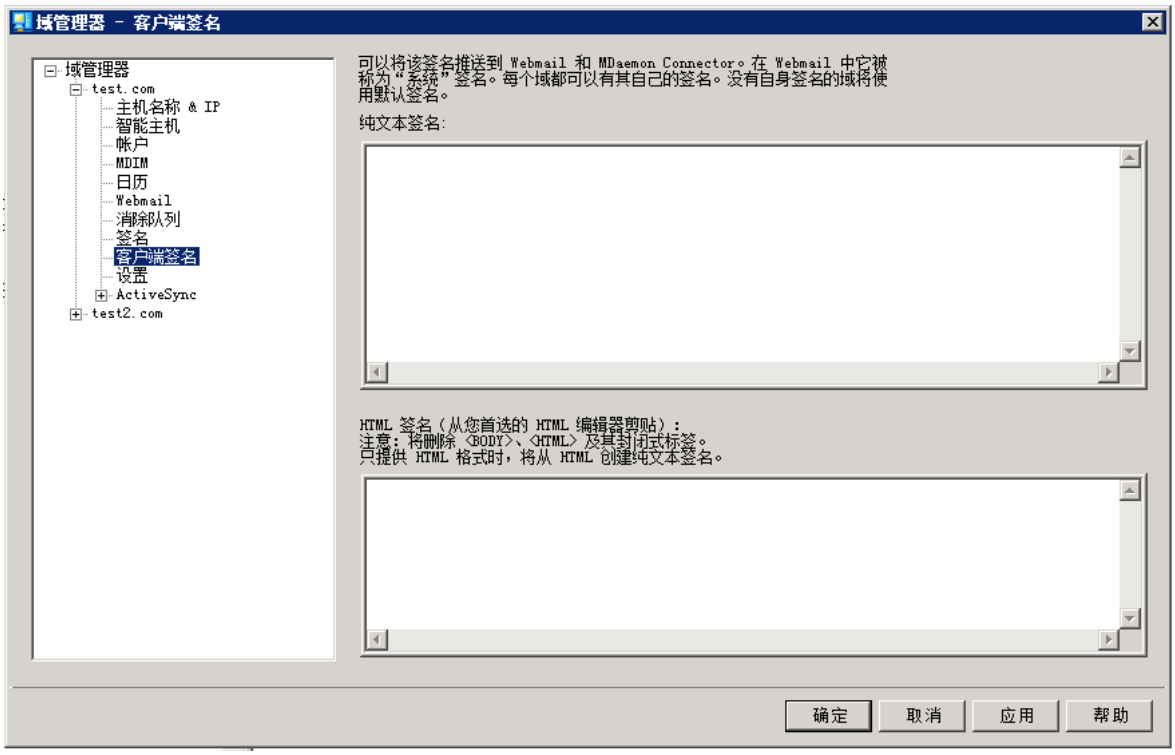
家庭地址	**$CONTACTHOMEADDRESS$**
家乡城市	**$CONTACTHOMECITY$**
家乡州	**$CONTACTHOMESTATE$**
家乡邮政编码	**$CONTACTHOMEZIPCODE$**
家乡国家	**$CONTACTHOMECOUNTRY$**
其他地址	**$CONTACTOTHERADDRESS$**
其他城市	**$CONTACTOTHERCITY$**
其他州	**$CONTACTOTHERSTATE$**
其他邮政编码	**$CONTACTOTHERZIPCODE$**
其他国家	**$CONTACTOTHERCOUNTRY$**
公司相关	
公司名称	**$CONTACTBUSINESSCOMPANY$**
Yomi公司名称	**$CONTACTYOMICOMPANYNAME$**
公司职位	**$CONTACTBUSINESSTITLE$**
公司办公室	**$CONTACTBUSINESSOFFICE$**
公司部门	**$CONTACTBUSINESSDEPARTMENT$**
公司经理	**$CONTACTBUSINESSMANAGER$**
公司助理	**$CONTACTBUSINESSASSISTANT$**
公司助理电话	**$CONTACTBUSINESSASSISTANTPHONE$**
公司总机	**$CONTACTBUSINESSMAINPHONE$**
公司电话	**$CONTACTBUSINESSPHONE$**
公司电话 2	**$CONTACTBUSINESSPHONE2$**
公司 IP 电话	**$CONTACTBUSINESSIPPHONE$**
公司传真	**$CONTACTBUSINESSFAX$**
公司寻呼机	**$CONTACTBUSINESSPAGER$**
公司无线电	**$CONTACTBUSINESSRADIO$**
公司地址	**$CONTACTBUSINESSADDRESS$**
公司所在城市	**$CONTACTBUSINESSCITY$**
公司所在州	**$CONTACTBUSINESSSTATE$**
公司邮政编码	**$CONTACTBUSINESSZIPCODE$**
公司所在城市	**$CONTACTBUSINESSCOUNTRY$**

公司网址	**$CONTACTBUSINESSWEBADDRESS$**
其他	
配偶	**$CONTACTSPOUSE$**
孩童	**$CONTACTCHILDREN$**
类别	**$CONTACTCATEGORIES$**
备注	**$CONTACTCOMMENT$**

还请参阅：

默认签名 109
账户编辑器 » 签名 632

3.2.9 客户端签名



使用此屏幕来创建此域的客户端签名，您可以将其推送至 MDaemon Webmail 160 和 MDaemon Connector 339，供您的用户在编写邮件时使用。您可以使用下方列出的宏 171 来个性化签名，这样签名对于每个用户都是唯一的，包括用户名、电子邮件地址和电话号码等元素。如果您希望创建一个不同的签名，在没有视域而定的客户端签名时进行使用，请使用默认客户端签名 113 屏幕。存在针对一个域的特定签名时，将使用这个签名来取代"默认客户端签名"。如果您希望将客户端签名推送至 Webmail，请使用 *"推送客户端签名* 160 "选项，如果您希望将其推送到 MDaemon Connector，请使用 *"推送客户端签名至 Outlook* 339 选

项。在 Webmail的 "编写"选项中，推送的客户端签名被称为 "系统"。对于 MDaemon Connector，您可以为 Outlook 中将显示的签名指定名称。

纯文本签名

此区域用于插入纯文本签名。如果您希望在多部分邮件 (multipart message)的文本/html部分中使用指定且相应的 html签名，请使用下方的 *"HTML 签名"*屏幕。如果一个签名同时存在于这两个位置，MDaemon 将为多部分邮件的各个部分使用正确的签名。如果未指定html签名，就会在两个部分中都使用纯文本签名。

HTML 签名 (剪贴自您首选的 HTML 编辑器)

此区域用于插入 HTML 签名，将在多部分邮件的文本/html部分使用。如果此处和上方的 *"纯文本签名"*区域都包括同一个签名，MDaemon 将为多部分邮件的各个部分使用正确的签名。如果未指定纯本文签名，就会使用 html格式来创建一个签名。

要创建您的 html签名，可以在此处手动输入 html代码，也可直接从您首选的 HTML 编辑器对签名进行剪切和粘贴操作。如果您希望在您的 HTML 签名中包含内嵌图像，您可以使用 $ATTACH_INLINE:path_to_image_file$ 宏来实现这点。

例如：

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

还有多种从 MDaemon 的Remote Administration 293 web 界面，将内嵌图像插入签名的方法：

- 在 Remote Administration 的 "客户端签名"屏幕上，点击 HTML 编辑器中的 "图像"工具栏按钮并选择上传选项卡。
- 在 Remote Administration 的 "客户端签名"屏幕上，点击 HTML 编辑器中的 "添加图像"工具栏按钮。
- 将一个图像拖放到 "客户端签名"屏幕的 HTML 编辑器 (使用 Chrome、FireFox、Safari或 MSIE 10+)
- 借助 Chrome、FireFox 或 MSIE 11+，将剪贴板中的图像复制粘贴到 "客户端签名"屏幕的 HTML 编辑器

签名中不允许 <body></body> 和 <html></html> 标签，而且在找到这些标签时会将它们删除。

签名宏

MDaemon 签名支持将发件人的联系信息插入签名的宏，该签名取自位于其域的公共联系人文件夹中的发件人联系人。这允许使用发件人的信息对默认和域签名进行个性化。例如 $CONTACTFULLNAME$ 插入发件人的全名，$CONTACTEMAILADDRESS$ 插入发件人的邮件地址。使用 Webmail、MDaemon Connector 或 ActiveSync 来编辑公共联系人。如果发件人不存在联系人，则使用空值。可用的宏如下所示。

用户可以通过使用 $SYSTEMSIGNATURE$ 宏放置默认/域签名，并使用 $ACCOUNTSIGNATURE$ 放置账户签名来控制 MDaemon 签名在其邮件中的位置。

Signature Selector	
$SYSTEMSIGNATURE$	Places the Default Signature 109 or Domain Signature 166 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 113 or Domain Client Signature 170 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 632 in the message.
姓名和 ID	
全名	**$CONTACTFULLNAME$**
名	**$CONTACTFIRSTNAME$**
中间名	**$CONTACTMIDDLENAME$,**
姓	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
后缀	**$CONTACTSUFFIX$**
昵称	**$CONTACTNICKNAME$**
Yomi名	**$CONTACTYOMIFIRSTNAME$**
Yomi姓	**$CONTACTYOMILASTNAME$**
账户名称	**$CONTACTACCOUNTNAME$**
客户 ID	**$CONTACTCUSTOMERID$**
政府 ID	**$CONTACTGOVERNMENTID$**
文件作为	**$CONTACTFILEAS$**
电子邮件地址	
电子邮件地址	**$CONTACTEMAILADDRESS$**
电子邮件地址 2	**$CONTACTEMAILADDRESS2$**
电子邮件地址 3	**$CONTACTEMAILADDRESS3$**
电话和传真号码	
手机号码	**$CONTACTHOMEMOBILE$**
手机 2	**$CONTACTMOBILE2$**
车载电话	**$CONTACTCARPHONENUMBER$**

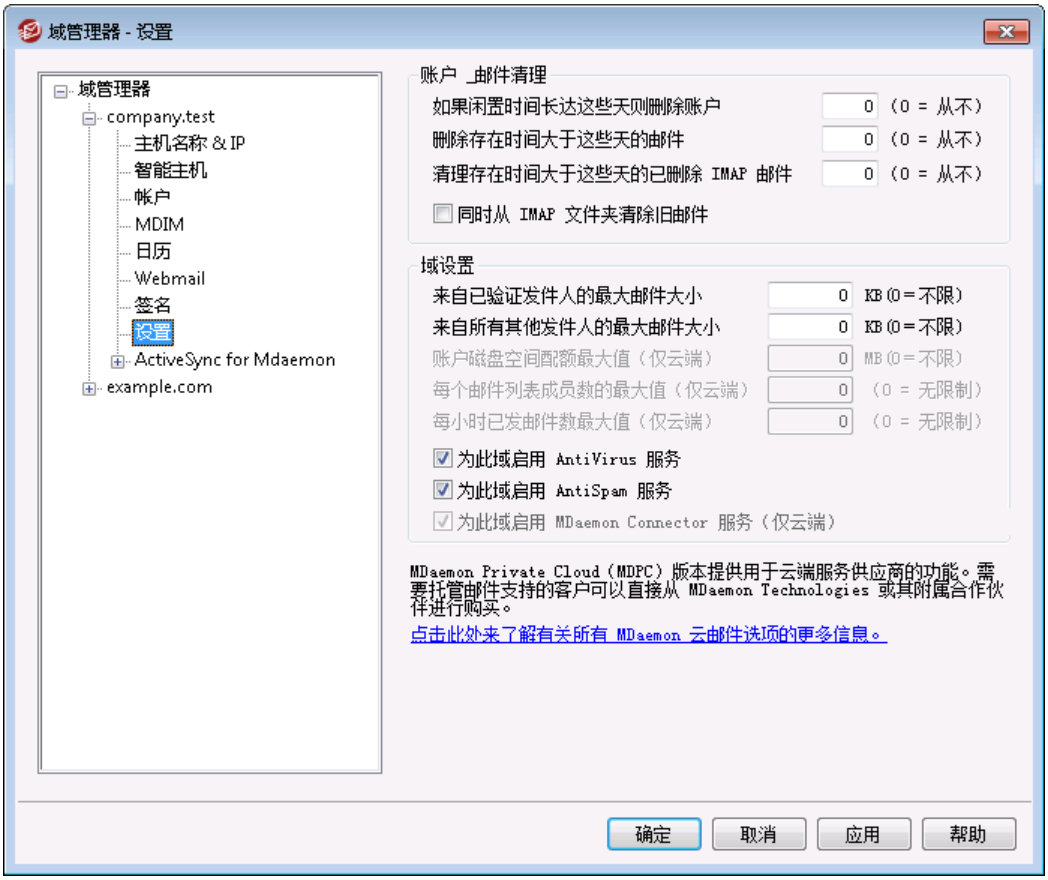
家庭电话	**$CONTACTHOMEPHONE$**
家庭电话 2	**$CONTACTHOMEPHONE2$**
家庭传真	**$CONTACTHOMEFAX$**
其他电话	**$CONTACTOTHERPHONE$**
即时通讯和 Web	
IM 地址	**$CONTACTIMADDRESS$**
IM 地址 2	**$CONTACTIMADDRESS2$**
IM 地址 3	**$CONTACTIMADDRESS3$**
MMD 地址	**$CONTACTMMSADDRESS$**
家庭网址	**$CONTACTHOMEWEBADDRESS$**
地址	
家庭地址	**$CONTACTHOMEADDRESS$**
家乡城市	**$CONTACTHOMECITY$**
家乡州	**$CONTACTHOMESTATE$**
家乡邮政编码	**$CONTACTHOMEZIPCODE$**
家乡国家	**$CONTACTHOMECOUNTRY$**
其他地址	**$CONTACTOTHERADDRESS$**
其他城市	**$CONTACTOTHERCITY$**
其他州	**$CONTACTOTHERSTATE$**
其他邮政编码	**$CONTACTOTHERZIPCODE$**
其他国家	**$CONTACTOTHERCOUNTRY$**
公司相关	
公司名称	**$CONTACTBUSINESSCOMPANY$**
Yomi公司名称	**$CONTACTYOMICOMPANYNAME$**
公司职位	**$CONTACTBUSINESSTITLE$**
公司办公室	**$CONTACTBUSINESSOFFICE$**
公司部门	**$CONTACTBUSINESSDEPARTMENT$**
公司经理	**$CONTACTBUSINESSMANAGER$**
公司助理	**$CONTACTBUSINESSASSISTANT$**
公司助理电话	**$CONTACTBUSINESSASSISTANTPHONE$**

公司总机	**$CONTACTBUSINESSMAINPHONE$**
公司电话	**$CONTACTBUSINESSPHONE$**
公司电话 2	**$CONTACTBUSINESSPHONE2$**
公司 IP 电话	**$CONTACTBUSINESSIPPHONE$**
公司传真	**$CONTACTBUSINESSFAX$**
公司寻呼机	**$CONTACTBUSINESSPAGER$**
公司无线电	**$CONTACTBUSINESSRADIO$**
公司地址	**$CONTACTBUSINESSADDRESS$**
公司所在城市	**$CONTACTBUSINESSCITY$**
公司所在州	**$CONTACTBUSINESSSTATE$**
公司邮政编码	**$CONTACTBUSINESSZIPCODE$**
公司所在城市	**$CONTACTBUSINESSCOUNTRY$**
公司网址	**$CONTACTBUSINESSWEBADDRESS$**
其他	
配偶	**$CONTACTSPOUSE$**
孩童	**$CONTACTCHILDREN$**
类别	**$CONTACTCATEGORIES$**
备注	**$CONTACTCOMMENT$**

还请参阅：

默认客户端签名 113
默认签名 109
域管理器 » 签名 166
账户编辑器 » 签名 632
域管理器 » Webmail设置 160
MC客户端设置 » 签名 339

3.2.10 设置



账户和邮件清理

这些选项用于指定何时或是否由 MDaemon 删除闲置账户或旧邮件。每晚午夜，MDaemon 将会删除所有超过规定时间限制的信息和账户。在 "账户编辑器"的 "配额 613"屏幕上也有用来为个人账户重设这些设置的类似选项。

请参阅 AccountPrune.txt (位于 "..\MDaemon\App\"文件夹)来获取更多信息和命令行选项。

账户闲置这些天后将其删除 (0=从不)
指定您希望属于该域的账户在被删除前可保持不活动状态的天数。该控件里的值 "0"表示账户不会因为处于闲置状态而被删除。

删除存在时间长于这些天的邮件 (0=从不)
在该控件中指定的值是任何给定邮件在被 MDaemon 自动删除前可在用户邮箱中驻留的天数。"0"值意味着邮件永远不会因其存在时间而被删除。**请注意：**此选项的设置不适用于包含在 IMAP 文件夹中的邮件，除非您还启用下方的 *"也清理 IMAP 文件夹中的旧邮件"*这个选项。

清理存在时间长于这些天的已删除 IMAP 邮件 (0=从不)
使用该控件来指定您希望允许带有删除标记的 IMAP 邮件在您的用户文件夹中保留的天数。标记为删除时间超过此天数的邮件将从邮箱中清理。值 "0"表示带有删除标记的邮件从不会因为其存在天数而被删除。

同时从 IMAP 文件夹清理旧邮件
如果您希望 *"删除存在时间超过以下天数的邮件"*这个选项同样应用于 IMAP 文件夹中邮件，请点击此选择框。禁用该选项时，IMAP 文件夹中的常规邮件将不会因为其存在时间而被删除。

域设置

来自已验证发件人的最大邮件大小 [xx]KB (0=无限制)
如果您希望为已验证的发件人可以向此域发送的邮件大小设置限制，请使用此项。该值的单位是千字节，而且默认情况下被设置成 "0"，表示无限制。如果您希望为未验证的发件人设置邮件大小限制，请使用下方的 *"..所有其他发件人"*选项。

来自所有其他发件人的最大邮件大小 [xx]KB (0=无限制)
如果您希望为未验证的发件人可以向此域发送的邮件大小设置限制，请使用此项。该值的单位是千字节，而且默认情况下被设置成 "0"，表示无限制。如果您希望为已验证的发件人设置邮件大小限制，请使用前一个选项。

账户磁盘空间配额最大值 [xx]MB (0=无限制)
如果您希望为域可以使用多少磁盘空间设置限制，请使用此项。此项仅适用于 MDaemon Private Cloud。

每邮件列表的成员最大值 [xx] (0=无限制)(仅云端)
如果您希望为此域的各个邮件列表设置所允许的成员数量的最大值，请使用此项。在 "邮件列表管理器"的 "设置 225"屏幕上拥有相应的全局选项。此项仅适用于 MDaemon Private Cloud。

每小时发送的邮件最大值 [xx] (0=无限制)(仅云端)
如果您希望指定这个域每小时可以发送邮件的最大值，请使用此项。一旦达到这个限制，在重置计数前会将之后的邮件留在队列中。邮件计数会每小时进行重置，在重启服务器时也会重置。此项仅适用于 MDaemon Private Cloud。

为此域启用 AntiVirus 服务
如果您希望将 AntiVirus 539 设置应用到此域，请点击此勾选框。

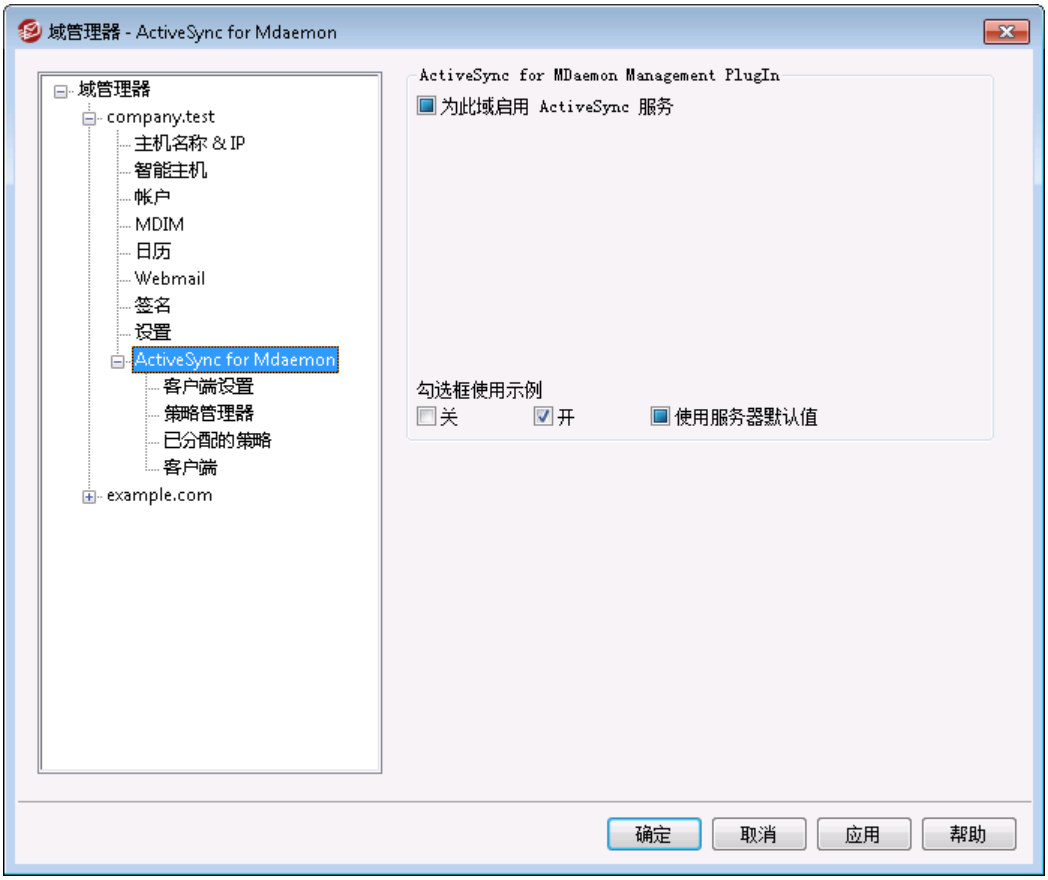
为此域启用反垃圾邮件服务
如果希望将 MDaemon 当前的 "垃圾邮件过滤器"设置应用到此域，请点击该选择框。

为此域启用 MDaemon Connector 服务 (仅 Cloud)
如果您希望为此域启用 MDaemon Connector 323 服务，请勾选此框。

还请参阅：

账户编辑器 » 配额 613

3.2.11 ActiveSync



使用 "域管理器"的这一部分来管理域的 ActiveSync[349] 设置。您可以从 "ActiveSync 管理器"的 "域[365]"屏幕来管理所有域的 ActiveSync 设置和默认值。

ActiveSync for MDaemon 管理插件

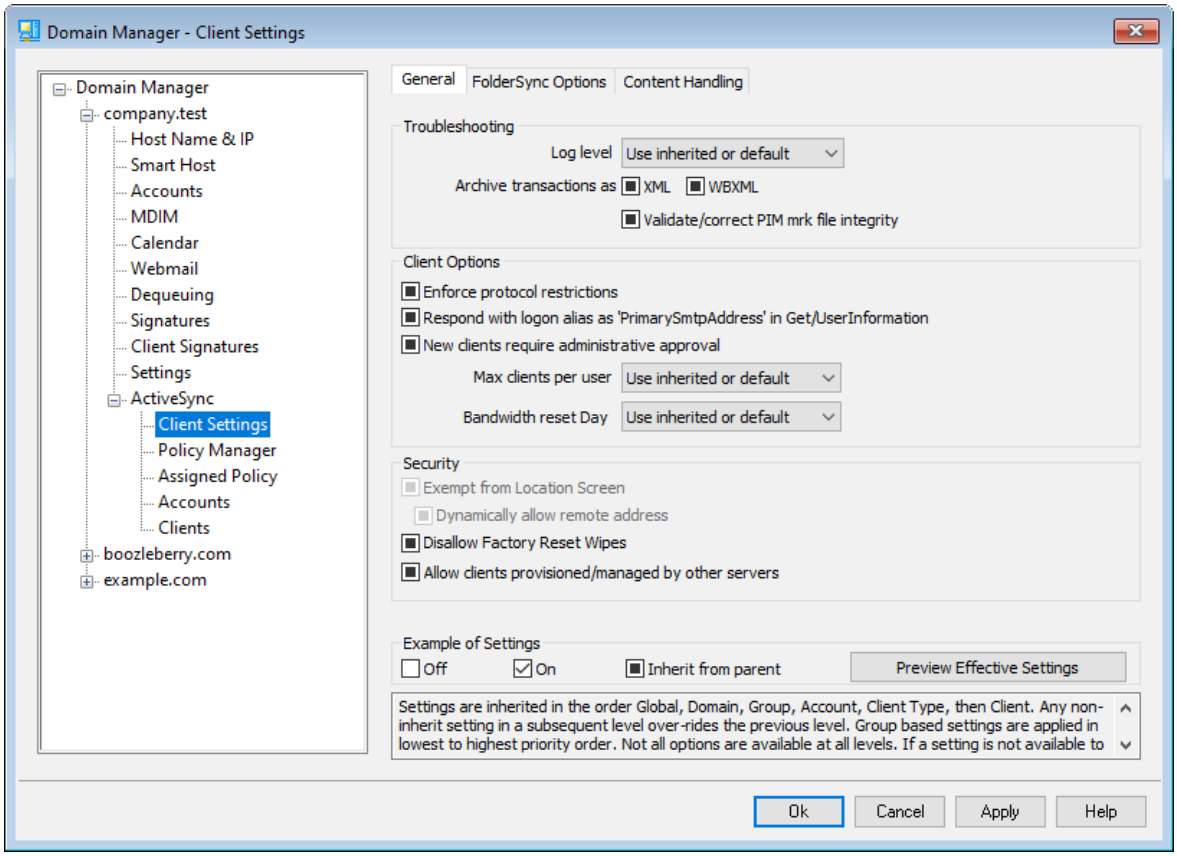
为此域启用 AntiVirus 服务
此项控制在默认情况下这个域的用户是否可以使用 ActiveSync 客户端来访问其电子邮件和 PIM 数据。默认情况下，这个设置的状态从 "默认 ActiveSync 状态[365]"继承，不过您可以通过勾选或取消勾选此框来选择是否覆盖这个设置。您也可以为不希望使用域设置的任何账户[380]或客户端[388]覆盖这个设置。**注意：**如果您为此域禁用 ActiveSync，将打开一个确认框，询问您是否要撤消所有域用户的 ActiveSync 访问权限。如果您希望允许当前使用 ActiveSync 的任何域用户继续使用它，请选择 "否"。如果您选择 "是"，将为该域的所有用户禁用 ActiveSync。

此设置仅控制在 ActiveSync 服务运行时是否允许任何域账户默认使用 ActiveSync。必须启用用于 "启用 ActiveSync 协议[349]"的全局选项来使您许可的任何域或账户都可以访问 ActiveSync。

还请参阅：

ActiveSync » 域 365
ActiveSync » 账户 380
ActiveSync » 客户端 388

3.2.11.1 客户端设置



这个屏幕允许您为与此域相关联的账户和客户端管理默认设置。

默认情况下，会将此屏幕上的所有选项设置成“使用继承或默认值”，这意味着每个选项都将从“全局客户端设置 353”屏幕上相应的选项获取其设置。类似的，此域的账户 155将从这个屏幕继承其设置，因为这是它们的父代屏幕。在此屏幕上对这些选项做出的任何变更都将在这些账户屏幕上反映。在此下方，个别客户端 199还拥有设置屏幕，从账户级别的设置继承其设置。该配置帮助您通过对这一个屏幕做出变更来对一个域的所有账户做出变更，还帮助您按需求为任何账户或客户端覆盖这些设置。

常规

故障诊断

日志级别

ActiveSync for MDaemon 支持 6 种日志级别，按所记录数据数量的多少分级，以下是从

高到低的级别一览：

调试 这是最丰富的日志级别。记录所有可用条目，而且通常只在诊断问题时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

Inherit 默认情况下，"日志级别"设置是从"客户端设置"层次结构继承的。因此，客户端从客户端类型继承，账户从客户端类型继承，群组从账户等继承其设置。此选项的"全局客户端设置"由故障诊断[361]对话框上的"日志级别"设置确定。

归档处理为 [XML | WBXML]
如果您希望保存此数据，请使用*"归档 XML..."*和*"WBXML"*选项，而且有时这些数据对调试很有帮助。默认情况下，禁用这些全局选项。

验证/修复 PIM mrk 文件完整性
该选项对客户端的 PIM 数据运行验证和修复进程来查询有碍正确同步的已知问题，例如重复的 iCalUID 或空的必填字段。默认情况下，禁用这个全局选项。

客户端选项

强制执行协议限制
如果有连接来自尝试使用指定的*"允许的协议版本"*以外的其他协议的客户端，您希望拒绝这些连接时请启用此项。默认情况下禁用此项，这就表示协议限制不防止客户端使用不同的协议：它们只是告诉客户端使用哪些协议。如果客户端无论如何都要尝试使用限制的协议，MDaemon 仍然允许这个连接。还请参阅：协议限制[363]来了解更多信息。

使用登录别名响应，作为 GetUserInformation 中的"PrimarySmtpAddress"
这允许该服务返回别名/次要地址作为主要地址来响应"设置/获取/用户信息"请求。这有助于解决 iOS9.x 更新所引起的一个问题：即导致客户端无法使用别名发送邮件。使用此项将导致对于"设置/获取/用户信息"不规范的响应。

新建客户端需要管理批准
如果您希望要求新的客户端必须先由管理员授权，才能开始与账户同步，请启用此选项。The 客户端[388]列表指示等候授权的任何客户端，管理员可以从相同的屏幕对其进行授权。默认情况下，禁用该设置。

每用户的客户端最大值
如果您希望限制 MDaemon 账户可以关联的 ActiveSync 客户端或设备的数量，请在此项中指定所需数量。默认情况下将这个全局选项设成"无限"。"全局"、"域"和"账户"客户端设置屏幕提供此项，但是个别客户端屏幕不提供此项。

带宽重置日期
如果您希望在每个月指定的一天为 ActiveSync 设备重置带宽使用统计，请使用此项。重置事件作为常规夜间维护过程的一部分进行，而且像其他维护例程一样被记录到系统日志中。默认情况下将这个全局选项设置成 "0"（从不），这就意味着从不重置使用统计。如果您希望重置的那一天与用户或客户端无线运营商计费的重置日期一致，请将子项设置成不同的一天。

安全

从"位置屏蔽"豁免
启用此项（位于 ActiveSync 客户端的设置屏幕）允许您将设备绕过位置屏蔽[477]。这使得有效的用户有可能通过 ActiveSync 继续访问他或她的账户，例如当前往一个阻止验证尝试的位置时。为了免除设备，它必须使用 ActiveSync 在配置的时间范围内进行连接和验证，请在位于"微调"屏幕的这些天后删除闲置的客户端[351]这个设置中进行配置。

动态允许远程地址
当从"位置屏蔽"豁免设备时，如果您还希望允许其连接的远程 IP 地址，请启用此选项。这对允许其他可能从相同 IP 地址连接的客户端很有用。

允许由其他服务器配置/管理的客户端
默认情况下，当 ActiveSync 服务器向特定客户端发送数据/策略，并报告它也受其他 ActiveSync 服务器管理时，也允许那个客户端连接到 MDaemon。不过在这种情况下，无法确保在与其他 ActiveSync 服务器的策略发生冲突时将应用您的策略。通常默认客户端在策略冲突时使用最具有限制性的选项。如果您不希望允许这些客户端进行连接，请禁用此项。

不允许出厂重置擦除
如果将其设置成启用/是，就不提供**完全擦除** ActiveSync 客户端的功能。如果您希望能够完全远程擦除客户端，您必须先禁用此项。默认情况下，禁用该选项。要了解更多详情，请参阅："客户端"页面上的完全擦除 ActiveSync 客户端[388]。

FolderSync 选项

FolderSync 选项

例外

已允许/已阻止发件人文件夹
默认情况下，无法和设备同步用户的"已允许发件人和已阻止发件人"联系人文件夹。它们通常只能由 MDaemon 用来吸住自动防止垃圾邮件。出于这个原因，它们无需在设备上显示为联系人。

非默认邮件文件夹
默认情况下能与设备同步所有由用户创建和默认的邮件文件夹。如果您仅希望允许同步默认的邮件文件夹（例如收件箱、已发送项目、已删除项目和草稿等），请启用此项。不会包含由用户创建的文件夹。默认情况下，禁用该选项。

非默认 PIM 文件夹
默认情况下，将与设备同步用户的所有 PIM 文件夹（例如联系人、日历、便笺和任务等）。如果您希望仅允许同步默认的 PIM 文件夹，请启用此项。例如，如果启用此项，

而且用户拥有多个日历文件夹，将仅同步默认的日历。默认情况下，禁用该选项。

包括

公告文件夹层次结构

如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的公共文件夹[258]，则勾选此框。默认启用此项。

允许屏蔽

允许客户端搜索它有权访问的公共文件夹[258]。默认情况下允许搜索操作。

公共文件夹遍历（显示文件夹名称）

默认情况下，为了让客户端同步/访问公共子文件夹，该账户必须拥有查询权限[260]，而且必须对子文件夹和所有父代公共文件夹[258]拥有该权限。如果该账户没有权限查看父文件夹，那么该账户也不能查看子文件夹，即使该账户有查看子文件夹的权限也是如此。如果您希望允许客户端访问这些子文件夹，请启用此项。**请注意：**启用此项必须向客户端显示父文件夹的名称，这会被视为安全风险。默认情况下，禁用该选项。

允许的公共文件夹数量最大值

如果您希望限制在设备上允许的“公共文件夹”的数量，请使用此项。在设置了限制时，该服务器遍历文件夹列表，直到达到这个限制为止，不会再将更多项目发送到设备。无法确保以何顺序处理这些文件夹。默认情况下未设置全局限制。

共享文件夹

如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的共享文件夹[97]，则勾选此框。默认启用此项。

允许屏蔽

允许客户端搜索它有权访问的共享文件夹[623]。默认情况下允许搜索操作。

内容处理

内容处理选项

在被客户端标记时为邮件项目创建任务/提醒

该选项可以在客户端请求时，使 MDaemon 通过为各个已标记的邮件创建任务项目来向用户提醒已标记的项目。。默认情况下，此控件的全局选项处于启用状态。

在事件被修改时始终发送会议更新

某些客户端在修改会议时未正确发送会议更新电子邮件。这指示 ActiveSync 服务在组织者更新会议项目时发送会议更新。这仅能在客户端[388]和无法恰当发送会议更新的客户端类型[402]上设置，否则将导致发送重复的会议更新。因此，此选项仅在“客户端”和“客户端类型”的设置页面上可用。

对所有已发送邮件请求已读回执

如果您希望服务器为客户端发送的所有邮件请求已读确认，请启用此项。默认情况下，禁用该选项。

当邮件被标记为已读时，以及发件人请求时，从服务器发送已读回执
如果您希望服务器支持已读确认请求，并在客户端将邮件标记为已读时发送已读回执，请启用此项。默认情况下，禁用该选项。

发送为在 ReplyTo 地址中指定的别名
某些客户端可能不允许发件人使用别名发送邮件。已在 Exchange ActiveSync (EAS) 协议 363 16.x 中添加该功能，不过一些客户端不支持 16.x。例如，Windows 版的 Outlook 仅使用 EAS 14.0，虽然它允许用户指定要发送的备用地址，但生成的邮件并不能正确反映用户的选择。该选项允许使用 ReplyTo (答复) 字段来发送电子邮件，只要 ReplyTo 地址是该用户的有效别名 699 即可。默认情况下启用这个全局选项。

虚拟地将公共联系人合并为默认联系人
如果您希望将设备上的公共联系人与用户的默认联系人合并在一起，请启用此项。这仅仅是一个虚拟合并，实际上未将它们复制到用户的联系人文件夹。这对不支持 "全局地址列表" (GAL) 搜索的客户端而言极其有用。默认情况下，禁用该选项。

在将邮件移入垃圾邮件文件夹时阻止发件人
启用后，当客户端将电子邮件移动到账户的垃圾邮件文件夹时，该服务将该电子邮件的发件人或从地址添加到阻止的发件人联系人文件夹。

在会议请求被接受/拒绝等时强制发送会议请求。
启用后，当客户端接受、拒绝或以其他方式选择响应会议请求的操作时，服务将向会议组织者发送会议响应。这是针对没有正确发送这些更新本身的特定客户端。

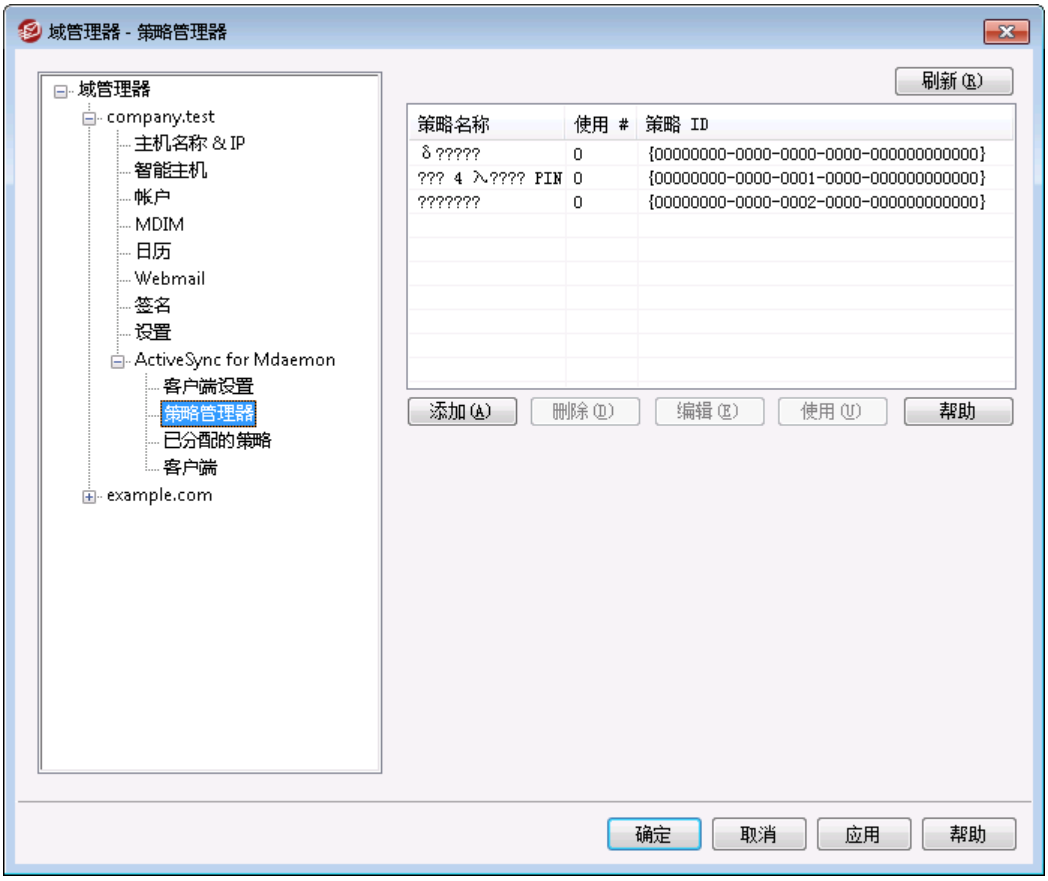
预览有效设置

该按钮在所有子 "客户端设置" 屏幕上可用 (例如域 365、账户 380 和客户端 388)。由于默认情况下，已将这些屏幕上的选项都设置成从父屏幕继承其设置，使用该功能来查看当前向显示的屏幕应用了什么设置。

还请参阅：

ActiveSync » 客户端设置 353
ActiveSync » 账户 380
ActiveSync » 客户端 388

3.2.11.2 策略管理器



使用此屏幕来管理 "ActiveSync 策略"，可以将这些策略分配给用户设备来管理各种选项。既提供预定义策略，您也可以创建、编辑和删除您自己的策略。可以在其各自的 "已分配策略"屏幕，将默认和覆盖的策略分配至域和各个账户 380 与客户端 388。

并非所有的 ActiveSync 设备都识别这些策略或按设置应用策略。有些设备可能忽略这些策略或一些策略元素，有些设备可能必须在重启后才能使策略设置生效。此外，在尝试将新策略分配到一个设备时，只有在该设备自身下一次连接到 ActiveSync 服务器时才会应用这个策略；而且只有在建立连接时才能将这些策略 "推送"到设备。

ActiveSync 策略

右键单击列表以打开快捷菜单，其中包含以下选项：

创建策略
点击此选项打开 ActiveSync 策略编辑器来创建和编辑您的策略。

删除
要删除策略，请从列表中选择一个自定义策略并点击 **"删除"**。点击 **"是"**来确认这个操作。预定义策略是无法删除的。

编辑策略
要编辑策略，请从列表中右键单击一个自定义策略并点击 **"编辑策略"**。在策略编辑器中完成了所需更改后，请点击 **"确定"**。预定义策略是无法进行编辑的。

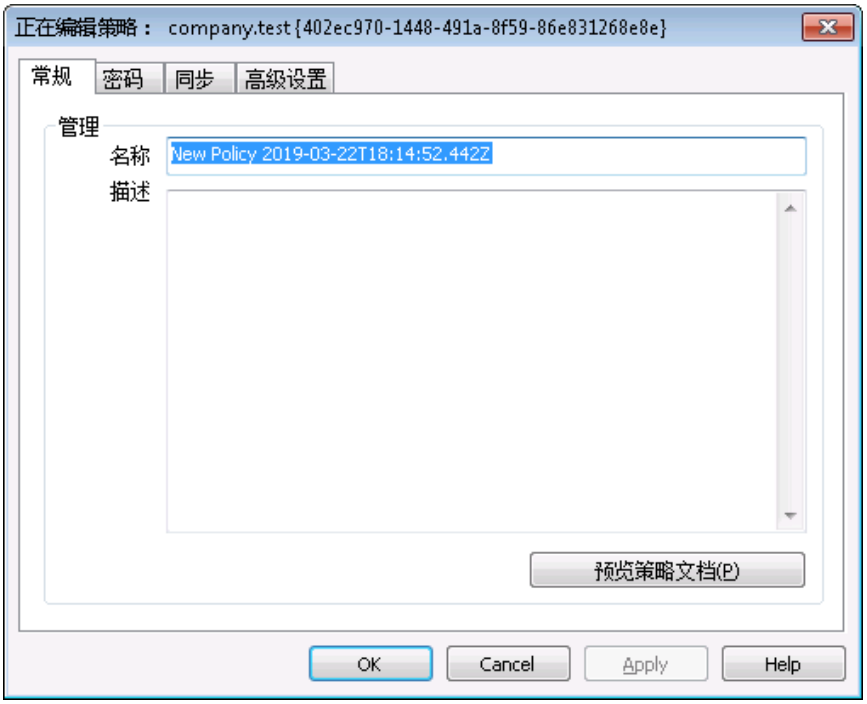
查看策略使用情况
右键单击策略，然后选择此选项来查看被设置成使用此策略的所有域、账户和客户端的列表。

ActiveSync 策略编辑器

ActiveSync 策略编辑器拥有四个选项卡：常规、密码、同步和高级设置。除非您激活了 "*启用高级策略选项编辑*349"（位于 ActiveSync 系统屏幕），否则将隐藏 "高级设置"选项卡。

常规

使用这个屏幕来指定您策略的名称和描述。您也可以预览 XML 策略文档。



管理

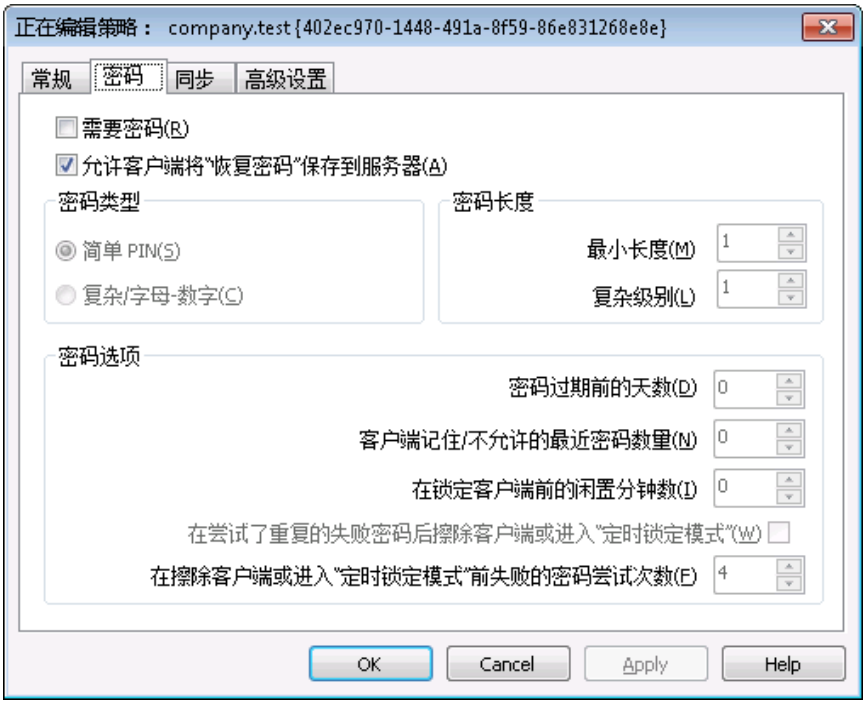
名称
请在此处为您的自定义策略指定一个名称。

描述
使用此区域来描述您的自定义策略。在选择要应用至域、账户或客户端的策略时，在 "应用策略"对话框上显示的描述。

预览策略文档
点击此按钮来预览这个策略的 XML 策略文档。

密码

在这个选项卡上指定密码选项和策略要求。



需要密码
如果您希望在设备上需要密码，请勾选此框。默认情况下，禁用该选项。

允许设备将"恢复密码"保存到服务器
如果您希望允许客户端使用 ActiveSync 的"恢复密码"选项，这将允许设备将临时恢复密码保存到服务器，以便在忘记密码时解锁设备，请启用此项。管理员可以在客户端的"详细信息 388"下找到这个恢复密码。大多数设备不支持此功能。

密码类型

简单 PIN
此项如何实施在很大程度上取决于设备，不过将*"Simple PIN"*选为密码类型通常意味着对设备密码不施加任何限制或复杂要求，不像下方的*"密码长度最小值"*选项。这允许如下所示的简单密码："111"、"aaa"、"1234"、"ABCD"等。

复杂/字母-数字
如果您需要比*"简单 PIN"*选项更复杂更安全的设备密码，请使用这个策略选项。使

用下方的 *"复杂级别"*选项来定义这个密码必须拥有的复杂性。在策略请求密码时，这是默认选项。

密码强度

最小长度
使用此项来设置设备密码必须包含的字符数最小值，从 1-16。默认情况下将此项设置成 "1"。

复杂级别
使用此项来为 *"复杂/字母-数字"*设备密码设置复杂级别要求。这个级别是密码必须包含的字符的不同类型数量：大写字母、小写字母、数字、非字母数字字符 (例如句号或特殊字符)。您可以要求 1-4 种字符类型。例如，如果将此项设置成 "2"，那么这个密码必须包含至少以下四种字符类型的两种：大写字母和数字、大写字母和小写字母、数字和符号等。默认情况下将此项设置成 "1"。

密码选项

密码过期前的天数 (0=从不)
这是在必须更改设备密码前允许的天数。默认情况下，禁用该选项 (设置成 "0")。

设备记住/不允许的最近密码数 (0=无)
如果您希望防止设备重复使用指定数量的旧密码，请使用此项。例如，如果将此项设置成 "2"而且您更改了您的设备密码，那么您无法将密码更改成上两个已使用过的密码。默认情况下，禁用该选项 (设置成 "0")。

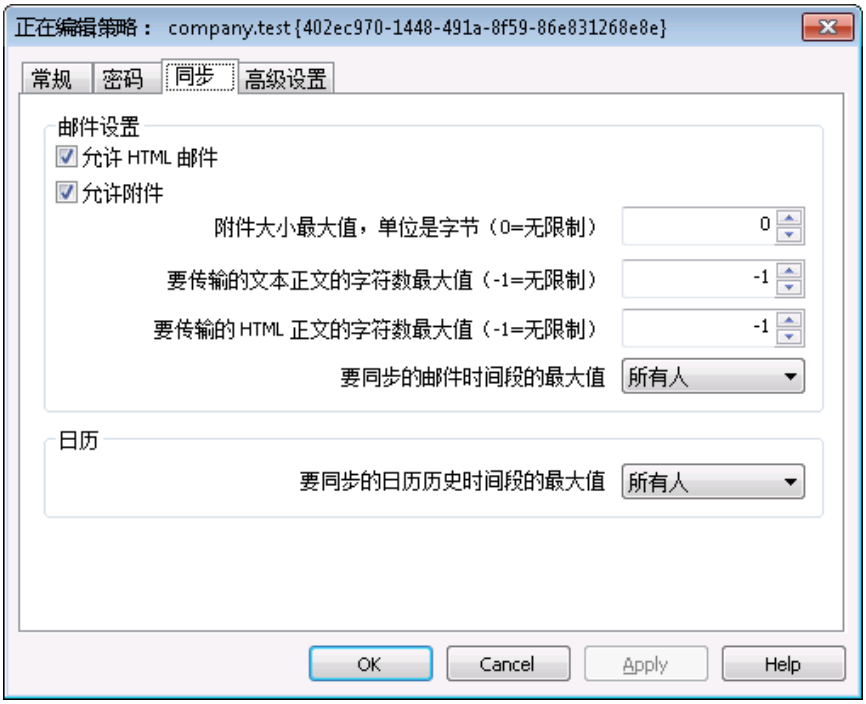
设备锁定之前闲置的分钟数 (0=从不)
这是设备在自我锁定前无需任何用户输入仍然能够正常运行的分钟数。默认情况下，禁用这个密码选项 (设置成 "0")。

反复尝试失败的密码后，擦除设备或进入 "定时锁定模式"
启用此项时，当用户达到指定次数的失败密码尝试后，设备将按照设置自我锁定一段时间或擦除所有数据。默认情况下，禁用该选项。

设备擦除或进入 "定时锁定模式"前失败的密码尝试次数
在启用上方的 *"擦除设备.."*选项，而且用户达到了指定的失败密码尝试次数时，该设备将按照设置进行擦除或进入 "定时锁定模式"。

同步

该屏幕含有各种设置，包括管理 HTML 邮件、允许附件、限制要传输的字符数、待同步的邮件数最大值和日历框架。



邮件设置

允许 HTML 邮件

默认情况下，可以向 ActiveSync 客户端同步/发送 HTML 格式的电子邮件。如果您希望仅发送纯文本，请取消勾选此框。

允许附件

允许设备下载文件附件。默认情况下启用此项。

附件大小最大值，单位是字节（0=无限制）

这是将自动下载到设备的附件的最大大小。默认情况下未为此项设置任何大小限制（设置成“0”）。

待传输的文本正文字符数最大值（-1=无限制）

这是将发送至客户端的纯文本格式正文中字符数的最大值。如果邮件正文包含的字符数大于允许的值，会将正文截短到指定限制。默认情况下没有限制设置（将此项设置成“-1”）。如果您将此项设置成“0”，将仅发送邮件报头。

待传输的 HTML 正文字符数最大值（-1=无限制）

这是将发送至客户端的 HTML 格式正文中字符数的最大值。如果邮件正文包含的字符数大于允许的值，会将正文截短到指定限制。默认情况下没有限制设置（将此项设置成“-1”）。如果您将此项设置成“0”，将仅发送邮件报头。

待同步的邮件时间框架的最大值

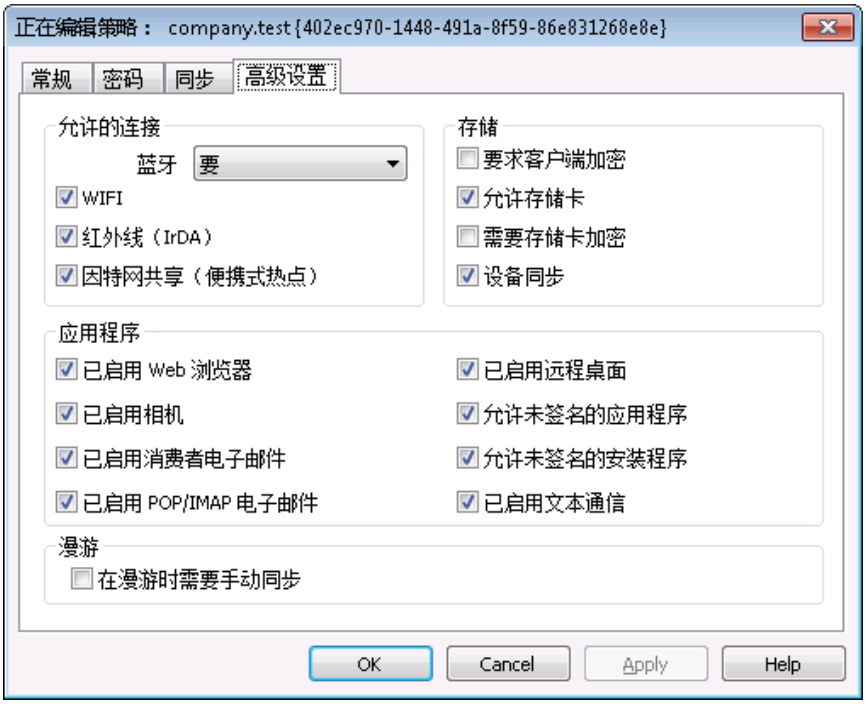
这是可以被设备同步的从今天开始到之后一段日期范围内的以往电子邮件的数量。默认情况下将此项设置成“所有”，这就意味着无论邮件的存在时间有多久，将会同步所有邮件。

日历

待同步的日志历史时间框架的最大值
这是从今天起此设备可以同步过去多久之前的日历条目。默认情况下将此项设置成 "所有"，这就意味着无论这些条目的存在时间有多久，都会同步所有过去的条目。

高级设置

"高级设置"选项卡包含各种选项管理，包括允许的连接类型、是否能够启用特定的应用程序、存储、加密和漫游。



除非您激活了 "*启用高级策略选项编辑*[349]" (位于 ActiveSync for MDaemon屏幕)，否则将隐藏 "高级设置"选项卡。

允许的连接

蓝牙
使用此项来指定是否在设备上允许蓝牙连接。您可以选择 "是"来允许 "蓝牙"连接，选择 "否"来进行阻止，或选择 "免提"将 "蓝牙"限制成仅在免提时使用。默认情况下将此项设置成 "是"。

WIFI
允许 WIFI连接。默认情况下启用此项。

红外线 (IrDA)
允许红外线 (IrDA)连接。默认情况下启用此项。

互联网共享（移动热点）
此项允许设备使用互联网共享（移动热点）。默认情况下，启用该选项。

存储

需要设备加密
如果您希望在设备上需要加密，请点击此项。并非所有设备要强制加密。默认情况下，禁用该选项。

允许存储卡
允许在设备中使用存储卡。默认启用此项。

需要存储卡加密
如果您希望在存储卡上需要加密，请使用此项。默认情况下，禁用该选项。

桌面同步
在设备上允许桌面同步。默认情况下启用此项。

应用程序

启用 web 浏览器
允许在设备上使用浏览器。某些设备不支持此项，而且无法应用到第三方浏览器。默认情况下，启用该选项。

启用相机
允许在设备上使用相机。默认情况下启用此项。

启用消费者电子邮件
设备允许用户配置个人邮件账户。禁用时，将取决于特定的 ActiveSync 客户端完全禁用邮件账户或服务类型。默认情况下启用此项。

启用 POP/IMAP 邮件
允许访问 POP 或 IMAP 电子邮件。默认情况下启用此项。

启用远程桌面
允许客户端使用远程桌面。默认情况下启用此项。

允许未签名的应用程序
此项允许在设备上使用未签名的应用程序。默认启用此项。

允许未签名的安装程序
此项允许在设备上运行未签名的安装程序。默认启用此项。

启用文本消息
此项允许在设备上进行文本通信。默认情况下启用文本通信。

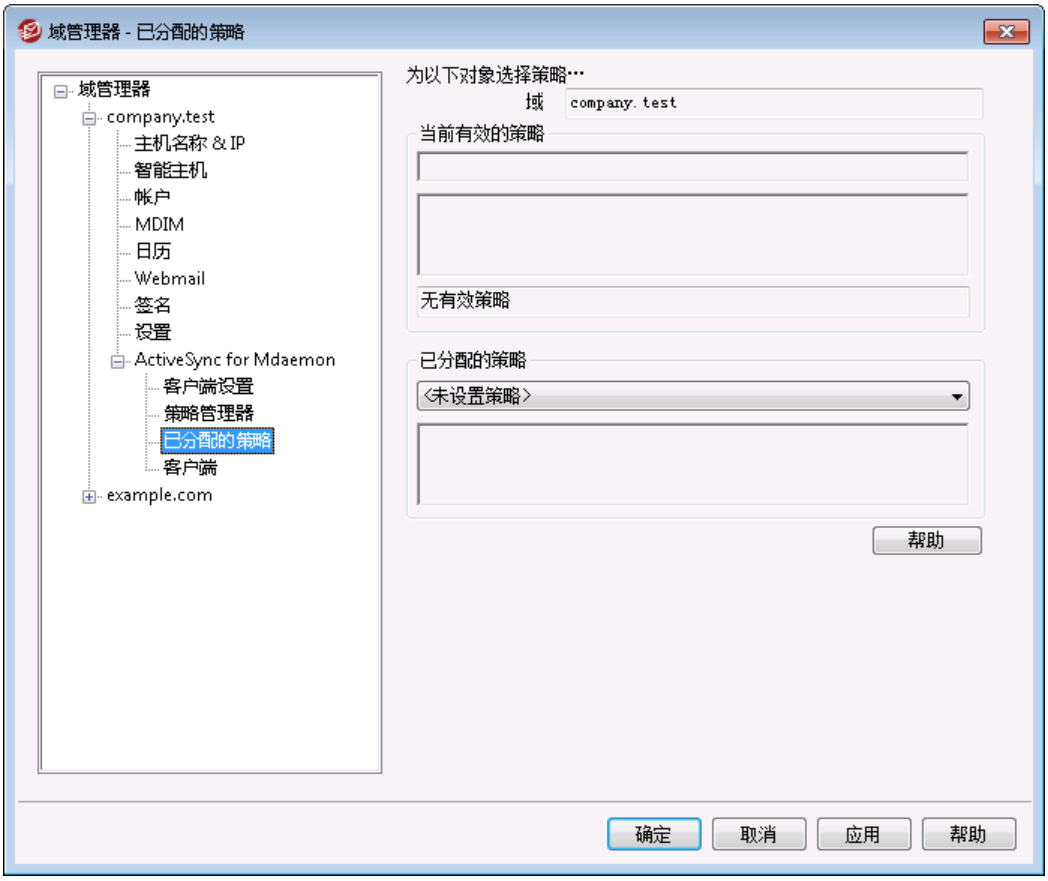
漫游

漫游时需要手动同步
如果您希望在设备漫游时对其进行手动同步，请使用这个策略选项。取决于设备运营商和数据规划项目，允许在漫游时自动同步可能增加设备的数据费用。默认情况下，禁用该选项。

还请参阅：

域管理器 » 已分配策略 190
ActiveSync » 账户 380
ActiveSync » 客户端 388

3.2.11.3 已分配策略



使用此屏幕来为域分配默认的 ActiveSync 策略 183。当 ActiveSync 客户端使用域的一个账户进行连接时，这是将分配到那个客户端的策略，除非已为这个账户专门设置了备选的策略。

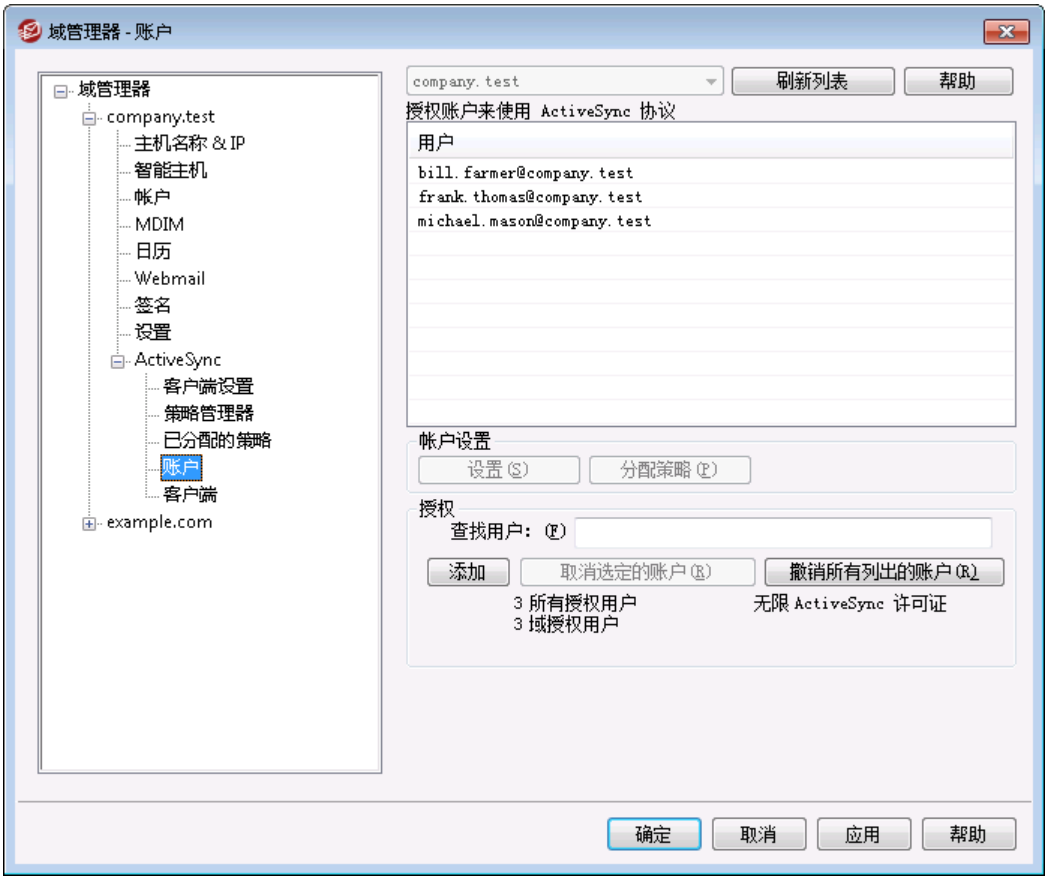
分配默认的 ActiveSync 策略

要为域分配默认的 ActiveSync 策略，请点击 **特分配策略**”下拉列表，选择所需策略，并点击 **确定**”。

还请参阅：

域管理器 » 策略管理器 183
ActiveSync » 账户 380
ActiveSync » 客户端 388

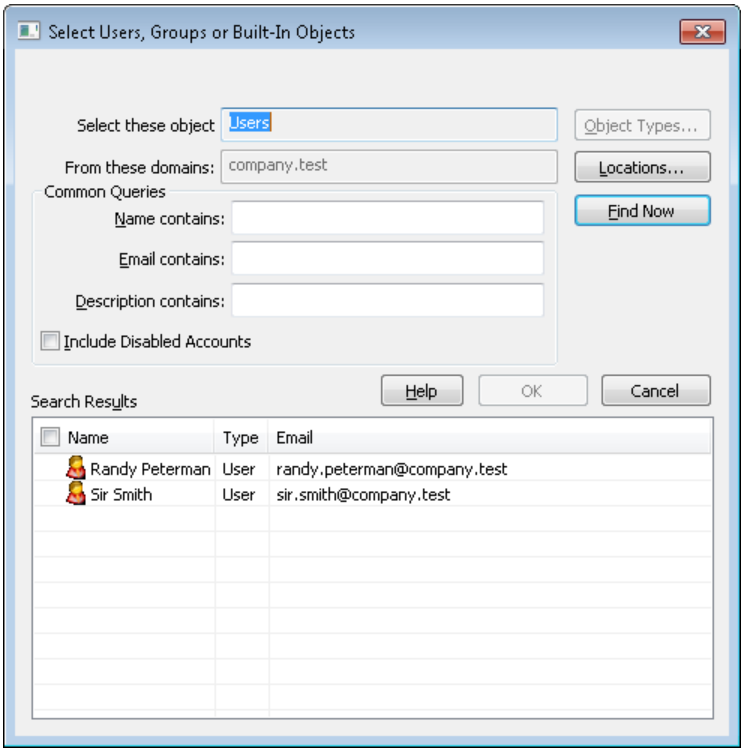
3.2.11.4 账户



使用此◆◆幕指定有权使用 ActiveSync 的域账户，您可以编辑每个授权账户的客户端设置，并分配其 ActiveSync 策略。

授权账户

点击 "添加"来手动授权一个或多个域账户来使用 ActiveSync。这将打开 "选择用户"对话框来查找和选择账户。



常规查询
使用这一部分的这些选项，通过指定所有或部分用户名、邮件地址或账户描述[598]的内容来缩小您的搜索范围。如果您希望这些搜索结果包含与上方指定的"位置"相匹配的各个用户，请留空这些字段。

包含"禁用账户"
如果您希望在搜索中包含禁用账户[598]，请勾选此框。

立即查找
在您指定了所有搜索条件之后，请点击"立即查找"来执行搜索。

搜索结果
执行完搜索后，请在"搜索结果"中选择任何所需用户，并点击"确定"来将其添加到授权账户的列表。

撤销账户

要撤销账户的 ActiveSync 使用授权，请从列表内选中它并点击"撤销选定账户"。如果您希望撤销所有账户，请点击"撤销所有账户"这个按钮。

> 如果您已启用了此项，以便在"*通过 ActiveSync 协议初次访问时授权所有账户*[380]"，撤销一个账户的访问权限会将其从列表删除，不过在设备下次连接账户时将再次授权。

分配 ActiveSync 策略

要向账户分配一个策略[372]:

1. 从列表中选择一个账户。
2. 点击 **"分配策略"**。这会打开 "应用策略"对话框。
3. 点击 **"特分配策略"**下拉列表并选择所需策略。
4. 点击 **"确定"**。

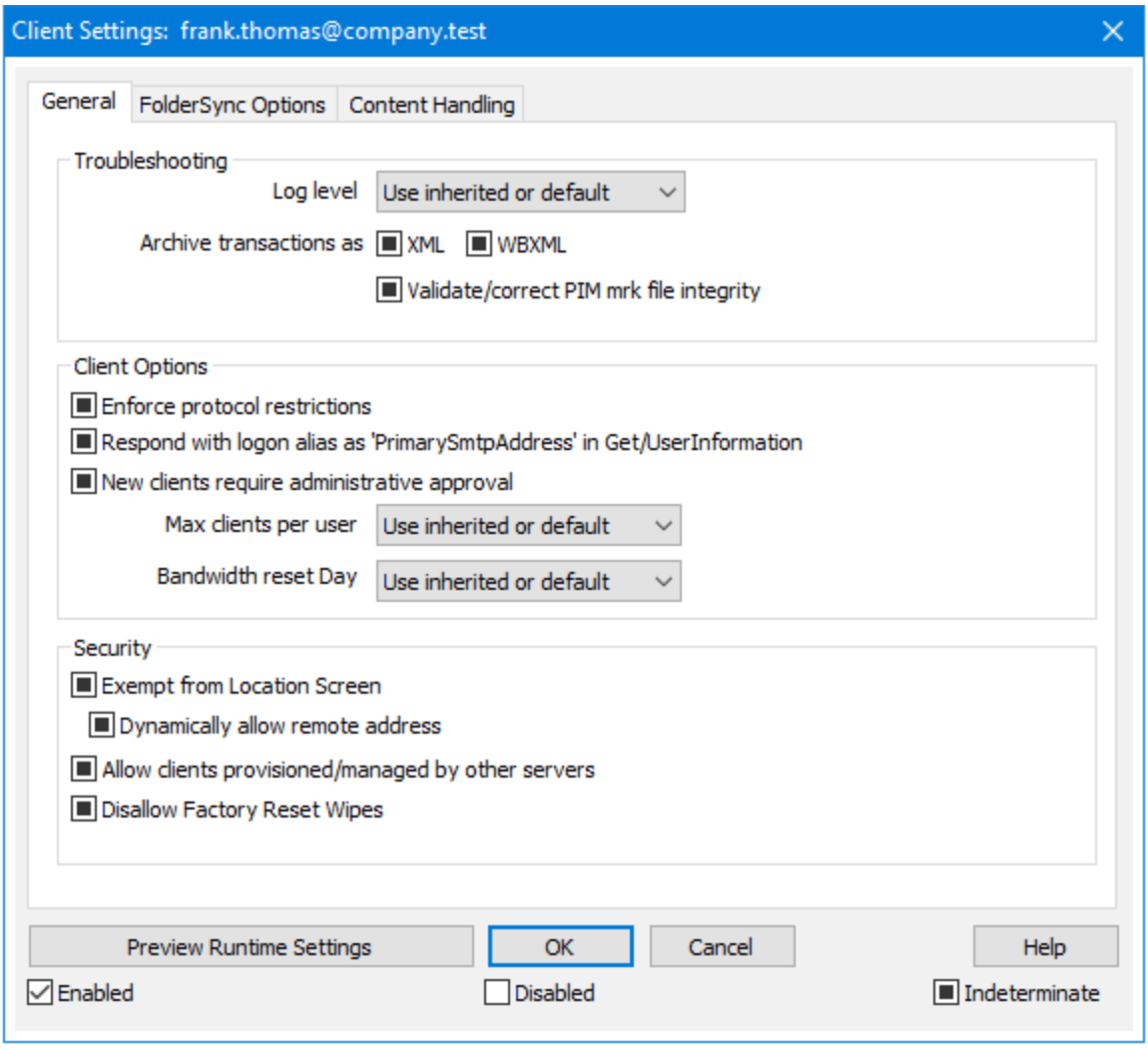
会将该策略分配给连接此账户的任何新设备。

搜索授权账户列表

如果您有许多被授权使用 ActiveSync 的账户，您可以使用 **"查找用户"**框来搜索特定账户列表。只需输入账户邮件地址的开头几个字母即可选择用户。

设置

选择一个账户并点击 **"设置"**来管理该账户的 "客户端设置"。会将这些设置应用至连接此账户的任何 ActiveSync 客户端。



默认情况下，会将此屏幕上的所有选项设置成“使用继承或默认值”，这意味着每个选项都将从“域的客户端设置 178”屏幕上相应的选项获取其设置。在此屏幕上对设置做出的任何变更都将在屏幕上反映。反之亦然，您在此屏幕上做出的任何变更将覆盖此账户的域级别设置。

常规

故障诊断

日志级别

ActiveSync for MDaemon 支持 6 种日志级别，按所记录数据数量的多少分级，以下是从高到低的级别一览：

调试 这是最丰富的日志级别。记录所有可用条目，而且通常只在诊断问题时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

Inherit 默认情况下，"日志级别"设置是从"客户端设置"层次结构继承的。因此，客户端从客户端类型继承，账户从客户端类型继承，群组从账户等继承其设置。此选项的"全局客户端设置"由故障诊断[361]对话框上的"日志级别"设置确定。

归档处理为 [XML | WBXML]
如果您希望保存此数据，请使用*"归档 XML..."*和*"WBXML"*选项，而且有时这些数据对调试很有帮助。默认情况下，禁用这些全局选项。

验证/修复 PIM mrk 文件完整性
该选项对客户端的 PIM 数据运行验证和修复进程来查询有碍正确同步的已知问题，例如重复的 iCalUID 或空的必填字段。默认情况下，禁用这个全局选项。

客户端选项

强制执行协议限制
如果有连接来自尝试使用指定的*"允许的协议版本"*以外的其他协议的客户端，您希望拒绝这些连接时请启用此项。默认情况下禁用此项，这就表示协议限制不防止客户端使用不同的协议：它们只是告诉客户端使用哪些协议。如果客户端无论如何都要尝试使用限制的协议，MDaemon 仍然允许这个连接。还请参阅：协议限制[363]来了解更多信息。

使用登录别名响应，作为 GetUserInformation 中的"PrimarySmtpAddress"
这允许该服务返回别名/次要地址作为主要地址来响应"设置/获取/用户信息"请求。这有助于解决 iOS9.x 更新所引起的一个问题：即导致客户端无法使用别名发送邮件。使用此项将导致对于"设置/获取/用户信息"不规范的响应。

新建客户端需要管理批准
如果您希望要求新的客户端必须先由管理员授权，才能开始与账户同步，请启用此选项。The 客户端[388]列表指示等候授权的任何客户端，管理员可以从相同的屏幕对其进行授权。默认情况下，禁用该设置。

每用户的客户端最大值
如果您希望限制 MDaemon 账户可以关联的 ActiveSync 客户端或设备的数量，请在此项中指定所需数量。默认情况下将这个全局选项设成"无限"。"全局"、"域"和"账户"客户端设置屏幕提供此项，但是个别客户端屏幕不提供此项。

带宽重置日期
如果您希望在每个月指定的一天为 ActiveSync 设备重置带宽使用统计，请使用此项。重置事件作为常规夜间维护过程的一部分进行，而且像其他维护例程一样被记录到系统日志中。默认情况下将这个全局选项设置成"0"(从不)，这就意味着从不重置使用统计。如果您希望重置的那一天与用户或客户端无线运营商计费的重置日期一致，请将子项设置成不同的一天。

安全

从“位置屏蔽”豁免
启用此项（位于 ActiveSync 客户端的设置屏幕）允许您将设备绕过位置屏蔽[477]。这使得有效的用户有可能通过 ActiveSync 继续访问他或她的账户，例如当前往一个阻止验证尝试的位置时。为了免除设备，它必须使用 ActiveSync 在配置的时间范围内进行连接和验证，请在位于“微调”屏幕的这些天后删除闲置的客户端[351]这个设置中进行配置。

动态允许远程地址
当从“位置屏蔽”豁免设备时，如果您还希望允许其连接的远程 IP 地址，请启用此选项。这对允许其他可能从相同 IP 地址连接的客户端很有用。

允许由其他服务器配置/管理的客户端
默认情况下，当 ActiveSync 服务器向特定客户端发送数据/策略，并报告它也受其他 ActiveSync 服务器管理时，也允许那个客户端连接到 MDaemon。不过在这种情况下，无法确保在与其他 ActiveSync 服务器的策略发生冲突时将应用您的策略。通常默认客户端在策略冲突时使用最具有限制性的选项。如果您不希望允许这些客户端进行连接，请禁用此项。

不允许出厂重置擦除
如果将其设置成启用/是，就不提供完全擦除 ActiveSync 客户端的功能。如果您希望能够完全远程擦除客户端，您必须先禁用此项。默认情况下，禁用该选项。要了解更多详情，请参阅：“客户端”页面上的完全擦除 ActiveSync 客户端[388]。

FolderSync 选项

FolderSync 选项

例外

已允许/已阻止发件人文件夹
默认情况下，无法和设备同步用户的“已允许发件人和已阻止发件人”联系人文件夹。它们通常只能由 MDaemon 用来吸住自动防止垃圾邮件。出于这个原因，它们无需在设备上显示为联系人。

非默认邮件文件夹
默认情况下能与设备同步所有由用户创建和默认的邮件文件夹。如果您仅希望允许同步默认的邮件文件夹（例如收件箱、已发送项目、已删除项目和草稿等），请启用此项。不会包含由用户创建的文件夹。默认情况下，禁用该选项。

非默认 PIM 文件夹
默认情况下，将与设备同步用户的所有 PIM 文件夹（例如联系人、日历、便笺和任务等）。如果您希望仅允许同步默认的 PIM 文件夹，请启用此项。例如，如果启用此项，而且用户拥有多个日历文件夹，将仅同步默认的日历。默认情况下，禁用该选项。

包括

公告文件夹层次结构
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的公共文件

夹[258]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的公共文件夹[258]。默认情况下允许搜索操作。

公共文件夹遍历（显示文件夹名称）
默认情况下，为了让客户端同步/访问公共子文件夹，该账户必须拥有查询权限[260]，而且必须对子文件夹和所有父代公共文件夹[258]拥有该权限。如果该账户没有权限查看父文件夹，那么该账户也不能查看子文件夹，即使该账户有查看子文件夹的权限也是如此。如果您希望允许客户端访问这些子文件夹，请启用此项。**请注意：**启用此项必须向客户端显示父文件夹的名称，这会被视为安全风险。默认情况下，禁用该选项。

允许的公共文件夹数量最大值
如果您希望限制在设备上允许的“公共文件夹”的数量，请使用此项。在设置了限制时，该服务器遍历文件夹列表，直到达到这个限制为止，不会再将更多项目发送到设备。无法确保以何顺序处理这些文件夹。默认情况下未设置全局限制。

共享文件夹
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的共享文件夹[97]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的共享文件夹[623]。默认情况下允许搜索操作。

内容处理

内容处理选项

在被客户端标记时为邮件项目创建任务/提醒
该选项可以在客户端请求时，使 MDaemon 通过为各个已标记的邮件创建任务项目来向用户提醒已标记的项目。。默认情况下，此控件的全局选项处于启用状态。

在事件被修改时始终发送会议更新
某些客户端在修改会议时未正确发送会议更新电子邮件。这指示 ActiveSync 服务在组织者更新会议项目时发送会议更新。这仅能在客户端[388]和无法恰当发送会议更新的客户端类型[402]上设置，否则将导致发送重复的会议更新。因此，此选项仅在“客户端”和“客户端类型”的设置页面上可用。

对所有已发送邮件请求已读回执
如果您希望服务器为客户端发送的所有邮件请求已读确认，请启用此项。默认情况下，禁用该选项。

当邮件被标记为已读时，以及发件人请求时，从服务器发送已读回执
如果您希望服务器支持已读确认请求，并在客户端将邮件标记为已读时发送已读回执，请启用此项。默认情况下，禁用该选项。

发送为在 ReplyTo 地址中指定的别名
某些客户端可能不允许发件人使用别名发送邮件。已在 Exchange ActiveSync (EAS) 协议 363 16.x 中添加该功能，不过一些客户端不支持 16.x。例如，Windows 版的 Outlook 仅使用 EAS 14.0，虽然它允许用户指定要发送的备用地址，但生成的邮件并不能正确反映用户的选择。该选项允许使用 ReplyTo（答复）字段来发送电子邮件，只要 ReplyTo 地址是该用户的有效别名 699 即可。默认情况下启用这个全局选项。

虚拟地将公共联系人合并为默认联系人
如果您希望将设备上的公共联系人与用户的默认联系人合并在一起，请启用此项。这仅仅是一个虚拟合并，实际上未将它们复制到用户的联系人文件夹。这对不支持“全局地址列表”(GAL)搜索的客户端而言极其有用。默认情况下，禁用该选项。

在将邮件移入垃圾邮件文件夹时阻止发件人
启用后，当客户端将电子邮件移动到账户的垃圾邮件文件夹时，该服务将该电子邮件的发件人或从地址添加到阻止的发件人联系人文件夹。

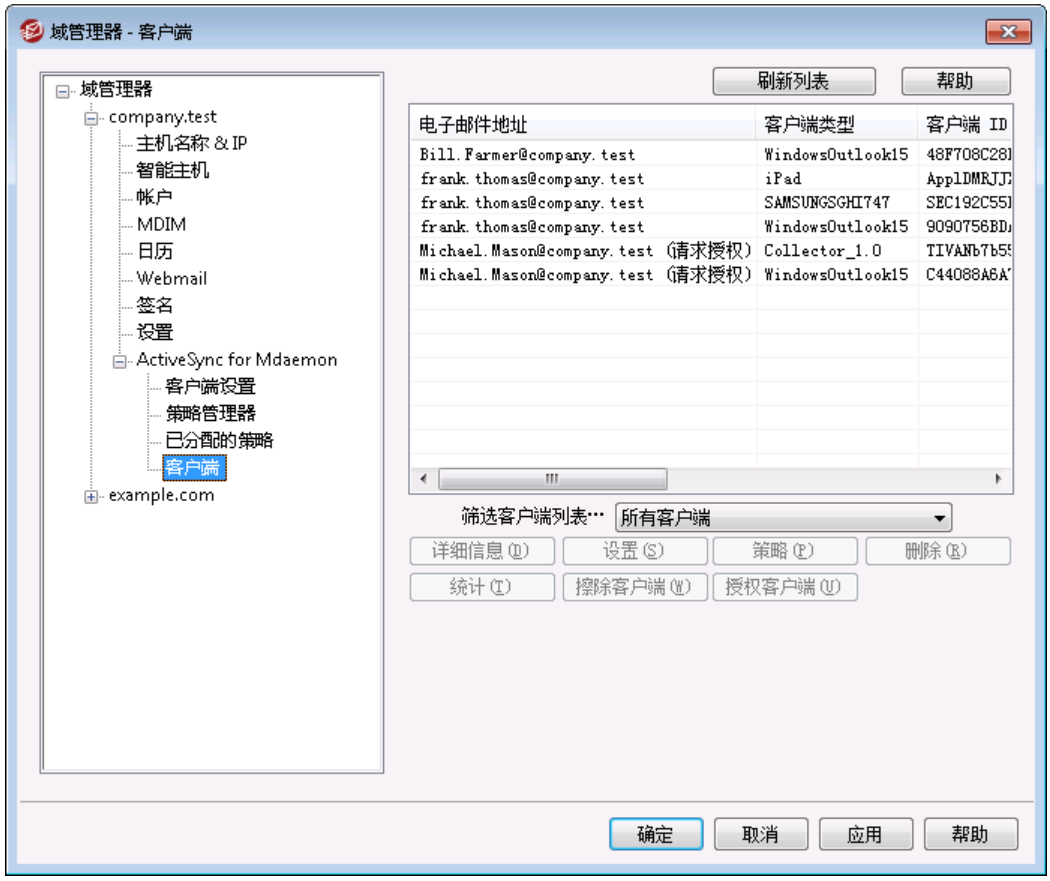
在会议请求被接受/拒绝等时强制发送会议请求。
启用后，当客户端接受、拒绝或以其他方式选择响应会议请求的操作时，服务将向会议组织者发送会议响应。这是针对没有正确发送这些更新本身的特定客户端。

预览有效设置
该按钮在所有子“客户端设置”屏幕上可用（例如域 365、账户 380 和客户端 388）。由于默认情况下，已将这些屏幕上的选项都设置成从父屏幕继承其设置，使用该功能来查看当前向显示的屏幕应用了什么设置。

还请参阅：

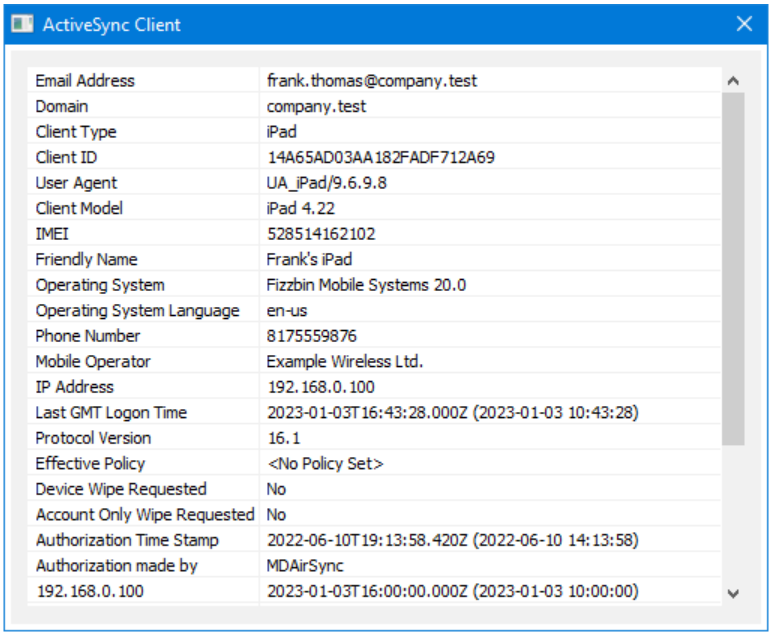
ActiveSync » 客户端设置 353
ActiveSync » 域 365
ActiveSync » 客户端 388

3.2.11.5 客户端



此屏幕含有针对各个与您域相关联的 ActiveSync 设备的条目。

ActiveSync 客户端详细信息



双击一个条目，或右键单击该条目并点击 **"查看详细信息"**来打开 "客户端详细信息"对话框。此屏幕包含有关客户端的信息，例如其客户端类型、客户端 ID 和上次登录时间等。

客户端设置

右键点击一个客户端并点击 **"自定义客户端设置"**来管理其 "客户端设置"。默认情况下，这些设置是从 "客户端类型"设置继承的，但是可以按需进行调整。请参阅下方的 管理设备的客户端设置 201 。

分配 ActiveSync 策略

要向设备分配一个策略 372:

1. 右键单击此列表中的一个设备。
2. 点击 **"分配策略"**。这会打开 "应用策略"对话框。
3. 点击 **"特分配策略"**下拉列表并选择所需策略。
4. 点击 **"确定"**。

统计

右键点击一个条目，并点击 **"统计"**来打开 "客户端统计"对话框，其中含有关于该客户端的各种使用统计。

重置统计

如果要重置客户端的统计信息，请右键单击该客户端，然后依次点击 **"重置统计"**和 **"确定"**来确认操作。

删除 ActiveSync 客户端

要删除 ActiveSync 客户端，右键单击客户端并点击**删除**，然后点击**是**。这将删除列表中的

客户端，并删除 MDaemon 中与其相关的所有同步信息。因此，如果该账户在未来使用 ActiveSync 来同步相同的客户端，MDaemon 会将该客户端视作从未在这台服务器上使用过的客户端；所有客户端数据必须重新与 MDaemon 进行同步。

完全擦除 ActiveSync 客户端

在将一个策略[372]应用到选定的 ActiveSync 客户端时，并且客户端已应用它并做出响应，则该客户端将有一个可用的 "完全擦除"选项。要进行完全擦除，请右键点击客户端（如果您使用 MDRA，请选择它），并点击 **"完全擦除"**。下次该客户端进行连接时，MDaemon 将告诉它擦除所有数据，或将自身重置成出厂默认状态。取决于该客户端，上述操作可能删除设备上的一切，包括已下载的应用程序。此外，只要客户端的 ActiveSync 条目存在，MDaemon 将在该设备日后进行连接的任何时候继续发送擦除请求。如果有时您希望删除客户端，请确保您先将其添加到阻止列表[359]，这样它以后就无法再次连接。最后，如果擦除的设备被恢复，并且您希望允许它再次连接，您应该选择该设备并点击 **"取消擦除操作"**。您也必须从 阻止列表将其删除。

账户擦除 ActiveSync 客户端

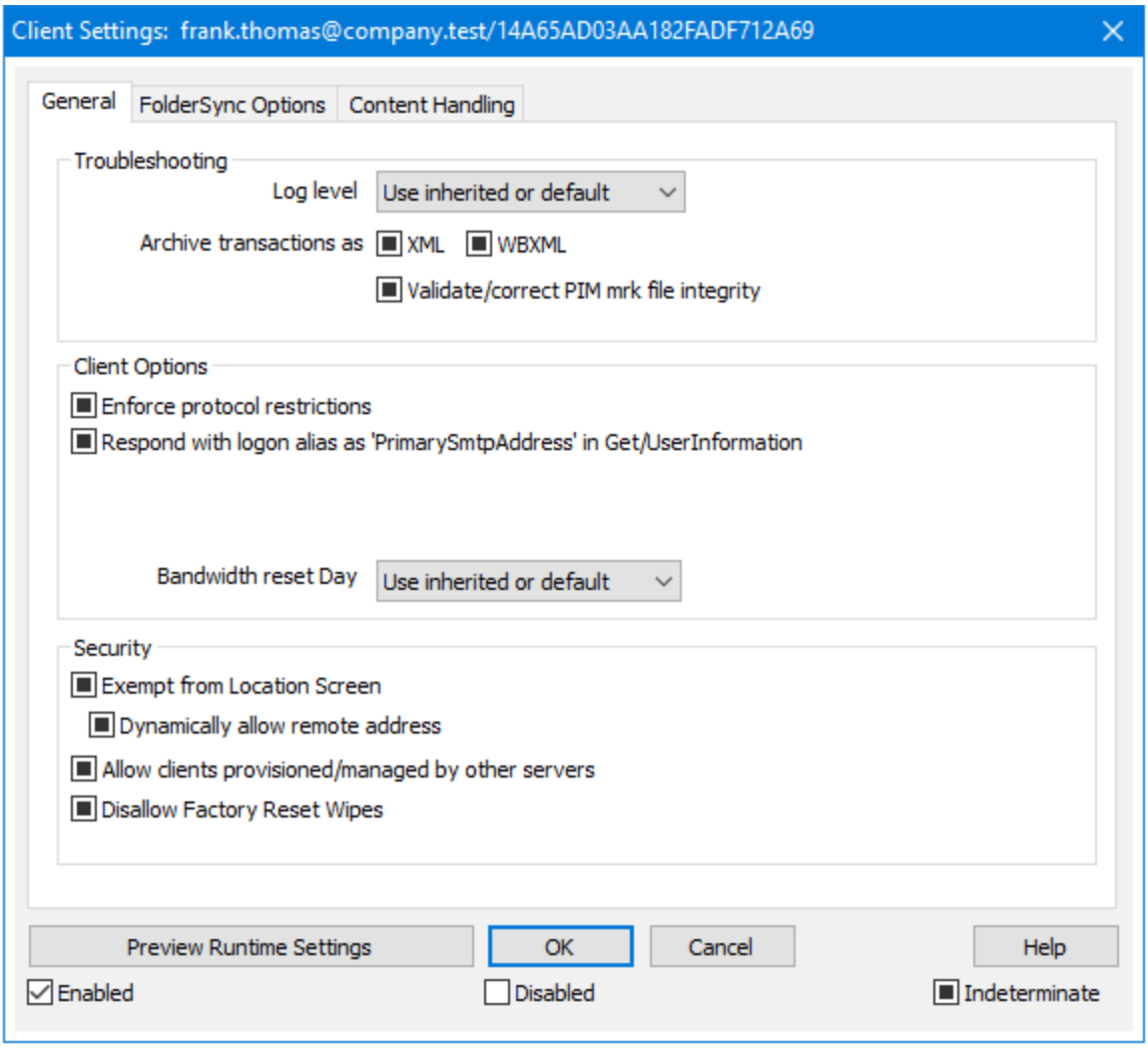
要从客户端或设备中擦除账户的邮件和 PIM 数据，请右键点击并选择 **"从客户端擦除账户邮件和 PIM"**。*"账户擦除"*选项与上述 *"完全擦除"*选项类似，不过该项不擦除所有数据，而是仅擦除这个账户的数据，例如其电子邮件、日历条目和联系人等。保留剩余所有项目，例如应用程序、照片或音乐。

授权客户端

如果将 *"新建客户端需要管理批准"*选项（位于 ActiveSync 客户端设置[353]屏幕）设置成需要批准，选择一个客户端并点击批准客户端进行同步来授权它与服务器进行同步。

管理设备的客户端设置

设备级别的 "客户端设置"屏幕允许您管理特定设备的设置。



默认情况下，此屏幕上的所有选项都被设置为 "使用继承或默认值"，表示每个选项都会从客户端类型客户端设置 402 屏幕上的相应选项中获取其设置。在此屏幕上对设置做出的任何变更都将在屏幕上反映。反之亦然，您在此屏幕上做出的任何变更将覆盖此设备的客户端类型级别的设置。

常规

故障诊断

日志级别

ActiveSync for MDaemon 支持 6 种日志级别，按所记录数据数量的多少分级，以下是从高到低的级别一览：

调试 这是最丰富的日志级别。记录所有可用条目，而且通常只在诊断问题时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

Inherit 默认情况下，"日志级别"设置是从"客户端设置"层次结构继承的。因此，客户端从客户端类型继承，账户从客户端类型继承，群组从账户等继承其设置。此选项的"全局客户端设置"由故障诊断 361 对话框上的"日志级别"设置确定。

归档处理为 [XML | WBXML]
如果您希望保存此数据，请使用*"归档 XML..."*和*"WBXML"*选项，而且有时这些数据对调试很有帮助。默认情况下，禁用这些全局选项。

验证/修复 PIM mrk 文件完整性
该选项对客户端的 PIM 数据运行验证和修复进程来查询有碍正确同步的已知问题，例如重复的 iCalUID 或空的必填字段。默认情况下，禁用这个全局选项。

客户端选项

强制执行协议限制
如果有连接来自尝试使用指定的*"允许的协议版本"*以外的其他协议的客户端，您希望拒绝这些连接时请启用此项。默认情况下禁用此项，这就表示协议限制不防止客户端使用不同的协议：它们只是告诉客户端使用哪些协议。如果客户端无论如何都要尝试使用限制的协议，MDaemon 仍然允许这个连接。还请参阅：协议限制 363 来了解更多信息。

使用登录别名响应，作为 GetUserInformation 中的"PrimarySmtpAddress"
这允许该服务返回别名/次要地址作为主要地址来响应"设置/获取/用户信息"请求。这有助于解决 iOS9.x 更新所引起的一个问题：即导致客户端无法使用别名发送邮件。使用此项将导致对于"设置/获取/用户信息"不规范的响应。

新建客户端需要管理批准
如果您希望要求新的客户端必须先由管理员授权，才能开始与账户同步，请启用此选项。The 客户端 388 列表指示等候授权的任何客户端，管理员可以从相同的屏幕对其进行授权。默认情况下，禁用该设置。

每用户的客户端最大值
如果您希望限制 MDaemon 账户可以关联的 ActiveSync 客户端或设备的数量，请在此项中指定所需数量。默认情况下将这个全局选项设成"无限"。"全局"、"域"和"账户"客户端设置屏幕提供此项，但是个别客户端屏幕不提供此项。

带宽重置日期
如果您希望在每个月指定的一天为 ActiveSync 设备重置带宽使用统计，请使用此项。重置事件作为常规夜间维护过程的一部分进行，而且像其他维护例程一样被记录到系统日志中。默认情况下将这个全局选项设置成"0"(从不)，这就意味着从不重置使用统计。如果您希望重置的那一天与用户或客户端无线运营商计费的重置日期一致，请将子项设置成不同的一天。

安全

从“位置屏蔽”豁免
启用此项（位于 ActiveSync 客户端的设置屏幕）允许您将设备绕过位置屏蔽[477]。这使得有效的用户有可能通过 ActiveSync 继续访问他或她的账户，例如当前往一个阻止验证尝试的位置时。为了免除设备，它必须使用 ActiveSync 在配置的时间范围内进行连接和验证，请在位于“微调”屏幕的这些天后删除闲置的客户端[351]这个设置中进行配置。

动态允许远程地址
当从“位置屏蔽”豁免设备时，如果您还希望允许其连接的远程 IP 地址，请启用此选项。这对允许其他可能从相同 IP 地址连接的客户端很有用。

允许由其他服务器配置/管理的客户端
默认情况下，当 ActiveSync 服务器向特定客户端发送数据/策略，并报告它也受其他 ActiveSync 服务器管理时，也允许那个客户端连接到 MDaemon。不过在这种情况下，无法确保在与其他 ActiveSync 服务器的策略发生冲突时将应用您的策略。通常默认客户端在策略冲突时使用最具有限制性的选项。如果您不希望允许这些客户端进行连接，请禁用此项。

不允许出厂重置擦除
如果将其设置成启用/是，就不提供完全擦除 ActiveSync 客户端的功能。如果您希望能够完全远程擦除客户端，您必须先禁用此项。默认情况下，禁用该选项。要了解更多详情，请参阅：“客户端”页面上的完全擦除 ActiveSync 客户端[388]。

FolderSync 选项

FolderSync 选项

例外

已允许/已阻止发件人文件夹
默认情况下，无法和设备同步用户的“已允许发件人和已阻止发件人”联系人文件夹。它们通常只能由 MDaemon 用来吸住自动防止垃圾邮件。出于这个原因，它们无需在设备上显示为联系人。

非默认邮件文件夹
默认情况下能与设备同步所有由用户创建和默认的邮件文件夹。如果您仅希望允许同步默认的邮件文件夹（例如收件箱、已发送项目、已删除项目和草稿等），请启用此项。不会包含由用户创建的文件夹。默认情况下，禁用该选项。

非默认 PIM 文件夹
默认情况下，将与设备同步用户的所有 PIM 文件夹（例如联系人、日历、便笺和任务等）。如果您希望仅允许同步默认的 PIM 文件夹，请启用此项。例如，如果启用此项，而且用户拥有多个日历文件夹，将仅同步默认的日历。默认情况下，禁用该选项。

包括

公告文件夹层次结构
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的公共文件

夹[258]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的公共文件夹[258]。默认情况下允许搜索操作。

公共文件夹遍历（显示文件夹名称）
默认情况下，为了让客户端同步/访问公共子文件夹，该账户必须拥有查询权限[260]，而且必须对子文件夹和所有父代公共文件夹[258]拥有该权限。如果该账户没有权限查看父文件夹，那么该账户也不能查看子文件夹，即使该账户有查看子文件夹的权限也是如此。如果您希望允许客户端访问这些子文件夹，请启用此项。**请注意：**启用此项必须向客户端显示父文件夹的名称，这会被视为安全风险。默认情况下，禁用该选项。

允许的公共文件夹数量最大值
如果您希望限制在设备上允许的“公共文件夹”的数量，请使用此项。在设置了限制时，该服务器遍历文件夹列表，直到达到这个限制为止，不会再将更多项目发送到设备。无法确保以何顺序处理这些文件夹。默认情况下未设置全局限制。

共享文件夹
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的共享文件夹[97]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的共享文件夹[623]。默认情况下允许搜索操作。

内容处理

内容处理选项

在被客户端标记时为邮件项目创建任务/提醒
该选项可以在客户端请求时，使 MDaemon 通过为各个已标记的邮件创建任务项目来向用户提醒已标记的项目。。默认情况下，此控件的全局选项处于启用状态。

在事件被修改时始终发送会议更新
某些客户端在修改会议时未正确发送会议更新电子邮件。这指示 ActiveSync 服务在组织者更新会议项目时发送会议更新。这仅能在客户端[388]和无法恰当发送会议更新的客户端类型[402]上设置，否则将导致发送重复的会议更新。因此，此选项仅在“客户端”和“客户端类型”的设置页面上可用。

对所有已发送邮件请求已读回执
如果您希望服务器为客户端发送的所有邮件请求已读确认，请启用此项。默认情况下，禁用该选项。

当邮件被标记为已读时，以及发件人请求时，从服务器发送已读回执
如果您希望服务器支持已读确认请求，并在客户端将邮件标记为已读时发送已读回执，请启用此项。默认情况下，禁用该选项。

发送为在 ReplyTo 地址中指定的别名
某些客户端可能不允许发件人使用别名发送邮件。已在 Exchange ActiveSync (EAS) 协议 363 16.x 中添加该功能，不过一些客户端不支持 16.x。例如，Windows 版的 Outlook 仅使用 EAS 14.0，虽然它允许用户指定要发送的备用地址，但生成的邮件并不能正确反映用户的选择。该选项允许使用 ReplyTo（答复）字段来发送电子邮件，只要 ReplyTo 地址是该用户的有效别名 699 即可。默认情况下启用这个全局选项。

虚拟地将公共联系人合并为默认联系人
如果您希望将设备上的公共联系人与用户的默认联系人合并在一起，请启用此项。这仅仅是一个虚拟合并，实际上未将它们复制到用户的联系人文件夹。这对不支持“全局地址列表”(GAL)搜索的客户端而言极其有用。默认情况下，禁用该选项。

在将邮件移入垃圾邮件文件夹时阻止发件人
启用后，当客户端将电子邮件移动到账户的垃圾邮件文件夹时，该服务将该电子邮件的发件人或从地址添加到阻止的发件人联系人文件夹。

在会议请求被接受/拒绝等时强制发送会议请求。
启用后，当客户端接受、拒绝或以其他方式选择响应会议请求的操作时，服务将向会议组织者发送会议响应。这是针对没有正确发送这些更新本身的特定客户端。

预览有效设置
该按钮在所有子“客户端设置”屏幕上可用（例如域 365、账户 380 和客户端 388）。由于默认情况下，已将这些屏幕上的选项都设置成从父屏幕继承其设置，使用该功能来查看当前向显示的屏幕应用了什么设置。

还请参阅：

ActiveSync » 账户 380
ActiveSync » 安全 359

3.3 网关管理器

“网关管理器”可以从“设置» 网关管理器...”菜单访问。此功能为多域（multiple domains）托管提供一个受限却有益的二级支持或者作为某人的备份邮件服务器。

例如：

假设您希望将其作为一个备份服务器或者第三方的邮筒，接收入站邮件并且在您的服务器上的一个文件夹中存储邮件，不过您若不希望完全托管其域，可以保留其个别用户账户。让我们使用“example.com”作为其名称。

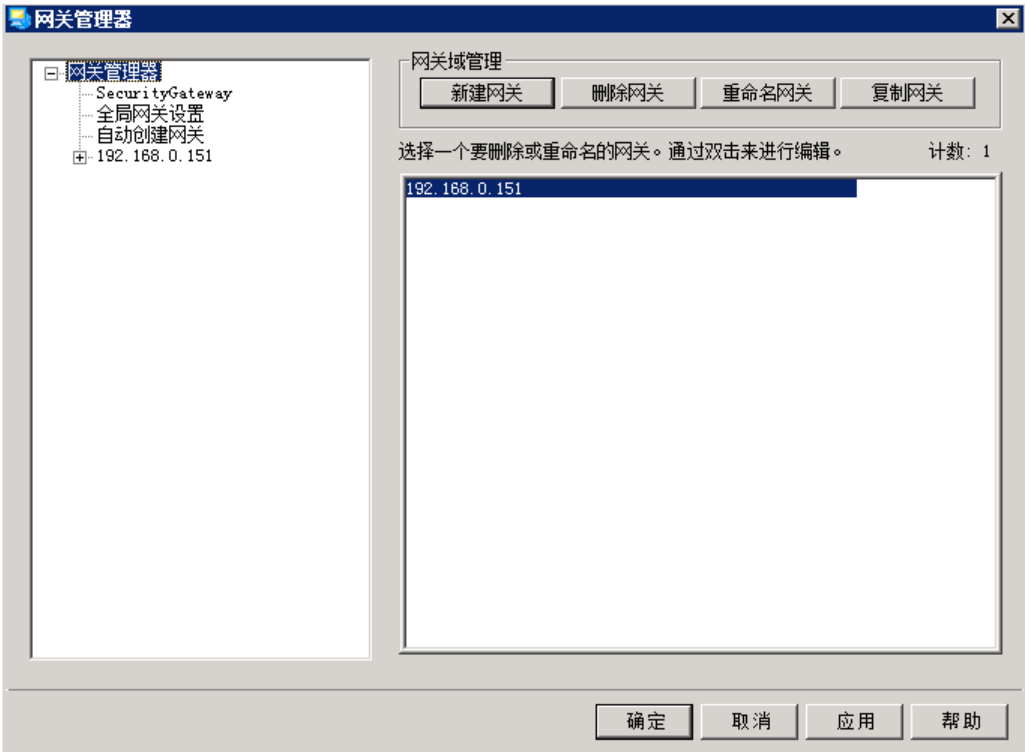
您要做的第一件事情是通过点击“网关管理器”上的“新建网关”并输入“example.com”作为其名称来创建网关。会将 MDaemon 为此域接收的所有邮件从主邮件流中分离出来，并将这些邮件放入在网关的“域 212”屏幕上指定的文件夹内，不管每封邮件所发往的指定个人是谁都是如此。

然后，您将指定您希望允许或用来将域的邮件投递至其实际邮件服务器（托管了其用户账户）的收集或投递方式。有两种方法：使用“*MDaemon 每次处理远程邮件后投递存储*

的邮件"选项（位于"域屏幕[212]")或使用消除队列[218]选项。您也可以选择创建一个 MDaemon 账户，并将其"邮件文件夹[601]"更改成与您网关所使用的相同的存储文件夹[212]。这将允许邮件客户端连接到 MDaemon 来收集 example.com 的邮件。

最后，您可能需要为"example.com"编辑 DNS 设置，这样您的 MDaemon 服务器就是该域所指定的 MX 主机。

还有许多其他的可用功能和选项，上述示例是典型网关将会采取的基本形式。不过，如果您需要一个非典型的配置，那么您可能需要做一些与众不同的事，例如如果您希望使用一个在互联网上不实际存在的域名，例如"company.mail。"可以接收一封无效域名的邮件，不过此域名必须"隐藏"在一个默认域[149]地址中。利用这种方法，地址可被构建成通过默认域并继续通过网关。例如，如果您的默认域是 example.com 并且您有一个网关名为 company.mail，然后通过使用地址"bob{company.mail}@example.com"，某人可以发送邮件到"bob@company.mail。"由于"example.com"是 MDaemon 所赋存的注册域，该邮件可以正确地投递，不过当 MDaemon 接收到这种格式的邮件时，将其地址转化为"bob@company.mail"，然后将邮件投递到此网关所指定的文件夹中。当然最简单的方法仍然是为网关注册一个有效的域名然后将其 DNS 或者 MX 记录指向example.com。



网关列表

这个对话框左侧的导航窗格含有您的网关列表，其中提供链接转至用于配置各种特定网关设置的屏幕。它还供您访问"全局网关设置[209]"和"自动网关创建[210]"屏幕。右侧的列表用于删除和重命名域。您可以双击此列表中的一个网关来切换至这个网关编辑器，并配置其设置。

网关域管理

新建网关
要新建网关：请点击 **"新建网关"**，然后在 "创建/更新网关"对话框中输入网关名称（例如 example.mail），并点击 **"确定"**。

通常，这里输入的值将是已经被注册过为网络域名并且可以让 DNS 服务器解析到本地运行服务器的 IP 地址或者此名称的一个有资格的别名。或者您可以为您的网关名称选择使用一个仅限于内部或者非有效，非公共域名（例如 "company.mail"）。不过这需要您使用如上例所述的嵌套域名方式，或使用一些其他内容过滤方案来获得邮件所属。

删除网关
要删除网关：从列表中选中它并点击 **"删除网关"**，然后点击 **"是"**来确认您的决定。

重命名网关
要更改网关名称：从列表中选中它，点击 **"重命名网关"**，然后在 "创建/重命名网关"对话框中输入新名称，并点击 **"确定"**。

复制网关
如果您要创建具有与另一个网关匹配设置的新网关，请从列表中选择一个网关，点击此按钮，然后指定新网关的名称。

网关编辑器

"网关编辑器"用来编辑各个网关的设置。包含下列屏幕：

域 212
使用这个屏幕来启用/禁用网关，指定用来保存域邮件的文件夹，并配置其他投递和附件处理选项。

验证 213
若将远程的域服务器配置为保持一个 LDAP 或者活动目录服务器，包括它所有的邮件箱，别名，邮件列表的时刻更新，或者若其运行一个 Minger 服务器来提供远程地址验证，您可以使用此对话框来指定该服务器，然后验证入站邮件的收件人地址的有效性。如接收地址无效，邮件将会被拒绝接受。通过这种方法，您不需假设域邮件的所有收件人都是有效的。

转发 217
在此屏幕内，您可以指定一个主机或地址，当邮件发送到该域的时候马上转发至该指定主机。还有选项用来声明邮件的副本是否应该保存为本地，以及用来指定转发的邮件应该发送的端口。

取消排队 218
使用此屏幕的选项，您可以配置 MDaemon 代表该域响应 ETRN 和 ATRN 的要求来消除邮件。你还可以配置一些其他和消除相关的选项。

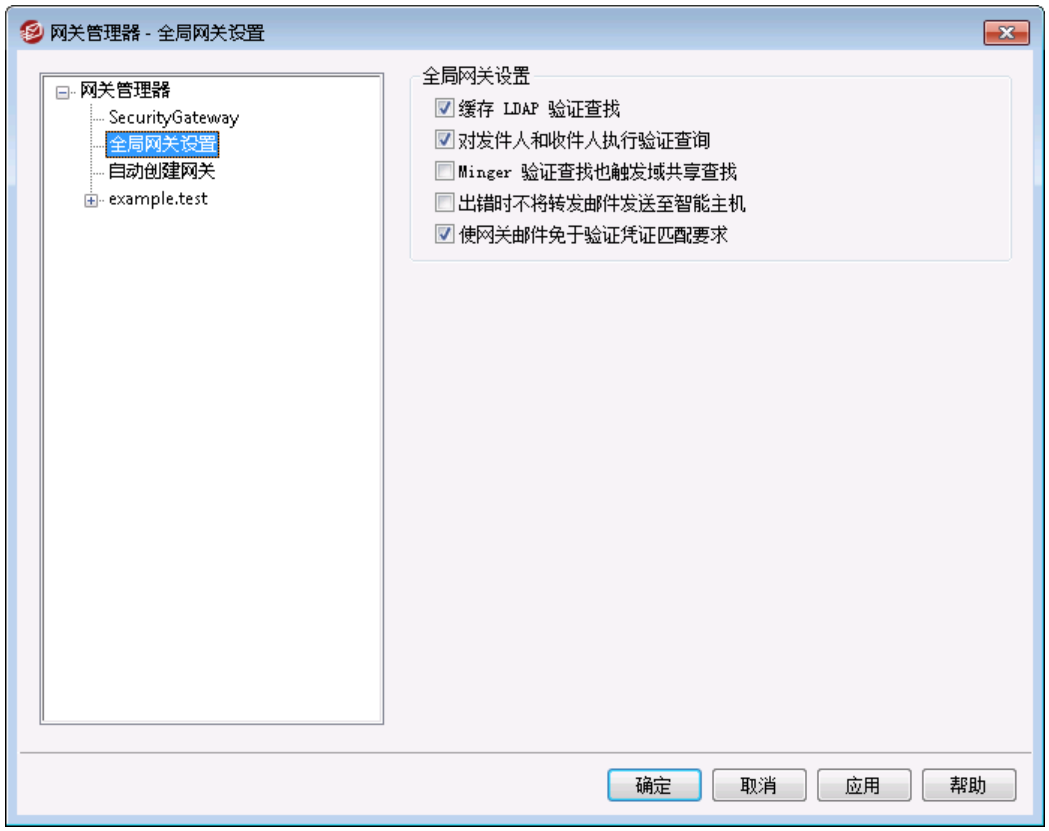
配额 220
此对话框用来为限定域所需的磁盘空间的大小和所邮件存储的最大数量。

设置 222
这个屏幕中页包含了数个其他的选项将会应用到选择的域网关。例如，您可以启用/禁用对于网关的 AntiVirus 和 AntiSpam 扫描、指定在消除邮件时需不需要验证、指定一个验证密码和许多其他选项。

还请参阅：

全局网关设置 209
自动创建网关 210
域管理器 149

3.3.1 全局网关设置



全局网关设置
以下是全局选项。它们并非受限于任何特定的网关。

缓存 LDAP 验证查询
如果您希望为您的域网关缓存 LDAP 验证 213 查询的结果，请点击此复选框。

对发件人和收件人执行验证查询
默认情况下，为网关启用了地址验证选项 213 时，MDaemon 将尝试验证网关邮件的收件人和发件人。如果您希望仅验证收件人，请禁用此项。

Minger验证查询也触发"域共享"查询
启用此选项并且对您任意网关的地址验证使用了 Minger[724]，除了查询了在"验证屏幕[213]"上所指定的 Minger 之外，MDaemon 还会查询您的"域共享[93]"主机。这是一个全局选项，适用于所有的网关组，以便使用 Minger 验证地址。

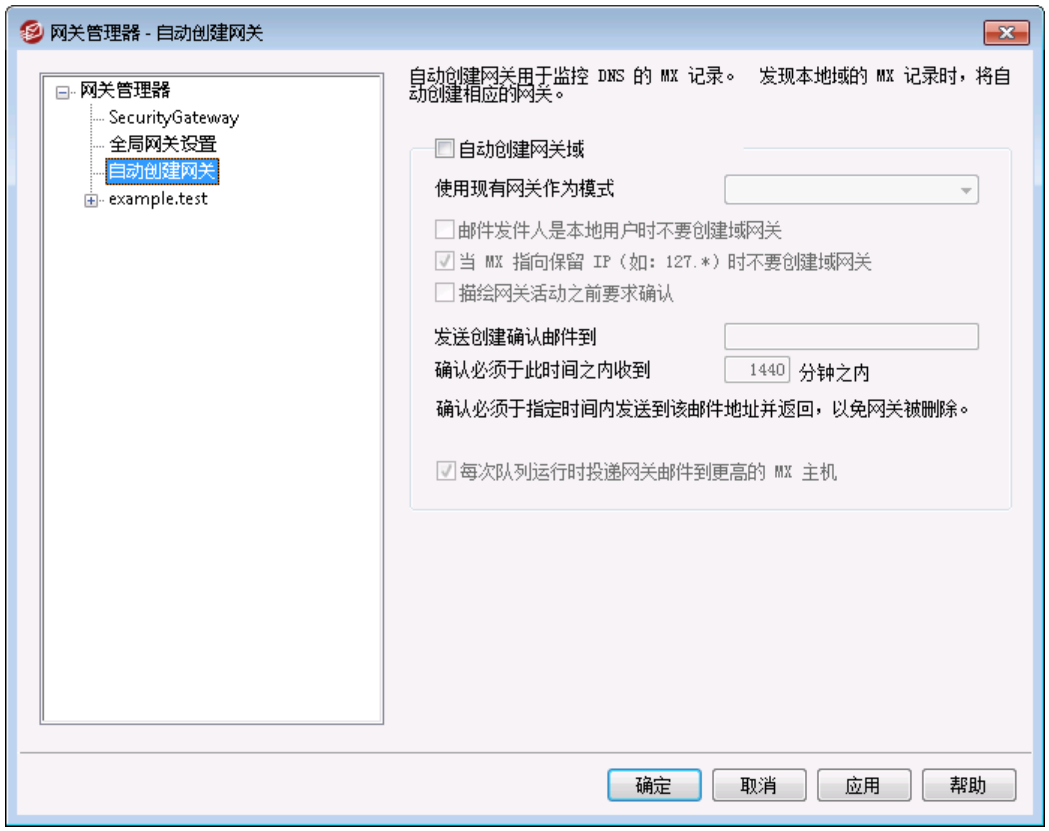
出现错误时不要将已转发的邮件发送到智能主机
点击此处，出现投递错误时，禁止发送已转发的邮件到智能主机。默认情况下，禁用该选项。

使网关邮件免于验证凭证匹配要求
默认情况下，网关邮件免于以下两个选项（位于SMTP 验证[438]屏幕）：*"使用的凭证必须匹配返回路径地址"*和*"使用的凭证必须匹配'发件人：'报头地址"*。如果您不希望网关邮件免于这些要求，请禁用此项。不过禁用此项会引起一些网关邮件的保存和转发问题。

还请参阅：

网关管理器[206]
网关编辑器 » 验证[213]
Minger[724]
域共享[93]

3.3.2 自动创建网关



自动网关创建

该功能用来为先前的未知域创建一个域网关[206]，当另一个源尝试投递该域的邮件到 MDaemon，并且 DNS 查询将 MDaemon 的位置列为一个有效的 MX 记录。

例如：

启用了自动网关创建后，若 MDaemon的默认域 IP 地址是192.0.2.0，经 SMTP 发送一封邮件到未知域 example.com，MDaemon 在 example.com 上执行 MX 和 A 记录查询 以查看 192.0.2.0 是否为一个已知的邮件中继主机。如果 DNS 查询的结果表明，对于 example.com 来说，MDaemon 的 IP 地址是一个有效的 MX 主机，那么 MDaemon 将会自动为其创建一个新的 "域网关"并接收它的邮件。example.com 的邮件将存储到指定的文件夹中，如果用户选择，则在每一个远程邮件处理间隙，假脱机到更高级别的 MX 主机。该功能有效地使之成为另一个域的备份服务器，通过使用您的 IP 替换 MX 主机来简单地配置 DNS 系统。

为保证此功能的安全性，可配置 MDaemon，让其发送一条确认要求到用户选择的邮件地址。当 MDaemon 等待确认响应时，将接收并保存此域的邮件，但不进行投递。必须在您指定的一段时间内回复确认请求，否则将删除自动创建的网关和所有已存储的邮件。如果在时间过期前收到确认信息，则所有存储的邮件将会正常地投递。

> 目前一些恶意攻击者或 "垃圾邮件制造者"试图利用此项功能来配置他们的 DNS 服务器，将您 MDaemon 的 IP 地址列为他们的 MX 主机之一。因此必须慎用 "自动创建网关"功能。为避免被恶意利用，推荐尽量使用 *"将创建确认发送到..."*功能。

自动创建网关域
如果您希望 MDaemon 基于 DNS 查询结果自动创建 "域网关"，请点击此勾选框。

使用现有的网关作为模式
从下载列表中选择域网关，MDaemon 将通过模板设置自动创建网关。

邮件发件人是本地用户时不要创建域网关
如果当信息来源为本地用户时，用户不希望自动创建网关，则点击此复选框。

当 MX 指向保留的 IP 时不创建域网关
如果当 MX 记录指向已保留的 IP 例如：127.*,192.*等)时，您希望阻止网关的自动创建，请点击此复选框。

在激活网关前需要确认
启用此控件时，MDaemon 会将确认信息发送到您指定的邮箱地址，由此来确定自动创建的网关是否有效。MDaemon 会持续接收来自有疑问域的邮件，直到收到确认才会投递邮件。

发送创建确认邮件到
使用此文本框来指定将要发送确认邮件的邮件地址。

必须在 xx 分钟内接收确认
该控件用来指定 MDaemon 对于任意确认邮件的响应所等待的分钟数。如果超过限定时间，"域网关"将停止追问。

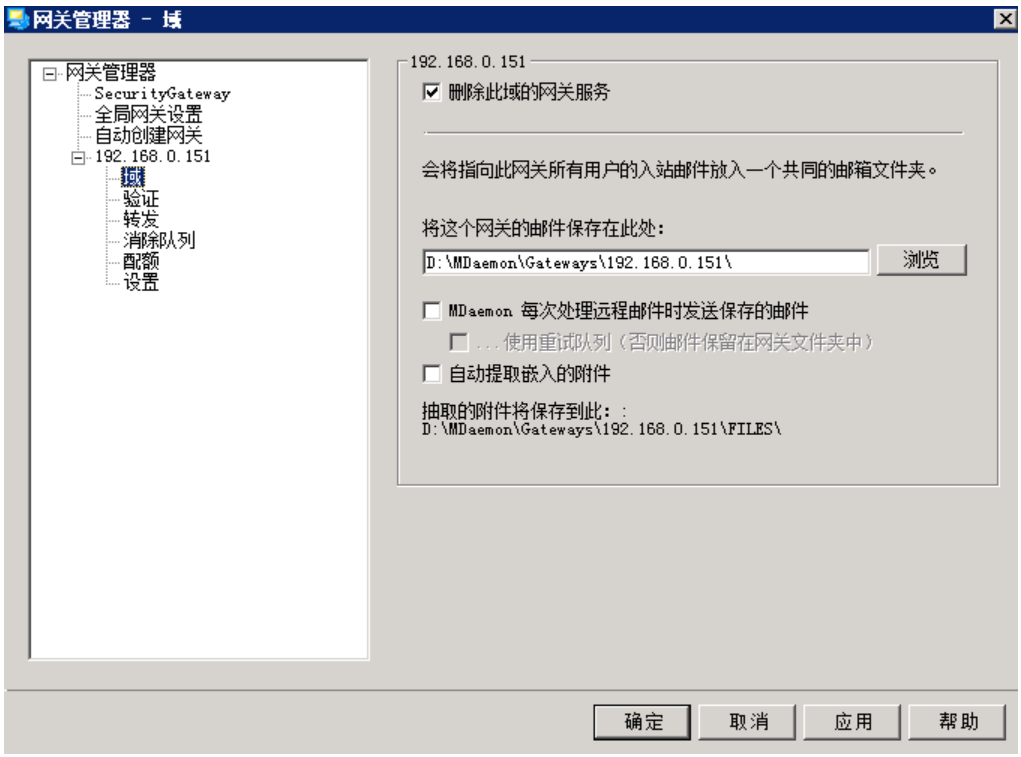
每次运行队列时将网关的邮件投递到更高级别的 MX 主机
如果您希望在每次处理远程队列时，都尝试将此网关的邮件投递至更高级别的 MX 主机，请启用此控件。

还请参阅：

网关管理器 206

3.3.3 网关编辑器

3.3.3.1 域



网关域

为此域启用网关服务
勾选此框来启用域网关。

将该网关的邮件保存于此
输入您希望该域存储入站邮件的目录。所有邮件都将存储在同一文件夹内，不管每封邮件所发往的个别收件人是谁。

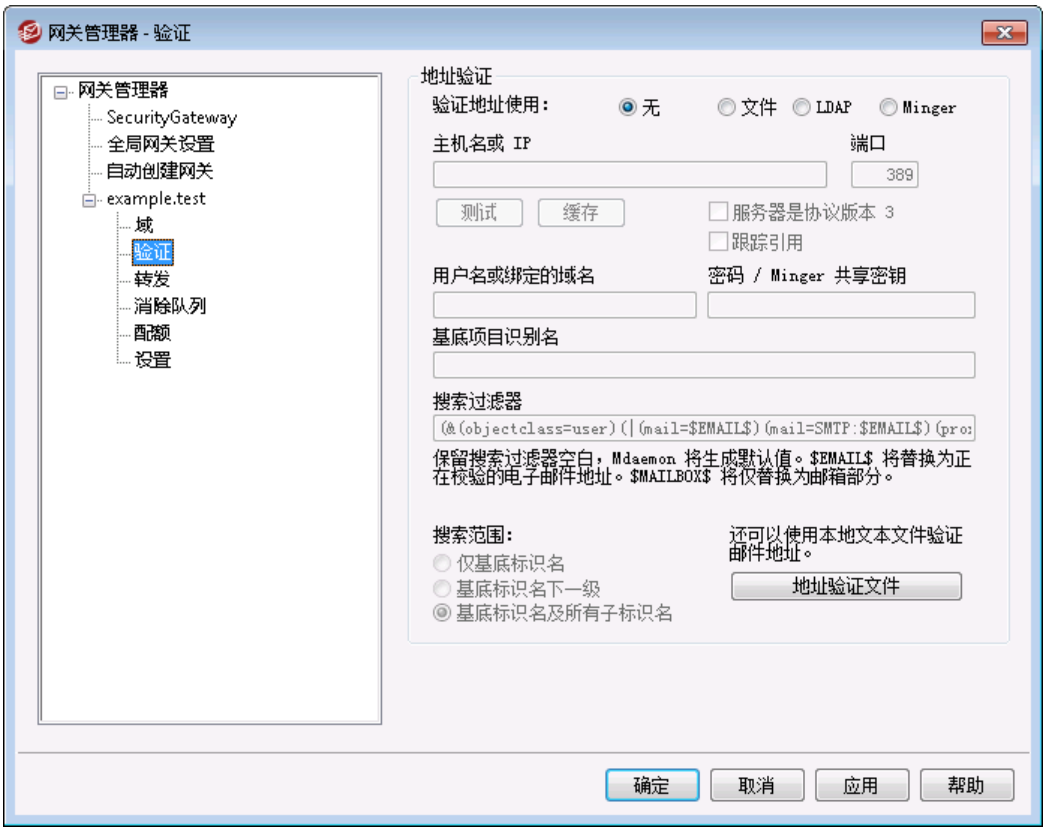
MDaemon 每次处理远程邮件时投递存储的邮件
通常，当 MDaemon 收到准备发往其某一网关的邮件时，它会存储邮件直至该域连接到 MDaemon 接收邮件为止。在某些情况下，您可能希望 MDaemon 通过 SMTP 直接投递邮件而不是等待域来收集。启用此选项时，MDaemon 将在每次处理远程邮件时投递该域的邮件。该网关的邮箱将临时作为远程队列并尝试投递。任何无法投递的邮件只会留在网关的邮箱里直至域接收这些邮件或者稍后被成功投递；不会将它们移至远程队列或

重试系统。不过，如果您没有正确配置域的 DNS，或配置 MDaemon 将所有出站邮件发送到其他主机以便投递，这将导致这些邮件陷入邮件循环并最终视为无法投递。

使用重试队列（否则邮件将留在网关文件夹）
如果您希望使用重试队列机制来投递邮件，请启用此项。默认情况下，此功能是禁用的，这意味着即使无法投递网关邮件，它也将永远保留在网关文件夹中。

自动提取内嵌附件
某些邮件系统要求将邮件提交至邮件流之前提取附件。便起见，MDaemon 可自动提取入站 MIME 附件并将其放在\Files\ 子文件夹（位于该域的邮件文件夹）中。如果您希望自动提取附件，请勾选此框。

3.3.3.2 验证



域网关和邮筒的一个常见问题是它们通常没有办法确定入站邮件的收件人是否有效。例如，如果您作为 example.com 的一个网关且邮件来自 user01@example.com，那么您将无从得知是否真实存在一个邮箱，别名或者邮件列表与 example.com 邮件服务器上的地址相对应。此时您别无选择，只能假定该地址有效并且接受邮件。此外，由于垃圾邮件制造者通常会发送邮件到多个无效地址，该问题将导致网关接受大量的垃圾邮件。

MDaemon 包含一种方法，通过验证收件人地址来防止这种情况的发生。若将远程的域服务器配置为保持一个 LDAP 或者活动目录服务器，包括它所有的邮件箱、别名、邮件列表的时刻更新，或者若其运行一个 Minger 服务器来提供远程地址验证，您可以使用此屏幕上的选

项存储该信息的 LDAP、活动目录或 Minger 服务器。那么，当一封邮件发送到 example.com，您可以在其他服务器上查询该收件人的地址，找出该地址是否有效。

地址验证

验证地址，使用：

无
如果您不希望为域网关使用邮件地址验证，请选择此选项。MDaemon 会把所有域的入站邮件当作收件人是有效地址，因为无法识别那个地址对于该域来说是真实存在的。

文件
如果您希望使用 GatewayUsers.dat 文件作为地址终极列表，用来验证该域的入站邮件收件人是否有效，请选择此选项。这是一个地址的全局列表，适用于您的一切域网关，而且即使您已选择使用其他验证方式中的一种，该列表仍将用作有效地址的一个附加源。当使用了 *"文件"*选项时，它将作为唯一的验证选项。您可以点击下方的 *"地址验证文件"*按钮来打开和编辑有效的地址列表。

LDAP
选择此选项，通过 LDAP 或者活动目录来激活远程地址验证。每当一封邮件到达远程域，将查询其 LDAP 或者活动目录服务器来决定收件人是否有效。如果是无效的，那么将拒收该邮件。若 MDaemon 无法连接到 LDAP/AD 服务器，那么将假定该地址有效。

Minger
如果您希望查询域的 Minger 服务器来验证该域的收件人地址，请使用此选项。如果 MDaemon 无法与该服务器建立连接，则假定该地址有效。还有一个位于 "全局网关设置 209"上的全局选项，您也可以使用此选项使 MDaemon 查询您的 "域共享 93"主机。

主机名或 IP
输入域的 LDAP/活动目录或者 Minger 服务器的主机名或者 IP 地址。这是 MDaemon 将会连接的 LDAP/AD 或者 Minger 服务器，用来验证入站邮件的收件人是 MDaemon 作为一个网关或者备份服务器的域中的有效地址。

端口
指定域的 LDAP/AD 或者 Minger 服务器正在使用的端口。当通过 LDAP、活动目录或者 Minger 来验证地址信息时，MDaemon 将会使用此端口。

测试
点击此按钮来测试您是否正确配置了远程地址验证设置。MDaemon 将简单尝试连接到指定的 LDAP/AD 服务器然后验证它应答了特定的信息。

缓存
点击此按钮来打开 LDAP/Minger 缓存。您可以在 "全局网关设置 209"上启用/禁用缓存。

服务器是协议版本 3
如果您希望网关验证对您服务器使用 LDAP 协议版本 3，请点击此框。

跟踪引用
有时 LDAP 服务器没有请求的对象，不过可能交叉引用其位置，可以将客户端引用到这个位置。如果您希望网关验证跟踪这些引用，请启用此项。默认情况下，禁用该选项。

用户名或绑定 DN
输入对于域的 LDAP/AD 服务器有管理权权限的用户名或者账户的 DN，便于 MDaemon 验证发往 MDaemon 作为网关或者备份服务器的域中入站邮件收件人的有效性。这是绑定操作中用于身份验证的识别名。

密码或 Minger共享密钥
这个密码可连同*认证的绑定的 DN* 值一起通过该域的 LDAP/AD 服务器。若使用了 Minger服务器，那么这将作为一个共享密钥或者密码。

基底项目识别名
这是一个目录信息识别树的根识别名 (DN)，MDaemon 将根据此识别名查询 LDAP/AD 服务器来进行地址验证。

搜索过滤器
当查询您的服务器来验证邮件地址的时候将使用这个 LDAP/AD 搜索过滤器。MDaemon 将设置一个在大多数情况下都可以使用的默认搜索过滤器。

搜索范围：

这是 LDAP/AD 搜索范围或区域。

仅基底识别名
如果您搜索仅限制在如上所填的仅基底项目识别名的话，请选择该选项。搜索不会深入到目录信息树 (DIT)中该点的以下部分。

基底识别名的下一级
如果您希望将您的 LDAP/AD 搜索延伸到您 DIT 中所提供的 DN 下方的一级，请使用这个选项。

基底识别名及其所有子识别名
该选项会将您的搜索范围扩展到提供的识别名及其所有的子识别名，一直深入到您 DIT 中最底层的子条目。

地址验证文件
点击此按钮来打开网关有效邮件地址列表 (例如：GatewayUsers.dat 文件)。它包含了一个地址列表，列出了 MDaemon 认为是发往您域网关入站邮件的有效收件人地址。不管上方所选中的验证选项，MDaemon 将使用此列表作为一个有效地址数据的附加源。当使用了上方的*文件*选项时，它将作为终极且唯一的验证选项。

对 LDAP 验证查询使用多重配置

您能为您的网关域指定多重 LDAP 配置。为了指定额外的 LDAP 参数集，正常设置你的首个集合，然后使用记事本手动编辑GATEWAYS.DAT文件。

您的新的参数集应该用如下的格式创建：

```
LDAPHost1=<host name>
LDAPPort1=<port>
```

```
LDAPBaseEntry1=<base entry DN>
LDAPRootDN1=<root DN>
LDAPObjectClass1=USER
LDAPRootPass1=<password>
LDAPMailAttribute1=mail
```

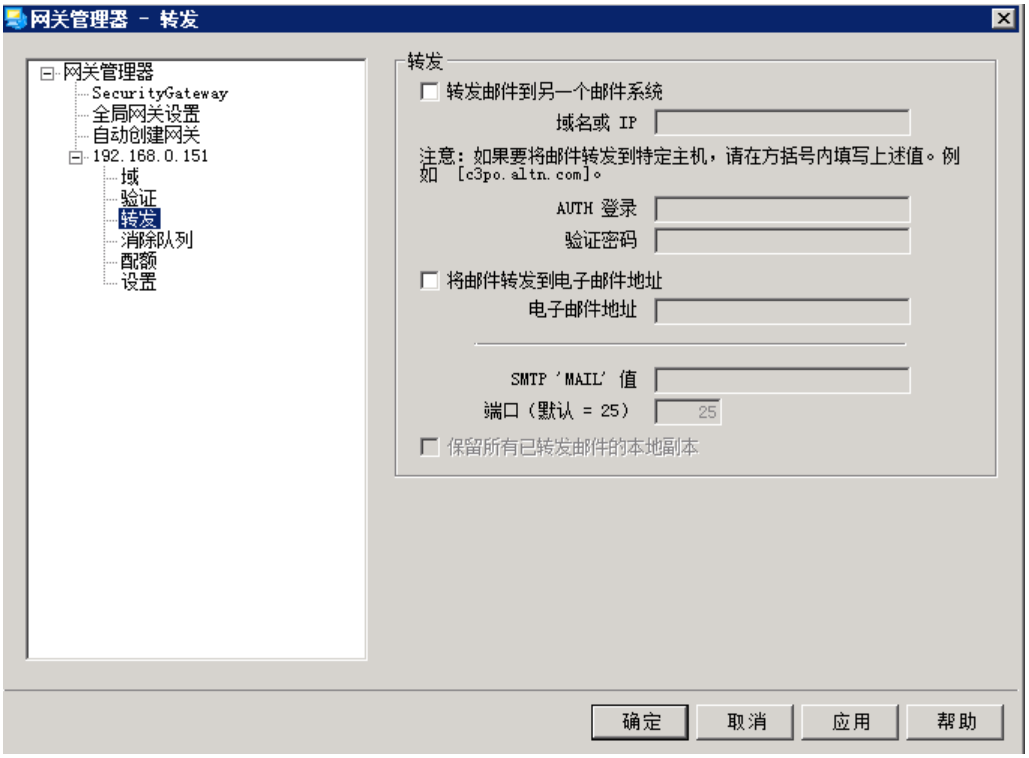
对于每个新的参数集，给每个参数名称中的数字增加1。例如，在上述的例子中，每个参数名都以“1”结尾。要创建另一个参数集，每个参数名将以“2”结尾。在又一个集合中，每个参数名将以“3”结尾，以此类推。

当 LDAP 查询发生时，MDaemon 将执行多重 LDAP 查询依次发现匹配。如果发现错误或发现匹配，不会进行进一步的检查。

还请参阅：

LDAP/地址簿选项 696
Minger 724

3.3.3.3 转发



转发

转发邮件到另一个邮件系统
有时在邮件送达时，为一个域转发所有邮件的副本是十分有利的。如果您希望配置MDaemon来完成此过程则输入名称或域名的IP地址，让此域的接收邮件副本都发送到上述地址。如果您希望把邮件转发到一个特定的主机，用方括号表示（如[host.example.com]）。使用"验证登录/密码"选项可以包括要将邮件转发到的服务器的所有必要登录凭证。

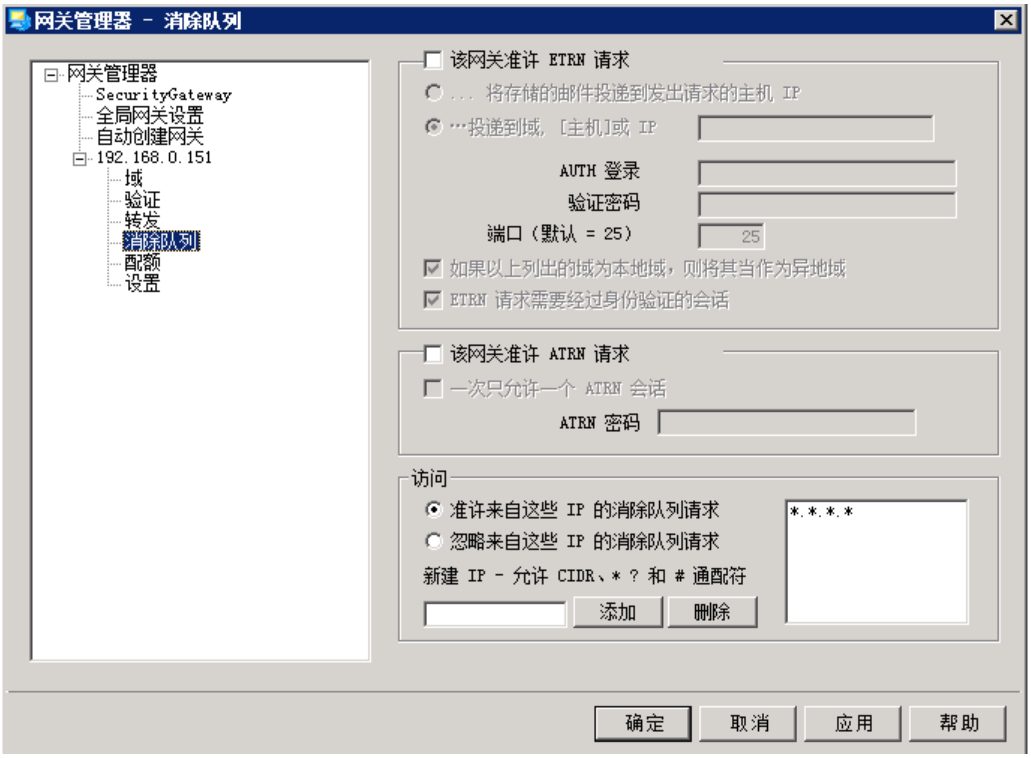
转发邮件到邮件地址
如果您希望将邮件转发至指定邮件地址，所有邮件都指向此用户域。

SMTP "MAIL"值
在转发邮件时，MDaemon将在SMTP "邮件来自于"处理过程中使用本地址。

端口（默认值 = 25）
转发邮件时，MDaemon将使用此端口。

保留所有已转发邮件的本地副本
如果您希望在MDaemon转发邮件后将该邮件的归档副本保留在本地，请选择此选项。

3.3.3.4 出队



ETRN

该网关准许 ETRN 请求
启用此切换时，MDaemon 将会响应由合格主机作出的 ETRN 请求，这些主机代表了 MDaemon 作为一个邮件网关时的域。ETRN 命令是 SMTP 的扩展，向一个存储特定域邮件的服务器发送可以开始假脱机邮件的信号。当 MDaemon 接收到域的 ETRN 请求时，它将立刻使用之后的 STMP 处理程序开始假脱机存储邮件以便投递。请注意发出 ETRN 请求的 STMP 会话不会接收任何存储邮件。MDaemon 将使用之后独立的 STMP 处理程序来发送为域存储的任何邮件。这样做保存了邮件的信封，也更加安全可靠。还需注意，MDaemon 假脱机任何存储邮件至的主机可能不会立刻开始接收这些邮件。ETRN 只能保证*假脱机*所有存储邮件以便投递。实际投递*过程*服从于其他管理者设置的限制，也可能必须在出站邮件队列中等待下一次预定远程邮件处理事件的执行。由于上述种种限制，我们建议您使用按需邮件中继 (ODMR)165及其 ATRN 命令而不是 ETRN。并非所有客户端和服务器都支持此方法，因此只有使用服务器的客户端域可使用此方法。MDaemon 完全支持客户端和服务器端上的 ODMR。

默认情况下，MDaemon 要求发出 ETRN 请求的连接主机首先使用*域名*212与网关*ATRN 密码*作为其登录凭证通过 ESMTP AUTH 进行自我验证。如果您不希望要求验证，您可以在设置222中将其禁用，只需清除*ETRN 出队需要验证*即可。

...将存储的邮件投递到发出请求的主机 IP
选中此选项将使 MDaemon 发送任何存储邮件到发出 ETRN 请求的 IP 地址。发出请求的机器必须运行一个 SMTP 服务器来接收这些邮件。

...投递到域、[主机]或 IP
这是在 ETRN 请求被接受或准许时，任何存储邮件将被发往的主机名，域名或者 IP 地址。收件的机器必须运行一个 SMTP 服务器来接收这些邮件。请注意：在此选项内指定一个域名后，可能会使用 A 和 MX 记录，这取决于投递过程中的 DNS 结果。如果您希望投递邮件到一个特定主机，那么将主机名置于方括号中（例如 [host1.example.net]）或指定 IP 地址来替代域名。输入投递到该位置所需的任何 *AUTH 徽标/密码*凭证。

端口（默认值 = 25）
使用此项来指定该域的邮件将被假脱机到的端口。

如果上方列出的域是本地的，则视其为外来域
如果域是本地但您希望假脱机邮件就好象是远程一样则激活此控键。

ETRN 请求需要验证过的会话
在准许 ESMTP ETRN 请求时，默认情况下将使用此项，要求连接主机首先使用 ESMTP AUTH 命令来进行身份验证。启用此选项时，必须在下方提供的 "ATRN 密码"选项中指定验证密码。

如果不希望对发出 ETRN 请求的主机请求验证，请清除此勾选框。

ATRN

该网关准许 ATRN 请求
如果您希望 MDaemon 响应来自网关域的 ATRN 命令，请启用此选项。ATRN 是在按需邮件中继（ODMR）165中使用的 ESMTP 命令，它是目前最好的用于邮件托管的中继方法。它远胜于需要认证的 ETRN 和其他方法，在邮件离队之前并且无需静态的 IP 地址。无需静态 IP 地址的原因是因为在 MDaemon 和客户端域之间的数据流被快速反向，而且无需创建新连接即可取消假脱机这些邮件，与 ETRN 不同，在发出 ETRN 命令之后将使用独立连接。这帮助带有动态（非静止）IP 地址的客户端域收集其邮件，无需使用 POP3 或 DomainPOP，因为已保存了原始的 SMTP 信封。

> ATRN 要求会话使用 AUTH 命令。您可以在设置222屏幕上配置验证凭证。

一次只允许一个 ATRN 会话
如果您希望限制一次只允许一个 ATRN 会话，请点击此选择框。

ATRN 密码
当使用 ATRN 来消除网关的邮件时，或者您通过"设置"屏幕上的"*ETRN 出队需要验证*"这个选项请求验证，请在此处指定该网关的 ATRN 密码。

> 使用 MDaemon 作为网关的域必须使用其域名作为登录参数。例如：如果域网关为"example.com"并且使用 ATRN 来消除邮件，那么将会使用"example.com"这个登录凭证以及在此处所指定的密码进行验证。

访问

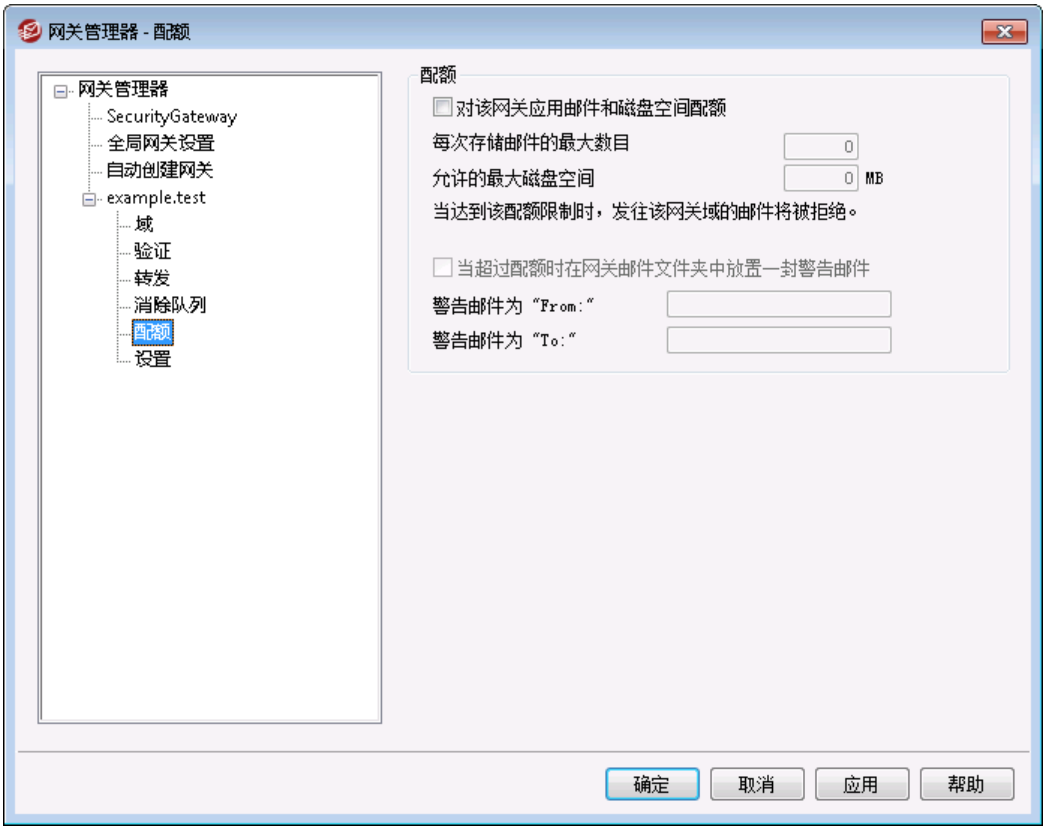
准许来自这些 IP 的出队请求
选择此项时，MDaemon 将准许在相关地址列表内罗列的任何 IP 生成的 ETRN/ATRN 请求。

忽略来自这些 IP 的出队请求
选择此项时，MDaemon 将忽略在相关地址列表内罗列的任何 IP 生成的 ETRN/ATRN 请求。

添加新 IP
要在现有列表内添加一个新的 IP，只需在此文本框内输入 IP，并点击 *"添加"*按钮即可。

删除
点击此按钮即可删除 IP 地址列表中的选定条目。

3.3.3.5 配额



配额

对该网关应用邮件和磁盘空间配额

如果您希望指定该域允许存储的最大邮件数，或者可以使用的最大磁盘空间（以千字节计算），请启用此选项。包括目录下的任何解码的附件。当达到配额的时候，将拒收任何再发往该域的入站邮件。

每次存储邮件的最大数目

使用此文本框来指定 MDaemon 网关域将存储的最大邮件数量。如果您不希望限制邮件的数量，在此选项中请使用“0”。

允许的最大磁盘空间

在此处指定允许的最大磁盘空间。当该域存储的邮件和文件达到配额的时候，任何近来发送到该域的邮件将被拒绝。如果您不希望设置磁盘空间限制，请使用“0”。

当超过配额时在网关邮件文件夹中放置一封警告邮件

当启用此选项，当发送到域的邮件超过最大信息数量及最大磁盘空间，则一封警告邮件将发到域网关的邮件文件夹。您可以指定警告邮件下方的“发件人：”以及“收件人：”报头。

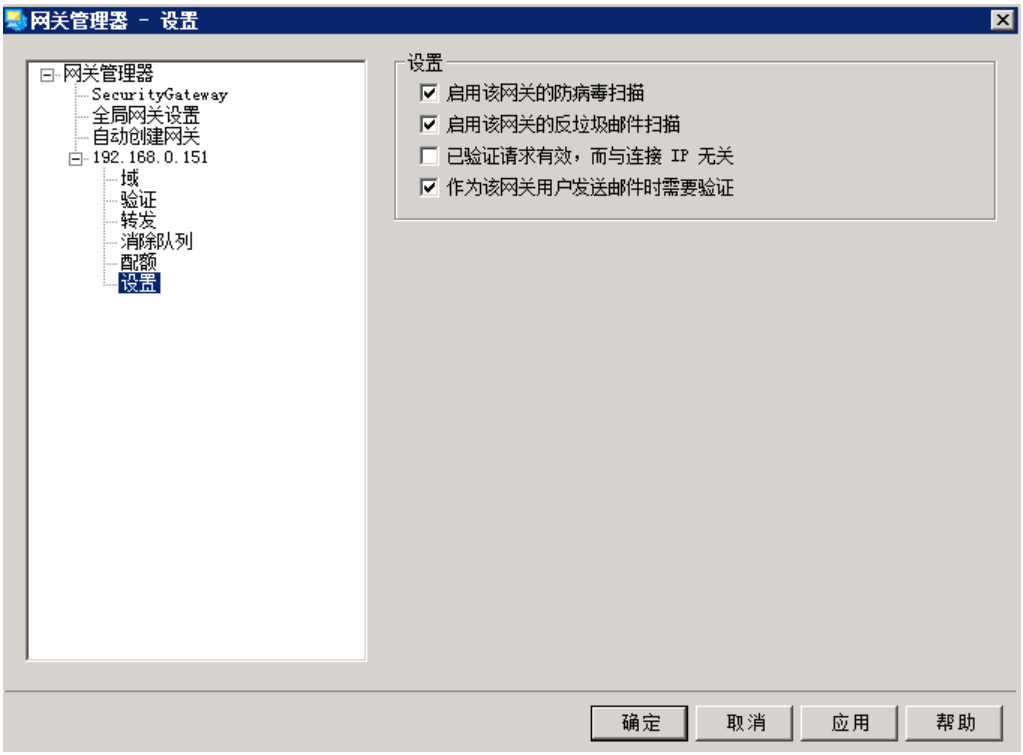
警告邮件的“发件人：”

使用此选项来指定“发件人：”地址，该地址将用于超过配额的警告邮件。

警告邮件是“收件人：”

使用此选项来指定“收件人：”地址，该地址将用于超过配额的警告邮件。

3.3.3.6 设置



设置

为此网关启用反病毒扫描
如果您正在使用可选的 MDaemon AntiVirus 539 功能，并希望扫描此域网关的邮件，请点击这个选项。如果您清除这个选项，AntiVirus 将不会扫描这个网关的邮件。

为该网关启用反垃圾邮件扫描
如果您希望为域网关的邮件应用垃圾邮件过滤设置，请点击此选项。否则，这些邮件将免于 "垃圾邮件过滤器"扫描。

已验证的请求有效，不管连接 IP 如何
如果您希望无论 IP 地址来自何方都准许验证请求，则启用此复选框。若未启用此控件，那么只会准许来自在下方 "访问"部分中指定的 IP 地址的验证请求。

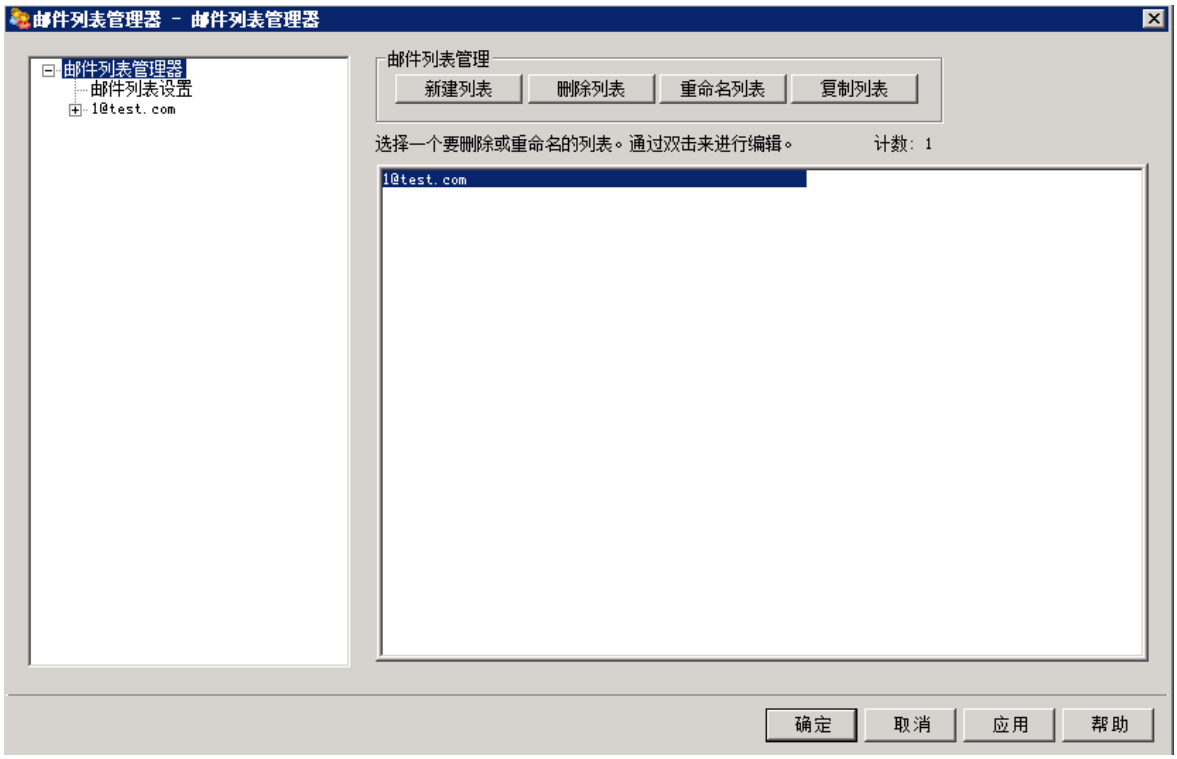
作为该网关的用户发送邮件时需要验证
如果您希望所有声称来自域的邮件都请求验证，则点击此复选框。如果一封邮件声称来自该域，那么它必须使用一个验证连接 (或是连接来自一个可信的 IP 地址)否则将拒收此邮件。默认情况下启用此项。

当新的域网关创建的时候，默认情况下将启用此选项。如果您希望改变默认设置以便让新的网关禁用这个选项，那么请在 MDaemon.ini 文件中编辑下列关键字：

```
[Special]
GatewaySendersMustAuth=No  (默认为 Yes)
```

3.4 邮件列表管理器

邮件列表有时候称之为邮件组或者分发列表，允许多用户组地址被组合起来就好像他们共享一个公共邮箱。发送到列表的电子邮件的副本分发到列表里的每一个成员。列表可以包含本地和/或远程目的地地址的成员，可以是公开的或是保密的，适中的或开放的，以摘要240格式或是以常规格式发送等等。



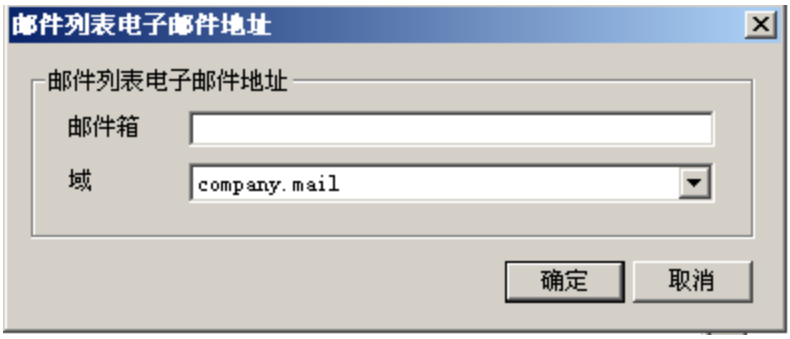
“邮件列表管理器”位于“设置» 邮件列表管理器..”菜单，用于管理您的列表。

邮件列表管理

这个对话框左侧的导航窗格为您各个邮件列表包含一个条目，提供链接转至用于配置各种特定列表设置的屏幕。它还供您访问“邮件列表设置225”屏幕，用来配置相关列表的许多全局选项。此对话框右侧的选项用来创建、删除和重命名您的列表。您可以双击邮件列表来切换至邮件列表编辑器，供您配置列表的设置。

新建列表

要新建邮件列表，请点击“**新建列表**”来打开“邮件列表邮件地址”对话框。创建邮箱名称并选择一个域，例如邮箱名为“MyList”，域为“example.com”。这将是邮件列表的邮件地址（例如 MyList@example.com）。会基于列表的特定设置，将发送至这个地址的邮件分发到列表的各个成员。点击“**确定**”来创建这个列表。创建完列表后，您可以双击其条目来配置相关设置并添加成员。**请注意：**列表的名称中不能包含“!”或“|”。



删除列表
要删除邮件列表：选中列表并点击 "**删除列表**"，然后点击 "**是**"来确认您的决定。

重命名列表
要重命名邮件列表，请选择 "**重命名列表**"来打开 "邮件列表邮件地址"对话框。进行所需的更改，然后点击 "**确定**"。

复制列表
如果您希望使用与另一个列表相同的设置和成员来创建邮件列表，请选择该列表，点击此按钮，然后为新列表指定邮箱名称和域。

修改现有的邮件列表

要配置邮件列表，请在 "邮件列表管理器"上双击其条目。然后在左侧的导航窗格上，点击您希望编辑的屏幕：

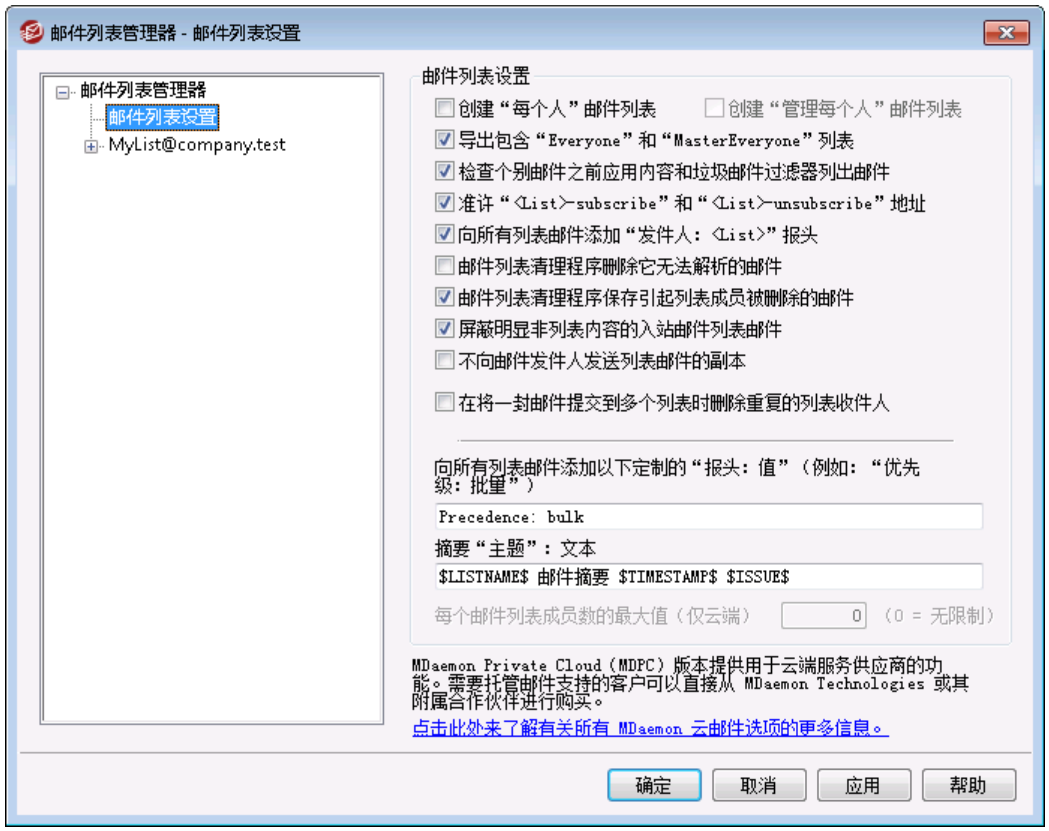
邮件列表设置

点击左侧窗格的 "**邮件列表设置**"来打开 "邮件列表设置 225"屏幕，以便配置与邮件列表相关的许多全局设置。

还请参阅：

邮件列表设置 225

3.4.1 邮件列表设置



邮件列表设置

创建“Everyone”邮件列表
如果您希望为您的所有域创建并维护一个“Everyone”邮件列表（比如“everyone@example.com”），请勾选该选框。将为每个域创建一个列表，帮助您通过将邮件指向“everyone@<domain>”，把一封邮件发送给域中的每个用户。“Everyone”邮件列表中隐藏私人账户 639。默认情况下，禁用该选项。

创建“MasterEveryone”列表
如果您希望创建一个“MasterEveryone”列表，请启用该选项。每个在“Everyone”列表中的成员都将会包含在此列表中。默认情况下，禁用该选项。

导出包括“Everyone”和“MasterEveryone”列表。
默认情况下，在您使用“账户 » 导出...”选项来导出列表时将包括“Everyone”和“MasterEveryone”邮件列表。如果您不希望在邮件列表导出中包含这些列表，则禁用此项。

检查个别邮件之前应用内容和垃圾邮件过滤器列出邮件
当选择了*"将列表邮件分别投递到每个成员"*选项（位于"邮件列表编辑器"的"路由 244"屏幕）时，启用此控件将会使得列表邮件在被复制并分发到列表成员前，应用内容过滤器规则和垃圾邮件过滤器。

准许"<List>-subscribe"和"<List>-unsubscribe"地址
如果您希望 MDaemon 将此格式的邮件地址视为合法（只要列表实际存在）以便为用户提供更方便的方法加入以及离开您的邮件列表。例如：假设您有一个列表叫做 MyList@example.com。用户可以通过向 MyList-Subscribe@example.com 与 MyList-Unsubscribe@example.com 发送一封邮件以订阅/取消订阅您的列表。邮件的内容和标题无关紧要。此外，启用该功能时，MDaemon 会插入以下报头至所有列表邮件：

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@example.com>
```

某些邮件客户端可以识别此报头并自动生成 UNSUBSCRIBE 按钮以供用户选择。

> 您可以通过在"邮件列表 URL"选项（位于"邮件列表编辑器"的"调节 243"屏幕）指定"List-Subscribe"和"List-Unsubscribe"报头的值来覆盖个别列表的这个选项。

添加"Sender:<List>"报头到所有列表邮件
如果您希望插入"发件人"报头到邮件列表的邮件，请启用该选项。

邮件列表清理程序删除无法解析的邮件
启用此项时，MDaemon 将删除未包含可解析地址的列表邮件。

邮件列表清理程序保存那些使列表成员被删除的邮件
当 MDaemon 扫描返回的列表邮件，并尝试删除不能被到达的成员地址时，此控件将会保存那些导致列表成员被删除的邮件。要了解更多信息，请参阅*"删除不可投递的邮件地址..."*选项（位于设置 231屏幕）。

屏蔽明显非列表内容的入站邮件列表邮件
如果您希望当 MDaemon 决定应该将发往邮件列表的邮件发往系统账户时拒收那些邮件，请勾选该选框。例如：一个用户可以通过在邮件开头放置订阅或取消订阅命令并将其发送到系统地址（例如"mdaemon@example.com"）以加入或退出列表。通常，用户错误地设法向列表本身发送那些邮件。启用此控件将会阻止这些邮件被投递到此列表。

不向邮件发件人发送列表邮件的副本
启用此项时，在一名列表成员向该列表发送邮件时，这名发件人不会受到邮件副本。默认情况下，禁用该选项。

在将一封邮件提交至多个列表时删除重复的列表收件人
启用此项后，在一封邮件指向多个邮件列表时，MDaemon 仅会将该邮件的一个副本投递到作为多个列表成员 228的任何收件人。例如，如果 frank@example.net 是 List-A@example.com 和 List-B@example.com 的成员，有一封入站邮件被同时投递到这个两个列表，那么 Frank 将仅收到该邮件的一个副本而不是两个副本。该选项仅适用于列表，因此在上例中如果该邮件被直接投递到 Frank 和这两个列表，那么 Frank 将收到该邮件的两个副本而不是一个副本。默认情况下，禁用该选项。

通常不建议使用此项。用户可以使用多种不同的方式来使用和整理邮件列表，不过在限制重复邮件的这种方式下，不知道是哪个列表将收到邮件。因此使用此项将为某些出于邮件线索偏爱，使用 "IMAP 过滤器 617"来将邮件排序到特定文件夹的用户带来不必要的困难。

添加以下定制的 "Header:value"到所有列表邮件
如果您希望添加一个静态的报头/值组合 (比如 "Precedence: bulk")到所有的列表邮件，则在此处指定文本。

摘要 "主题："文本：
如果您希望在 MDaemon 发送 "邮件列表摘要 240"邮件时定制所用的主题，则使用此项。默认值是："$LISTNAME$ 邮件摘要 $TIMESTAMP$ $ISSUE$。"这些宏可以扩展成邮件列表名称、摘要邮件创建的时间戳和发送编号。

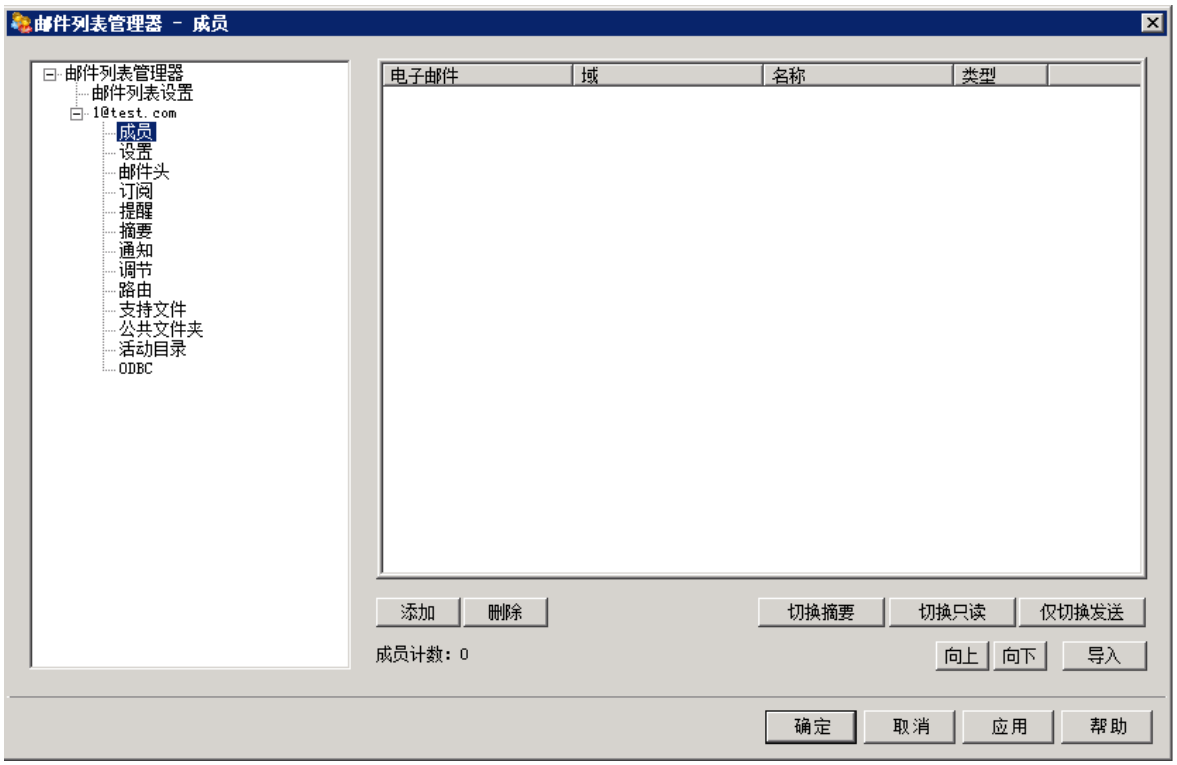
每邮件列表的成员最大值 [xx] (0=无限制)
如果您希望设置每个邮件列表允许的成员数量最大值，请使用此项。您可以在 "域管理器"的 "设置 175"屏幕上设置每个域的最大值。此项仅适用于 MDaemon Private Cloud。

还请参阅：

邮件列表管理器 223

3.4.2 邮件列表编辑器

3.4.2.1 成员



该屏幕显示了当前订阅列表的所有成员的邮件地址与名称。每个成员的条目还说明了其成员的 "类型"：常规、摘要、只读、仅发送。要编辑成员设置，请双击该成员的条目。

添加
该按钮打开 "新建列表成员"屏幕来添加新成员 229。

删除
要从列表删除一个成员，请选择其条目并点击此按钮。

切换摘要
选择一个成员，点击此按键使之成为摘要 240 成员。再次点击此按钮来将成员转变回 "常规"模式。

切换只读
选择成员的条目并点击该按钮以将其切换至 "只读"模式。成员仍可从列表接收邮件但不可发送邮件至列表。再次点击此按钮来将成员转变回 "常规"模式。

切换仅发送
选择一个成员后点击此按键可使之成为 "仅发送"成员。仅发送成员可以向列表发送邮件但不能接收到任何邮件。再次点击此按钮来将成员转变回 "常规"模式。

向上/向下
选择一个或多个成员，然后点击这些按钮在列表中上移或下移。您还可以通过点击任何列的标题来对列表进行排序。**注意：**如果按列标题对列表进行排序，它将覆盖您使用"向上/向下"按钮所做的任何手动排序。

导入
点击该按钮从文本文件中导入列表成员，文件由逗号分隔各字段。(比如：一个以逗号分隔的文件)。每个条目必须位于自身的行上，而且其所有字段必须由逗号分隔。此外，文件的首行(基线)必须列出字段名称，以及各字段在余下行中的顺序。其中一个字段必须叫做"**电子邮件**"并包含电子邮件地址。还有两个可选字段："**全名**"和"**类型**"。全名是列表成员的姓名。"类型"可以含有以下值："只读"、"仅发送"、"摘要"或"常规"。导入程序将忽略其余所有字段。

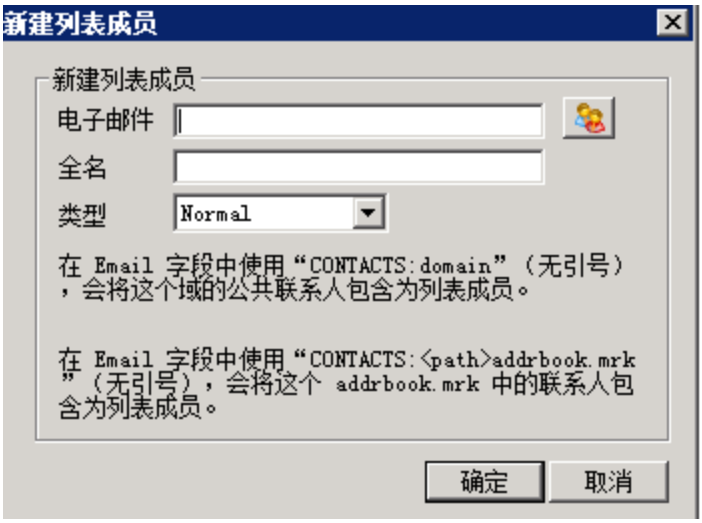
例如：

"电子邮件"、"全名"、"类型"、"地址"、"电话"
"user01@altn.com"、"Michael Mason"、"摘要"、"123 Street St"、"519.555.0100"

被导入的成员不会收到列表的欢迎信息包，且导入程序将不会检查成员副本。

成员计数：
会在该屏幕底部显示当前订阅列表的所有成员数。

添加新成员



新建列表成员

电子邮件
输入您希望添加至邮件列表的邮件地址，如果您希望浏览 MDaemon 账户和群组啦将其添加到该列表，请点击"账户"图标。列表成员地址不能包含"!"或"|"。

如果您希望添加一个域的所有用户或属于特定群组的所有用户，您可以分别输入 **ALL_USERS:<domain>** 或 **GROUP:<group-name>**，而不是输入特定的电子邮件地址。例如，将 ALL_USERS:example.com 添加为列表成员的效果与分别添加每个 example.com 用户账户的效果相同。

您还可以使用 **CONTACTS:<domain>** 来将域的公共联系人[97]包含为列表成员。例如 CONTACTS:example.com。

全名
在此字段内输入成员的姓名。当选中 *"用成员的全名 替换 "TO:" 报头"*选项（位于报头[233]屏幕，将在列表邮件的 "To:"报头中显示这个名称。

类型
使用下拉框来为用户选择成员类型：

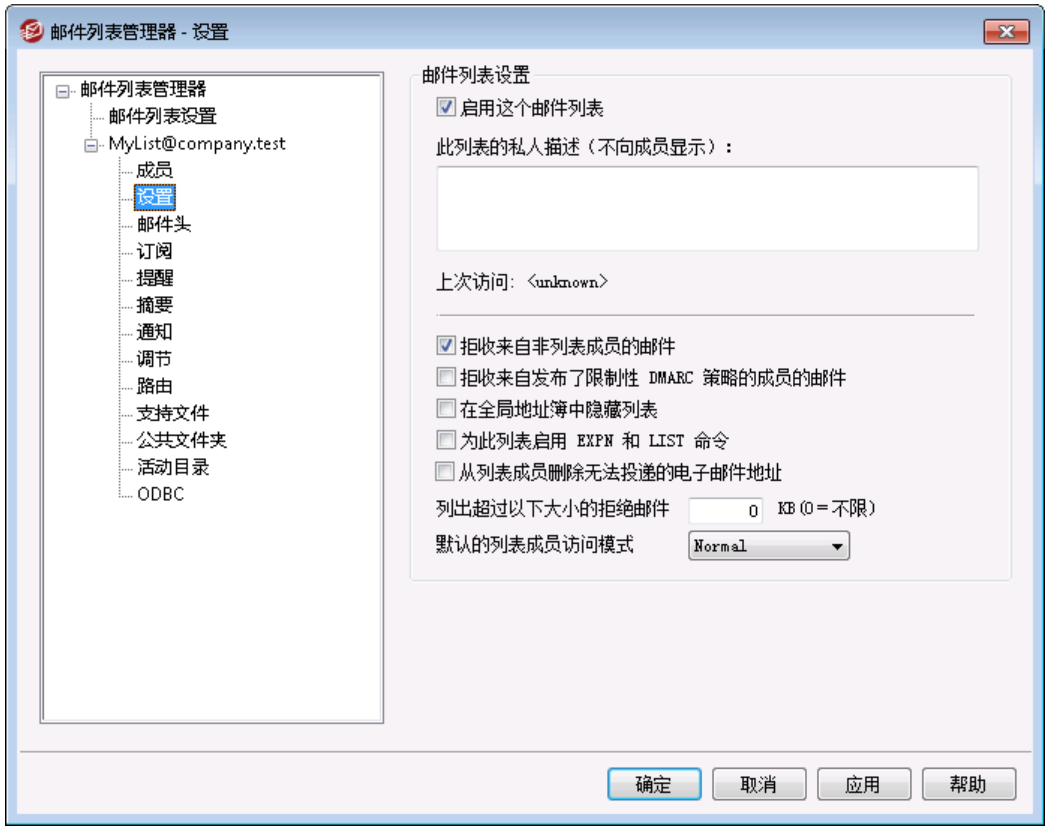
常规—该成员可以正常收发列表邮件。

摘要—该成员可以收发列表邮件，不过接收到的邮件将以摘要格式显示。

只读—该成员将接收列表的邮件，不过无法向其发送邮件。

仅发送—该成员可以向列表发送邮件，但无法接收任何邮件。

3.4.2.2 设置



邮件列表设置

启用这个邮件列表
如要临时禁用邮件列表，请清除此复选框。在禁用这个列表时，来自或发往这个列表并通过 SMTP 抵达的任何邮件都将生成 451 临时错误并被拒收。

这个列表的私人描述（不向成员显示）
您可以在此处为列表输入私人描述。这仅供您自己参考，而且不会向任何成员或在任何报头中显示。

上次访问
显示某人上次访问此列表的时间。这可以帮助您轻松简便地识别极少或不再使用的列表。

拒收来自非列表成员的邮件
启用该控制项时，会将列表视作“私人”列表，表示只有列表成员可以向该列表发送邮件。将拒收非成员发送的邮件。

拒收发件域使用受限 DMARC 策略的邮件
如果发送至此列表的入站邮件发自所在域发布了受限 DMARC[449] 策略（例如 p=quarantine or p=reject）的人员，在您希望拒收任何这种邮件时请启用此项。如果您

正在使用 *"使用列表的邮件地址取代 "from:"邮件地址..."*这个选项（位于"报头[233]"屏幕），您不必启用此项。

如果同时禁用了此项和 *"使用列表的邮件地址取代 "from:"邮件地址..."*[233]选项，就会使一些列表邮件被某些收件服务器拒收，而且在某些情况下，会自动从列表成员删除[232]收件人。因此您应该小心谨慎，并确保至少启用了其中一项。

在全局地址簿中隐藏列表
点击此选项，隐藏 Webmail 和 LDAP 公共地址簿里的邮件列表。

为此列表启用 EXPN 和 LIST 命令
默认情况下，MDaemon 不对这些列表准许 EXPN 和 LIST 命令，由此来保护成员的隐私。如果您启用了此项，那么在邮件会话期间，此列表中的成员会被告知响应 EXPN 或 LISTS 命令。

删除列表成员中不可投递的邮件地址
一旦启用此功能，在 MDaemon 发送邮件过程中，若遇到永久性致命错误，MDaemon 将会从列表用户中自动删除该地址。当邮件被移动到重试[732]系统，并在该系统内过了有效期，该邮件地址也被自动删除。

只有当远程邮件服务器拒收邮件时，*"删除不可投递的邮件地址..."*这个选项才起作用。只有在选中 *"分别向各个成员投递列表邮件"*选项（位于路由屏幕[244]）时，此项才起作用。如果您希望将列表邮件路由至智能主机时，请参阅以下的"增强的列表清理[232]"以了解更多信息。

列出超过 [xx] KB 的拒收邮件
此控件进一步限制了从邮件列表内接收的邮件大小。拒收大于该限制的邮件。

默认列表成员访问模式
使用这个下拉列表来设置用于新成员的默认访问模式。您可以从"成员[228]"屏幕更改任何现有成员的访问模式设置。提供四种成员模式：

常规—该成员可以正常收发列表邮件。

摘要—该成员可以收发列表邮件，不过接收到的邮件将以摘要格式显示。

只读—该成员将接收列表的邮件，不过无法向其发送邮件。

仅发送—该成员可以向列表发送邮件，但无法接收任何邮件。

增强的列表清理

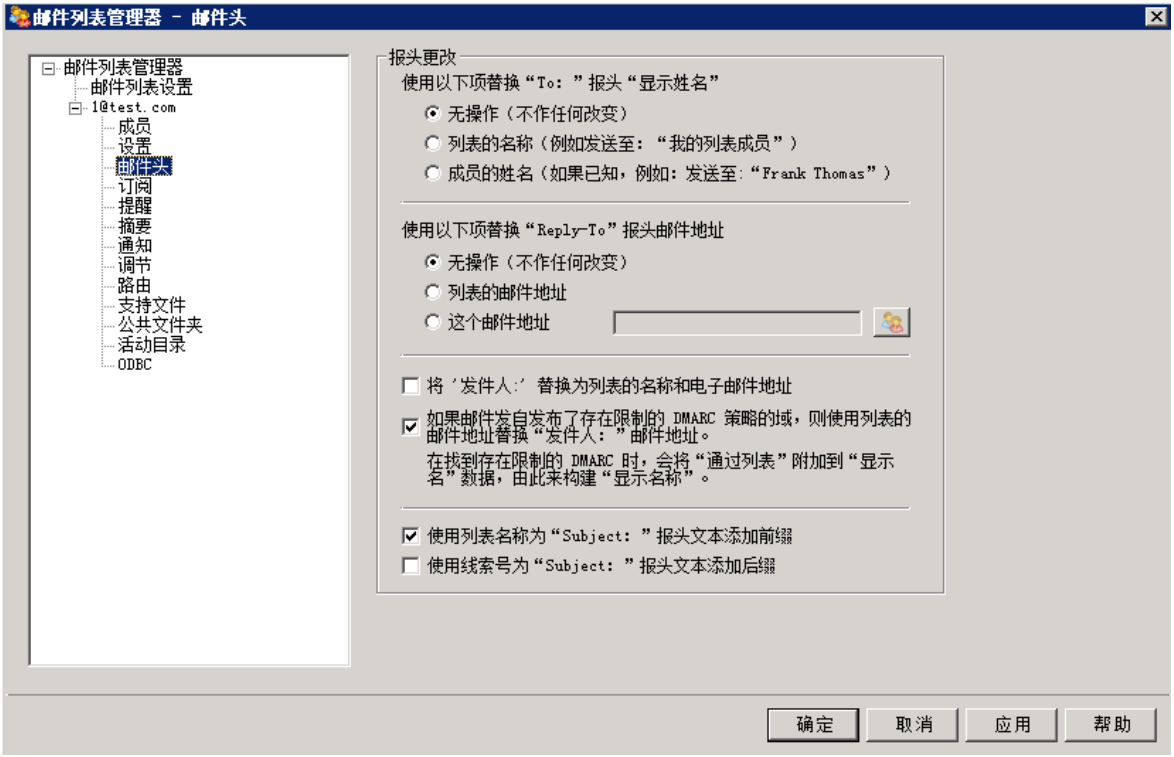
当启用了 *"删除列表成员中不可投递的邮件地址"*这一选项，并且您已经指定了一个本地邮箱作为列表邮件的返回路径时，（请参见 *列表的 SMTP "退回"地址*选项，其位于通知[241]），每晚午夜 MDaemon 将尝试从被退回的邮件中分析问题地址并删除那些无法抵达的成员。这将有助于提高从邮件列表中筛选无效地址，特别是当您不是直接发送邮件信息而是发送至智能主机的时候。

"邮件列表设置[225]"上有两个相关该功能的选项。*"邮件列表清理程序删除无法解析的邮件"*选项将删除那些不包含可分析地址的被退回的邮件，*"邮件列表清理程序保存引起列表成员被删除的邮件"*选项将保存所有导致列表成员被删除的邮件。

将*列表的 SMTP 退回地址*[241]设置成本地用户的地址，可能导致此用户的邮件被删除，因为在邮件列表设置[225]屏幕中指定的列表清理程序设置会促成这种结果。

在投递到一个地址导致 5xx 错误时，会将该地址附加到日志文件夹内的 BadAddress.txt 文件中。这可以帮助您比搜索出站 SMTP 日志这种方式更快地识别您邮件列表中的坏地址。每晚午夜将自动删除这个文件来防止其越变越大。

3.4.2.3 报头



报头变更

替换 "TO:" 报头 "Display Name (显示名称)"为
使用此选项来指定每当 MDaemon 接收一封指向该列表的邮件时，显示在注释或 "TO:"字段实际名称上的文本。

无变化（不做变更）——选定此项时，MDaemon 不做任何变更。包含在 TO:报头中的显示名称和地址 会正确按照发件人所输入的显示。

列表名称 - 此项使用列表名称和 "List Member (列表成员)"来取代显示的名称。例如：如果邮件列表的名称为 "My-Family"，那么 "To:"报头的显示名称部分将为 "My-Family List Member"。

成员的全名（如果已知） - 选择该选项时，"TO:"报头将包含邮件名称 (如有)以及将发往的列表成员的地址。

> "*成员姓名*"选项只有在选定 "*向每个成员单独投递邮件列表*" (在路由屏幕 244选择)的情况下才能选择。当选中 "*为每个成员用单独的 RCPT 命令投递列表邮件*"时，MDaemon 将默认 *列表的名称选项*。

替换 "Reply-To:" 报头邮件地址为
此项用来指定将在各个列表邮件的 "Reply-To:"报头中出现的邮件地址

无变化 (不做变更)
如果您希望无论分发到此列表的原始邮件的报头如何，都不更改 "Reply-To:"报头，则选择此项。在您希望将回复直接发送回将邮件发送到此列表的人而不是此列表的所有成员时，这是您应该选择的常规选项。

列表的邮件地址
如果您希望将回复直接发送回列表而不是特定的人或地址，则选择此项。如果您希望将此列表用作群聊工具，将回复直接发送给所有成员，您应该选择此项。

这个邮件地址
如果您希望将回复发送至特定的邮件地址，请在此输入。如果您希望浏览至特定的 MDaemon 账户进行使用，请点击 "账户"图标。您也可以将此项用于具有特定回复联系地址的电子邮件通讯。

替换 "From:"为列表的名称和邮件地址
如果您希望替换 "发件人:"的内容，请选中此框。包含邮件列表的名称和电子邮件地址的报头。

替换 "From:"邮件地址为列表的邮件地址 (如果邮件发自发布了存在限制的 DMARC 策略的域)
默认情况下，如果发送到此列表的入站邮件来自所在域发布了存在限制的 DMARC 449 策略的用户 (例如：p=quarantine 或 p=reject)，MDaemon 会在将这封邮件发送到此列表前，使用此列表的地址来替换 "From:"报头中用户的邮件地址。在防止此列表邮件被顺

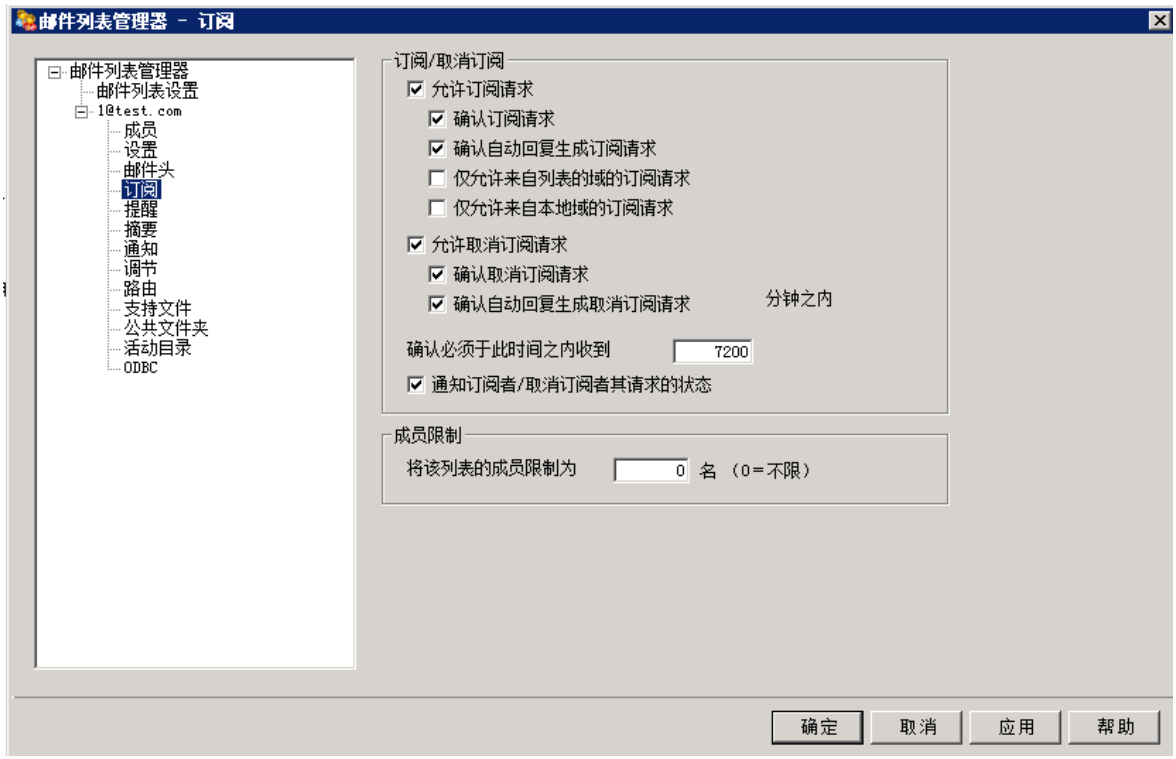
应存在限制的 DMARC 策略的服务器拒收时，上述步骤十分必要。除了更改 "From："报头的邮件地址以外，也将修改显示名称，为其添加 "通过列表名称"来表示这封邮件由代表指定人员的邮件列表所发送。此外，每当这个功能更改 "From："报头时，会将原始 "From："报头的数据移至 "Reply-To："报头，不过只有在邮件开头没有 "Reply-To："报头，而且未将列表配置成显示自定义 "Reply-To："报头。

您不得禁用此项，除非您完全理解了这么做的后果并确认您真的需要禁用此项。禁用此项会使某些列表邮件被一些收件服务器拒收，而且在某些情况下，会自动从列表成员中删除收件人。取而代之的，您应启用 *"拒收来自使用了受限 DMARC 策略的域的邮件"*这个选项，当发送自此列表的入站邮件来自使用了受限 DMARC 策略的域时，将拒收这封邮件。

在 "Subject："报头文本前附加列表名称
此设置使 MDaemon 将列表名称用方括号括起来 (比如[ListName])并在所有发送至该列表的邮件中将其添加到 Subject: 的开头部分。默认启用此项。

在 "Subject："报头文本中附加线索数
该选项允许您切换是否在列表邮件的 Subject: 报头里显示线索数量。将它们用方括号括起附加至 Subject 行末尾作为伪线索数。按 Subject 排序您的收件箱会将您的列表邮件按时间顺序排列。默认情况下，禁用该选项。

3.4.2.4 订阅



订阅/取消订阅

允许订阅请求
该选项控制列表是否会通过特定格式的邮件或自动应答器允许订阅请求。要了解更多详情，请参阅：订阅邮件列表 238。

确认订阅请求
选中该选框时，MDaemon 将尝试确认订阅请求，它会产生一个唯一代码并将其放在一封邮件中发送至请求加入列表的地址。如果申请者回复了这封确认邮件，MDaemon 会自动将该成员添加到列表。确认邮件是有时效的，这表示用户必须在以下指定的分钟数内回复邮件。

确认自动应答器生成的取消订阅请求
当选中该选框时，MDaemon 将尝试确认订阅请求，订阅请求会通过自动应答器 607 选项中的*"添加发件人到该邮件列表"*自动产生。和上述选项一样，MDaemon 将产生一个唯一代码并将其放入邮件发送至等待被加入列表的地址。如果申请者回复了这封确认邮件，MDaemon 会自动将该成员添加到列表。这些确认邮件也是有时效的，因此必须在以下指定的分钟数内回复邮件。

取消订阅

允许取消订阅请求
该选项控制列表是否会通过特定格式的邮件或自动应答器允许取消订阅请求。要了解更多详情，请参阅：订阅邮件列表 238。

确认取消订阅请求
选中该选框时，MDaemon 将尝试确认订阅请求以将成员从列表删除，它会产生一个唯一代码并将其放在一封邮件中发送至请求取消订阅该列表的地址。如果申请者回复了这封确认邮件，MDaemon 会自动将该成员从列表中删除。确认邮件是有时效的，这表示用户必须在以下指定的分钟数内回复邮件。

确认自动应答器生成的取消订阅请求
当选中该选框时，MDaemon 将尝试确认取消订阅请求，该请求会通过自动应答器[607]选项中的 *"从邮件列表删除发件人"*自动产生。和上述的 *"确认取消订阅请求"*选项一样，MDaemon 将产生一个唯一代码并将其放入邮件发送至等待被移出列表的地址。如果申请者回复了这封确认邮件，MDaemon 会自动将该成员删除。这些确认邮件也是有时效的，因此必须在以下指定的分钟数内回复邮件。

确认必须于 [xx] 分钟之内收到
这是订阅或取消订阅确认邮件的收件人在邮件过期之前拥有的分钟数。如果在 MDaemon 收到该邮件的回复之前超过了时间限制，那么列表就不会添加或删除该地址。该地址必须重新提交一份加入或退出列表的新请求。该选项的默认设置是 7200 分钟。（比如 5 天）。

这是全局值——它应用于您所有的邮件列表而不是您正在编辑的特定列表。

通知订阅者/取消订阅者其请求的状态
启用该复选框时，MDaemon 会发送一封完整的通知邮件给订阅或取消订阅邮件列表的用户。

成员限制

将改列表的成员限制为 [xx] 名（0 = 不限）
使用这项功能，您可以设置一个无上限的人数，允许他们订阅邮件列表。如果您不希望限制订阅的人数，键入 0。

只有通过使用在*订阅邮件列表*[238]中概述的邮件方法才能对订阅的地址应用这项限制。该限制对在成员[228]屏幕中手工输入的订阅不适用，也不适用于涉及列表密码[243]时通过邮件发送的订阅请求。

还请参阅：

订阅邮件列表[238]
自动应答器[607]

3.4.2.4.1 订阅邮件列表

通过邮件命令订阅/取消订阅

要订阅或取消订阅邮件列表，将邮件地址发送到某个域的 MDaemon (或其别名)所控的邮件列表，把 Subscribe 或 Unsubscribe 命令写在邮件正文的第一行。例如，有一个名为 MD-Support 的邮件列表正在被 mdaemon.com 托管。 您可以通过以下方式订阅列表：编写一封指向 "mdaemon@mdaemon.com"的电子邮件，并将数值 SUBSCRIBE MD-Support@mdaemon.com 作为邮件正文的第一行以订阅列表。邮件的主题无关紧要，可略写。

要了解如何完成此订阅和其他控件的详细信息，请参阅：通过电子邮件远程控制服务器 752 。

有时，用户会尝试通过电子邮件向列表本身而不是向 MDaemon 系统账户发送命令以订阅或取消订阅列表。这将会导致命令被发送至列表而不是被订阅或被取消订阅的用户。为了防范这些邮件发往邮件列表，在设置» 首选项» 系统 414 有一个选项，叫做 *"屏蔽明显非列表内容的入站邮件列表邮件。"* 默认情况下启用此项。

通过邮件地址订阅/取消订阅

该选项，*"准许 "<List>-subscribe"和 "<List>-unsubscribe"地址*，其位于设置» 邮件模板管理器» 邮件列表设置 225，使用户可以通过向专门的邮件地址发送邮件就能加入或退出邮件列表，而不用使用在以上*通过邮件命令订阅/取消订阅*中描述的邮件命令。要使用这个方法加入或退出列表，用户只要向列表的地址发送一封邮件即可，但是一定要在地址的邮箱部分附加 "-subscribe"或 "-unsubscribe"。例如：如果列表的名称是 "franks-list@example.com"，那么用户可以发送一封邮件到 "franks-list-subscribe@example.com"以订阅列表。要取消订阅列表，邮件应发往 "franks-list-unsubscribe@example.com"。上述两种情况中，邮件主题与邮件正文都无关紧要。此外，启用该功能时，MDaemon 会插入以下报头至所有列表邮件：

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@example.com>
```

某些邮件客户端可以识别此报头并自动生成 UNSUBSCRIBE 按钮以供用户选择。

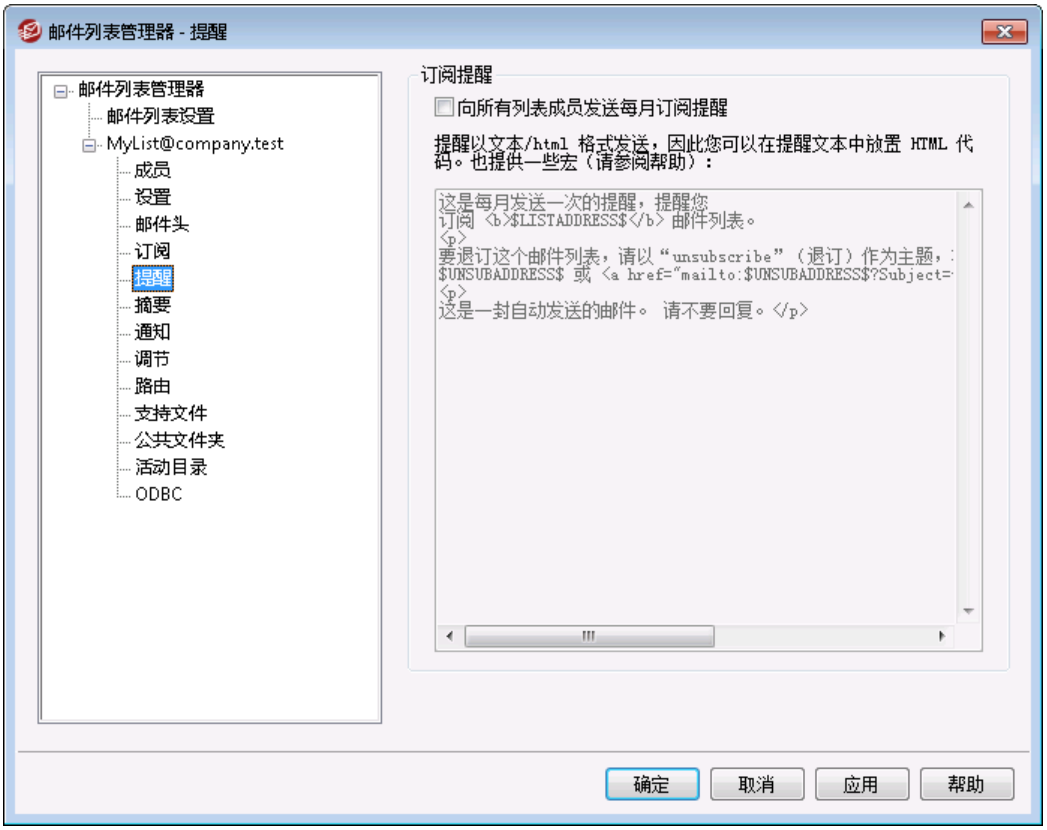
通过自动应答器订阅/取消订阅

您还可以使用自动应答器 607 来自动添加或删除列表成员。要做到这点，您要创建一个或多个 MDaemon 账户，并使用自动应答器为每个一账户进行配置，使这些账户的唯一目的就是典型地自动添加或删除将向这些账户发送邮件的地址。例如：如果您有一个叫做 "franks-list@example.com"的邮件列表，您可以使用以下地址创建一个 MDaemon 账户："join-franks-list@example.com"。之后您要为那个账户配置一个自动应答器以在 "franks-list@example.com"里添加任何向其发送邮件的地址。要加入该列表，您所要做的只是发送一封邮件到 "join-franks-list@example.com"。这是为用户设计的简单的解决方案，因为它不要求用户记住任何在上述*通过邮件命令订阅/取消订阅*方法中要求的专用邮件命令。

还请参阅：

订阅 236
通过电子邮件远程控制服务器 752
自动应答器 607
首选项 » 系统 414
首选项 » 其他 421

3.4.2.5 提醒



订阅提醒

向所有列表成员发送月度订阅提醒
如果您希望将提供的文本框中作为订阅提醒邮件的内容，在每月的第一天发送至各名列表成员，请启用此项。将以文本/html格式发送提醒邮件，这样您便能在做出相应选择时在提醒文本中使用 HTML 代码。提醒邮件中可以使用以下宏：

$LISTADDRESS$ - 将扩展成邮件列表的电子邮件地址（例如：MyList@example.com）

$LISTNAME$ - 将扩展成邮件列表的电子邮件地址的本地部分（例如：MyList）

$UNSUBADDRESS$ - 将扩展成列表的取消订阅地址（MDaemon 系统地址，例如：mdaemon@example.com）

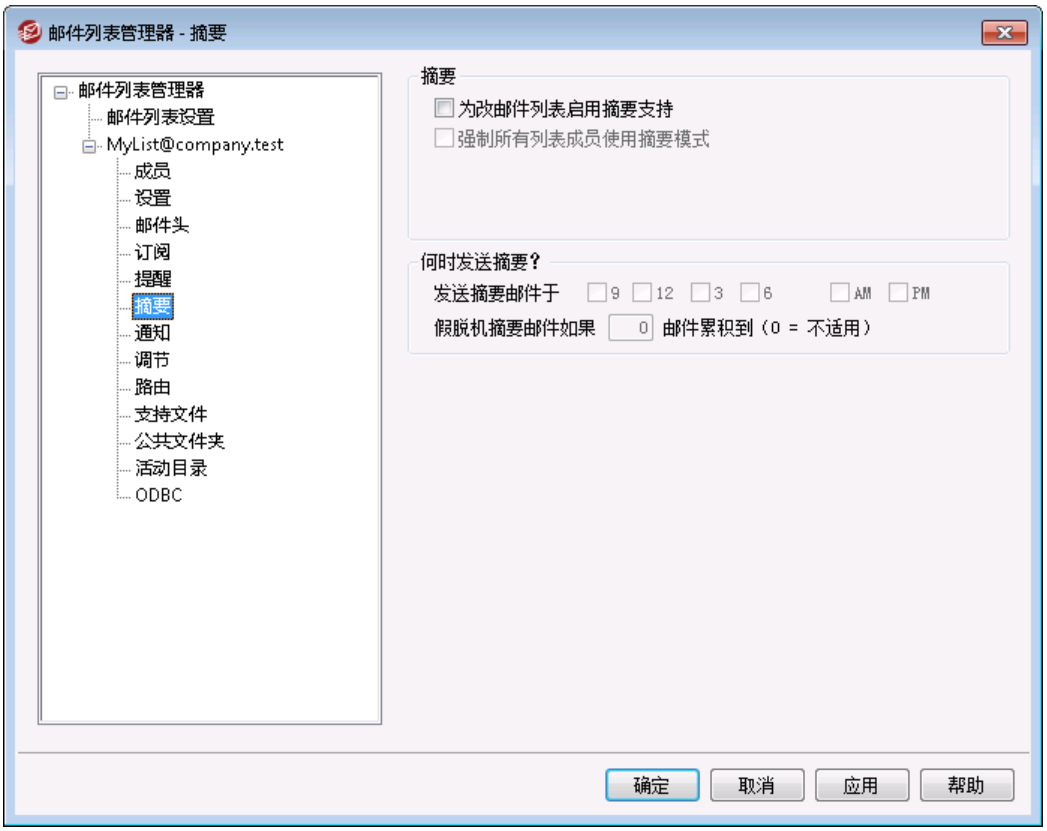
$MEMBERADDRESS$ - 将扩展成接收此提醒的列表成员的电子邮件地址 (例如: frank.thomas@example.com)

如果您希望在每月的其他日子发送提醒，您可以通过在 MDaemon.ini文件中设置以下项来实现这一点：

```
[Special]
ListReminderDay=X
```

将 "X"设置成 1 - 28 之间的一个数字，表示您希望在这一天发送提醒。

3.4.2.6 摘要



摘要

为该邮件列表启用摘要支持
如果您希望允许摘要支持用于邮件列表，请点击此框。启用摘要支持时，将归档发送至邮件列表的每封邮件的副本，这样已将他们的成员类型 228 设置为*摘要*的列表成员将被定期发送这样一批小巧的索引格式的归档邮件而不是一次收到一封。

强制所有列表成员使用摘要模式
默认情况下，列表用户可控制所接收的列表为摘要模式还是普通模式。如果您希望强制所有的成员使用摘要模式而不顾他们可能已为自己选择好的模式，请点击该框。

何时发送摘要？

以下的选项决定发每隔多久，以及在何种情形下发送摘要至已设置为以摘要格式接收邮件的列表成员。所有的选项都相互独立地进行处理，这表示任何一个或所有选项都能使摘要被发送。

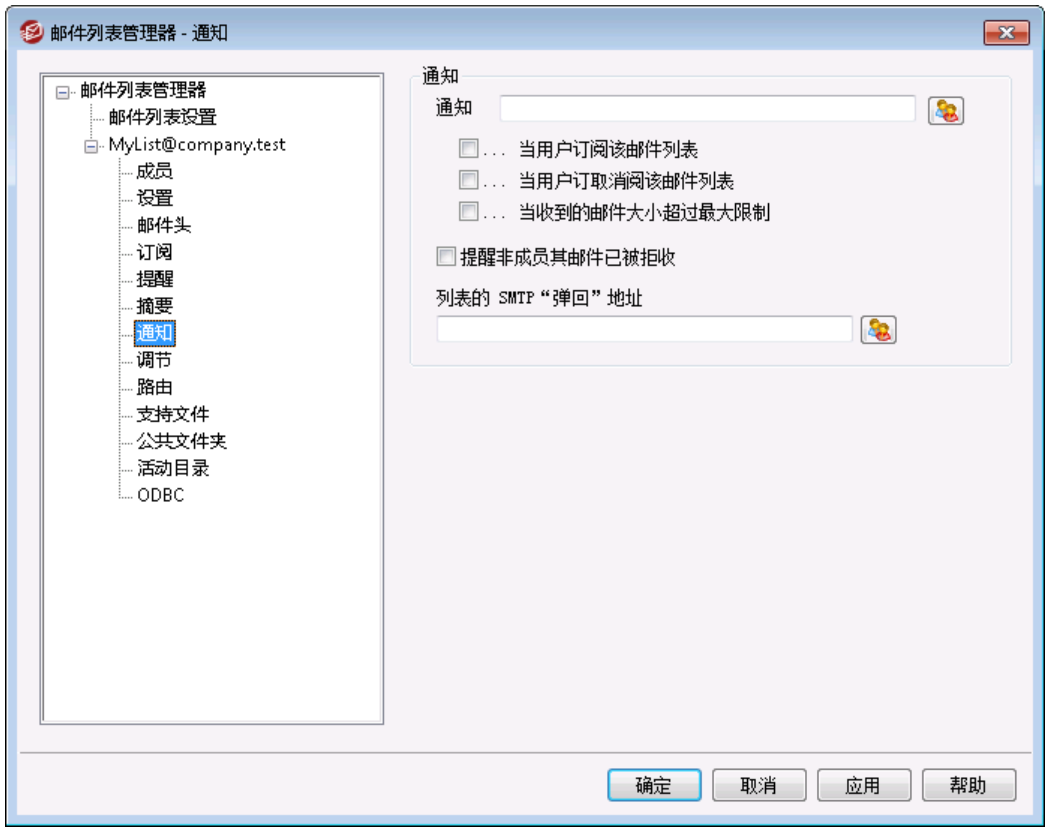
发送摘要邮件于上下午9，12，3，6时
使用该选项来调度每隔多久发送该列表的摘要。如果您勾选该选项中的所有选框，那么将每隔三小时发送一次摘要，任何可能由以下选项引起的事件除外。

假脱机摘要邮件如果 [xx]邮件累积到 (0 = 不适用)
如果您希望只要累积到一定数量的邮件就自动发送摘要，请在此处指定该数字。如果您不希望使用该选项则使用 "0"。"0"是默认设置。

还请参阅：

成员 228
通过电子邮件实现远程服务器控制 752

3.4.2.7 通知



通知

通知

当所选事件发生时，使用该选项以列出将被通知的地址。

...当用户订阅该邮件列表

如果您希望在每次有人订阅邮件列表时向指定的地址发送一个通知，请勾选该选框。

...当用户取消订阅该邮件列表

如果您希望在每次有人取消订阅邮件列表时向指定的地址发送一个通知，请勾选该选框。

...当收到的邮件大小超过最大限制

如果您希望在每次有人向邮件列表发送大于*列表拒绝大于 [xx] KB 的邮件*限制（其在设置 231 上指定）的邮件时，向指定的地址发送一个通知，请勾选该选框。

提醒非成员其邮件已被拒收

启用此项时，当不是私人列表的成员将邮件发送到列表时，MDaemon 将通知他们该列表是私人的。他们还将收到关于如何订阅列表的说明。使用*仅列表成员可以发送到该列表*选项，其位于设置 231，就可将列表指定为私人的了。

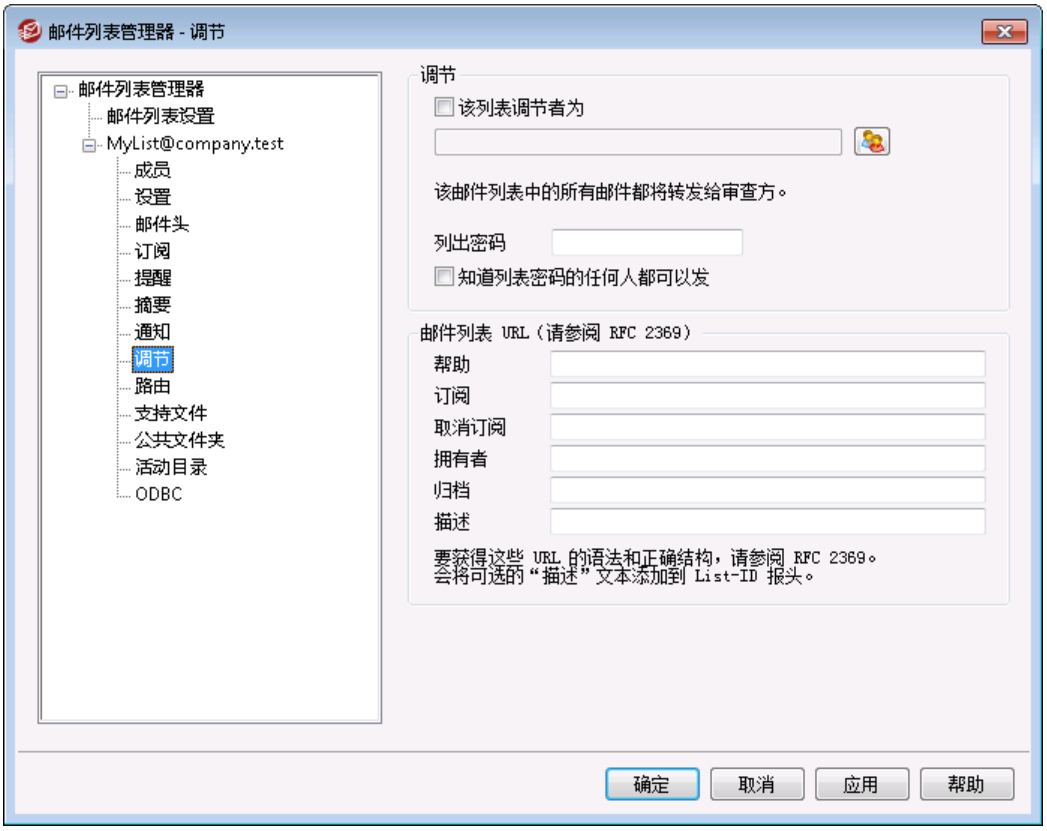
退回的邮件

列表的 SMTP "退回"地址

使用该选项以指定地址，该地址应该接收任何"退回"邮件或投递自列表产生的状态提示邮件。任何发往有 100 个收件人的邮件列表的指定邮件可能会有一些无法进行投递，比如，因为地址变更，服务器无法运作或其他原因导致有 10 个无法投递的地址。SMTP 系统将生成一封有关这些无法投递状态的通知邮件，并退回给此邮件的发件人。利用此项您可以指定地址，该地址应该接收您邮件列表的邮件。您还可以选择无人接收这些邮件，在这种情况下，MDaemon 会将列表邮件置入邮件流，这样一来就不可能退回邮件了。该地址不应该是邮件列表的地址。

将*"列表的 SMTP 退回地址"*设置成本地用户的地址，可能导致此用户的邮件被删除，因为在邮件列表设置 225。在将此项设置成本地用户的地址时，请谨慎。要获得更多信息，还请参阅"高级列表清理 232"。

3.4.2.8 调节



调节

该列表调节者为
如果您希望由指定用户来调节此列表，请勾选此框并指定一名账户。被调节的列表会将所有邮件转发至调节者。只有调节人可将这些邮件提交或转发至那个列表。

列出密码
如果您希望指定一个密码到该列表，请在此处输入。列表密码可以和以下的*知道列表密码的任何人都可以发*选项一起使用，以覆盖*成员限制*选项，其位于订阅屏幕 236 上。它们还能供您访问在*通过电子邮件控制远程服务器* 752 部分概述的若干功能。

知道列表密码的任何人都可以发
如果向列表指定了一个密码，并启用了该选项，那么在邮件主题的开头包含列表密码的任何人都可以向此列表进行邮件投递，即使发件人并非调节列表的调节者。

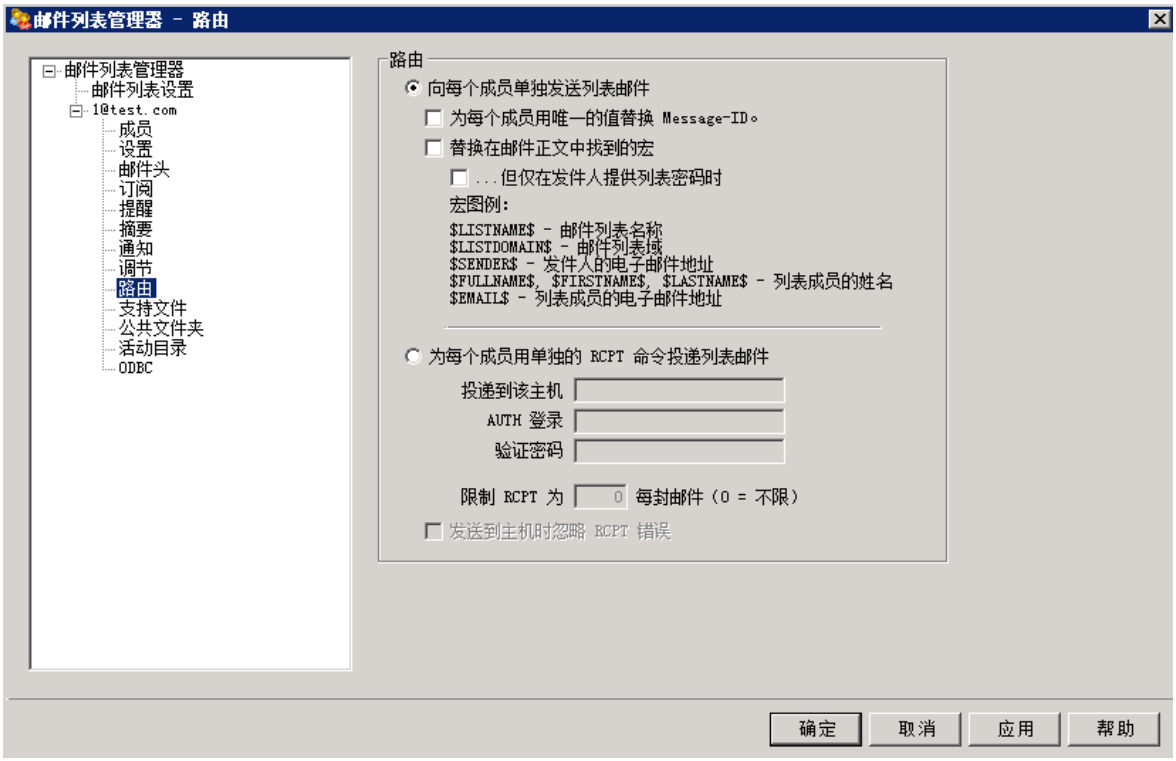
邮件列表 URL（请参阅 RFC 2369）

MDaemon 可以在邮件列表邮件中添加 RFC 2369 中概述的 6 个报头字段：*使用 URL 作为“核心邮件列表命令”及其“通过邮件标题字段传输”的元语法*。这 6 个报头是：**List-Help**、**List-Subscribe**、**List-Unsubscribe**、**List-Post**、**List-Owner** 和 **List-Archive**。如果您希望在列表邮件中使用上述任何报头，只需在下方任何字段中输入所需的报头值即可。这些报头值的格式必须严格按照 RFC 2369 规范（例如：<mailto:list@example.com?subject=help>）。请参阅链接文档来了解各个报头的若干示例。MDaemon 不更改这些数据，因此如果数据不正确，它将不实现任何结果。

描述（用于“List-ID:”报头）
如果您希望将邮件列表的简短描述添加到“List-ID:”报头内。将在此报头中包含这个描述和列表的标识符（例如：List-ID: “Frank 的个人邮件列表”<MyList.example.com>）注意：列表的标识符是邮件列表的地址，使用“.”取代“@”来符合“RFC-2919 的 List-ID 规范”。如果您留空“描述”选项，那么“List-ID:”报头将仅包含列表标识符（例如 List-ID: <MyList.example.com>）。如果一封入站邮件指向的列表已拥有“List-ID”: 报头，MDaemon 将为此列表使用合适的报头来取代旧报头。

默认情况下，在所有邮件列表邮件中包含 List-Subscribe 和 List-Unsubscribe 报头，如果您启用了“*准许 <List>-subscribe 和 <List>-unsubscribe 地址*”选项（位于“首选项 » 其他 421”屏幕。如果您希望为此列表覆盖这个选项，使用不同的报头值来取代由此项自动添加的报头值，请在此处输入所需值。如果禁用了此项，便不会将 List-Subscribe 和 List-Unsubscribe 报头添加到列表邮件，除非您在此处为其指定了一个值。

3.4.2.9 路由



路由

向每个成员单独发送列表邮件
如果选中此项，当收到分发至列表的邮件时，就会为每封邮件创建一个单独的副本并分发到每个列表成员。这将导致创建大量单独的邮件从而影响服务器的性能，这取决于列表大小与服务器上的负载。默认情况下，选中该选项。

为每个成员用唯一的值替换 Message-ID。
将 MDaemon 设置成为每个成员生成每封邮件的单独副本时，如果希望每封邮件具有唯一的邮件 ID，请点击此复选框。默认情况下，此选项是禁用的，除非您有特殊情况需要，否则不建议使用此项。

替换在邮件正文内找到的宏
如果您希望允许在邮件列表邮件中使用特殊的宏，请启用此选项。找到宏后，对于每封单独的邮件，MDaemon 会将其替换为宏代表的相应值，然后再将其发送给每个列表成员。

...不过仅在发件人提供列表的密码时
在邮件正文内允许宏的前提下，如果您希望需要列表的密码[243]来允许某些人在其邮件中使用宏，请点击此项。禁用此选项后，可以向列表发送邮件的任何人都可以使用宏。

宏：

$LISTNAME$	列表的名称、或列表地址的“邮箱”部分（例如 MyList@example.com 的“MyList”）。
$LISTDOMAIN$	列表的域（例如 MyList@example.com 的“example.com”）。
$SENDER$	邮件发件人的邮件地址。
$FULLNAME$ $FIRSTNAME$ $LASTNAME$	列表成员的全名、名字或姓氏（如果有）。
$EMAIL$	邮件地址的列表成员。

为每个成员用单独的 RCPT 命令投递列表邮件
如果选中该选项，MDaemon 会将每封列表邮件的单独副本路由到特定的智能主机，而不是向每个成员发送单独的邮件。在与指定的主机进行 SMTP 会话期间，该方法使用多重 RCPT To 语句。

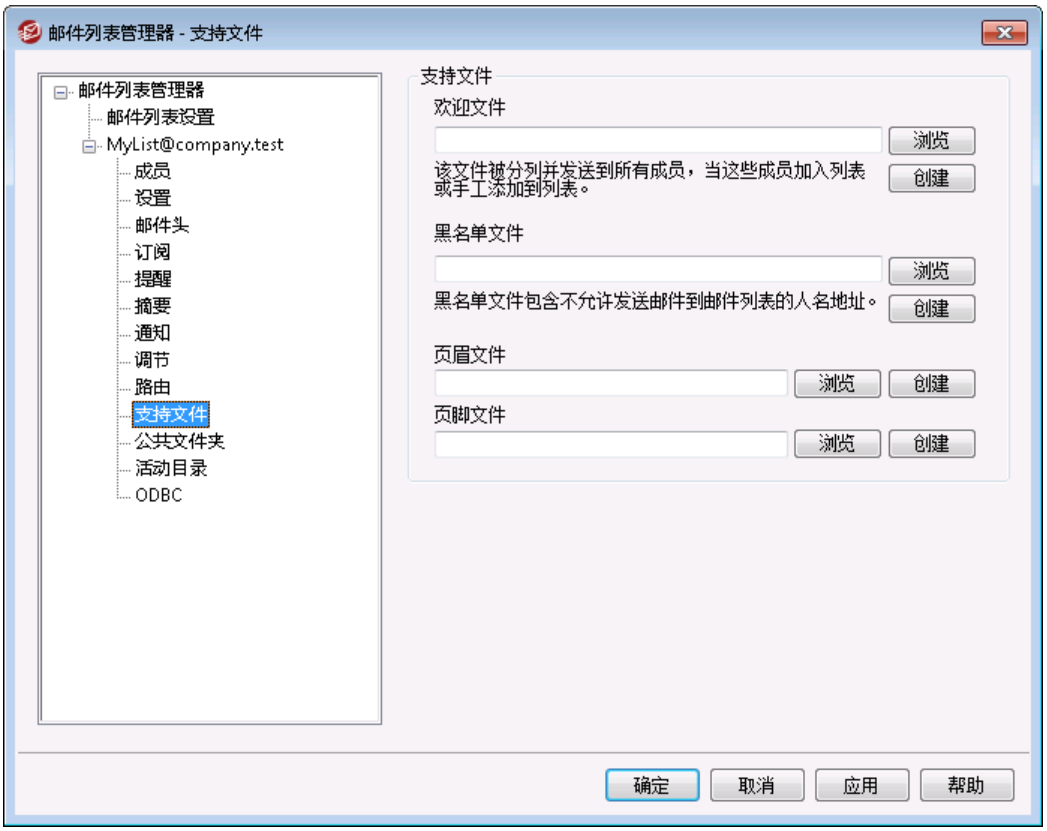
投递到该主机
指定您希望将列表的所有邮件投递到的智能主机，且为每个成员使用 RCPT To 语句。

AUTH 登录/密码
主机需要的任何登录凭证。

限制 RCPT 为 [xx]每封邮件 (0 = 不限)
当您试图通过主机路由单个邮件副本的时候，一些主机将会限制它们将接收到的 RCPT To 语句数量。如果您在此控件内指定了限制，MDaemon 会通过创建额外的邮件副本，并将列表划分成更小的群组来遵守所指定的限制。然后它会将邮件投递到那些群组，从而避免超出限制。这与以上的*"向每个成员单独发送邮件列表"*选项类似，但是它产生较少量的副本，向地址群组发送每个副本而不是为每个成员产生单独的副本。

发送到主机时忽略 RCPT 错误
由于一些智能主机拒绝为某些域的邮件进行排队或假脱机操作，已选择的发送路径会引起大量问题。从智能主机返回的一个错误代码会造成 MDaemon 投递任务的异常中断。如果您希望 MDaemon 忽略在投递列表邮件期间自智能主机返回的错误代码，从而允许已接收承担风险的成员接收列表邮件，请选中该选项。

3.4.2.10 支持文件



技术支持文件

欢迎文件
如果启用本功能，当新成员完成订阅后，此处所罗列的文件将会被处理并将其内容通过邮件发送至所有的新成员。您可以在新成员欢迎文件中使用以下的宏指令：

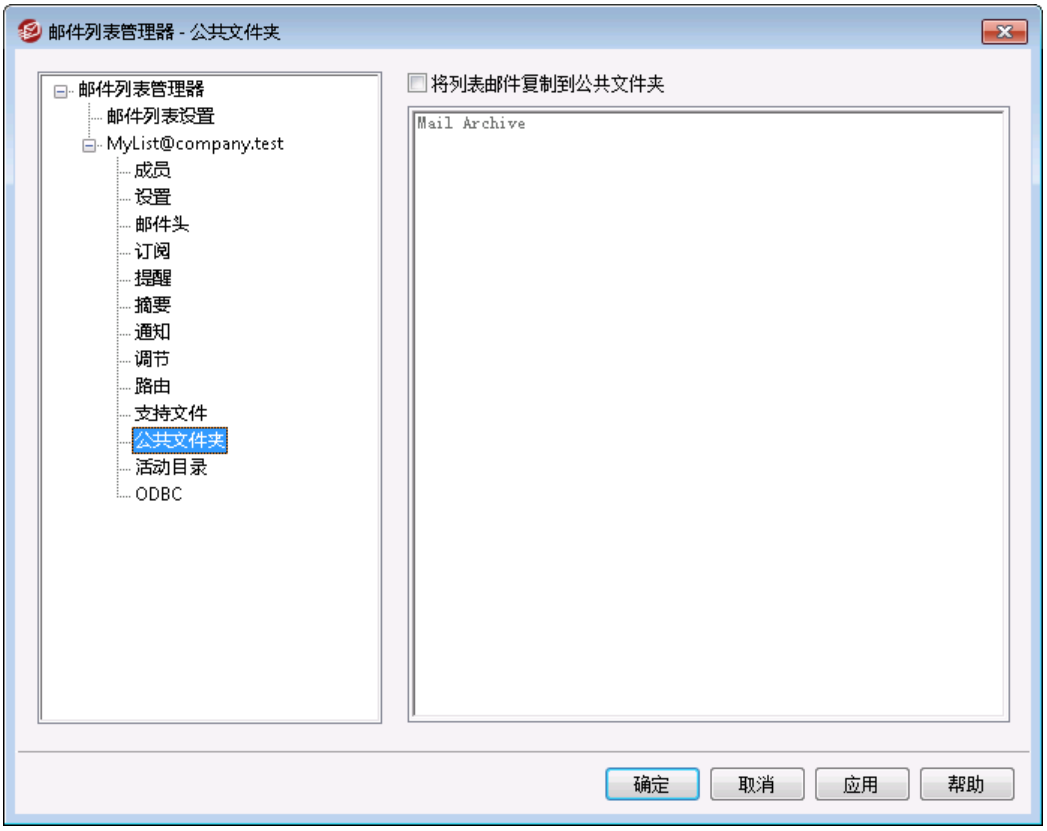
$PRIMARYDOMAIN$	该宏扩展 MDaemon 的默认域名，在域管理器[149]上指定。
$PRIMARYIP$	此宏将返回与 MDaemon 的默认域[149]相关联的 IPv4 地址。
$PRIMARYIP6$	此宏将返回与 MDaemon 的默认域[149]相关联的 IPv6 地址。
$DOMAINIP$	此宏将返回与这个域相关联的 IPv4 地址。
$DOMAINIP6$	此宏将返回与这个域相关联的 IPv6 地址。
$MACHINENAME$	该宏返回在域屏幕上指定的 FQDN 选项的内容。
$LISTEMAIL$	显示列表的邮件地址。示例：MyList@example.com
$LISTNAME$	显示邮件列表名。示例：MyList
$LISTDOMAIN$	该宏返回邮件列表的域。示例：example.com
%SETSUBJECT%	使用该宏以为欢迎邮件指定一个备用的主题。指定的主题文本可以包括其他列表宏，比如 $LISTEMAIL$。示例：%SetSubject%=Welcome to the $LISTNAME$ list.

阻止列表文件
如果启用这个功能，所列的文档将会用于禁止某些用户发来的邮件。

页眉/页脚文件
此处指定的文件内容将会作为列表邮件的页眉和/或页脚文件。

创建
要创建一个新文件，请点击*创建*按钮，该按钮对应您希望创建的文件，指定一个名称并点击*打开*。这将以记事本打开一个新创建的文件供您编辑。

3.4.2.11 公共文件夹

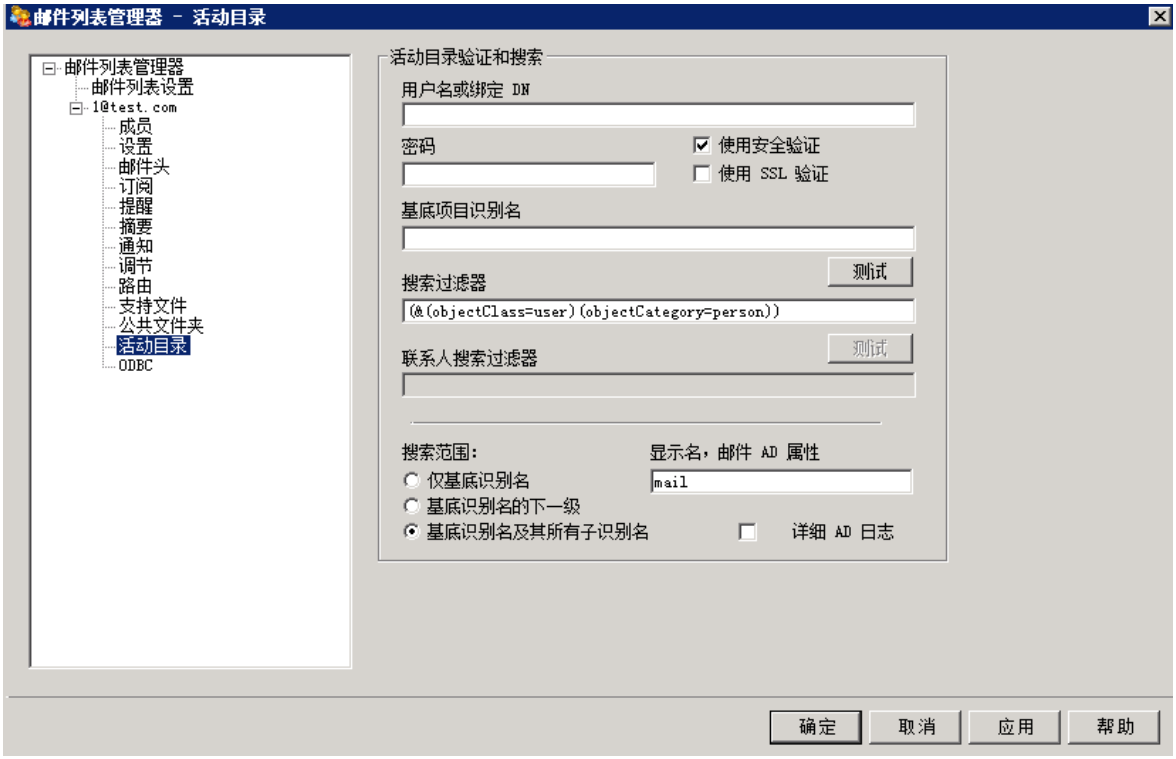


MDaemon 支持在邮件列表里使用公共 IMAP 文件夹[95]。不像个人 IMAP 文件夹，只是典型地供个人用户访问，公共文件夹是提供给 IMAP 用户的额外文件夹。位于该屏幕的这个选项，用于将发往此邮件列表的所有邮件自动复制到您的某一公共文件夹中。

将列表邮件复制到公共文件夹
如果您希望此列表的邮件除可以投递到本列表之外还被复制到您的某一公共文件夹中，请启用该控件。

选择公共文件夹
点击您希望与列表的邮件相关联的公共文件夹。。

3.4.2.12 活动目录



如果要从活动目录中获取列表成员地址，可以使用该屏幕中的选项。

活动目录 » 验证和搜索

用户名或绑定识别名
这是在通过 LDAP 绑定到 "活动目录"时 MDaemon 将使用的 Windows 账户登录或 DN。"活动目录"允许绑定时使用 Windows 账户或 UPN。

在此选项中使用识别名而不是 Windows 登录时，必须禁用或清除以下的 *"使用安全验证"*选项。

密码
这是在上述 *"绑定识别名"*选项中使用的识别名或 Windows 登录所对应的密码。

使用安全验证
执行活动目录搜索时如果要使用安全验证，请点击此复选框。当您在以上 *"绑定识别名"*选项中使用识别名而非 Windows 登录时，则无法使用本选项。

使用 SSL 验证
执行 "活动目录"搜索时如果要使用 SSL 验证，请点击此选择框。

使用该选项需要在您的 Windows 网络和 "活动目录"中存在 SSL 服务器和架构。如果不确定网络是否按此方式设置，请联系您的

IT 部门，并确定是否应启用该选项。

基底项目识别名
指定识别名 (DN)或目录信息树 (DIT)的起点，MDaemon 将从此处搜索活动目录的地址。您可以使用此选项中的 "LDAP://rootDSE"从 RootDSE 开始搜索，它是活动目录层次中最顶层的条目。指定更精确的起点，使其靠近您特定活动目录树中用户账户或所需组的地址，可以减少搜索 DIT 所需的时间。如果不想从活动目录中获取任何列表地址，请将该字段留空。

搜索过滤器
这是可以在搜索活动目录时使用的 LDAP 搜索过滤器。使用该过滤器可以使 MDaemon 更精确地定位您希望作为列表成员的用户账户或地址。

测试
使用这个按钮来测试您的搜索过滤器设置。

显示名、邮件 AD 属性
您必须使用此字段指定该列表使用的包含电子邮件地址的属性。比如，如果您在该字段里使用 "Mail"，则作为列表成员的每个活动目录帐户都必须使用 "Mail"属性，且该属性必须包含电子邮件地址。您还可以在电子邮件地址属性之前为列表成员的全名字段输入 "活动目录"属性，并用逗号分隔。例如，您可以输入："显示名，邮件"，而不仅是选项中的 "邮件"。第一个是全名所在的 "活动目录"属性，第二个是电子邮件属性。

搜索范围：
这是 "活动目录"的搜索范围或区域。

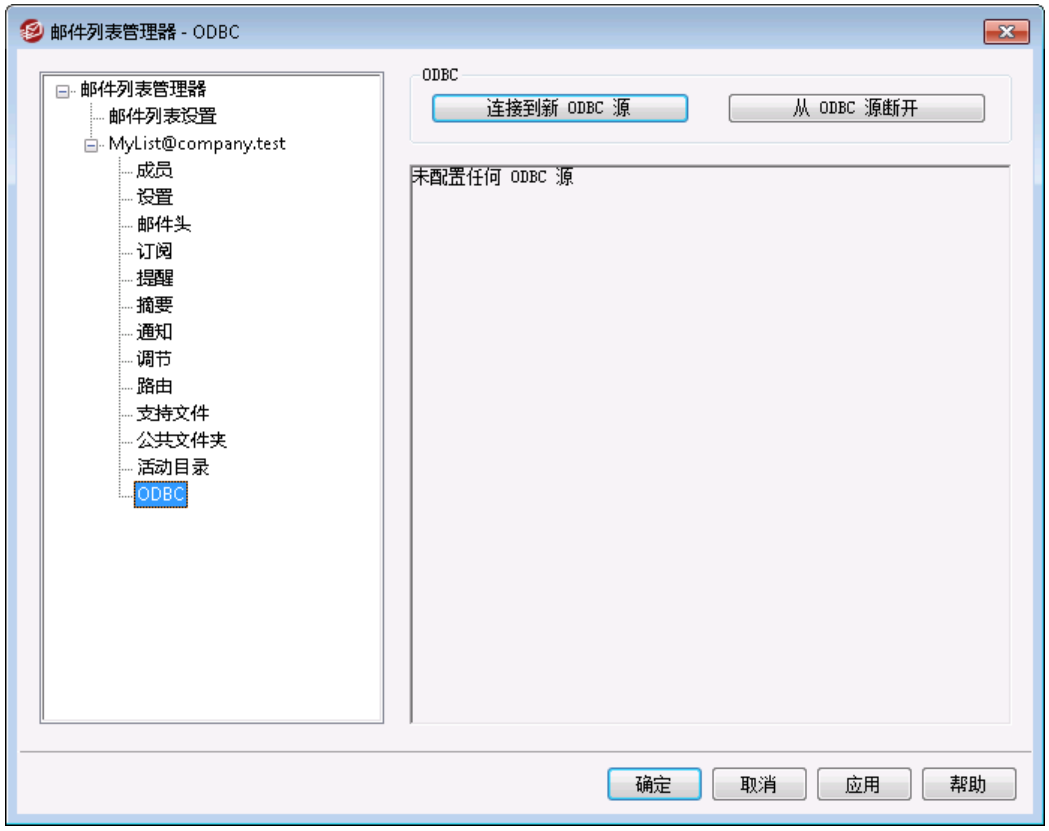
仅基底识别名
如果您搜索仅限制在如上所填的仅基底项目识别名的话，请选择该选项。搜索不会深入到目录信息树 (DIT)中该点的以下部分。

基底识别名的下一级
如果要将您的活动目录搜索扩展到您 DIT 中提供的基底识别名的下一级，请使用该选项。

基底识别名及其所有子识别名
该选项会将您的搜索范围扩展到提供的识别名及其所有的子识别名，一直深入到您 DIT 中最底层的子条目。

详细 AD 日志
根据默认，MDaemon 将为 "活动目录"使用详细日志。如果您希望所使用的 "活动目录"日志无需非常详细，请清除该选择框。

3.4.2.13 ODBC



使用该功能您可以在 ODBC 适应数据库里维持一个列表的成员列表。邮件列表编辑器的 ODBC 屏幕是用来为 MDaemon 选择数据源，图表和字段映射使之能链接到列表。当邮件发送到您的列表时，将会有一个或多个 SQL 询问自动执行，产生的邮件地址也会作为列表成员之一。

您可在数据库中使用您选择的任一 ODBC 适应的数据库应用程序来添加，删除以及修改您的列表成员。

ODBC

这部分显示了您当前为邮件列表设置的 ODBC 属性。它显示了数据库中您已经配置好的字段映射与 SQL 查询，以指定每一个成员的会员资格状态（比如普通、只发送、只读、和/或摘要模式）。

连接到新 ODBC 源
点击此按钮以打开 ODBC 选择向导来选择您希望在邮件列表上使用的系统数据源。

从 ODBC 源断开
点击该按钮以断开以上列出的 ODBC 数据源的列表。

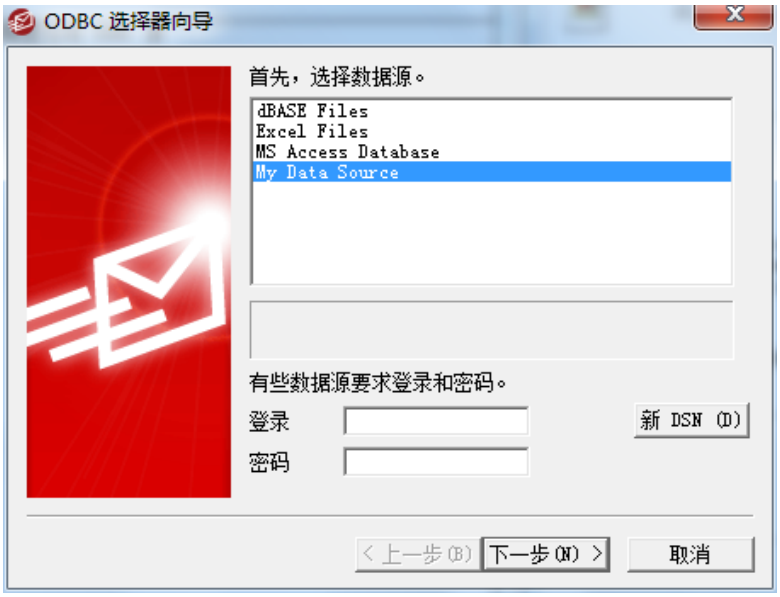
还请参阅：

为邮件列表配置 ODBC 系统数据源 252
创建一个新的系统数据源 254

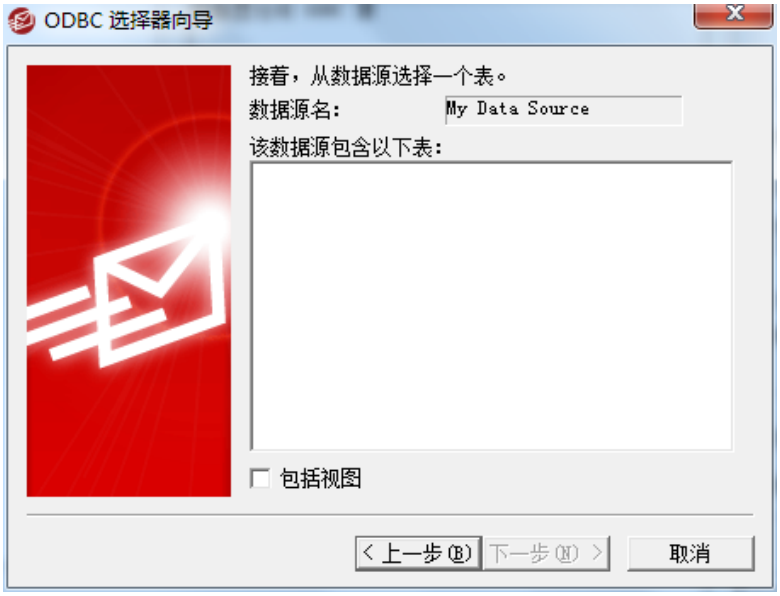
3.4.2.13.1 配置 ODBC 数据源

将 ODBC 可存取数据库与邮件列表一起使用：

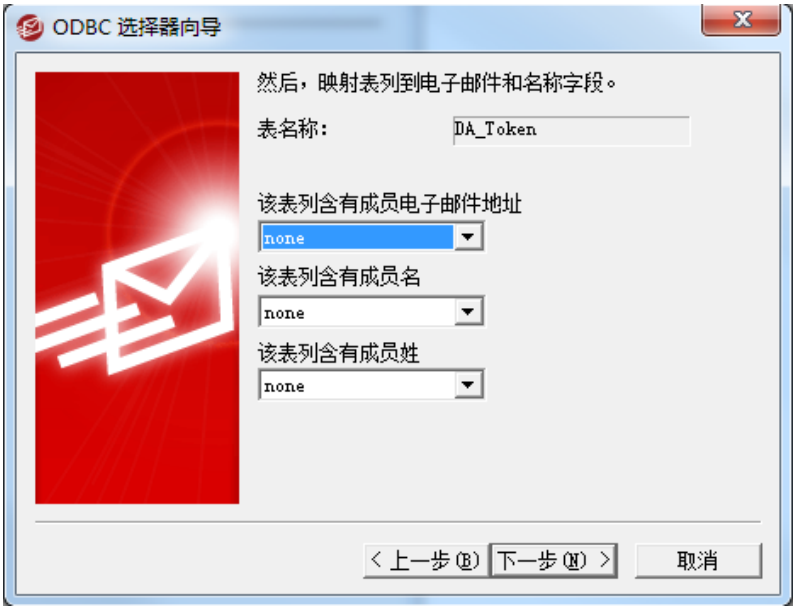
1. 在邮件列表编辑器的 ODBC 屏幕 251 上，点击 **连接到新 ODBC 源**”以打开 ODBC 选择器向导。



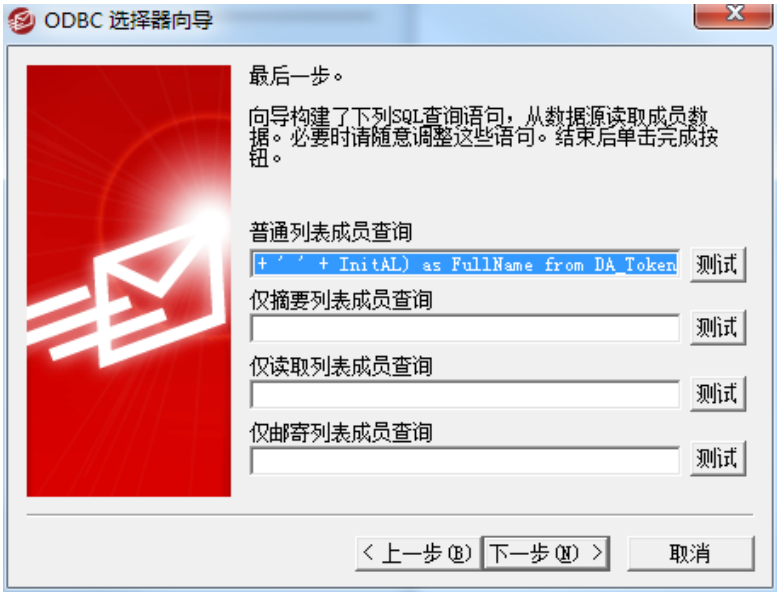
2. 选择您希望用于邮件列表的 **数据源**”。如果列表中没有兼容的数据源，请点击 **新建 DSN**”并根据以下列出的指导说明，创建新的 ODBC 数据源 254。
3. 需要时，请输入数据源的 **登录名**”和 **密码**”。
4. 点击 **下一步**”。
5. 数据源必须包含至少一个表以及填写地址和姓名的字段。如果此数据源包含一个或更多符合要求的表，选择合适的表并点击 **下一步**”。否则，请点击 **取消**”以退出 ODBC 选择向导，然后在下一步骤前使用您自己的数据库应用程序以将表添加至相应的数据库。



6. 使用下拉列表框指明与 **"邮件地址"**, **"姓"**及 **"名"**对应的图表字段。点击 **"下一步"**。



7. ODBC 选择向导会根据您在**步骤 6** 中的选择来创建一个 SQL 查询语句。MDaemon 会使用它以从您的数据库中检索普通列表成员数据。您可编辑此语句为希望检索到的，并在剩余的控键中包括进其余询问语句，使成员在摘要模式中接受邮件，也可指定成员类型为 **"只读"**或 **"仅发送"**。每个控制旁都提供一个 **"测试"**按钮，这样您可以测试您的查询语句以确保它们会取回正确的数据。配置完您的查询语句后，请点击 **"下一步"**。



8. 请点击 **完成**”。

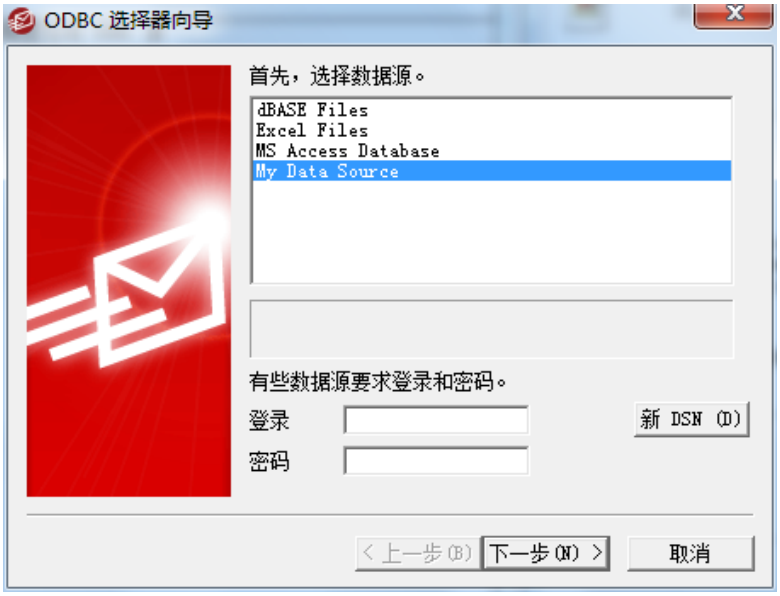
还请参阅：

邮件列表编辑器 » ODBC 251
创建新的 ODBC 数据源 254

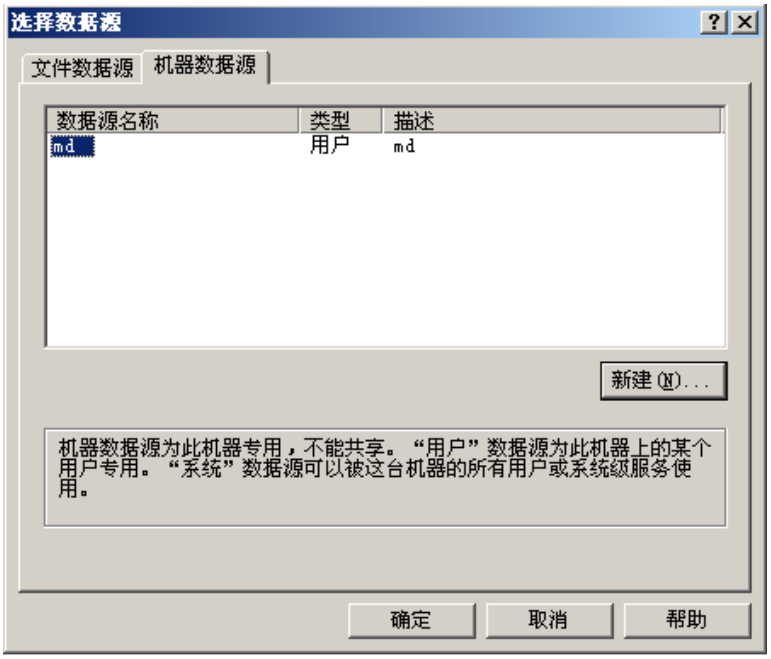
3.4.2.13.2 创建新的 ODBC 数据源

通过邮件列表创建一个新的 ODBC 系统数据源供使用：

1. 在邮件列表编辑器的 ODBC 屏幕 251 上，点击 **连接到新 ODBC 源**”以打开 ODBC 选择器向导。
2. 点击 **新建 DSN**”以打开 “选择数据源”对话框。



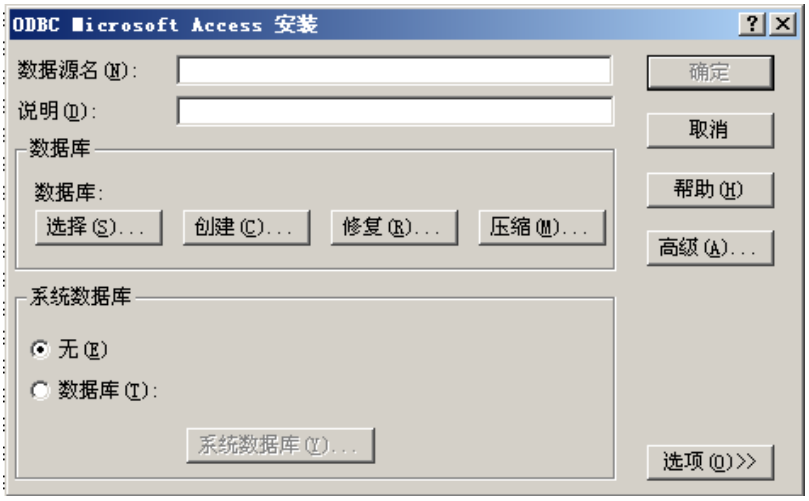
3. 切换到 **机器数据源**”选项卡并点击 **新建...**”以打开 创建新数据源”对话框。



4. 选择 **系统数据源**”并点击“**下一步**”。

5. 选择您想为其安装数据源的**数据**库驱动,**并点**击"**下一步**"。

6. 点击 **完成**"来显示指定驱动的安装对话框。此对话框的样式会根据您所选的不同驱动程序而改变 (以下为 "Microsoft Access 安装"对话框)。

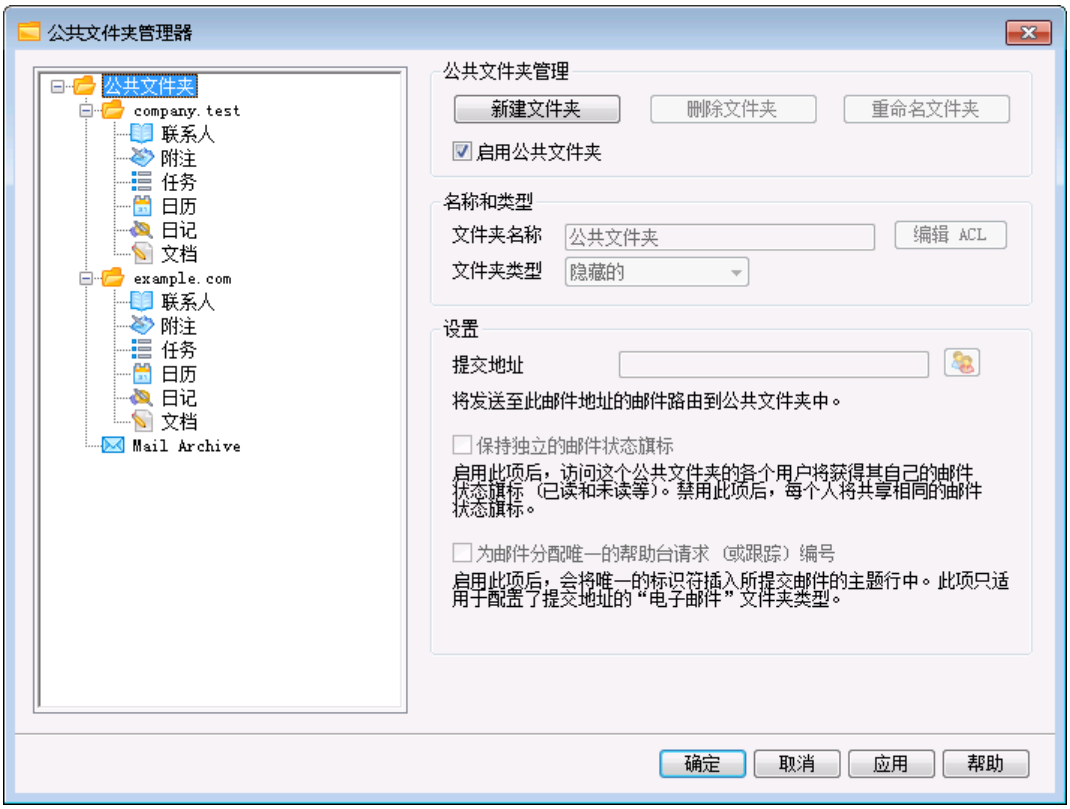


7. 为您的新数据源指定一个 **数据源名称**"并填写指定驱动对话框所要求的任何其他信息（比如创建或指定一个数据库，请选择目录或服务器等）。
8. 点击 **确定**"以关闭特定的驱动对话框。
9. 点击 **确定**"以关闭 "选择数据源"对话框。

还请参阅：

ODBC——邮件列表 251
为邮件列表配置 ODBC 系统数据源 252

3.5 公共文件夹管理器

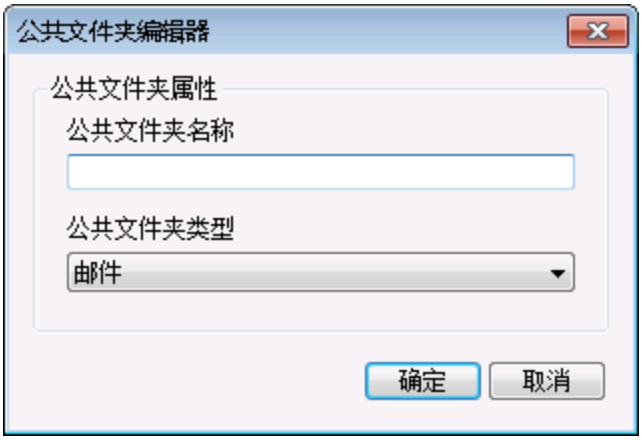


使用此屏幕来管理您的公共文件夹[95]。要抵达“公共文件夹管理器”，请点击“设置» 公共文件夹管理器...”。

公共文件夹管理

新建文件夹

要新建一个公共文件夹，请在列表中选中您想作为其父文件夹的文件夹，然后点击*新建文件夹*。为您的文件夹输入一个名称，选择文件夹类型，然后点击*“确定”*。



删除文件夹
要从列表中删除公共文件夹，选择所需文件夹，然后点击 *"删除文件夹"*按钮。

重命名文件夹
要重命名一个公共文件夹，请选定一个文件夹，然后点击 *"重命名文件夹"*。输入一个新名称并点击 *"确定"*。

启用公共文件夹
如果您希望允许用户获得公共文件夹的访问权，请点击此框。通过选定一个文件夹并点击 *"编辑 ACL"*按钮，来控制可以进行访问的用户和授予的访问权限级别。

名称和类型

文件夹名称
此框显示您在这个列表中选定的文件夹的名称。会将此屏幕上的其余选项应用到选定的文件夹。

文件夹类型
使用下拉列表来指定文件夹类型：邮件、联系人、日历等。

编辑 ACL
选择一个文件夹，然后点击该按钮打开此文件夹的 "访问控制列表 260"对话框。使用 "访问控制列表"来指定能访问此文件夹的用户或群组，以及每个用户或群组的权限。

设置

提交地址
输入本地电子邮件地址或选择特定的 MDaemon 账户与共享文件夹关联，这样指向 *"提交地址"*的邮件将被自动路由到共享文件夹。然而，只有那些被授予了该文件夹 "投递"权限的用户才能发送到此地址。

保持独立的邮件状态旗标
如果希望按用户而不是在全局范围内设置该文件夹的邮件旗标（已读、未读、已答复、已转发等），请点击该复选框。每个用户都可以按照他们与邮件进行的交互，在共享文件夹中查看显示的邮件状态。未读取邮件的用户看到该邮件标记为“未读”，而已读取该邮件的用户看到的状态为“已读”。如果禁用该选项，所有用户都将看到相同的状态。因此，一旦有用户读取了邮件，则所有用户都将看到该邮件标记为“已读”。

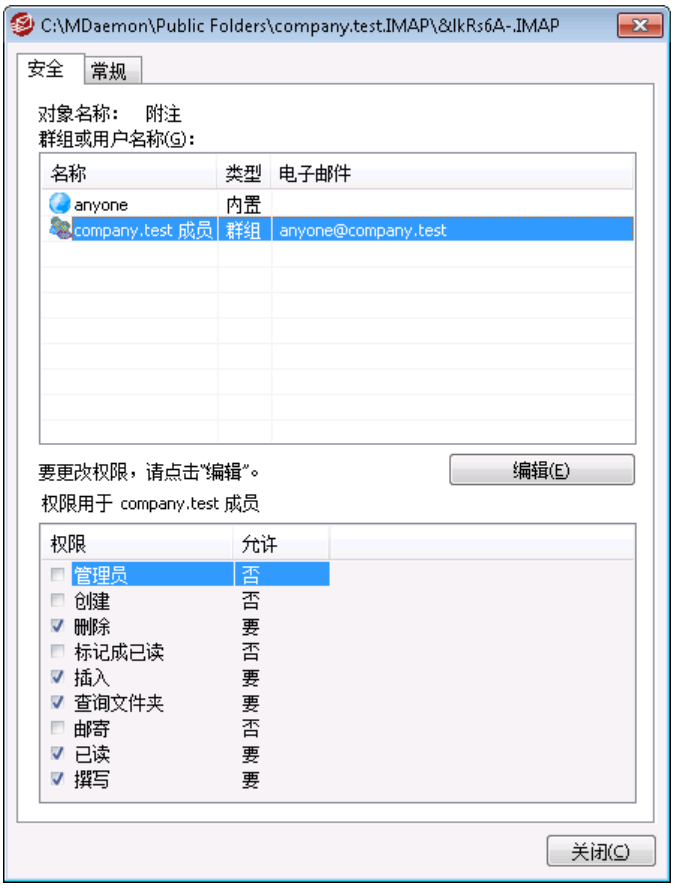
为邮件分配唯一工单（或跟踪）号
如果您希望将公共文件夹配置成通过邮件提交帮助台请求的公共文件夹，请使用此项。MDaemon 会将*文件夹名称*和唯一标识符添加到发送至公共文件夹*提交地址*的邮件主题中。拥有这种特殊格式化主题的任何出站邮件会将其发件人地址更改成此公共文件夹的提交地址，并将这封出站邮件的副本放置到公共文件夹中名为 "Replied To（收件人）"的子文件夹中。此外，会将拥有这种特殊格式化主题的任何入站邮件自动重定向到这个公共文件夹，无论该邮件被发送至哪个地址。

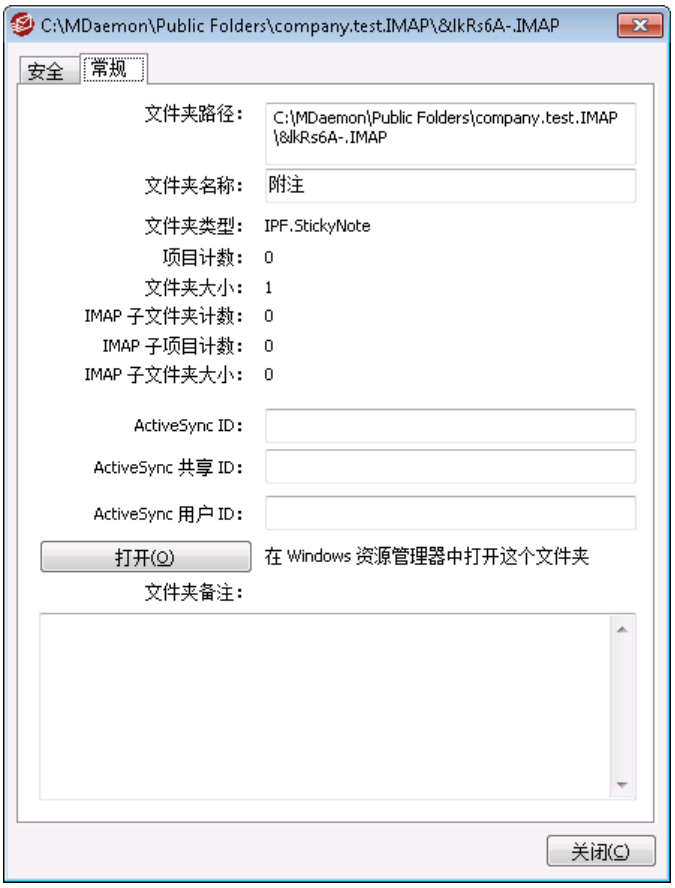
还请参阅：

访问控制列表 260
公共文件夹概述 95
公共文件夹和共享文件夹 97
账户编辑器 » 共享文件夹 623
邮件列表 » 公共文件夹 248

3.5.1 访问控制列表

访问控制列表 (ACL)用来为您的公共和共享文件夹 95设置用户或群组访问权限。可以从 *"编辑 ACLs"*按钮 (位于公共文件夹管理器 258)或 *"编辑访问控制列表"*按钮 (位于 "账户编辑器"的 "共享文件夹 623"屏幕)访问此项。





安全

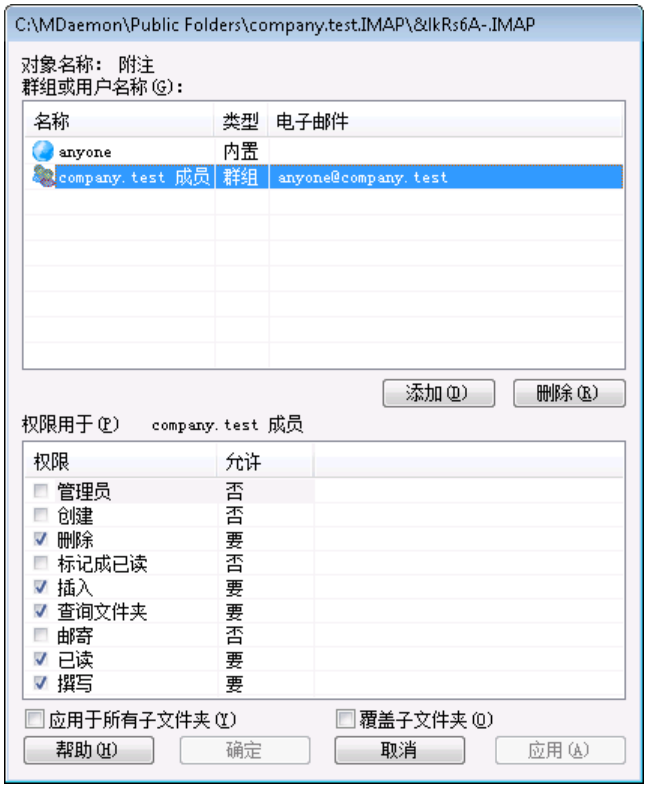
此选项卡显示与文件夹相关联的群组或用户列表，以及授予各自的特定访问权限。选择此列表中的一个群组或用户来显示其权限[263]，以便在下方的“权限”窗口中审核。要编辑这些权限，请点击“编辑[262]”。

常规

该选项卡显示文件夹的属性，例如其路径、名称、类型和大小等。

ACL 编辑器

点击 ACL“安全”选项卡上的“编辑”来打开 ACL 编辑器修改访问权限。



对象名称
这是将应用 ACL 权限的对象或文件夹的名称。

群组或用户名
这些是将授予一些访问权限级别的群组或用户。选择群组或用户，以便在下方的 *"群组或用户>权限"*窗口中显示。对于您希望授予群组或用户的任何访问权限，请勾选其附近的选框。

添加
要向未列于上方的群组或用户授予访问权限，请点击 "添加 264"。

删除
要删除一个群组或用户，请选择上方列表中相应的条目并点击 **"删除"**。

<群组或用户>(<group oruser>)权限
对于您希望授予上方选定的群组或用户的任何访问权限，请勾选其附近的选框。

您可以授予以下访问控制权限：

管理员——用户可管理该文件夹的访问控制列表。

创建——用户可在该文件夹中创建子文件夹。

删除——用户可从该文件夹中删除项目。

标记已读——用户可更改该文件夹中邮件的已读/未读状态。

插入——用户可以添加或复制项目到该文件夹中。

查询文件夹——用户在其个人 IMAP 文件夹列表中可以看到该文件夹。

投递——用户可直接发送邮件到该文件夹中 (如果文件夹运行的话)。

读取——用户可打开该文件夹并查看其内容。

写入——用户可以更改该文件夹中邮件的标记。

应用于所有子文件夹
如果您希望向文件夹当前包含的任何子文件夹应用这个文件夹的访问控制权限，请勾选此框。这将向这些子文件夹添加这个文件夹的用户和群组权限，并在发生任何冲突时进行替换。不过它不会删除当前对这些文件夹拥有访问权限的任何其他用户或群组权限。

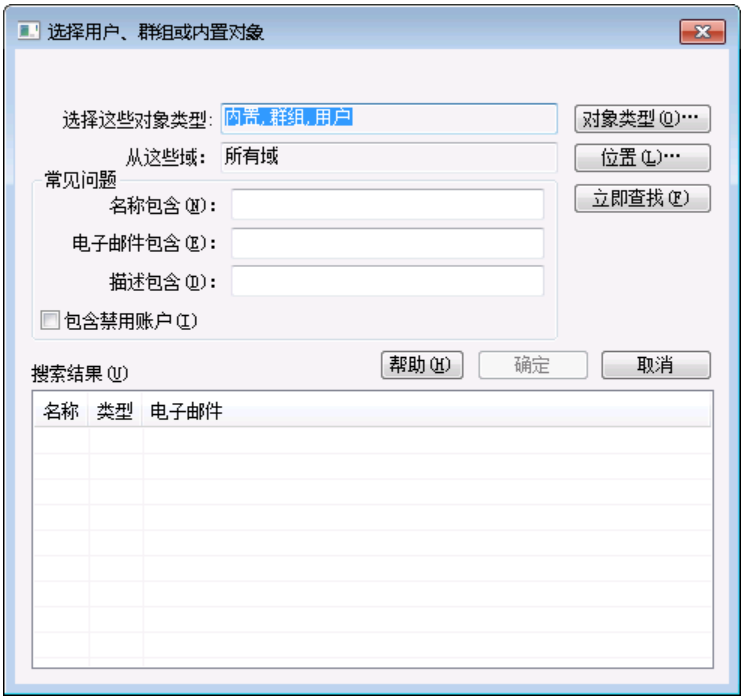
举例来说，

父文件夹向 User_A 和 User_B 授予特定权限。子文件夹向 User_B 和 User_C 授予访问权限。此项会将 User_A 权限添加到子文件夹，并使用父文件夹的权限来替换子文件夹的 User_B 权限，对 User_C 的权限不做任何操作。因此，这个子文件夹将拥有 User_A、User_B 和 User_C 的权限。

覆盖子文件夹
如果您希望使用父文件夹的当前权限来替换所有子文件夹的访问权限，请勾选此框。子文件夹的权限将与父文件夹的权限相同。

添加群组或用户

如果您希望将其他群组或用户添加到 "访问控制列表"，请点击 "ACL 编辑器"上的 "**添加**"。这将打开 "添加群组"或 "用户"屏幕，您可以使用这两个屏幕来进行添加。



选择这些对象类型
点击 "**对象类型...**"来选择您希望为要添加的群组或用户搜索的对象类型。您可以选择："内置"、"群组"和 "用户"。

从这些位置
点击 "**位置...**"来选择您希望搜索的域。您可以选择所有 MDaemon 域或特定的域。

常规查询
使用这一部分的这些选项，通过指定所有或部分用户名、邮件地址或账户描述[598]的内容来缩小您的搜索范围。如果您希望这些搜索结果包含与上方指定的 "对象类型"和 "位置"相匹配的各个群组和用户，请留空这些字段。

包含 "禁用账户"
如果您希望在搜索中包含 "禁用账户[598]"，请勾选此框。

立即查找
在您指定了所有搜索条件之后，请点击 "**立即查找**"来执行搜索。

搜索结果
执行完搜索后，请在 "搜索结果"中选择任何所需群组或用户，并点击 "**确定**"来将其添加到 ACL。

访问权限可通过 MDaemon 对访问控制列表 (ACL) 的支持进行控制。ACL 是 Internet 邮件访问协议 (IMAP4)的扩展，它使您得以为每个 IMAP 邮件文件夹创建访问列表，从而将文件夹访问权限授

> 予在您的邮件服务器上拥有账户的其他用户。如果您的邮件客户端不支持 ACL，您仍可通过本对话框内的控件设置权限。
>
> 在 RFC 2086 中对 ACL 作了完整讨论，可访问以下网址来查阅该文档：http://www.rfc-editor.org/rfc/rfc2086.txt。

还请参阅：

公共文件夹管理器 258
公共文件夹概述 95
公共文件夹和共享文件夹 97
账户编辑器 » 共享文件夹 623
邮件列表 » 公共文件夹 248

3.6 Web & IM 服务

3.6.1 Webmail

3.6.1.1 概述

MDaemon Webmail是包含在 MDaemon 中的一个基于 web 的电子邮件解决方案，设计用来让用户使用他们自己喜欢的 web 浏览器获得邮件客户端功能。相对传统邮件客户端而言，Webmail可以很轻松地进行控制，只要用户有因特网或网络连接 Webmail就能提供它自身能力的附加优点以保证用户可以任何时间任何地点访问他们的电子邮件。此外，因为用户所有的邮件文件夹，联系人，日历等都位于服务器上而不是他们的本地计算机上，所以他们可以随时访问所有数据，就仿佛坐在办公桌前办公。

MDaemon Webmail也为邮件管理员提供许多便利。因为 Webmail不是独立的工作站，您可以从服务器配置所有选项，与大量客户端应用程序的用法不同。帮助您不用配置和维护每个单独的邮件客户端。您还可以在 Webmail中自定义图形图片和 HTML 页面，以满足您的企业或客户的需求。此外，您可以给予用户权利让他们维护自己的账号设置，这样就节省了您的时间——您可以根据自己的需要给予用户或多或少的控制权限。

最后，除了有一个非常方便的基于 web 的客户端外，WorldClient 还有许多其他功能为您的用户带来利益，比如：扩展邮件功能、约 30 种语言的客户端界面、私人和全局地址簿、可进行管理的邮件文件夹与过滤器、发送/接收文件附件、多视觉界面 “主题”、移动设备主题、日历功能、群件功能、可以下载到您桌面的集成化即时通信等等。

日历和调度系统

MDaemon 配备了一套完整的日历和时间日程协作系统。从 Webmail中您可以简单地创建约会，安排会议以及照地址簿工作。完全支持复发约会，而且提供大量可用字段对约会进行描述。此外，联系人、日历以及任务数据都作为 IMAP 文件夹储存在每个用户的根邮件目录里。通过 Webmail，您的用户可以访问这些个人文件夹并控制哪些其他用户可以访问它们。所有 Webmail主题都有模板，会以既富逻辑性又充满吸引力的方式显示联系人，日历，通知，任务文件夹。

由于日历系统是集成到 MDaemon 中的，因此无论是由您还是由第三方安排的约会，都会有约会邮件通知的附加便利。无论何时，如果其他人为您安排了一个约会，您将收到一封电

子邮件信息，其中概括了这个约会。每一位指定的约会参与者都将收到一封详述约会日期、时间、地点、主题和参与者列表的电子邮件。此外，在安排上与约会时间档有冲突的参与者，都将收到一封提醒他们会议和时间表上有安排冲突的提示。安排会议的人将会收到一封显示所有会议细节和可以参加会议或因安排有冲突不能参加的邀请人的名单。

日历系统也支持 Microsoft Outlook 使用的 Internet 日历 (iCal)和其他电子邮件程序所适用的 iCalendar。日历系统可以检测并执行 iCanlendar 信息发送到您的用户，从而更新他们的日历。当用户从 Webmail中打开 iCalendar 附件时，其中包含的信息会反映到用户的 Webmail日历中。而且，当用户创建新的会议或者约会时，它们可以列出一个或者多个用户希望 iCalendar 电子邮件将被发往的邮件地址。该功能可以由个人用户通过他们的 Webmail选项来设置。

MDaemon Instant Messenger

MDaemon Instant Messenger (MDIM) 是 MDaemon 的安全即时通讯 客户端和托盘小程序，提供对于 Webmail邮件功能的快速访问。每个 Webmail用户都可以下载 MDIM，然后安装到个人用户的本地计算机上。可以在下载时，为特殊用户预先配置它，将需求限制为对其进行手动配置。

在后台运行的 MDIM，会通过直接询问 Webmail服务器来检查您账户中的新邮件。这样可以避免打开一个浏览器或者保持一个浏览器以检查您的电子邮件——MDIM 会检查新邮件并且当有新邮件到达时，用声响或者可视化提示来提醒您。MDIM 也会显示您的邮件文件夹以及每个文件夹内所含邮件数量与类型的列表。 (新，未读，已读)。而且，它可以用来启动您的浏览器，并立即将它移至指定的邮件文件夹中。

MDIM 还配备了一个完整的即时通讯客户端。您可以查看您的 MDIM 联系人和每一位在线状态 (在线，离开，离线)的列表，启动任意成员或者一组成员的对话，设置您自己的在线状态，以及在历史文件夹中查看过去的通话记录。

更多关于如何使用 MDaemon Instant Messenger的特定指令，请参阅其在线帮助系统。

MDaemon Instant Messenger的即时通讯系统

MDIM 配备了使用 MDaemon XMPP 312 服务器的即时通讯 (IM)客户端。使用此功能，您可以将共享您域 (以及可选的 MDaemon 服务器上托管的其他域)的其他用户添加到 MDIM 联系人列表，然后立即与他们进行通信。您可以设置在线状态，查看联系人的状态，使用表情符号，设置文本颜色，发送文件，设置通知声音和控制其他首选项。您也可以一次性发起涉及多个联系人的群聊。所有 IM 功能都可以通过 MDIM 窗口中托盘图标的快捷菜单获得。

MDaemon Instant Messenger的 IM 系统也是可编写的，允许在界面上自定义程序。通过在\MDaemon\WorldClient\文件夹里创建信号 (SEM)文件，外部的应用程序可以向您的 MDIM 用户发送即时消息。以下是 SEM 文件格式：

收件人： user1@example.com	MDIM 用户的电子邮件地址
发件人： user2@example.com	即时消息发送者的电子邮件地址。
<blank line>	
即时消息的文本。	这是作为即时消息发送的文本。

SEM 文件名必须以“字母 IM-”开头，后面必须跟随唯一的数字值。例如，“IM-0001.SEM”。应用程序将会创建一个对应的文件叫做“IM-0001.LCK”来锁定“SEM”文件。一旦 SEM 文件移除了 LCK 文件，则开始处理 SEM 文件。MDaemon 使用此脚本方案来发送即时消息，提醒您即将到来的约会和会议。

内容过滤器系统配备了一项使用此脚本方案来发送即时消息的操作。而且，使用该操作的规则可以在 IM 中使用内容过滤器宏。例如，您可以创建一条规则来发送包含类似以下行的即时消息规则：

```
You have received an email from $SENDER$. 您从 $SENDER$ 收到了一封电子邮件）
主题：$SUBJECT$
```

此规则是通过 MDIM 发送新邮件提示的一个有效方法。

由于考虑到集中式账户管理的固有缺陷，以及传统检测 IM 通信量和众所周知的 IM 客户端的不足，许多企业和管理员对在他们的公司内部使用 "即时通讯"系统持保留意见，因此我们用 MDIM 的即时通信系统来弥补这种不足。首先，我们的系统不是点对点的——个人 MDIM 客户端不会直接连接到其他客户端来进行即时通讯。而且因为每个即时消息都要通过服务器，每一个信息都被记录在 MDaemon 管理员可访问的中心位置。这样就能维护所有的会话记录，保障了您公司和您员工或用户的安全。记录 IM 活动的文件叫做 XMPPServer-<date>.log，位于 MDaemon\LOGS\ 目录中。

Instant Messaging 按域提供。激活即时通讯的全局控件位于 Webmail对话框的 MDIM 屏幕 278 (设置» Web & IM 服务» Webmail» MDIM)。域管理器 156上有一个类似的选项，用于为特定域启用或禁用此功能。

MDaemon Instant Messenger 皮肤

MDIM 的界面与 *msstyles* 皮肤兼容，便于从因特网获得。包括若干样式，不过要安装新样式，请下载 *.msstyles 文件并将其放在 MDIM \Styles\ 文件夹下的子文件夹中，子文件夹名与该文件名相同。例如，如果这个文件叫做 Red.msstyles，则该文件的路径应为："\.\Styles\Red\Red.msstyles"

Dropbox 集成

已向 Ctrl+W |Webmail|Dropbox 添加了一个新屏幕。您可以在此处找到控件，在其中输入 Dropbox "应用程序密钥"，"应用程序面"和隐私策略文本。上述这些都是必填的，以便启用集成服务，并且当您通过访问 Dropbox 网站注册 MDaemon Webmail为 Dropbox 的 "应用程序"时，可以获得这些信息。我们不能为您完成这些步骤，但只需要完成一次即可。请参阅知识库文章 1166 来获取如何注册您的 Webmail作为 Dropbox 应用程序的完整指示。

一旦配置了 "应用程序密钥"和 "应用程序密码"，Webmail就可以将其账户连接到 Dropbox 账户。用户首次登录到 Webmail主题或 LookOut 主题时，将在页面顶部显示一个下拉列表。用户有三个选项，查看下次登录的下拉列表，不再显示，或转到新的 "选项 | 云端应用程序"视图。在 "选项 | 云端应用程序"视图上，用户可以点击 "设置 Dropbox"按钮。这将打开 OAuth 2.0 弹窗。该弹窗详细说明了用户正在连接的内容，以及 Webmail要求的授权。还提供指向隐私策略的链接和 "连接到 Dropbox"按钮。一旦用户点击 "连接到 Dropbox"按钮，页面将导航到 Dropbox。如果用户没有登录到 Dropbox，Dropbox 将提供一个网站供他们登录或创建一个账户。完成此步骤后，用户将看到另一个 Dropbox 页面，询问用户是否希望允许 Webmail对其账户进行完全访问。点击 "允许"，将使用户回到 Webmail，告诉用户授权是否成功。该授权在一个星期内有效，之后再次显示相同的屏幕，并获得另一个访问令牌并用于下一周。授权完成后，用户将在每封邮件附件旁边显示一个 Dropbox 图标。点击图标将导致附件保存到 /WorldClient_Attachments 文件夹下用户的 Dropbox 账户中。

在 WorldClient 和 LookOut 主题的编写视图中，用户可以通过点击 HTML 编辑器工具栏中的 "Dropbox"图标 (左上角)从其 Dropbox 账户中选择文件。此功能不需要用户通过 "选项 | 云端应用程序"视图和 OAuth 2.0 设置对其账户的访问 。这只需要 "应用程序密钥"和 "应用程序密码"。

默认情况下禁用 Dropbox 支持，但可以在 MDaemon 的 Dropbox 282 屏幕上启用。如果您希望按用户启用或禁用 Dropbox，可以通过在 User.ini 文件中添加 "DropboxAccessEnabled=Yes"来实现这点。

使用 Webmail

启动 Webmail

有三种方法可以启动或停止 Webmail 服务器：

1. 在 MDaemon GUI 的左侧状态窗格上，右单击 **Webmail** 条目并在快捷菜单上选择*切换活动/非活动*部分。
2. 在主界面上点击“**文件 » 启用 Webmail 服务器**”。
3. 在主界面上点击“**设置 » Web 及 SyncML 服务**”并在 Web 服务器屏幕上点击*使用内置 web 服务器运行 Webmail*。

登录到 Webmail

1. 将您的 web 浏览器指向 http://example.com:WebmailPortNumber。该端口在 Webmail 部分的 Web 服务器 270 屏幕上指定。如果您配置 Webmail 监听默认的 web 端口（端口 80），那么您无需指定在登录 URL 中的端口号（比如由 www.example.com 替代 www.example.com:3000）。
2. 输入您 MDaemon 账户的用户名和密码。
3. 点击登录。

更改 Webmail 的端口设置

1. 在菜单栏上点击“**设置 » Web 及 SyncML 服务**”。
2. 在标记为*使用该 TCP 端口运行 Webmail 服务器*的控件中输入所需的端口号。
3. 点击确定。

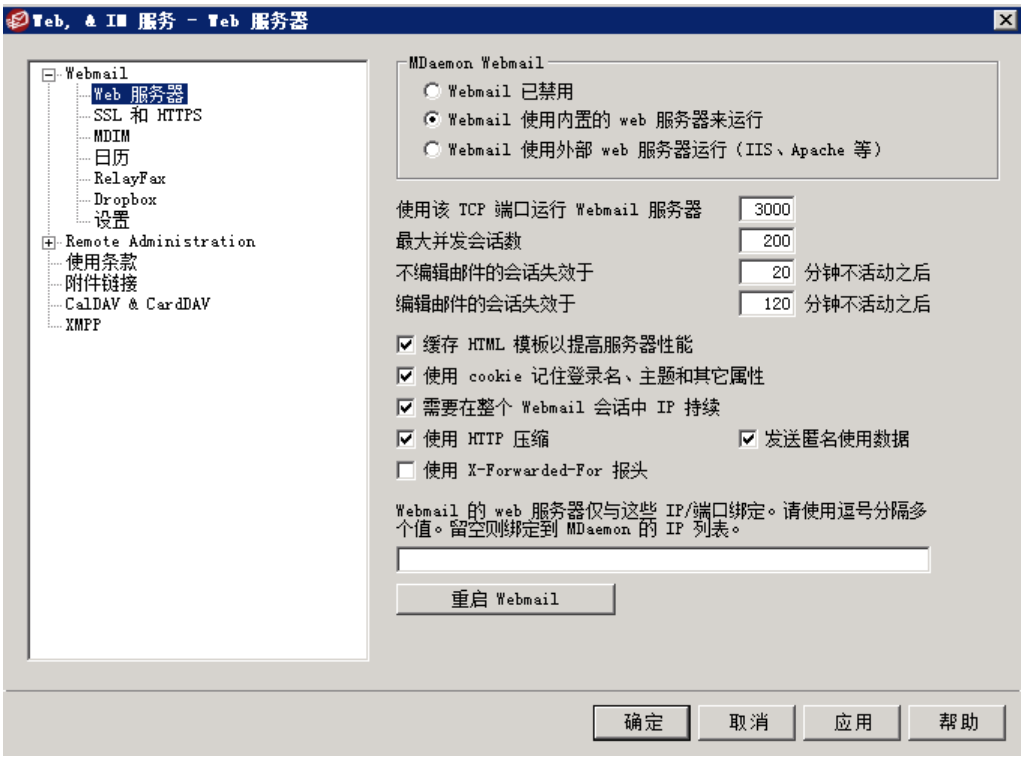
客户端帮助

Webmail 为您的用户配置了广泛的客户端帮助。要了解客户端特性和功能信息，请参阅 Webmail 中的在线帮助系统。

要了解更多地址簿选项详细信息，请参阅：

Webmail » MDIM 278
LDAP 696

3.6.1.2 Web 服务器



此屏幕中包括控制 Webmail配置和行为的各种全局及服务器级别的设置，无论它们属于哪个用户或者域。

MDaemon Webmail

禁用 Webmail
选择此项来禁用 Webmail服务。您还可以从文件菜单或从主 MDaemon GUI上统计框的服务器部分切换 Webmail活动/非活动状态。

> 在使用附件链接[305]功能时必须激活 Webmail。

Webmail使用内置的 web 服务器来运行
选择此项以使用 MDaemon 的内置 web 服务器来运行 Webmail。您还可以从文件菜单或从主 MDaemon GUI上统计框的服务器部分切换 Webmail活动/非活动状态。

Webmail使用外部 web 服务器 (IIS，Apache 等)运行
如果您希望 Webmail运行在 IIS 下或其他 web 服务器之下而不是 MDaemon 的内置服务器，请选择此选项。这防止在访问某些 GUI元素时和您的备用服务器产生冲突。

要了解更多详情，请参阅在 IIS 下运行 Webmail[272]。

使用该 TCP 端口运行 Webmail服务器
这是 Webmail监听您用户的 web 浏览器连接所用的端口。

最大并发会话数
这是同时可以连接到 Webmail的会话最大数。

闲置 xx 分钟后非编写邮件的会话超时
当一个用户登录到 Webmail时，但没有编写邮件，这就是他们的会话在 Webmail关闭它前，保持不活动的时间。

闲置 xx 分钟后编写邮件的会话超时
该计时器控制的是当用户编写邮件时，会话保持打开状态以及会话保持非活动的时间长度。将此计时器设置得比*"非编写邮件的会话..."*的计时器高一些是非常好的，因为在用户编写邮件时不活动时间通常要更长一点。这是由于从编写邮件开始直到邮件被发送，都不需要与服务器通信。

缓存 HTML 模板来提高 web 服务器性能
点击此框可以使 Webmail将模板缓存到内存中，而不是每次在需要访问它们的时候再进行读取。这样可以显著地提高服务器性能，但是如果您对某一模板文件作了改动，您必须重启 Webmail。

使用 Cookie 来记忆登录名、主题和其他属性
如果您希望 Webmail在他或她本地计算机上的 Cookie 中存贮每位用户的登录名，主题和某些其他属性，请点击此选项。使用此功能给您的用户更多的"自定义"登录体验，但需要在他们的浏览器中，启用对 cookie 的支持。

持续通过 Webmail会话请求 IP
作为一个附加的安全措施，在会话开始时，您可以点击此复选框使 Webmail限制每一个用户会话到用户连接上来的那个 IP 地址。因此，由于要求 IP 保持不变，没有任何人可以"窃取"用户的会话。这个配置更安全，但如果用户使用代理服务器或动态指定与更改 IP 地址的因特网连接，该配置可能会引起一些问题。

使用 X-Forwarded-For报头
勾选此框来启用 X-Forwarded-For 报头，有时代理服务器会添加这些报头。默认情况下，禁用该选项。只有在您的代理服务器插入此报头时，才启用此项。

使用 HTTP 压缩
如果您希望在您的 Webmail通话中使用 HTTP 压缩，请单击此复选框。

发送匿名使用数据
默认情况下，Webmail发送匿名的良性使用数据，例如：操作系统所用、浏览器版本所用和语言等。MDaemon Technologies 使用这些数据来帮助我们改善 Webmail。如果您不希望发送匿名使用数据，请禁用此项。

仅绑定 Webmail的 web 服务到这些 IP/端口
如果您希望限制 Webmail服务器只到特定的 IP 地址或端口，然后在此指定这些 IP 和端口，以逗号分隔。使用格式："IP_address:Port"来指定一个端口 (例如：192.0.2.0:80)。如果您没有包含端口，那么将会使用上方指定的默认 TCP 端口和 SSL & HTTPS 274 屏幕 上指定的 HTTPS 端口。如果您希望 Webmail监听所有的端口，那么请使用"*"。例如"*,*:80"将允许 Webmail在指定的默认端口 (3000和443)上监听所有的 IP 地址，同时也将监听 80 端口上的所有 IP 地址。如果您将此字段留空，那么 Webmail将监控为您的域 149 指定的所有 IP 地址。

重新启动 Webmail（当端口或 IIS 值变更时需要）
如果您希望重启 Webmail服务器，请点击此按钮。请注意：当改变 Webmail的端口设置时，为了可以识别这些设置您必须重启 Webmail。

3.6.1.2.1 在 IIS6 下运行 Webmail

Webmail配备了一个内置的 web 服务器，因此不需要因特网信息服务器 (IIS)来处理。然而，Webmail确实支持 IIS，所以可以作为 ISAPI DLL 运行。以下关于如何配置 Webmail以在 IIS 6 下运行的信息摘自 www.altn.com 上 MDaemon 知识库的 #01465 文章 www.mdaemon.com:

1. 打开 "因特网信息服务管理控制台"(Internet Information Services Management Console)。
2. 右单击 "应用程序池"。
3. 选择**新建/应用程序池**。
4. 将此程序池命名为 Alt-N 并点击 "确定"按钮。
5. 右单击 "Alt-N"。
6. 点击 "属性"。
7. 点击 "属性"选项卡。
8. 取消**在空闲此段时间后关闭工作进程（分钟）**：与**限制核心请求队列为（请求次数）**两个选项。
9. 点击 "身份"选项卡。
10. 在预定义下拉列表中选择 "本地服务"。
11. 点击 "确定"按钮。
12. 右单击 "网站"。
13. 选择 "新建"。
14. 点击 "网站"。(出现创建向导)
15. 点击 "下一步"按钮。
16. 输入网站名称比如 "Webmail"。
17. 点击 "下一步"按钮。
18. 再次点击 "下一步"按钮。
19. 浏览根目录：(默认安装)C:\MDaemon\WorldClient\HTML。
20. 点击 "下一步"按钮。
21. 确保勾选了 "读取"、"运行脚本"以及 "执行"选项。
22. 点击 "下一步"按钮。
23. 点击 "完成"按钮。
24. 右单击您刚才创建的网站 "(Webmail)"。
25. 选择 "属性"。
26. 点击 "文档"选项卡。

27. 删除所有列出的文档。
28. 添加 "WorldClient.dll"。
29. 选择 "根目录"选项卡。
30. 在应用程序池下拉列表选择 "Alt-N"。
31. 点击 "确定"按钮。
32. 点击 "网络服务扩展"。
33. 启用 "所有未知 ISAPI 扩展"或为 "WorldClient.DLL"创建一个新扩展。

Internet Guest 账户——IUSER_<SERVER_NAME>——需要对 MDaemon 目录和所有的子目录拥有 "完全访问"NTFS 权限。

1. 右单击 MDaemon 目录。(C:\MDaemon)
2. 选择 "属性"。
3. 选择 "安全"标签。
4. 点击 "添加"按钮。
5. 点击 "高级"按钮。
6. 点击 "立即查找"按钮。
7. 选择 IUSER_<SERVER_NAME> ("SERVER_NAME>"是本地计算机的名称)。
8. 点击 "确定"按钮。
9. 点击 "确定"按钮。
10. 选中 "完全控制"框。
11. 点击 "确定"按钮。

上面的每一步都要应用到 MDaemon 的每一个文件夹。

设置完网络以后，在进行 MDaemon 升级时：

1. 打开 "因特网信息服务管理控制台"(Internet Information Services Management Console)。
2. 打开 "应用程序池"列表。
3. 右单击 "Alt-N"。
4. 选择 "停止"。
5. 关闭 MDaemon。
6. 安装升级。
7. 一旦完成安装，启动 MDaemon。
8. 再次打开 "因特网信息服务管理控制台"(Information Services Management Console)，右单击 "Alt-N"。
9. 选择 "启动"。

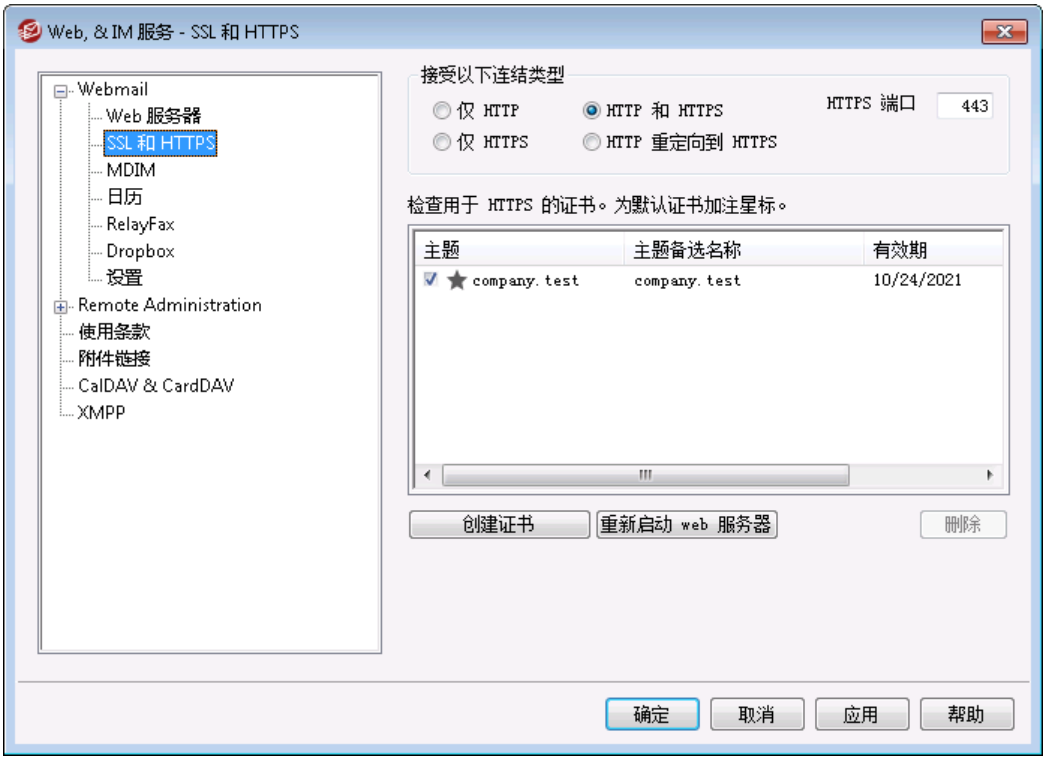
如果您按照上述方法，会出现如下现象。

1. 停止 "应用程序池"之后，用户将得到 "服务不可用"这条信息。
2. 按照这些步骤帮助您将升级完 MDaemon 后重启的可能性减到最小。

在 IIS 下该程序的设置没有技术支持，选择在 IIS 下运行 Webmail的用户必须注意所有的安全事项和运行在 IIS 下的其他应用程序。建议在把 Webmail作为 ISAPI扩展安装在 IIS 下之前，安装 IIS 最新的补丁和更新。

当在 IIS 下运行 Webmail时，您将不能从 MDaemon 的界面中，启动或者停止它。您必须使用IIS提供的工具才能这么做。

3.6.1.3 SSL & HTTPS



MDaemon 内置的 Web 服务器支持安全套接字层 (SSL)协议。SSL 是保护服务器/客户端 web 通信安全的标准方案。它提供了服务器验证、数据加密和用于 TCP/IP 连接的可选客户端验证。此外，由于在所有主要的浏览器中都内置了 HTTPS 支持 (比如通过 SSL 的 HTTP)，只要在您的服务器上安装一个有效的数字认证将会激活连接客户端的 SSL 能力。

启用和配置 Webmail来使用 HTTPS 的选项位于“设置» Web & IM 服务» Webmail (web 配置)下的SSL & HTTPS 屏幕”。但是为了您使用起来更加方便，这些选项还被镜像于“安全» 安全管理器» SSL & TLS » Webmail”之下。

要了解 SSL 协议与证书的更多详情，请参阅：“SSL 和证书 479”

在使用 MDaemon 内置的 web 服务器时，该屏幕仅应用于 Webmail。如果您配置 Webmail使用其它的网络服务器，如 IIS，则不会使用这些选项——SSL/HTTPS 支持必需使用其它网络服务器的工具来配置。

接受以下连接类型

仅 HTTP
如果您不允许任何 HTTPS 连接到 Webmail，请选择此项。仅接受 HTTP 连接。

HTTP 和 HTTPS
如果您希望在 Webmail中启用 SSL 支持，但不希望强迫您的 Webmail用户使用 HTTPS，请选择此选项。Webmail对在以下指定的 HTTPS 端口上的连接进行监听，但是它仍将会回应 Webmail端口上正常的 http 连接，该端口在 Webmail (web 邮件)的 Web 服务器 270屏幕上指定。

仅 HTTPS
如果想在连接 Webmail时要求使用 HTTPS，请选择此选项。当此选项启用时，Webmail将会只响应 HTTPS 连接——它不会响应 HTTP 请求。

HTTP 重定向到 HTTPS
如果您希望重定向所有的 HTTP 连接到在 HTTPS 端口上的 HTTPS，请选择此选项。

HTTPS 端口
这是 Webmail将为 SSL 连接监听的 TCP 端口。默认 SSL 端口是 443。如果使用默认 SSL 端口，则在通过 HTTPS 进行连接时，您将不必在 Webmail的 URL 中包含端口号 (比如“https://example.com”等于“https://example.com:443”)。

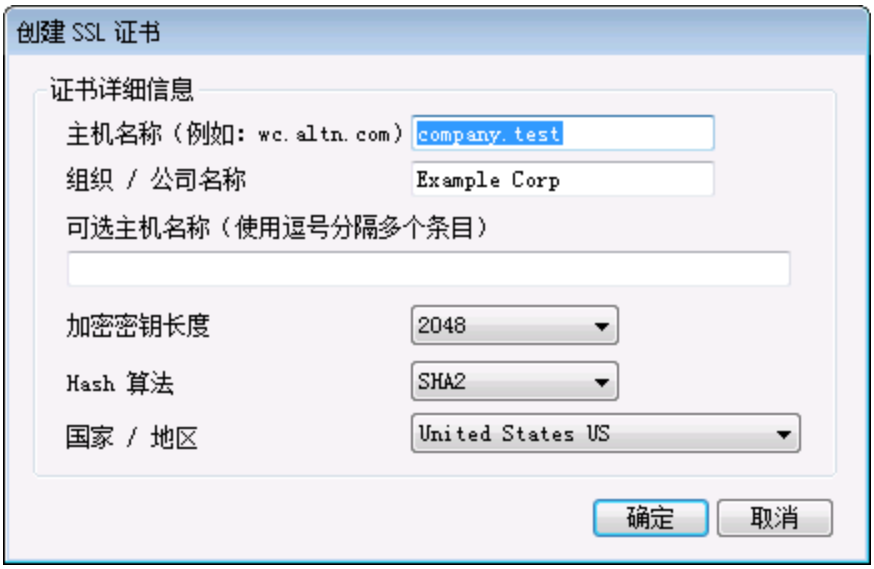
这不同于在 Webmail (web 配置)的 Web 服务器 270屏幕上指定的 Webmail端口。如果你仍允许 HTTP 连接到 Webmail，则那些连接必须使用其他端口连接才能成功。HTTPS 连接必须使用 HTTPS 端口。

选择用于 HTTPS/SSL 的证书

该框显示您的 SSL 证书。选中您希望激活的任何证书旁边的框。点击要设置为默认证书旁边的星号。MDaemon 支持 TLS 协议的服务器名称指示 (SNI)扩展，它允许为您的每个服务器主机名使用不同的证书。MDaemon 将查看活动证书，并在“主题备选名称”字段中选择具有所请求主机名的证书 (您可以在创建证书时指定备选名称)。如果客户端未请求主机名，或者未找到匹配的证书，则使用默认证书。双击证书以在 Windows“证书”对话框中将其打开以供审阅 (仅在应用程序界面中可用，而不在基于浏览器的远程管理中可用)。

删除
在此列表中选择一个证书，然后点击此按钮将其删除。会打开一个确认框并询问您是否确定删除该证书。

创建证书
点击此按钮来打开“创建 SSL 证书”对话框。



证书详细信息

主机名
在创建证书时，输入您用户将会连接的主机名称（例如“wc.example.com”）。

企业/公司名
在此输入“拥有”此证书的机构或公司。

替换主机名（用逗号分隔多个项目）
如果您的用户可能连接到备选主机名，您也希望此证书应用到那些名称，那么请输入那些域名，通过逗号分隔。允许通配符，所以“*.example.com”可以应用于所有 example.com 的子域（例如“wc.example.com”、“mail.example.com”等等）。

> MDaemon 支持 TLS 协议的服务器名称指示 (SNI)扩展，它允许为您的每个服务器主机名使用不同的证书。MDaemon 将查看活动证书，并在其“使用者备用名称”字段中选择具有所请求主机名的证书。如果客户端未请求主机名，或者未找到匹配的证书，则使用默认证书。

密钥长度
为此证书选择所需位长度的加密密钥。加密密钥的位数越长，已传输的数据也将越安全。不过请注意，并非所有的应用程序都支持大于 512 的密钥长度。

国家/地区
选择您的服务器所在国家或地区。

Hash 算法
选择您希望使用的 hash 算法：SHA1 或 SHA2。默认设置是 SHA2。

重启 web 服务器
点击此按钮来重启 web 服务器。使用新证书前，必须重启 web 服务器。

使用 Let's Encrypt 来管理您的证书

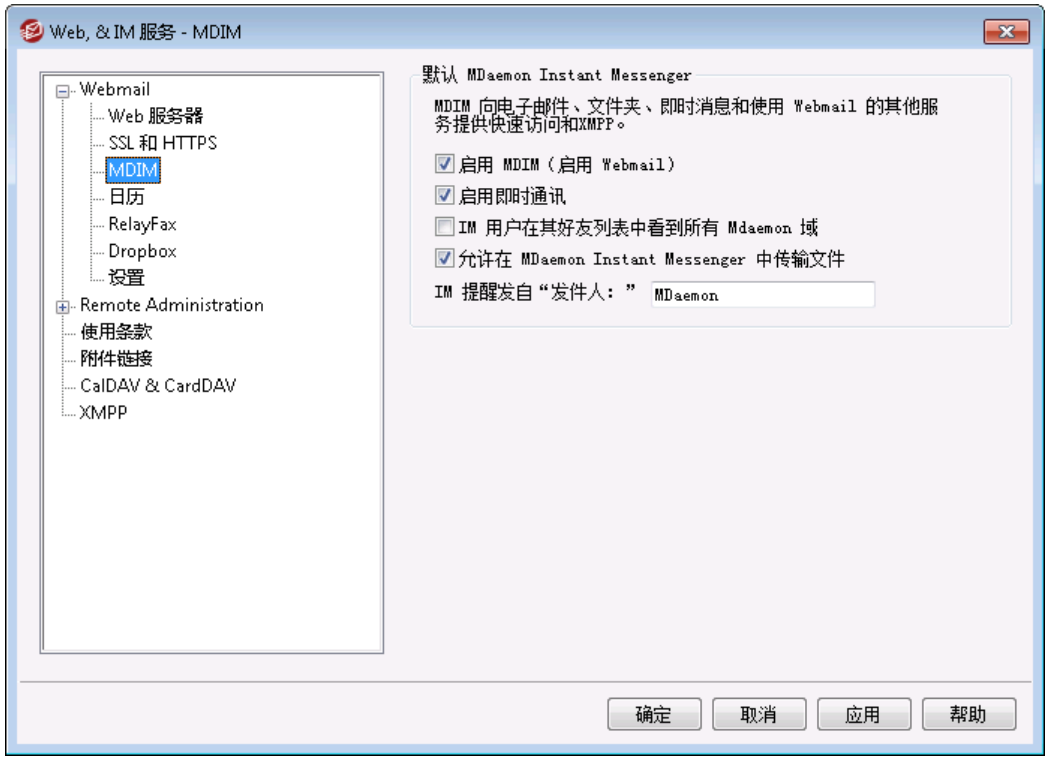
Let's Encrypt 是一个证书颁发机构 (CA)，通过专门设计的自动化流程来为 "传输安全层 (TLS)"加密提供免费的证书，该流程使您可以免于现在复杂的手动创建、验证、签名、安装、以及续订证书这些用来保护网站安全的环节。

要支持使用 Let's Encrypt 的自动化流程来管理证书，提供 Let's Encrypt 496 屏幕来帮助您轻松简便地配置和运行 PowerShell 脚本，位于 "MDaemon\LetsEncrypt"文件夹。运行该脚本将使一切为 LetsEncrypt 准备就绪，包括将一些必要的文件放置在 WebmailHTTP 的目录中来完成 http-01 挑战。它将 SMTP 主机名 151 (属于默认域 149)用作证书域，包含您已指定的任何*备选主机名称*，检索证书，将其导入 Windows，并配置 MDaemon 如何使用针对 MDaemon、Webmail 和 Remote Administration 的证书。此外，该脚本将在名为 LetsEncrypt.log 的 "MDaemon\Logs\"目录中创建一个日志文件 LetsEncrypt.log。每次运行脚本时,都会删除并重新创建该日志文件，并且包含脚本的开始日期和时间。此外，如果您指定了*通知的管理员邮件*，将在出错时发送通知邮件。请参阅 Let's Encrypt 496 主题了解更多信息。

还请参阅：

SSL 和证书 479
创建和使用 SSL 证书 764

3.6.1.4 MDIM



此屏幕为新建域控制 MDaemon Instant Messenger (MDIM)[267] 的默认设置。可以通过 "域管理器"的 MDIM 屏幕[156]修改特定域的设置。可以通过 "Web 服务[603]"和 "群组属性[658]"屏幕分别为特定账户或群组启用或禁用 MDaemon Instant Messenger 服务。

默认的 MDaemon InstantMessenger

启用 MDIM (启用 Webmail)
如果您希望在默认情况下，可以从Webmail内下载 MDaemon Instant Messenger，请启用此项。用户可以从 *"选项 » MDaemon Instant Messenger"*页面下载这个部件。下载好的安装文件将自动定制每一个用户的账户，便于安装和设置。此选项还使 MDIM 可以使用 "我的邮件文件夹"功能，允许用户检查新的电子邮件，并直接从 WCIM 的快捷菜单打开 Webmail。默认启用 MDIM。

启用即时通讯
默认情况下，账户可以使用 MDIM 和第三方 XMPP[312] 客户端来与其域的其他成员进行即时通讯。如果您不希望默认情况下允许即时通讯，那么请清理此选择框。

IM 用户在其好友列表中看见所有 MDaemon 域
如果您希望用户在默认情况下能够将联系人添加到所有 MDaemon 域的好友列表，请点击此选项。当禁用此项时，联系人必须位于同一个域。例如，如果您的 MDaemon 正在为 example.com 和 example.org 托管邮件，则激活此项就意味着用户可以从这两个域添加即时通讯联系人。禁用此项意味着 example.com 用户只能添加其他 example.com 用户，而 example.org 只能添加 example.org。默认情况下禁用此选项。域管理器上[156]有一个同等的选项，用于为特定域启用或禁用此功能。

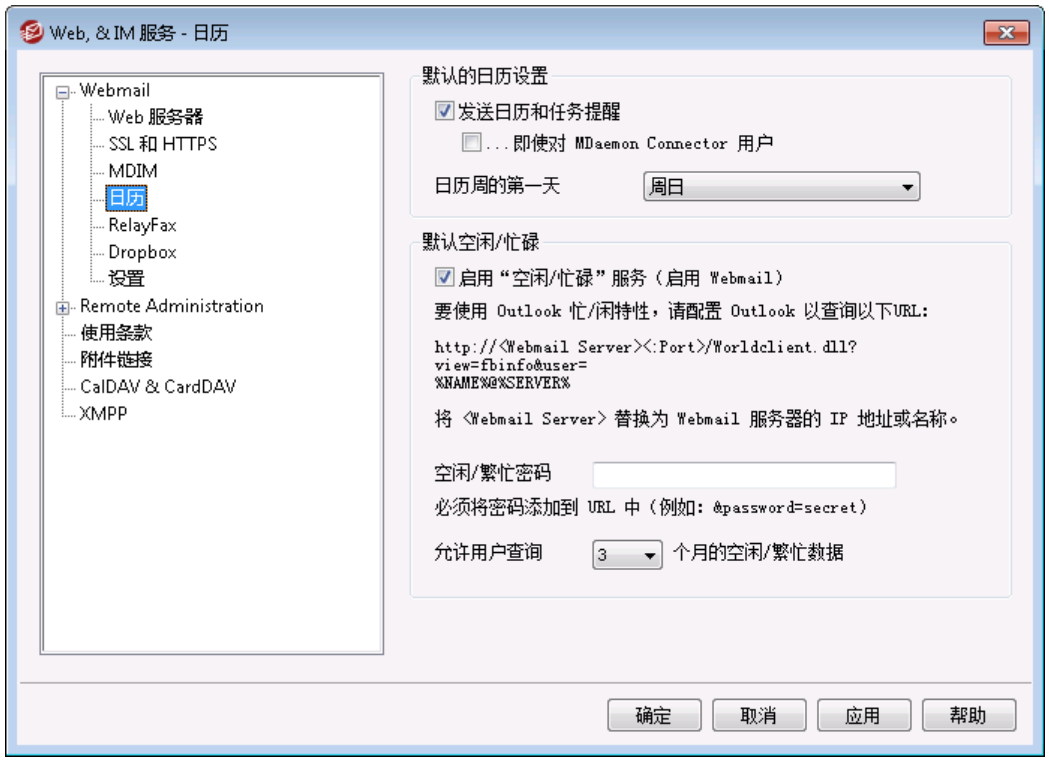
允许 MDaemon InstantMessenger 中的文件传输
默认情况下，MDIM 用户可以将文件传输到其 MDIM 联系人。如果您不希望允许 MDIM 用于传输文件，请清除此复选框。

IM 提醒发送 "发件人:"
当一个约会被安排到用户的 Webmail 日历中时，可以设置事件在指定时间向用户发送一个提示。如果对于每个用户的域，IM 系统都是激活的，则在即时消息中向该用户发送提醒。使用此文本框来指定您希望在消息中显示的 "From:"名称。这是针对新域的默认设置。您可以通过 "域管理器"的 MDaemon Instant Messenger 156 屏幕，为特定域更改此项。

还请参阅：

域管理器 » MDaemon InstantMessenger 156
账户编辑器 » Web 服务 603
群组属性 658

3.6.1.5 日历



此屏幕控制 MDaemon 日历功能的默认设置。可以通过 "域管理器"的日历 158 屏幕控制特定域的设置。

默认日历设置

发送日历和任务提醒
如果您希望允许 Webmail的日历和任务提醒通过电子邮件和 MDaemon Instant Messenger发送给您的用户，请点击此勾选框。

...也发送至 MDaemon Connector用户
如果您已启用以上的 *"发送日历和任务提醒"*选项，如果您还希望为 MDaemon Connector[323] 用户启用提醒，请点击此选项。

每周第一天
从下拉菜单中选择一天。选中的那天将出现在日历中，作为每周的第一天。

默认的空闲/忙碌

MDaemon 包含了空闲/忙碌服务器，使得会议组织者可以查看潜在出席者能否参加。要访问此功能，请在创建新的日程时在 Webmail中点击**调度**。这将打开调度窗口，其中包含出席者列表和针对每位出席者的一行用颜色区分的日历网格。每位出席者所在的行都用颜色区分标识出其有空参加会议的时间。有可以表示忙碌、不确定、外出和无信息的颜色。**自动选择下一个**按钮可以用来在服务器上查询下一个所有出席者都有空的时间空挡。当您创建完预约后，它向所有出席者发送邀请，出席者可以接受或拒绝邀请。

Webmail的空闲/忙碌服务器同样可以与 Microsoft Outlook 兼容。要使用该功能，只需配置 Outlook 来查询以下列出的 "空闲/忙碌"数据的 URL。例如在 Outlook 2002 中，空闲/忙碌选项位于 "工具» 选项» 日历选项.. » 空闲/忙碌选项.."

用于 Outlook 空闲/忙碌服务器的 URL：

```
http://<Webmail><:Port>/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

使用 Webmail服务器的 IP 或域名替换 "<Webmail>"，并且用端口号替换 "<:Port>"（如果没有使用默认的 Web 端口）。例如：

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

有关如何使用 Webmail的空闲/繁忙功能调度预约的更多信息，请参考 Webmail的在线帮助系统。

启用空闲/繁忙服务器
如果您要为用户启用空闲/忙碌服务器功能，则点击该选项。

空闲/忙碌密码
如果您希望在用户试图通过 Outlook 访问 "空闲/忙碌"服务器功能时要求他们提供密码，请在此处输入密码。当用户在 Outlook 中配置其空闲/忙碌设置时，密码必须追加在以上列出的 URL 后（格式："&password=FBServerPass"）。例如：

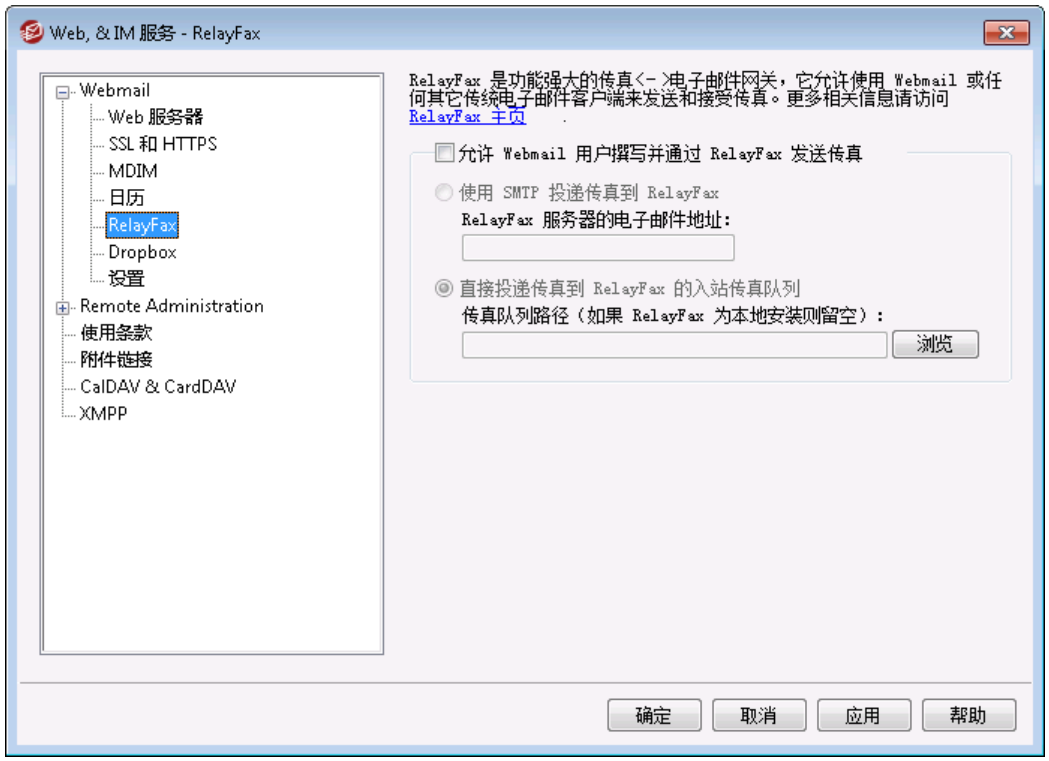
```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%&password=MyFBServerPassword
```

允许用户查询 X 月的空闲/忙碌数据
使用该选项指定您的用户可以查询空闲/忙碌数据的月份数目。

还请参阅：

域管理器 » 日历 158

3.6.1.6 RelayFax



MDaemon Technologies 的 RelayFax Server 服务器是电子邮件到传真与传真到电子邮件的网关，且与 Webmail无缝集成以向您的用户提供传真服务。当此功能启用时，Webmail 用户将会被赋予访问各种功能的权利，使他们可以通过 Webmail客户端页面来编写和发送传真。要了解更多详情，请访问 RelayFax 部分www.mdaemon.com。

RelayFax 集成选项

允许 Webmail用户通过 RelayFax 编写并发送传真
点击此选项将 Webmail与 RelayFax 集成。激活时，它会使 "编写传真"控件和其他传真相关功能出现在 Webmail页面上。

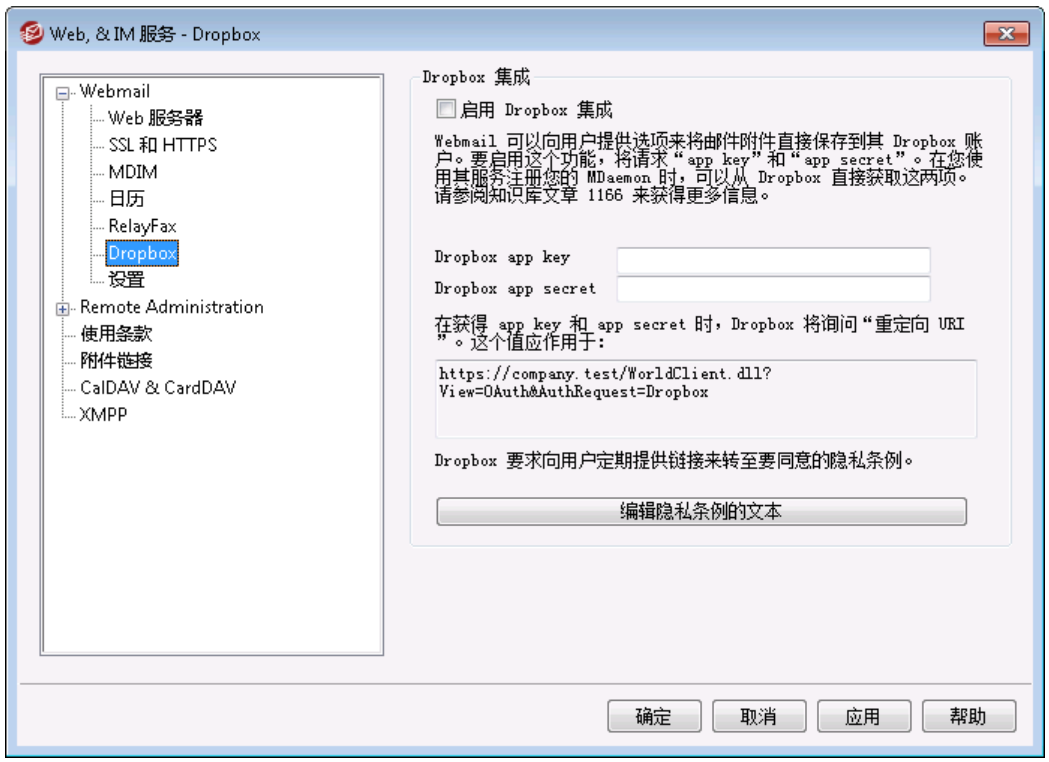
使用 SMTP 投递传真到 RelayFax
Relayfax 会监视一个指定邮箱，该邮箱用于即将进行传真的入站邮件。单击此选项，MDaemon 将会使用常规的 SMTP 电子邮件投递进程来发送这些邮件到该邮箱地址。当 RelayFax 监视其他地方的邮箱而不是您本地网◆◆的邮箱时，此选项是很有用的。如果 RelayFax 位于您的网络，您可能选择让 MDaemon 直接向 RelayFax 的邮件队列投递邮件，如此可以完全绕过 SMTP 投递进程。要了解该方案的更多详情，请参见以下的*直接投递传真到 RelayFax 的入站传真队列*。

RelayFax 服务器的邮件地址
指定您希望邮件作为传真发送的电子邮件地址。该值必须和您配置 RelayFax 来监视这些邮件的地址相匹配。

直接投递传真到 RelayFax 的入站传真队列
如果 RelayFax 位于您的 LAN 中，您可以选择此方法而不是使用 SMTP 通过分发邮件来发传真。当 MDaemon 收到一封要进行 RelayFax 的邮件时，会将该邮件直接置于 RelayFax 的入站队列而不是使用 SMTP 进行投递。

传真队列路径
如果 RelayFax 位于 MDaemon 运行的同一台机器上，您可以留空此文件路径。否则，您必须指定网络路径到 RelayFax 的 \app\ folder。

3.6.1.7 Dropbox



Webmail提供针对 Dropbox 的直接支持，允许用户将文件附件保存到其 Dropbox 账户，并在外发邮件中插入转至 Dropbox 文件的直接链接。要向您的 Webmail用户提供此功能，您必须将 Webmail设置为 Dropbox 应用程序，设置页面位于 Dropbox 平台。这是一个简单的操作过程，您只需登录 Dropbox 账户，为具有 Dropbox 完全访问权限的应用程序创建唯一名称，指定重定向到 WebmailURI，并更改一个默认设置即可。然后，您将 Dropbox “应用密钥 (app key)”和 “应用密码 (app secret)”复制并粘贴到 MDaemon 中的 Dropbox 屏幕上即可。之后，当用户下次登录 Webmail时，您的用户将能够将其 Dropbox 账户与 Webmail建立连接。有关如何创建 Dropbox 应用程序并将其链接到 Webmail的逐步说明，请参阅：创建和链接您的 Dropbox 应用 284 。

当您创建 Dropbox 应用程序时，它最初将具有 "开发"状态。这允许多达500个 Webmail用户将其 Dropbox 账户链接到该应用。根据 Dropbox 的说法，"一旦您的应用程序链接了50个 Dropbox 用户，在您的应用程序能够链接其他 Dropbox 用户的功能被冻结之前，您将拥有两个星期的时间来申请并获得 "生产"状态许可，无论你的应用已经链接了多少用户（0到500）。"这就意味着，在收到 "生产"许可之前，Dropbox 集成将继续工作，但没有额外用户能够链接其账户。获取生产许可是一个简单的过程，以确保您的应用符合 Dropbox 的指南和服务条款。要了解更多信息，请参阅 "生产许可"部分，位于 Dropbox Platform 开发人员向导.

一旦您的 Webmail应用程序被正确创建和配置，每个 Webmail用户登录到 Webmail时，都可以选择将他们的账户连接到其 Dropbox 账户。用户需要登录到 Dropbox，并授予该应用访问 Dropbox 账户的权限。然后，该用户将使用在认证过程中传递给 Dropbox 的 URI 重定向回 Webmail。为了安全起见，URI 必须与您指定的重定向 URI 之一（见下）相匹配，在 Dropbox.com 的应用信息页面指定。最后 Webmail和 Dropbox 将交换访问代码和访问令牌，这允许 Webmail连接到用户的 Dropbox 账户，以便用户可以在其中保存附件。交换的访问令牌每隔七天到期，这就意味着用户必须重新授权该账户才能使用 Dropbox。用户还可以手动将其账户从 Dropbox 断开，或者在必要时从 Webmail中的 Cloud Apps 选项屏幕重新授权。

Dropbox 集成

启用 Dropbox 集成

一旦您创建了 Dropbox 应用程序，并将其链接到 Webmail，请点击此复选框以允许您的 Webmail用户链接到其 Dropbox 账户。如果您希望按用户启用或禁用 Dropbox，可以通过添加 "DropboxAccessEnabled=Yes（或 No，位于 User.ini）来实现。

Dropbox 应用密钥和应用密码

这些应用密钥和应用密码位于 Dropbox.com 的应用信息页面。在此处输入它们将 Webmail链接到您的 Dropbox 应用程序。

重定向 URI

您必须在 Dropbox.com 的应用信息页面指定重定向 URI。MDaemon 自动显示您应该可以在那里使用的 URI。不过您可以添加多个重定向 URI。因此，您可以为每个域添加一个 URI，甚至为本地主机添加一个 URI，如果从运行服务器的计算机登录到 Webmail，则可以使用该 URI。

例如：

```
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 需要您的重定向 URI 是安全的，因此必须启用 HTTPS 274，用于Webmail。

编辑隐私策略文本

点击此按钮可编辑包含 Webmail应用程序隐私政策的文本文件。因为 Dropbox 要求向用户定期显示批准的隐私策略，所以在向您用户显示的 "连接至 Dropbox"页面上提供转至文件内容的 "隐私策略"链接。该链接打开一个包含文本的小窗口，用户可以点击 "下

载”按钮来下载文件。如果您希望格式化文本或希望包含任何链接，请在文件中使用 HTML 代码。

创建和链接您的 Dropbox 应用

创建 Dropbox 应用程序，并将其链接到 Webmail的逐步说明。

1. 在您的浏览器中，导航至 Dropbox Platform
2. 登录您的 Dropbox 账户
3. 选择 **Dropbox API**
4. 选择**完整 Dropbox**
5. 为您的应用程序命名
6. 点击**创建应用**
7. 点击**启用额外用户**，并点击 **确定**
8. 更改**允许隐式授权**为**不允许**
9. 输入一个或更多 URI，在每一个 URI 后点击**添加**。对于 Webmail而言，它们必须是安全的 URL（必须在 Webmail中启用 HTTPS）。

   例如：

   https://mail.company.test/WorldClient.dll?View=OAuth&AuthRequest=Dropbox

   https://localhost/WorldClient.dll?View=OAuth&AuthRequest=Dropbox
10. 将浏览器打开到您的应用信息页面，打开 MDaemon GUI
11. 点击**设置**
12. 点击 **Web & IM 服务**
13. 点击 **Dropbox**，位于 **Webmail** 下方
14. 将您浏览器中的**应用密钥**和**应用密码**复制/粘贴到 MDaemon 中的 **Dropbox** 屏幕。
15. 点击**应用**
16. 点击**确定**

有关将 Webmail用户账户与用户的 Dropbox 账户相关联的说明，请参阅 Webmail中的在线帮助系统，或参阅知识库文章 1166。

3.6.1.8 Google Drive

此页面仅在 MDaemon Remote Administration (MDRA) 293 的 web 界面中可用。

Google Drive 集成

MDaemon Webmail可以向用户提供将邮件附件直接保存到其 Google Drive 账户，以及编辑和处理存储在那里的文档的选项。要实现这一点，需要 **API Key、Client ID** 和 **Client Secret**。所有这些都是直接从 Google 获得的，方法是使用 Google API Console 创建一个应用程序，并在他们的服务中注册你的 MDaemon。OAuth2.0 验证组件是此应用程序的一部分，它允许您的 Webmail用户登录 Webmail，然后通过 MDaemon 授权访问其 Google Drive 账户。一旦授权，用户可以查看他们在 Google Drive 中的文件夹和文件。此外，他们还能上传、下载、移动、复制、重命名和删除文件，以及将文件复制/移动到本地文档文件夹。如果用户想要编辑文档，点击在 Google Drive 中查看文件的选项将允许用户根据其在 Google Drive 中设置的权限对其进行编辑。Google Drive 的设置过程与 MDaemon 的 Dropbox 集成 282 和 MultiPOP OAuth 集成 118 功能类似。

启用 Google Drive 集成
点击此勾选框来启用 Google Drive 集成。还请参阅：下方的**设置 Google Drive 集成**。

Google Drive API Key:
这是您在创建应用时，在 Google Drive API 控制台中，为您生成的唯一 API 密钥。将该密钥复制并粘贴到此处。

Google Drive Client ID
这是您在 Google API 控制台中创建 Google Drive 应用时，分配给它的唯一客户端 ID。创建完应用程序后，复制其客户端 ID，并将其粘贴到此处。

Google Drive Client Secret
这是您在 Google API 控制台中创建 Google Drive 应用时，分配给它的唯一 Client Secret。创建完应用程序后，复制其 Client Secret，并将其粘贴到此处。

重定向 URI
您必须在创建 Google Drive 应用时，指定一个或多个重定向 URI。作为示例的“重定向 URI”从您默认域的 149 SMTP 主机名称 151 构建而成，在登录到 Webmail时应能适用于该域的用户。您应该在用户登录 Webmail时，为他们前往的任何其他 MDaemon 域，将额外的重定向 URI 添加到您的应用程序。例如，“https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive”将适用于在登录 Webmail时，前往 mail.example.com 的任何用户。还请参阅：下方的**创建并链接您的 Google Drive App**来获取更多信息。

编辑隐私策略文本
Google Drive 集成需要您定期向用户提供一个转至批准的隐私策略的链接。点击此按钮来编辑您的隐私策略。

创建和链接您的 Google Drive 应用

创建 Google Drive 应用的按步指南。

按照以下步骤来创建一个 Google 应用程序，由此来允许用户在**文档**页面上的 Webmail内访问 Google Drive。

1. 登录 MDaemon Remote Administration 293 并前往 Google Drive 页面（位于“主页 » Webmail设置”下），然后启用“**启用 Google Drive 集成**”这个选项。

2. 在单独的浏览器选项卡上，登录您的 Google 账户并前往 Google API 控制台.
3. 如果位于 "项目列表"上，请点击 **NEW PROJECT**"，如果位于管理资源页面，请点击 **(+) CREATE PROJECT**。
4. 输入**项目名称**，例如 "Google Drive for MDaemon"，如果您希望编辑项目 ID 或使其保留默认值，请点击 **编辑**"。**请注意：**在创建项目后无法更改项目 ID。
5. 如果您有组织资源。请在 **Location** 中将其选中。否则，保持 "无组织"的设置。
6. 一旦加载，请点击 **+ ENABLE APIS AND SERVICES**。
7. 在搜索字段，请输入 "Google Drive"，选择 **Google Drive API** 并点击 "启用"。
8. 在左窗格的 "**APIs & Services**"下，请点击 **Credentials**。
9. 点击位于页面顶部的 **+ Create Credentials**，并在下拉菜单中选择**API Key**。
10. 复制**您的 API 密钥**（附近有一个 "复制到剪贴板"的图标）。
11. 切换到您浏览器的 MDaemon 选项卡并将其贴入 MDaemon 中 Google Drive 页面上的 "**Google Drive API Key**"字段（人如果您想稍后执行这一步，请将其保存到其他位置）。
12. 在左窗格的 "**APIs & Services**"下，请点击 **OAuth 同意屏幕**。
13. 在 "User Type"下，选择 "**External**"并点击 "**Create**"。**请注意：**如果您有组织资源，或取决于您应用的发布状态，选择 "Internal"可能会更好。还请参阅发布状态 287来获得更多信息。
14. 输入**应用名称**（例如 Google Drive for Webmail）、供用户联系的**技术支持邮件地址**、供 Google 对于项目变更可以联系到的**开发人员邮件地址**。这就是该页面上需要完成的全部设置，不过取决于您特定的组织或验证要求，您还能输入公司徽标并链接到您的服务条款 304和隐私策略（见上）。会为您自动填写 "**Authorized domains**"字段，在您稍后添加 "*Redirect URIs*"这一步时。**请注意：**此信息用于 Consent(同意)屏幕，该屏幕将呈现给用户，以授权 Webmail 访问用户的 Google Drive。
15. 点击 "**Save and Continue**"。
16. 点击 "**ADD OR REMOVE SCOPES**"，并将下方的 URI 复制/粘贴到（您可以一次性全部复制/粘贴）"Manually add scopes"下方的框。然后点击 "**ADD TO TABLE**"。

```
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. 点击 "**Save and Continue**"。
18. 在 "Test Users"下，请点击 "**ADD USERS**"，输入 MDaemon 通过这个应用访问其 Google Drive 的每个 Google 账户，然后点击 "**ADD**"（请参阅下方有关您应用的发布状态 287的注释）。
19. 点击 "**Save and Continue**"。

20. 在 Summary 上，点击位于页面底部的 **"BACK TO DASHBOARD"**。
21. 点击左窗格中的 **"Credentials"**，点击 **(+) Create Credentials** 并选择 **OAuth client ID**。
22. 在 "Application type"下拉框中选择 **"Web application"**，在 "Authorized redirect URIs"下点击 **"+ ADD URIs"**。输入重定向 URI。在 MDaemon 中 Google Drive 页面上显示的 "重定向 URI"是从您默认域的[149] SMTP 主机名称[151]构建而成的示例，在登录到 Webmail时应能适用于该域的用户。您应该在用户登录 Webmail时，为他们前往的任何其他 MDaemon 域，将额外的重定向 URI添加到您的应用程序。例如，"https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive"将适用于在登录 Webmail时，前往 mail.example.com 的任何用户。如果您还托管着名为 "mail.company.test"的域，您需要为该域输入 "重定向 URI"，例如 "https://mail.company.test/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive"。
23. 点击 **"CREATE"**。
24. 将 **"Your Client ID"**和 **"Your Client Secret"**中的值复制到 MDaemon 中 Google Drive 页面上的 *"Google Drive Client ID"*和 *"Google Drive Client Secret"*框中。如果您之前没有这样做，您也可以输入您的 Google Drive APIKey。

> **发布状态** — 这些指示用于通过 发布状态 (被设置成 **"Testing"**)来创建 Google 应用。这需要您添加将使用该应用程序访问其 Google Drive 的每个特定 Google 账户，并且仅限于 100 个用户。此外在 Webmail中，当您的用户被要求授权 MDaemon 访问 Google 时，会显示一条警告消息："确认用户对您的项目有测试访问权限，但应考虑向未验证的应用程序授予对其数据的访问权限所存在的相关风险。"此外，授权在七天后到期，因此每个用户都需要每周重新授权 Google 访问。
>
> 如果您希望删除这些要求和限制，那么您必须将您的状态更改为 **"In Production"**，这可能需要也可能不需要您将 UserType 从外部更改为内部，进行应用程序验证过程，或两者兼而有之。有关应用程序验证和发布状态的更多信息，请参阅以下 Google 文章：设置您的 OAuth 同意屏幕和 OAuth API验证常见问题解答.

在 Webmail中授权 Google Drive

一旦您创建了您的 Google Drive 应用程序，并根据上述说明配置了 MDaemon 的谷 Google Drive 页面，每个希望在 Webmail中访问其 Google Drive 的用户必须首先授权访问才能这样做。要实现这点，每名用户应该：

1. 登录到 Webmail
2. 点击右上角的 "选项"图标，并点击 "云端应用"。
3. 点击 "设置 Google Drive"(这将打开 **OAuth 2.0** 页面)。
4. 点击 "连接至 Google Drive"。
5. 如果未登录，Google Drive 将询问他们登录信息或选择账户。

6. 他们可能会收到一条警告消息，上面写着 "Google 尚未验证此应用程序。您已被授权访问当前正在测试的应用程序。只有在您知道邀请您的开发人员时才继续。"点击 **继续**"。
7. 选择 Webmail可以访问的 Google Drive 功能，点击 **继续**"。
8. 最后一个页面将显示，说明 MDaemon 现在已连接到 Google Drive。然后他们可以关闭此窗口。
9. 现在他们可以从其 Webmail中的 **文档**"页面来访问 Google Drive 了。

还请参阅：

MultiPOP OAuth 118
Dropbox 集成 282

3.6.1.9 类别

"类别"选项位于 MDaemon 的 Remote Administration 界面，具体是：**主页 » Webmail设置 » 类别**。

Webmail支持 LookOut 和 WorldClient 主题中用于邮件、事件、便笺和任务的类别。用户可以通过前往 **选项 » 列**"并勾选 "邮件列表"部分中的 **类别**来向 "邮件列表"添加 "类别"列。

要为 "邮件列表"中的一封或多封邮件设置类别，请选中邮件并右键点击其中之一。使用上下文菜单来设置类别。此外，您可以使用工具栏上的选项打开邮件并设置类别。

类别

在 MDaemon 的 Remote Administration 界面的 "类别"页面上，可以设置 "域类别"，这是用户将在 Webmail中看到的类别的固定列表，但不能对其进行编辑或删除。您还可以创建 "个人类别"的默认列表，向新用户显示。

域类别

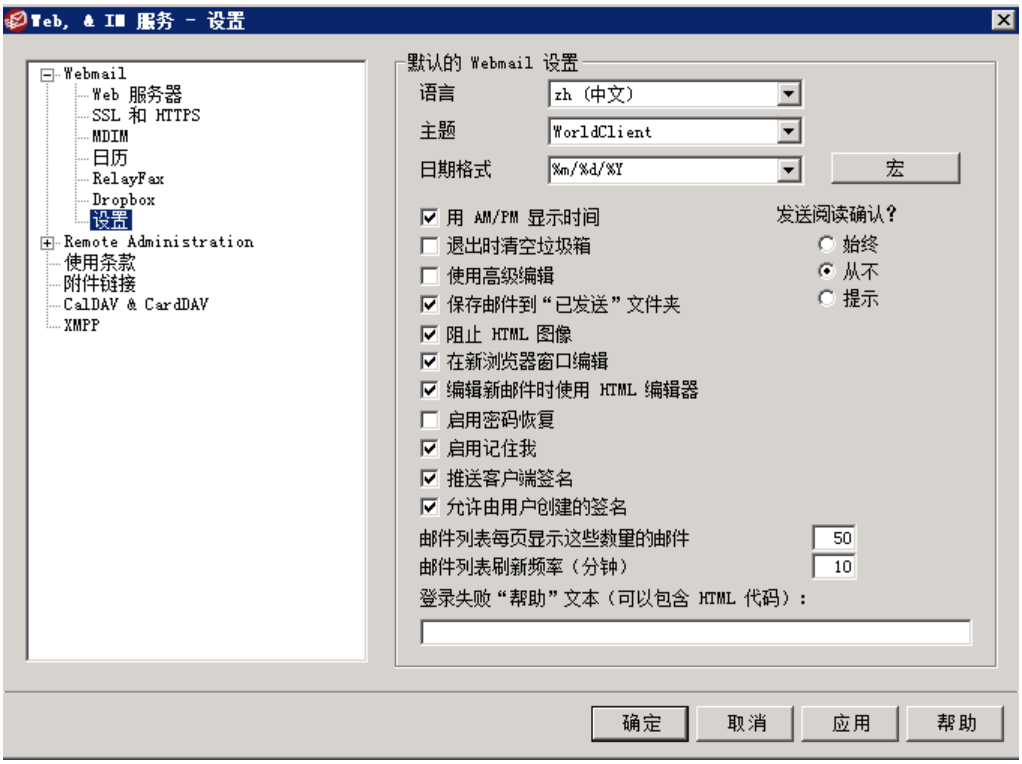
"域类别"是固定类别，无法由您的用户对其进行重新排序、编辑或删除。在启用 *"启用域类别"*这个选项时，将在 Webmail中您用户的类别列表顶部显示该列表。您可以使用提供的选项重新排序、编辑、删除或创建新的域类别。

个人类别

这是将复制到新的 Webmail用户账户的默认类别列表。用户可以完全控制自己的个人类别列表。他们可以重新排序，编辑或删除它们，并且可以创建新的类别。如果您还使用 "域类别"，则这些类别将在每个用户的顶部列出，并且不能被他们编辑或复制。其名称匹配域类别的任何个人类别都能进行隐藏。如果您不希望允许个人类别，则取消勾选 **用户可以编辑个人类别**"这一项。在这种情况下，只会显示域类别。如果也禁用了 "域类别"，则用户无法使用任何 "类别"选项。

有关与管理类别和类别转换有关的 MDaemon 文件的更多详细信息，请参阅：MDaemon\WorldClient\CustomCategories.txt。

3.6.1.10 设置



此屏幕指定 “域管理器”Webmail设置 160屏幕的默认设置。在用户登录 Webmail时，这些选项控制各种 Webmail功能初次为用户提供的服务和工作方式。用户可以稍后通过 Webmail内的 “选项”页面定制其中的大量设置。

默认的 Webmail设置

语言

当您的用户初次登录到所选域时，使用下拉列表框来选择 Webmail界面中的默认语言。用户可以在 Webmail登录页面更改他们的个人语言设置，该选项位于 Webmail中的 “选项» 个性化”中。

主题

当用户第一次登录时，使用下拉列表框来指定用于他们的默认 Webmail主题。用户可以从 Webmail中的 “选项» 个性化”来自定义主题设置。

日期格式

使用此文本框指定 Webmail内的日期将以何种格式显示。点击 “宏”按钮以显示可以在此文本框中使用的宏代码列表。您可以在此控件中使用以下宏：

%A——完整的平日名称

%B——完整的月份名

%d——日（显示为“01-31”）

%d——月（显示为“01-12”）

%y——2 位数字年

%Y——4 位数字年

例如，“%m/%d/%Y”在 Webmail中显示为“12/25/2011”。

宏
点击此按钮以显示可以在*“日期格式”*中使用的宏代码列表。

发送已读确认？
该选项控制 Webmail如何答复包含已读确认请求的入站邮件。

始终
如果选定此项，MDaemon 将向发件人发送通知，告之邮件已读。收到邮件的 Webmail用户将不会看到任何关于已请求或已回复已读确认的提示。

从不
如果您希望 Webmail忽略已读确认请求，请选择此选项。

提示
如果您希望每次打开邮件收到此请求时，都询问 Webmail用户是否发送已读确认，请选择此选项。

使用 AM/PM 显示时间
如果您希望在 Webmail中使用带 AM/PM 的 12 小时时钟作为显示时间，请点击此选项。如果您希望使用 24 小时时钟，请清空此复选框。个人用户可以通过 Webmail中位于*“选项 » 日历”*页面的“以AM/PM 格式显示我的时间”选项修改这项设置。

退出时清空垃圾箱
用户注销 Webmail时，此选项可以清空用户的垃圾站。个人用户可以从 Webmail中的“选项» 个性化”页面修改这项设置。

使用高级编写
如果您希望用户在 Webmail中看到高级编写屏幕而不是默认情况下的常规编写屏幕，请勾选此选框。个人用户可以从 Webmail中的“选项» 编写”修改这项设置。

保存邮件到“已发送”文件夹
如果您希望发送的每封邮件副本都被保存到您邮箱中的*“已发送”*文件夹，请点击该选项。个人用户可以从 Webmail中的“选项» 编写”页面修改这项设置。

阻止 HTML 图像
如果您希望在 Webmail中查看 HTML 电子邮件时阻止远程图像自动显示，请启用此选框。用户必须点击浏览器窗口中邮件上方的一栏，才能查看图像。这是垃圾邮件防范功

能，因为大量垃圾邮件包含带有特殊 URL 的图像，这些 URL识别查看此图像的用户的邮件地址，以向垃圾邮件制造者确保这是有效地址。默认情况下启用此项。

在新浏览器窗口编写
如果您希望打开一个单独的浏览器窗口来编写邮件而不是简单地将主窗口切换到编写屏幕，请点击此选项。如果您不希望打开单独的窗口，清空此框。个人用户可以从 Webmail中的 "选项» 编写"页面修改这项设置。

编辑新邮件时使用 HTML 编辑器
如果您希望 Webmail在默认情况下能让用户看见 HTML 编写编辑器，请勾选此框。他们可以从 Webmail中的选项» 编写为他们自己控制这项设置。

启用密码恢复
若启用此项，有权编辑其密码[603]的用户将能在 Webmail中输入备选的电子邮件地址，可以向其发送链接，以便在用户忘记密码时重置其密码。要设置此功能，用户必须在 Webmail中的 "选项 » 安全"页面上输入密码恢复邮件地址及当前密码。一旦设置完毕，如果用户尝试使用不正确的密码登录 Webmail，将显示 "忘记密码？"这个链接。该链接将他们带往一个页面，让其确认密码恢复邮件地址。如果输入正确，将发送一封电子邮件，其中提供一个转至更改密码页面的链接。默认情况下禁用此功能。

您可以通过向 Webmail用户的 user.ini 文件 (例如 \Users\example.com\frank\WC\user.ini)添加以下键来按用户启用或禁用此项：

```
[User]
EnablePasswordRecovery=Yes （或 "=No"来为用户禁用此项）
```

允许双重验证记住我 (也适用于 Remote Admin)
当某人在登录 Webmail或 Remote Admin 时使用 "双重验证 (2FA)"时，通常在 2FA 验证页面上有一个可供用户使用的 "记住我"选项，这将阻止服务器再次要求该用户设置 2FA 天数 (请参阅下方的 *"启用记住我"*选项)。如果您不希望显示 "2FA 记住我"选项，请清除此复选框，这意味着所有启用 2FA 的用户每次登录时都必须输入 2FA 代码。**注意：**此项仅在 MDaemon Remote Administration (MDRA)[293] web 界面中可用。

启用 "记住我"
如果您希望 MDaemon Webmail的登录页面上存在 *"记住我"*勾选框，(在域的用户通过 https[274] 端口进行连接时)，请勾选此框。如果用户在登录时勾选此框，则将为该设备记住其凭证。然后，无论他们何时使用该设备连接到 Webmail，他们都将自动登录，直至他们手动注销其账户或其 "记住我"令牌过期。

默认情况下，在用户被强制重新登录之前，最多可以记住30天的用户凭证。如果您希望延长过期时间，可以通过更改 *"这些天后过期记住我令牌"*这个选项的值 (位于 MDaemon Remote Administration (MDRA)[293] web 界面)来实现这点。您也可以通过编辑 RememberUserExpiration=30 键值 ([Default:Settings] 部分，位于 Domains.ini 文件，在 \MDaemon\WorldClient\ 文件夹中)。过期值的最大值可以设置成 365 天。**请注意：**双重验证[603] (2FA) 拥有其自身的 "记住我"键值 (TwoFactorAuthRememberUserExpiration=30)，位于 [Default:Settings] 部分，Domains.ini 文件，位于 \MDaemon\WorldClient\ 文件夹。因此，当 2FA 记住我令牌过期时，即使常规令牌仍然有效，登录时也需要 2FA。

默认禁用 *"记住我"选项，并应用至您的所有域。如果您希望为特定的 Webmail域覆盖此设置，请使用 "记住我"*设置，位于 MDaemon 桌面界面 "域管理器"的 Webmail[160] 屏幕。

因为 *"记住我"*允许用户在多台设备上进行永久登录，因此用户不应该在公共网络上使用它。此外，如果您怀疑某个账户可能存在安全漏洞时，MDRA 中有一个 *"重置记住我"*选项，帮助您为所有用户重置 "记住我"令牌。这将要求所有用户再次登录。

推送客户端签名
如果您希望将默认客户端签名[113]推送至 Webmail用户，请勾选此框。在 Webmail中，这将在以下签名选项下创建一个名为 "系统"的签名：**选项 » 编写**。然后，用户可以选择在编写新邮件时，将此签名自动插入到编写视图中。如果您希望为特定的域定制或启用/禁用客户端签名，请使用 "域管理器"的客户端签名[170]和 Webmail[160] 选项。

允许用户创建的签名
如果您希望允许用户在 Webmail中创建自己的自定义签名，请选中此框。然后用户可以选择在编写邮件时希望将哪些签名自动插入到编写视图中。在您不允许用户创建的签名，但启用了上方的 *"推送客户端签名"*选项时，只会自动插入客户端签名[113] (例如 Webmail中的 "系统"签名)。在 Webmail中，签名选项位于：**选项 » 编写**。

允许用户编辑其别名显示名称
如果您希望允许用户编辑与其账户关联的任何别名的显示名称，请勾选此选项。这可以通过使用 *"编辑别名显示名称"*选项 (位于 Webmail的 Pro 主题) 来实现。默认情况下，禁用该选项。**请注意：**此项仅在 MDaemon Remote Administration (MDRA)[293] 的 web 界面中可用。

邮件列表每页显示这些数量的邮件
这是在您的每一个邮件文件夹中，每一页邮件列表显示的邮件数。如果一个文件夹中包含超出这个数量的邮件，那么将会在列表的上方和下方出现几个控件，帮助您过渡到其他页。个人用户可以从 WorldClient 中的 "选项» 个性化"修改这项设置。

邮件列表刷新频率 (分钟)
这是 Webmail在自动刷新邮件列表前等待的分钟数。个人用户可以从 Webmail中的 "选项» 个性化"修改这项设置。

登录失败 "帮助"文本 (可包含 HTML 代码)
您可以使用此选项指定在用户遇到登录问题时，显示在 Webmail登录页面上的文本句 (纯文本或 HTML 格式)。该文本在以下默认文本下方显示：*"错误登录，请重试。如果您需要帮助，请联系您的邮件管理员。"*可使用此文本引导用户到有关登录 Webmail的帮助页面或联系信息。

自定义已允许发件人和已阻止发件人文件夹

您可以通过编辑 MDaemon\WorldClient\ 文件夹内的特定文件来定制各种标准的 Webmail功能：

默认情况下，您可以为 Webmail用户隐藏 已允许发件人和已阻止发件人文件夹。要实现这点，请打开 MDaemon\WorldClient\Domains.ini，并在 [Default:UserDefaults] 部分下，将 "HideWhiteListFolder="或 "HideBlackListFolder="的值从 "否"更改成 "是"。您可以通过编辑 User.ini 文件 (位于 [User] 部分下)来为特定的用户隐藏或显示这些文件夹。

还请参阅：

域管理器 » Webmail设置 160

3.6.1.11 贴牌

如果您希望定制在登录页面和导航边栏出现的 Webmail横幅标语图像，您可以从 MDaemon 的 Remote Administration 293 web 界面来实现这点。

要使用您自己的定制图像：

1. 请点击 "定制"部分的 "使用定制图像"。
2. 在 "登录页面图像"部分，请使用 "选择文件"或 "浏览"选项（取决于您的浏览器）来选择您希望上传的文件。此部分还列出了登录页面图像的默认大小。
3. 点击 "上传定制图像"。
4. 请为 "导航侧栏图像"和 "反转导航侧栏图像"重复第二和第三步骤。

将在其相应的框中出现已上传的图像，并取代 Webmail的默认图像。

3.6.2 Remote Administration

MDaemon's Remote Administration (MDRA) 界面的设计旨在允许您使用一个 web 浏览器来远程管理 MDaemon。它是一个服务器应用程序，设计成与 MDaemon 在同一台计算机上的后台运行。要访问 Remote Administration，请输入远程管理服务器所位于的 URL 和端口号打开您的浏览器（例如 www.example.com:1000）。在提供您的登录认证后，将给予您控制和设置 MDaemon 的权限。您能够访问的设置类型和数量取决于您被给予的访问级别。可以向 Remote Administration 用户提供三个访问级别：全局、域和用户。

全局管理员——全局管理员是那些拥有全局访问权限的用户，可以在 MDaemon 中他们的账号设置下启用。全局访问意味着用户可以通过 Remote Administration 查看和配置可以访问的任何设置与控制。全局管理员可以添加、编辑和删除用户、域和邮件列表。他们可以编辑产品的 INI 文件，指定其他用户作为域管理员，管理密码等；他们拥有完全的管理控制权限。

域管理员——与全局管理员类似，域管理员可以通过 Remote Administration 完全管理所有用户和可访问的产品设置。其管理控制受限于此域、他们有权访问的域以及在 "Web 服务 603"屏幕上指定的权限。域管理员和他们所控制的域是从 Remote Administration 中由全局管理员指定的，或者由其他可以访问那些域的管理员指定。

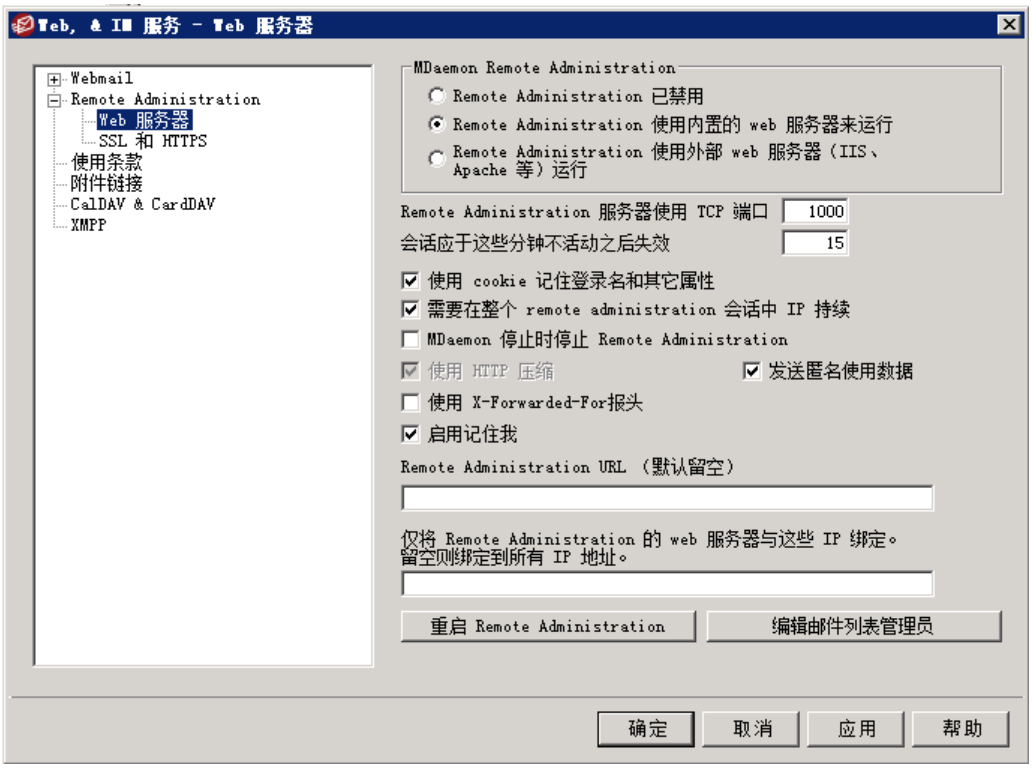
用户——用户访问是 Remote Administration 访问中的最低级别。例如，MDaemon 用户可以登录到 Remote Administration，并查看他们的个人账户设置以及编辑他们的 MultiPOP 条目、邮件过滤器和自动回复等等。可进行编辑的设置类型和数量取决于每位用户账户设置中被给予的权限。

拥有权限访问 Webmail和 Remote Administration 的任何人都可以从 Webmail内访问 Remote Administration，而不用分别登录。点击 "选项"下的 "高级设置"链接可以从 Webmail中以一个单独的浏览器窗口打开 Remote Administration。

还请参阅：

Remote Administration » Web 服务器 294
Remote Administration » HTTPS 297
模板管理器 » Web 服务 672
账户编辑器 » Web 服务 603
在 IIS 下运行 Remote Administration 300

3.6.2.1 Web 服务器



MDaemon Remote Administration

禁用 Remote Administration
选择此项来禁用 Remote Administration。您还可以从 "文件"菜单或从主 MDaemon GUI 上 "统计"选项卡的 "服务器"部分切换 Remote Administration 的活动/闲置状态。

Remote Administration 使用内置的 web 服务器来运行
选择此项以使用 MDaemon 的内置 web 服务器来运行 Remote Administration。您还可以从 "文件"菜单或从主 MDaemon GUI 上 "统计"选项卡的 "服务器"部分切换 Remote Administration 的活动/闲置状态。

Remote Administration 使用外部 web 服务器 (IIS 和 Apache 等)运行
如果您希望 Remote Administration 运行在 IIS 或其他 web 服务器下而不是 MDaemon 的内置服务器，请选择此选项。这防止在访问某些 GUI 元素时和您的备用服务器产生冲突。

要了解更多详细信息，请参阅在 IIS 下运行 Remote Administration 300。

Remote Administration 服务器使用 TCP 端口
Remote Administration 将会监听此端口来响应您 web 浏览器的连接。默认的端口是 1000。

闲置 xx 分钟后会话过期
当您登录到 Remote Administration 时，这个值是允许您的会话在 Remote Administration 关闭它之前可以处于闲置状态的时间。默认值是 15 分钟。

其他设置

使用 cookies 来记住登录名和其它属性
默认情况下，Remote Administration 界面使用 cookies，这样用户的浏览器便能记住用户的登录姓名和其他属性。如果您不希望使用 cookies，请禁用该勾选框。使用此功能给予用户更多的 "自定义"登录体验，但需要在他们的浏览器中，启用对 cookie 的支持。

持续通过 Remote Administration 会话请求 IP
作为一个附加的安全措施，在会话开始时，您可以点击此复选框使得 Remote Administration 限制每一个会话到您连接的 IP 地址。因此，没有人可以 "窃听"会话，因为在不断请求 IP。这个配置更安全，但如果您使用代理服务器或动态指定与更改 IP 地址的因特网连接，该配置可能会引起一些问题。

在停止 MDaemon 时停止 Remote Administration
如果您希望无论何时，只要 MDaemon 关闭，也关闭 Remote Administration，请点击该选项。否则，Remote Administration 服务会在后台一直运行。

使用 HTTP 压缩
如果您希望在您的 Remote Administration 通话中使用 HTTP 压缩，请单击此复选框。

发送匿名使用数据
默认情况下，MDaemon 的 Remote Administration web 客户端发送匿名的良性使用数据，例如：操作系统所用、浏览器版本所用和语言等。MDaemon Technologies 使用这些数据来帮助我们改善 Remote Administration。如果您不希望发送匿名使用数据，请禁用此项。

X-Forwarded-For 报头
勾选此框来启用 X-Forwarded-For 报头，有时代理服务器会添加这些报头。默认情况下，禁用该选项。只有在您的代理服务器插入此报头时，才启用此项。

启用 "记住我"
如果您希望 Remote Administration 的登录页面上存在 *"记住我"*勾选框，(在域的用户通过 https 297 端口进行连接时)，请勾选此框。如果用户在登录时勾选此框，则将为该设备记住其凭证。然后，无论他们何时使用该设备进行连接，他们都将自动登录，直至他们手动注销其账户或其 "记住我"令牌过期。

默认情况下，在用户被强制重新登录之前，最多可以记住30天的用户凭证。如果您希望延长过期时间，可以通过更改 *"这些天后过期记住我令牌"*这个选项的值（位于 MDaemon Remote Administration (MDRA) 界面）来实现这点。您也可以通过编辑 RememberUserExpiration=30 键值（[Default:Settings] 部分，位于 Domains.ini 文件，在 \MDaemon\WorldClient\ 文件夹中）。过期值的最大值可以设置成 365 天。**请注意：**双重验证 603 (2FA) 拥有其自身的"记住我"键值 (TwoFactorAuthRememberUserExpiration=30)，位于 [Default:Settings] 部分，Domains.ini 文件，位于 \MDaemon\WorldClient\ 文件夹。因此，当 2FA 记住我令牌过期时，即使常规令牌仍然有效，登录时也需要 2FA。

默认情况下，禁用 *"记住我"*选项。

因为 *"记住我"*允许用户在多台设备上进行永久登录，因此用户不应该在公共网络上使用它。此外，如果您怀疑某个账户可能存在安全漏洞时，MDRA 中有一个 *"重置记住我"*选项，帮助您为所有用户重置"记住我"令牌。这将要求所有用户再次登录。

Remote Administration URL
当用户点击"高级设置"链接以通过 Remote Administration 来编辑他们的"账户设置"时，这是 Webmail 会在内部使用的 URL。如果您使用内置的 web 服务器来运行 Remote Administration，请将此字段留空。如果您使用其他 web 服务器例如 IIS，并且您已将 Remote Administration 配置为在某 URL 或 IP 地址上运行，请在此处指定该 URL。

仅绑定 Remote Administration 的 web 服务器到这些 IP。
如果您希望仅限制 Remote Administration 服务器到某些 IP 地址，请在此处指定那些地址，由逗号分隔。如果您留空此字段，那么 Remote Administration 将监控您为"域 149"指定的所有 IP 地址。

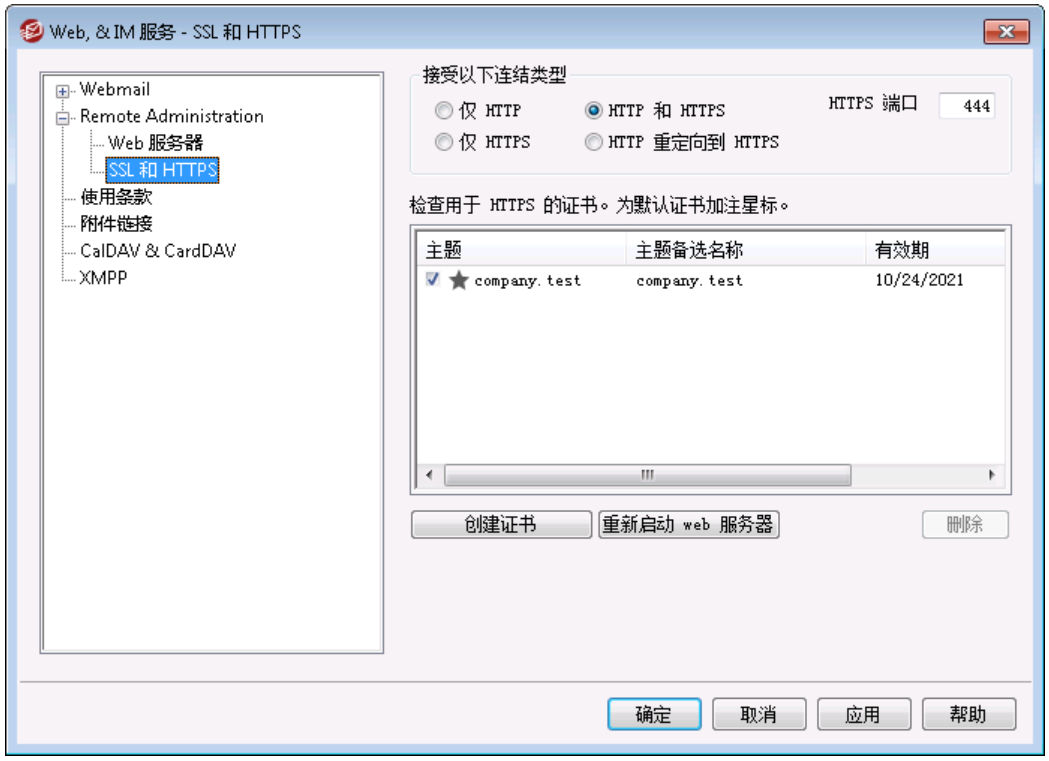
重启 Remote Administration（当端口或 IIS 值更改时需要）
如果您希望重启 Remote Administration 服务器，请点击此按钮。请注意：更改端口设置时，为了识别新设置，您必须重启 Remote Administration。

编辑邮件列表管理员
如果您希望打开邮件列表管理员文件进行查看或编辑，请点击此项。

还请参阅：

Remote Administration 293
Remote Administration » HTTPS 297
在 IIS 下运行 Remote Administration 300
模板管理器 » Web 服务 672
账户编辑器 » Web 服务 603

3.6.2.2 SSL & HTTPS



MDaemon 的内置 Web 服务器支持安全套接字层 (SSL)协议。SSL 是保护服务器/客户端 web 通信安全的标准方案。它提供了服务器验证、数据加密和用于 TCP/IP 连接的可选客户端验证。此外，由于在所有主要的浏览器中都内置了 HTTPS 支持 (比如通过 SSL 的 HTTP)，只要在您的服务器上安装一个有效的数字认证将会激活连接客户端的 SSL 能力。

启用和配置 Remote Administration 来使用 HTTPS 的选项位于“设置» Web & IM 服务» Remote Administration”下的“SSL & HTTPS”屏幕。不过为方便起见，这些选项也镜像到“安全» 安全设置» SSL & TLS » Remote Administration”。

要了解 SSL 协议与证书的更多详情，请参阅：“SSL 和证书 479”

在使用 MDaemon 的内置 web 服务器时，该屏幕仅应用于 Remote Administration。如果您配置 Remote Administration 使用其它的网络服务器，如 IIS，则不会使用这些选项——SSL/HTTPS 支持必需使用其它网络服务器的工具来配置。

接受以下连接类型

仅 HTTP
如果您不允许任何 HTTPS 连接到 Remote Administration，请选择此项。仅接受 HTTP 连接。

HTTP 和 HTTPS
如果您希望在 Remote Administration 中启用 SSL 支持，但不希望强制您的 Remote Administration 用户使用 HTTPS，请选择此选项。Remote Administration 将监听在下方指定的 HTTPS 端口上的连接，但是它仍会响应 Remote Administration TCP 端口上正常的 http 连接，该端口在 "Web 服务器"[294]屏幕上指定。

仅 HTTPS
如果您希望连接到 Remote Administration 时要求 HTTPS，选择此选项。当此选项启用时，Remote Administration 只会响应 HTTPS 连接——不会响应 HTTP 请求。

HTTP 重定向到 HTTPS
如果您希望重定向所有的 HTTP 连接到在 HTTPS 端口上的 HTTPS，请选择此选项。

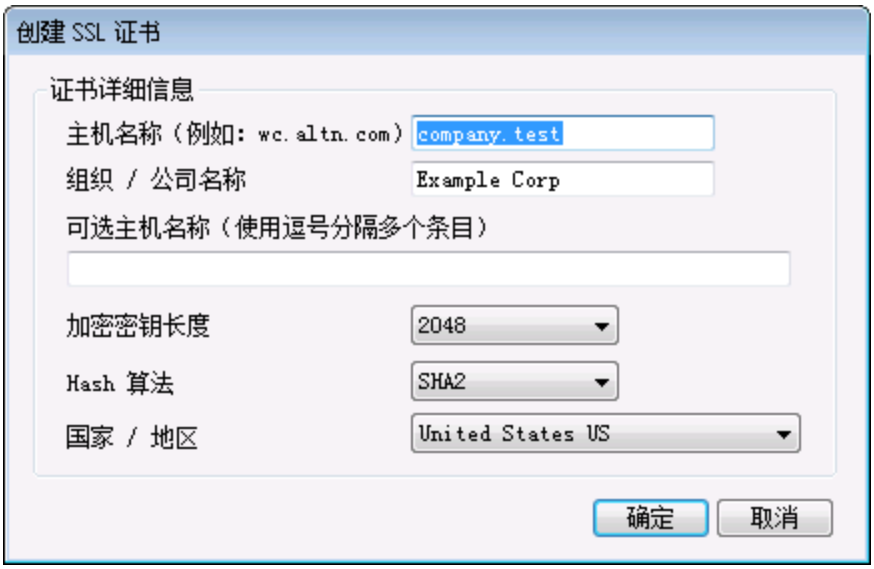
HTTPS 端口
这是 Remote Administration 将为 SSL 连接监听的 TCP 端口。默认的 SSL 端口是 444. 如果使用默认的 SSL 端口，在通过 HTTPS 连接时，您不必在 Remote Administration 的 URL 中包含端口号（例如 "https://example.com" 等于 "https://example.com:444"）。

这不同于在 "Web 服务器"[294]屏幕上指定的 Remote Administration 端口。如果您仍然允许 HTTP 连接到 Remote Administration，则那些连接必须使用其他端口才能连接成功。HTTPS 连接必须使用 HTTPS 端口。

选择用于 HTTPS/SSL 的证书
此选框显示您的 SSL 证书。选中您希望激活的任何证书旁边的框。点击要设置为默认证书旁边的星号。MDaemon 支持 TLS 协议的服务器名称指示 (SNI) 扩展，它允许为您的每个服务器主机名使用不同的证书。MDaemon 将查看活动证书，并在 "主题备选名称" 字段中选择具有所请求主机名的证书（您可以在创建证书时指定备选名称）。如果客户端未请求主机名，或者未找到匹配的证书，则使用默认证书。双击证书以在 Windows "证书" 对话框中将其打开以供审阅（仅在应用程序界面中可用，而不在基于浏览器的远程管理中可用）。

删除
在此列表中选择一个证书，然后点击此按钮将其删除。会打开一个确认框并询问您是否确定删除该证书。

创建证书
点击此按钮来打开 "创建 SSL 证书" 对话框。



证书详细信息

主机名
在创建证书时，输入您用户将会连接的主机名称（例如“wc.example.com”）。

企业/公司名
在此输入“拥有”此证书的机构或公司。

替换主机名（用逗号分隔多个项目）
如果您的用户可能连接到备选主机名，您也希望此证书应用到那些名称，那么请输入那些域名，通过逗号分隔。允许通配符，所以“*.example.com”可以应用于所有 example.com 的子域（例如“wc.example.com”、“mail.example.com”等等）。

> MDaemon 支持 TLS 协议的服务器名称指示（SNI）扩展，它允许为您的每个服务器主机名使用不同的证书。MDaemon 将查看活动证书，并在其“使用者备用名称”字段中选择具有所请求主机名的证书。如果客户端未请求主机名，或者未找到匹配的证书，则使用默认证书。

密钥长度
为此证书选择所需位长度的加密密钥。加密密钥的位数越长，已传输的数据也将越安全。不过请注意，并非所有的应用程序都支持大于 512 的密钥长度。

国家/地区
选择您的服务器所在国家或地区。

Hash 算法
选择您希望使用的 hash 算法：SHA1 或 SHA2。默认设置是 SHA2。

重启 web 服务器

点击此按钮来重启 web 服务器。使用新证书前，必须重启 web 服务器。

使用 Let's Encrypt 来管理您的证书

Let's Encrypt 是一个证书颁发机构 (CA)，通过专门设计的自动化流程来为 "传输安全层 (TLS)"加密提供免费的证书，该流程使您可以免于现在复杂的手动创建、验证、签名、安装、以及续订证书这些用来保护网站安全的环节。

要支持使用 Let's Encrypt 的自动化流程来管理证书，提供 Let's Encrypt 496 屏幕来帮助您轻松简便地配置和运行 PowerShell 脚本，位于 "MDaemon\LetsEncrypt"文件夹。运行该脚本将使一切为 LetsEncrypt 准备就绪，包括将一些必要的文件放置在 WebmailHTTP 的目录中来完成 http-01 挑战。它将 SMTP 主机名 151 (属于默认域 149)用作证书域，包含您已指定的任何*备选主机名称*，检索证书，将其导入 Windows，并配置 MDaemon 如何使用针对 MDaemon、Webmail 和 Remote Administration 的证书。此外，该脚本将在名为 LetsEncrypt.log 的 "MDaemon\Logs\"目录中创建一个日志文件 LetsEncrypt.log。每次运行脚本时,都会删除并重新创建该日志文件，并且包含脚本的开始日期和时间。此外，如果您指定了*通知的管理员邮件*，将在出错时发送通知邮件。请参阅 Let's Encrypt 496 主题了解更多信息。

更多 SSL 协议与证书的更多信息，请参阅：

在 IIS 下运行 Remote Administration 300
SSL 与证书 479
创建和使用 SSL 证书 764

要了解有关 Remote Administration 的更多信息，请参阅：

远程配置 293
Remote Administration » Web 服务器 294
Web 访问默认值 672
账户编辑器 » Web 603

3.6.2.3 在 IIS 下运行 Remote Administration

MDaemon 配备了一个内置的 web 服务器，这就意味着 Remote Administration 不需要互联网信息服务器 (IIS)来处理。但是，它确实支持 IIS，因此可以作为一个 ISAPI DLL 运行。

要配置成在 IIS 5 下运行：

1. 停止 Remote Administration 的运行。您只要在 MDaemon GUI 左窗格中位于 "*服务器*"之下的 Remote Administration 条目上右单击，接着点击 "**切换活动/闲置**"即可。
2. 打开 IIS 管理程序 (**开始→设置→控制面板→管理工具→因特网服务管理器**)。
3. 右键单击**默认网站**并选择**新建→虚拟目录**。

4. 根据 "向导"指领您的步骤创建 "虚拟目录"。下面是建议输入到 "向导"中的名称和数据位置，但会根据您的 MDaemon 及其 Remote Administration 组件的安装位置有所改变。

   a. 别名: "WebAdmin"。点击**下一步**。
   b. 目录: "c:\mdaemon\webadmin\templates"。点击"**下一步**"。
   c. 点击**下一步**。
   d. 点击**完成**。

5. 将执行许可设置成**仅脚本**。

6. 将应用程序保护级别设置成 **低(IIS 进程)**。

7. 点击虚拟目录标签上应用程序设置部分的**配置**按钮。

8. 在**映射**标签上点击**添加**。

9. 在"**可执行**"字段输入 "c:\mdaemon\webadmin\templates\WebAdmin.dll"。请注意：该字段不能包括空格。如果路径中包括空格，则必须转换成 8.3 格式。 dir /x 命令将显示一个文件或目录的 8.3 名称。

10. 在"**扩展名**"字段输入 ".wdm"并选择"**全部动作**"这个单选按钮。

11. 点击**脚本引擎**框。

12. 点击**确定**。

13. 如果您希望可以删除所有其他映射，则点击**确定**。

14. 在"**文档**"选项卡上添加 "login.wdm"作为 "默认文档"并从此列表删除所有其他条目。

15. 在 MDaemon 中选择"**设置 ➜ Web & IM 服务 ➜ Remote Administration**"并点击 "**Remote Administration 使用内置的 web 服务器来运行**"。

16. 在 "**Remote Administration URL**"中输入 "/WebAdmin/login.wdm"。

17. 点击**确定**。

要配置成在 IIS 6 下运行：

为 Remote Administration 创建一个新的应用程序池：

1. 停止 Remote Administration 的运行。您只要在 MDaemon GUI 左窗格中位于 "*服务器*"之下的 Remote Administration 条目上右单击，接着点击 "**切换活动/闲置**"即可。

2. 打开 IIS 管理程序 (**开始 ➜ 设置 ➜ 控制面板 ➜ 管理工具 ➜ 因特网服务管理器**)。

3. 右单击 **应用程序池**。

4. 点击**新建 ➜ 应用程序池**。

5. 在应用程序池 ID 字段中输入 "Alt-N"并点击**确定**。

6. 右单击“**Alt-N**”
7. 点击**属性**。
8. 点击**性能**标签。
9. 清除“**在空闲后关闭工作进程**”与“**限制内核请求队列**”。
10. 点击**标识**标签。
11. 在预定义下拉列表中选择**本地系统**。
12. 点击**确定**。

为 Remote Administration 创建虚拟文件夹

1. 打开 IIS 管理程序（“**开始**➪**设置**➪**控制面板**➪**管理工具(互联网服务管理器)**”。
2. 右单击您的网站并选择“新建”(虚拟目录)。
3. 为虚拟目录指定别名(例如“WebAdmin”)。
4. 在“路径”字段，输入路径到 Remote Administration 的“模板”目录，例如“C:\Program Files\Alt-N Technologies\WebAdmin\Templates”。
5. 勾选“读取”和“运行脚本”这两个选项。
6. 完成向导并右单击已创建的虚拟目录。
7. 选择“属性”。
8. 在“生目录”选项卡上将应用程序池更改为“Alt-N”。
9. 点击配置按钮。
10. 点击“添加”来添加一个 ISAPI 扩展映射。
11. 在“可执行”字段输入文件 WebAdmin.dll 的路径。例如“C:\Program Files\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll”。
12. 在“扩展名”字段输入“.wdm”。
13. 点击**脚本引擎**与**验证文件是否存在**的选框。
14. 点击**确定**。
15. 如果您希望可以删除所有其他映射，则点击**确定**。
16. 选择**文档**标签。

17. 确保勾选了**启用默认内容**页。

18. 确保只有“login.wdm”在队列中。

19. 点击**确定**并退出虚拟目录属性对话框。

添加 .WDM 到允许网络扩展的列表：

1. 点击**网络服务器扩展**文件夹(在 IIS MMC 中)。

2. 点击**添加新 web 服务扩展**。

3. 在扩展名字段输入“WebAdmin”。

4. 点击**添加**并浏览以找到 WebAdmin ISAPI 扩展。例如：
C:\Program Files\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll。

5. 勾选**设置扩展状态为允许**。

6. 点击**确定**。

7. 在 MDaemon 中选择“**设置 Web & IM 服务 Remote Administration**”并点击“**Remote Administration 使用内置的 web 服务器来运行**”。

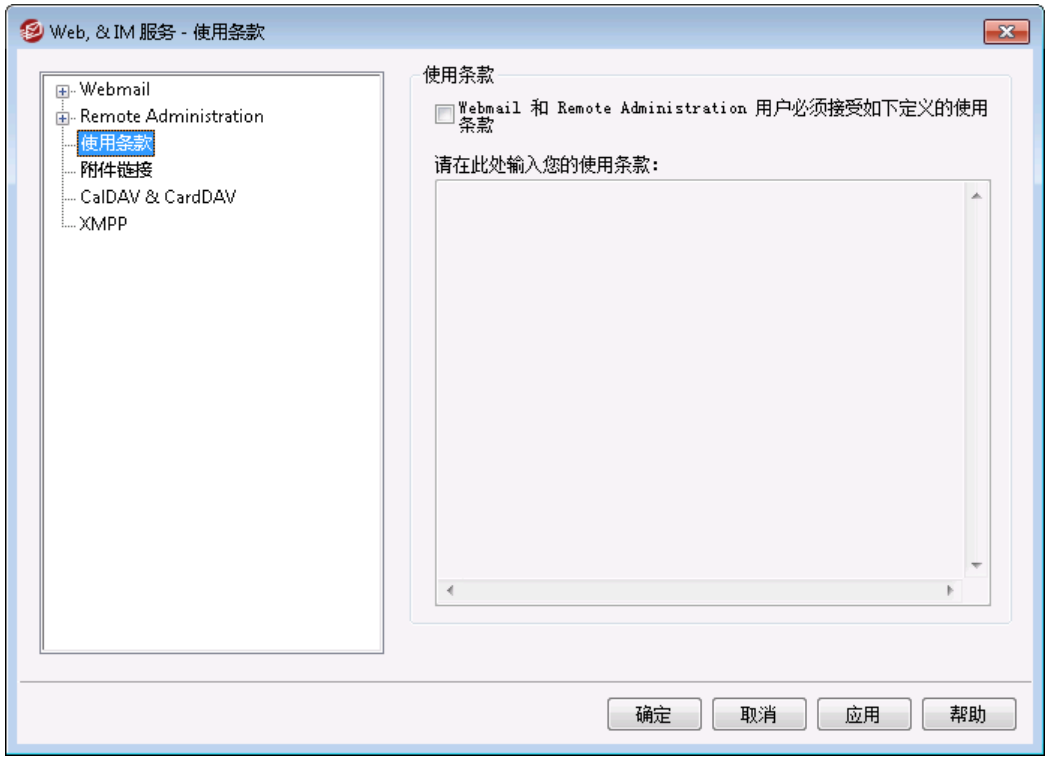
8. 在“**Remote Administration URL**”中输入“/WebAdmin/login.wdm”。

9. 点击**确定**。

要了解有关 Remote Administration 的更多信息，请参阅：

Remote Administration 293
Remote Administration » Web 服务器 294
Remote Administration » SSL & HTTPS 297
模板管理器 » Web 服务 672
账户编辑器 » Web 服务 603

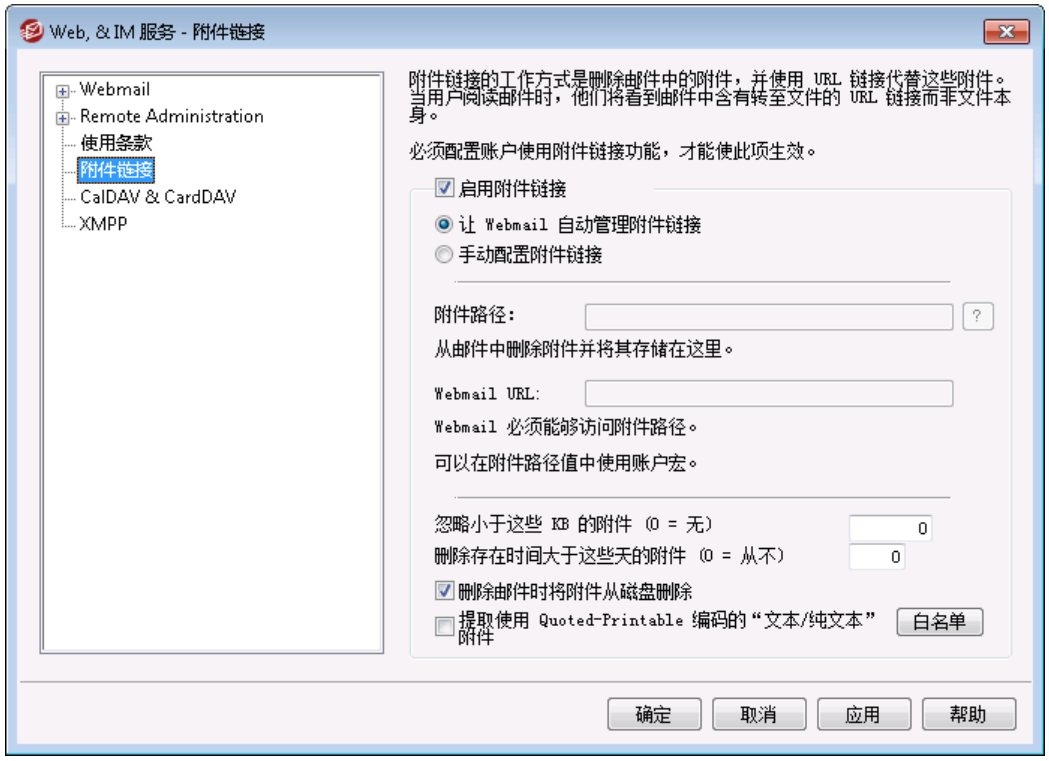
3.6.3 使用条款



Webmail和Remote Administrations用户必须接受下方的使用条款

如果您希望要求Webmail和Remote Administration用户在每次登录时接受使用条款声明，请选中此框并在提供的空白处输入您的使用条款声明。

3.6.4 附件链接



附件链接（*设置» Web & IM 服务» 附件链接*）让 MDaemon 能够删除入站邮件中的所有附件，将其存储在指定位置，并将 URL 链接放到每封邮件提取附件时的文件位置。之后收件人便可点击这些链接来下载文件。当您的用户检索邮件或者同步化邮件文件夹时，这样做能够显著加速邮件的处理，因为邮件没有大量附件。同样还能提高安全性与对您用户的保护级别，因为附件存储于一个中心位置，可供管理员监控，并且不能通过邮件客户端（客户端有可能会自动执行）自动下载。此外，如果您选择*“让 Webmail 自动管理附件链接”*这个选项，将自动处理对于文件位置的管理和 WebmailURL。如果您选择手动管理附件链接，您可以指定存储这些文件的位置，并且您可以使用特殊宏使该位置动态化。若您希望使用附件链接功能，必须使用此屏幕上的该选项将其全局启用，而且您希望使用的每个账户必须按照账户编辑器中附件 616 屏幕上的内容进行专门配置。在这个屏幕上还有一个选项将附件链接功能应用到出站邮件；将提取账户的出站邮件中的附件，并使用转至已存储文件的链接替代附件。最后，MDaemon 将要放入邮件中的附件链接将不包含直接文件路径。而是包含该服务器所使用的独特标识符（GUID）来映射文件到实际路径。GUID 映射图存储在 AttachmentLinking.dat 文件中。

附件链接功能将尝试使用 MIME 报头中提供的文件名（若存在）。如果文件名长度超过 50 个字符，那么仅会使用前 50 个字符。如果文件名缺少扩展名，则附加“.att”。

默认情况下，“附件链接”功能会将“MDaemon 使用这些链接替换以下文件：”这个文本 放入特定邮件。如果您希望更改这个文本，请向 \app\ 文件夹中的 MDaemon.ini 文件添加以下键：

```
[AttachmentLinking]
HeaderText=This Is My Text。
```

启用附件链接
点击此选择框为账户编辑器附件[616]屏幕上专门配置为使用“附件链接”的所有账户启用此功能。当您启用此全局选项，会询问您是否希望为所有 MDaemon 账户启用该账户的特定选项。如果您选择“是”，那么将为所有账户启用附件链接，同时启用新建账户[683]模板下的相应选项。如果您选择“否”，那么将启用附件链接功能，不过将不启用该账户的特定选项——您必须为您想要使用的各个账户手动启用这些选项。启用附件链接时，Webmail服务器必须处于激活状态。

让 Webmail自动管理附件链接
启用附件链接时，这是默认选项。如果您希望让 Webmail自动处理附件链接，请使用此选项。被提取的文件将存储在：“...\MDaemon\Attachments\$DOMAIN$\$MAILBOX$\”。

手动配置“附件链接”
如果您希望指定提取文件附件时存储的文件夹，请选择此选项。当您选择该选项时，您必须同时指定附件路径和 WebmailURL。

附件路径
使用此文本框指定您希望存储已提取文件附件的文件夹。您可以设置静态的文件路径或使用模板[669]和脚本[707]宏以动态化该路径。例如，“$ROOTDIR$\Attachments\$DOMAIN$\”会把所有附件归组到一个子文件夹，此子文件夹是根据用户所在域命名的，位于包含于 MDaemon 根文件夹下名为“附件”的另一个子文件夹下（通常是 C:\MDaemon\）。所以，对于“user1@example.com”上方示例会使得被提取的附件置于C:\MDaemon\Attachments\example.com\ 子文件夹中。您可以通过附加“$MAILBOX$”模板宏到上述示例中，从而进一步细分附件存储。这将使 user1 的文件存储于“example.com\”下名为“user1”的子文件夹中。因此新的文件路径是：“C:\MDaemon\Attachments\example.com\user1\。

Webmail URL
在此输入 Webmail的 URL（例如：“http://mail.example.com:3000/WorldClient.dll”）。当插入此链接到邮件的已提取附件时，MDaemon 会使用此 URL。

忽略小于这些 KB 的附件（0 = 无）
这是从邮件提取附件前需要的最小附件大小。如果您不希望提取很小的附件，请使用此项。如果将此值设置成“0”，不管附件有多小，附件链接功能将始终提取所有附件。

删除存在时间长于这些天的附件（0=从不）
如果您希望为附件设置将要存储的天数限制，请使用此项。作为日常清理事件的一部分，如果默认的附件文件夹或其子文件夹中含有这些存在时间超过指定限制的附件，MDaemon 将删除这些附件。默认的文件夹是：“<MDaemonRoot>\Attachments\...”。如果您通过自定义将附件文件夹指向其他位置，就不会删除这些附件。默认情况下，禁用该选项（设置成“0”）。

当邮件被删除时从磁盘删除附件
如果您希望在这些附件所链接的邮件被删除时，从服务器上删除提取的附件，请点击此选项。

启用此项时，并且通过 POP3 客户端收集其邮件的用户未被配置成在服务器上留下邮件，那么所有他已提取的附件将会不可挽回地丢失。如果未启用此项，就不会丢失任何附件。不过这样一来，您大量的硬盘空间将永久性地被原始收件人不再需要的过时或无用的文件所占据。实际上所有 POP 客户端都能在服务器上保留邮件。

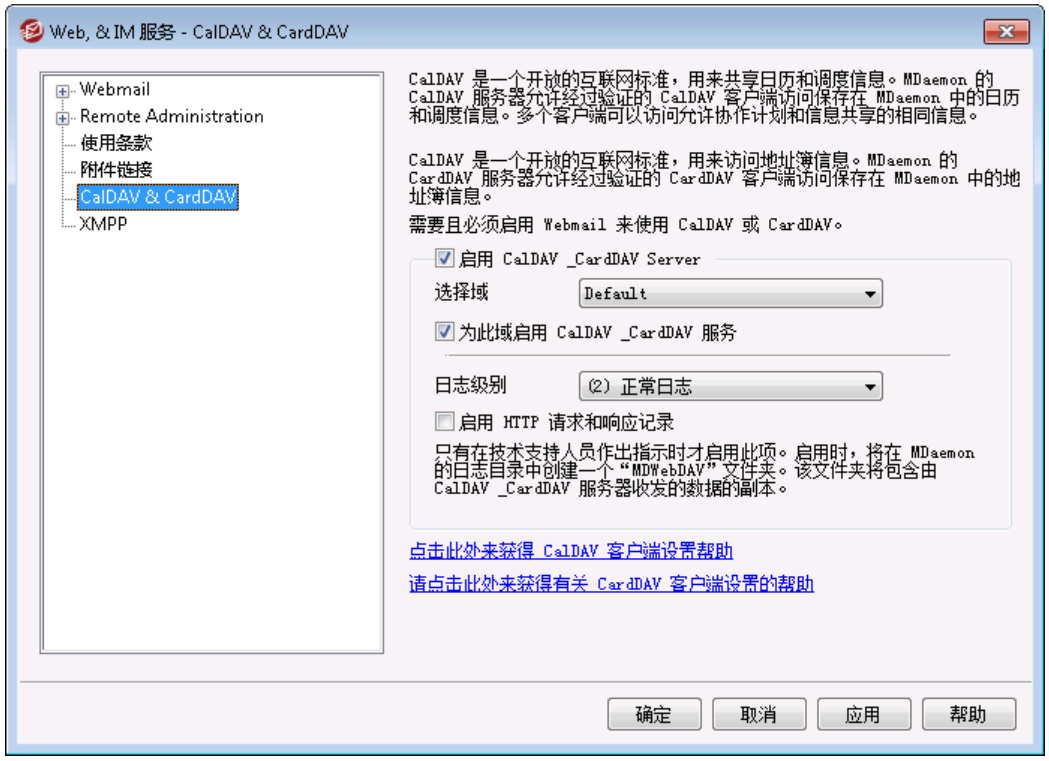
提取 Quoted Printable 编码的 "文本/纯文本"附件
默认情况下，不会提取 Quoted Printable 编码的文本/纯文本这种附件。如果您希望在自动提取中包含那些类型，请点击该选择框。

豁免列表
点击此按钮可打开 "附件链接"豁免列表。其中包括您不希望从邮件提取的任何文件名。默认情况下，在此列表中包含 Winmail.dat。

还请参阅：

新建账户模板 667
用户编辑器 » 附件 616
模版宏 669
脚本宏 707

3.6.5 CalDAV & CardDAV



CalDAV 是用来管理和共享日历并调度信息的互联网标准。MDaemon 的 CalDAV 支持”帮助您的账户使用那些可以通过 CalDAV 来访问和管理其个人日历和任务的任何客户端。他们还能访问任何公共 258 或共享 623 日历或任务，只需遵照其访问权限 260 即可。CardDAV 是用来访问联系人/地址簿信息的标准。MDaemon 的 CardDAV 服务器允许经过验证的 CardDAV 客户端访问保存在 MDaemon 中的联系人信息。

启用 CalDAV & CardDAV 服务器
默认情况下，启用 CalDAV/CardDAV 支持。不过 Webmail 是必需的，因此必需启用它 270 来进行使用。如果您不希望支持 CalDAV 或 CardDAV，请禁用该选项。要为个别域启用/禁用它，请使用下方的选项。

为域更改默认的 CalDAV/CardDAV 设置
首先，MDaemon 的所有域都将基于 *“默认”*选项（位于 *“选择域”*下拉列表）启用或禁用 CalDAV/CardDAV。要更改默认设置：

1. 在 *“选择域”*下拉列表中，选择 **“默认”**。
2. 如果您希望在默认情况下为所有域启用 CalDAV & CardDAV，请勾选 **“为此域启用 CalDAV/CardDAV 服务”**附近的选框，如果您希望在默认情况下禁用它，请清除此框。
3. 点击 **“确定”**。

为特定域启用/禁用 CalDAV/CardDAV
要为个别域覆盖 *“默认”*CalDAV/CardDAV 设置：

1. 在 *“选择域”*下拉列表中选择一个特定域。

2. 如果您希望为此域启用 CalDAV/CardDAV，请勾选 "为此域启用 CalDAV & CardDAV 服务"附近的选框，如果您希望禁用它，请清除此框。
3. 点击 "确定"。

日志

日志级别
使用该下拉列表来指定记录 CalDAV/CardDAV 活动的等级。有六种记录等级可供选择：1—调试记录，2—普通记录（默认），3—仅警告和错误，4—仅错误，5—仅严重错误，6—无记录。这是全局设置——无法应用到特定域。

启用 HTTP 请求和响应日志
若启用，这将在 MDaemon 的日志文件夹中创建一个 MDWebDAV 文件夹。会将 CalDAV/CardDAV 服务器收发的所有数据记录到那个文件夹。通常此项仅用于诊断，不应启用，除非技术支持团队指导您这么做。

配置 CalDAV 客户端

要配置支持 RFC 6764(Locating Services for Calendaring Extensions to WebDAV (CalDAV)) 的客户端，只需要服务器、用户名和密码。您可以设置您的 DNS 记录将客户端指向正确的 URL。未配置 DNS 记录时，用户可以在这个客户端中输入专用的 "well-known URL"："主机名/.well-known/caldav"。例如：http://example.com:3000/.well-known/caldav。Webmail 内置的 web 服务器支持这个 well-known URL。

对于不支持自动定位 CalDAV 服务的客户端（例如通过 Lightning 插件的 Mozilla Thunderbird）将需要为各个 "日历"和 "任务"列表请求完整的 URL。MDaemon 的 CalDAV URL 如下所示：

日历和任务
用户默认的日历或任务列表：

```
http://[host]/webdav/calendar
(例如 http://example.com:3000/webdav/calendar)

http://[host]/webdav/tasklist
(例如 http://example.com/webdav/tasklist)
```

用户定制的日历或任务列表：

```
http://[host]/webdav/calendar/[calendar-name]
(例如 http://example.com/webdav/calendar/personal)

http://[host]/webdav/tasklist/[tasklist-name]
(例如 http://example.com/webdav/tasklist/todo)
```

子文件夹中用户定制的日历或任务列表：

```
http://[host]/webdav/calendar/[folder]/[calendar-name]
(例如 http://example.com/webdav/calendar/my-stuff/personal)
```

http://[host]/webdav/tasklist/[folder]/[tasklist-name]
(例如 http://example.com/webdav/tasklist/my-stuff/todo)

共享日历和任务
其他用户默认的日历或任务列表：

http://[host]/webdav/calendars/[domain]/[user]
(例如 http://example.com/webdav/calendars/example.net/frank)

http://[host]/webdav/tasks/[domain]/[user]
(例如 http://example.com/webdav/tasks/example.net/frank)

其他用户定制的日历或任务列表：

http://[host]/webdav/calendars/[domain]/[user]/[calendar-name]
(例如
http://example.com/webdav/calendars/example.net/frank/personal)

http://[host]/webdav/tasks/[domain]/[user]/[tasklist-name]
(例如 http://example.com/webdav/tasks/example.net/frank/todo)

公共日历和任务
域的默认日历或任务列表：

http://[host]/webdav/public-calendars/[domain]
(例如 http://example.com/webdav/public-calendars/example.com)

http://[host]/webdav/public-tasks/[domain]
(例如 http://example.com/webdav/public-tasks/example.com)

公共文件夹层次结构的根目录中的日历或任务列表：

http://[host]/webdav/public-calendars/[calendar-name]
(例如 http://example.com/webdav/public-calendars/holidays)

http://[host]/webdav/public-tasks/[tasklist-name]
(例如 http://example.com/webdav/public-tasks/projects)

在测试 OutlookDAV 客户端时请慎用。如果存在多个 MAPI 配置文件，我们已看到客户端为服务器返回的所有日历项目，向服务器发送了删除命令。OutlookDAV 仅支持默认的 MAPI 配置文件。

要获取有关设置 CalDAV 客户端的更多信息，请在 MDaemon 知识库搜索“CalDav”。

配置 CardDAV 客户端

要配置支持 RFC 6764 (Locating Services for Calendaring Extensions to WebDAV (CalDAV) and vCard Extensions to WebDAV (CardDAV))的客户端，只需要服务器地址、用户名和密码即可。Apple 地址簿和 iOS 支持这个标准。可以设置 DNS 记录将客户端指向正确的 URL。在未配置 DNS 记录的情况下，当 CardDAV 是/.well-known/carddav 时，客户端查询 "well-known URL"。Webmail 内置的 web 服务器支持这个 well-known URL。不支持自动定位 CardDAV 服务的客户端将需要完整的 URL。

注意，CardDAV 客户端是 Apple Contacts (包含于 Mac OS X)、Apple iOS (iPhone) 和 Mozilla Thunderbird (通过 SOGO 插件)。

至于 OS X 10.11 (EL Capitan)，Apple Contacts 应用程序仅支持一个集合/文件夹。在 CardDAV 服务器检测到 Apple Contacts 应用程序时，它仅返回已验证用户的默认联系人文件夹。此外，OS X 10.11 (EL Capitan) 有一个已知问题：无法使用对话框的 "高级"视图添加 CardDAV 账户。

访问地址簿

"地址簿"路径是指向您默认地址簿的快捷方式。

http://[host]/webdav/addressbook - 您默认的联系人文件夹。

http://[host]/webdav/addressbook/friends - 您的 "好友"联系人文件夹。

http://[host]/webdav/addressbook/myfolder/personal - 您位于 "myfolder"子文件夹中的 "个人"联系人文件夹。

访问您有权访问的另一个用户的共享文件夹

"联系人"路径是指向共享联系人文件夹的快捷方式。

http://[host]/webdav/contacts/example.com/user2 - user2@example.com 的默认联系人文件夹

http://[host]/webdav/contacts/example.com/user2/myfolder - user2@example.com 的 "myfolder"联系人文件夹

访问您有权访问的公共文件夹

"公共联系人"路径是指向公共联系人文件夹的快捷方式。

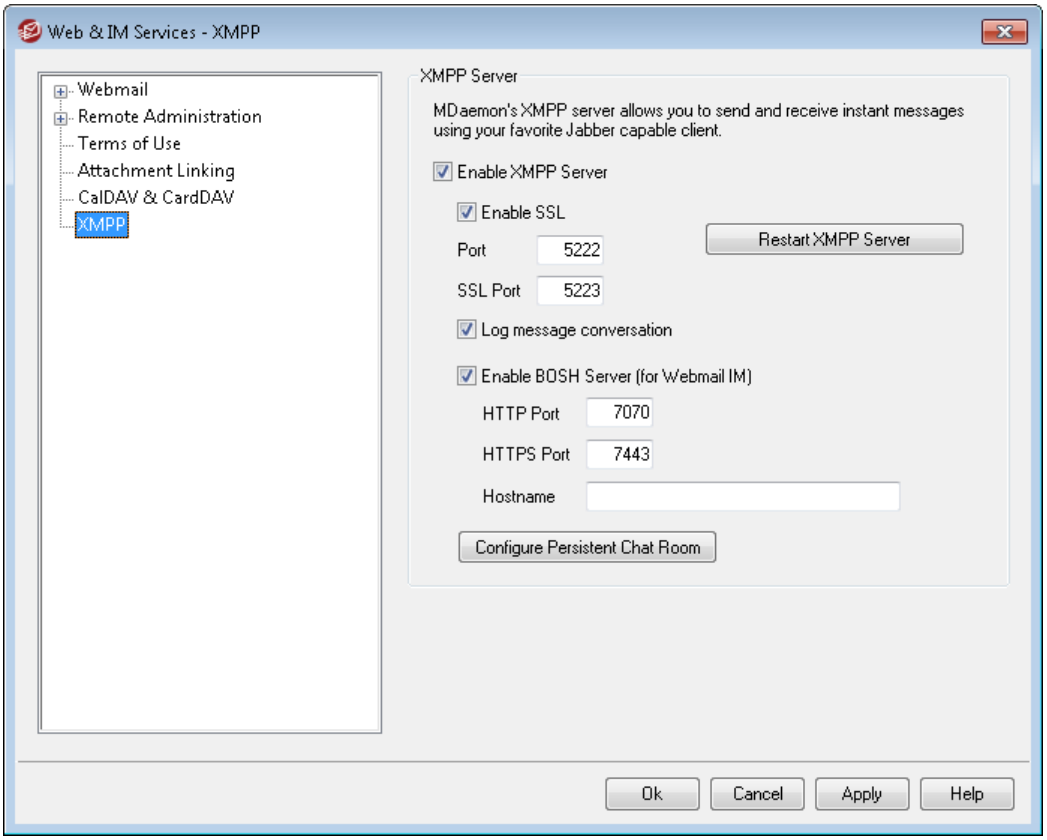
http://[host]/webdav/public-contacts/example.com - example.com 的默认联系人文件夹

http://[host]/webdav/public-contacts/foldername - 位于公共文件夹层次结构的根目录中的 "foldername"联系人文件夹

在测试 OutlookDAV 客户端时请慎用。OutlookDAV 仅支持默认的 MAPI 配置文件。如果存在多个 MAPI 配置文件，客户端可能为服务器返回的所有项目，向服务器发送了删除命令。

要获取有关设置 CardDAV 客户端的更多信息，请在 MDaemon 知识库搜索 "CardDav"。

3.6.6 XMPP



MDaemon 现在自带 Extensible Messaging & Presence Protocol (XMPP 可扩展消息在线协议) 服务器，有时叫做 Jabber 服务器。这允许您的用户使用 MDaemon Instant Messenger 267 和第三方 XMPP 客户端，例如 Pidgin、Gajim、Swift 等来收发即时消息。这些客户端适用于大多数操作系统和移动设备平台。

XMPP 服务器作为 Windows 服务安装，而且默认的服务器端口是 5222 (通过 STARTTLS 的 SSL) 和 5223 (专用的 SSL)。如果在 MDaemon 中启用 XMPP 服务器，它将使用 MDaemon 的 SSL 配置。此外，一些 XMPP 客户端为主机名称的自动发现使用 DNS SRV 记录。请参阅 http://wiki.xmpp.org/web/SRV_Records 获取更多信息。

用户通过使用其电子邮件和密码的所选 XMPP 客户端进行登录。不过一些客户端需要将邮件地址划分成单独的组件来进行登录。例如有些客户端不需要 "frank@example.com"，而要求您使用 "frank"作为登录/用户名，将 "example.com"用作域。

对于多用户/群聊天服务，客户端通常将其显示成 "房间"或者 "会议"。当您希望开始一个群聊天会话时，请创建一个房间/会议 (为其命名)，然后邀请其他用户进入这个房间。大多数客户端无需您输入会议的服务器位置，您只需输入会议名称即可。在要求您这么做时，请

将 "conference.<your domain>"用作位置 (例如 conference.example.com)。一些客户端要求您使用以下格式输入名称和位置："room@conference.<your domain>"(例如 Room01@conference.example.com)。

一些客户端(例如 Pidgin)支持用户搜索服务，允许您按姓名或邮件地址搜索服务器中的用户，这使联系人的添加更加简便。通常您不必提供搜索位置，不过如被要求，请使用 "search.<your domain>"(例如 search.example.com)。在进行搜索时，可以将 % 符号用作通配符。因此您可以在邮件地址字段中使用 "%@example.com"来显示邮件地址以 "@example.com"结尾的所有用户的列表。

XMPP 服务器

启用 XMPP 服务器
点击此选项来启用 XMPP 服务器。要允许即时通讯，您还必须确保 "**启用即时通讯**"这个选项 (位于 MDIM 278 屏幕)。

启用 SSL
如果您希望支持 SSL 用于 XMPP 服务器，而且使用以下指定的 *SSL 端口*，请点击这个按钮。**请注意：**这还应用于下方的 BOSH 服务器 *HTTPS 端口*选项。

端口
用于 XMPP 的默认端口是 5222，支持通过 STARTTLS 的 SSL。

SSL 端口
XMPP 专用的 SSL 端口是 5223。

重启 XMPP 服务器
点击此按钮来重启 XMPP 服务。

记录邮件会话
默认情况下，所有即时通讯对话都会记录在一个名为 XMPPServer-<date>.log 的文件中，位于 MDaemon\Logs\ 文件夹中。如果您不希望记录会话，请清除此勾选框。

启用 BOSH 服务器 (用于 Webmail)
点击此选项可启用 BOSH 服务器，允许在 MDaemon Webmail 中进行即时消息传递。

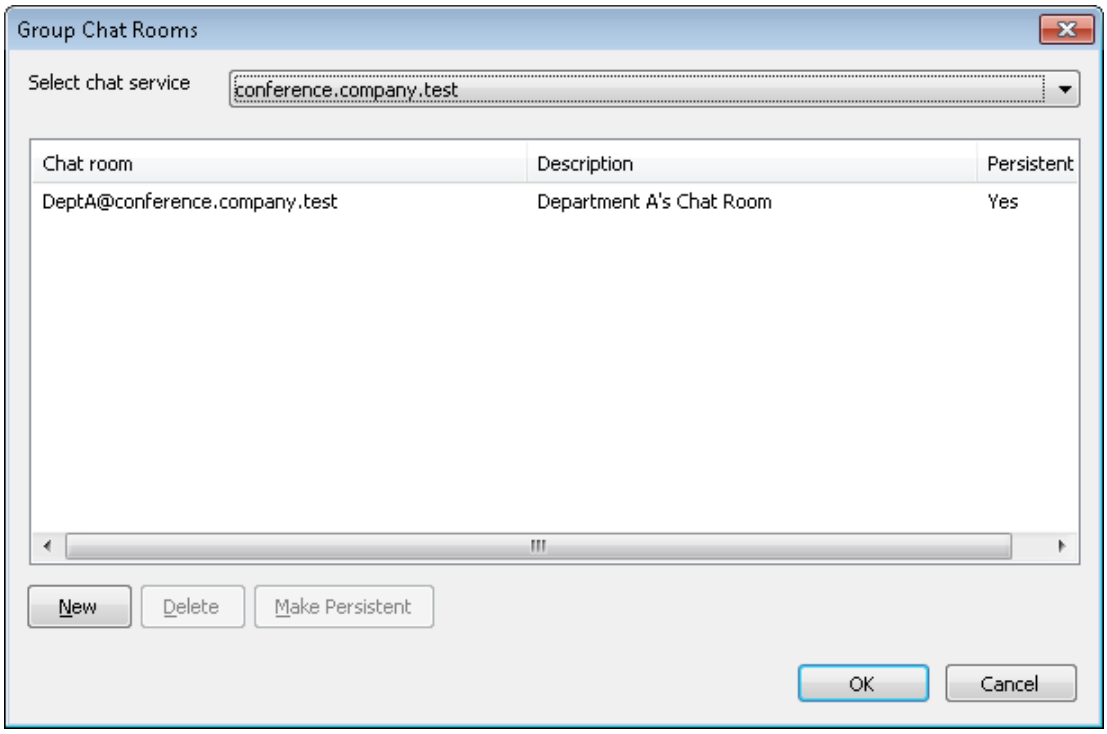
HTTP 端口
默认情况下，BOSH 服务器使用 HTTP 7070 端口。

HTTPS 端口
在激活上方的 *"启用 SSL"*选项时，BOSH 服务器使用这个 HTTPS 端口。默认的端口是 7443。

主机名
如有必要，请使用此选项来指定主机名。

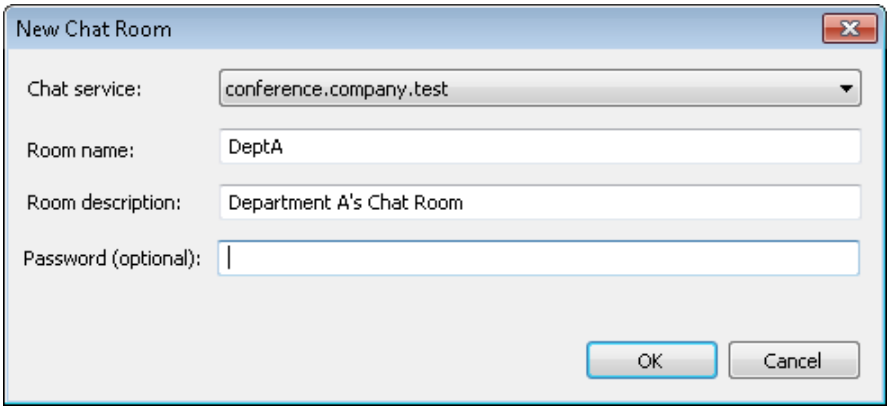
配置持续聊天室

点击此按钮来打开 "群组聊天室"对话框。通常，在用户创建聊天室时，当最后一个人离开时，该聊天室将消失，但是您可以使用这些选项来创建持久聊天室，这些聊天室在无人时仍将保留。您该能删除房间并将现有的临时房间转换为永久房间。



选择聊天服务
选择聊天服务来显示该域的聊天室。

新建
点击此按钮来添加持续聊天室。



选择聊天服务
为房间选择聊天服务。

房间名称
输入聊天室的名称，不含任何空格。

房间描述
在此处包含房间的描述。用户在选择要加入的房间时，将看见这个名称。

密码 (可选)
如果您希望需要输入密码来加入聊天，请在此处输入密码。

删除
如果您希望删除房间，请选择该房间并点击此按钮来将其删除。

变成持续
当列表中有一个临时聊天室时，请选择该聊天室，如果要使其成为持续聊天室，请点击此按钮。

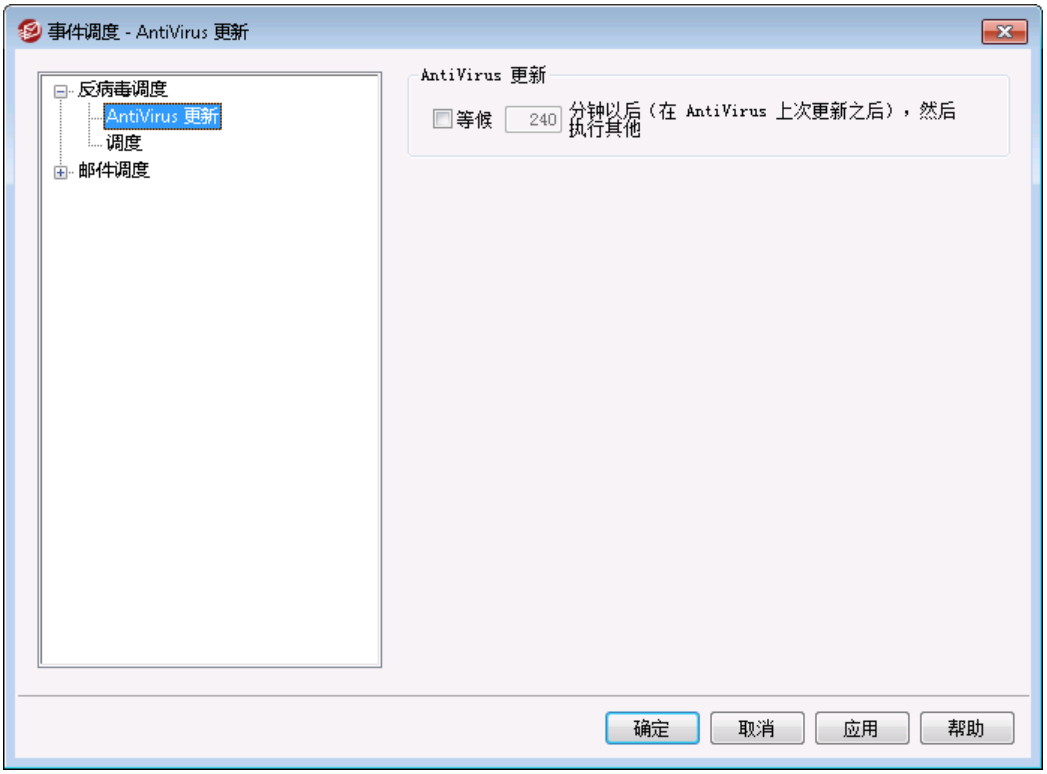
还请参阅：

Webmail » MDIM 278

3.7 事件调度

3.7.1 AntiVirus 调度

3.7.1.1 反病毒更新



反病毒更新

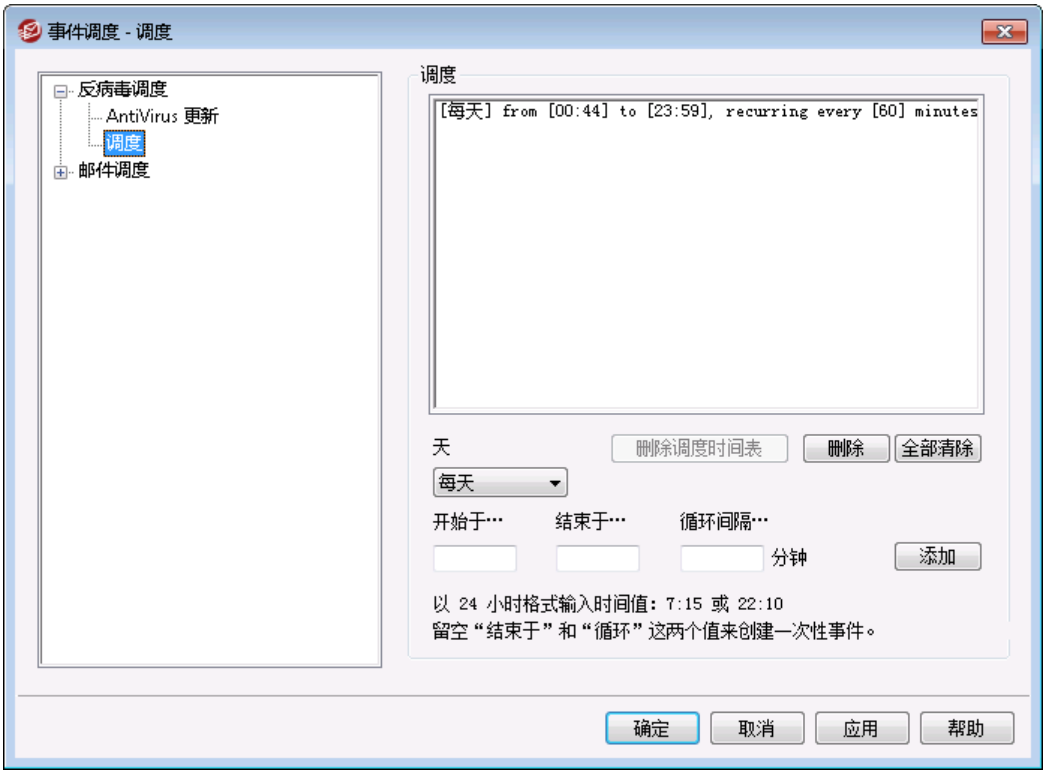
在上次反病毒更新后等待 XX 分钟，然后进行下次更新
点击该复选框并指定希望 AntiVirus 在检查新的病毒定义更新前等待的分钟数。请注意，这实际上是 AntiVirus 在上次检查更新后（无论更新是由调度程序还是手动触发的）

*尝试*等待的分钟数。由调度程序或手动触发的更新优先于该设置，因而如果由这些方式触发了一个 AntiVirus 更新事件，那么计数器将被重置。例如，如果该选项被设置为每隔 240 分钟检查一次更新，而您在 100 分钟后手动检查更新，则该计数器将被重置为 240。

还请参阅：

反病毒更新调度 316
AntiVirus 558
反病毒更新程序 562

3.7.1.2 调度



使用“AntiVirus 更新调度”来指定检查 AntiVirus 更新的特定时间。调度位于：“设置» 事件调度» 反病毒更新» 调度”。

调度

删除
要从列表中删除事件，请选择一个条目然后点击该按钮。

全部删除
该按钮从调度事件列表中删除所有条目。

创建调度事件

天
创建新的调度事件时，首先选择该更新检查事件预订发生的日子。您可以选择：每天、工作日（星期一到星期五）、周末（星期六和星期天）、或一周中的特定日子。

开始于...
输入希望开始更新检查的时间。时间值必须采用 24 小时的格式，从 00:00 直到 23:59。如果希望它是单次事件而不是重复发生的事件，您只需输入该时间值（留空*"结束于..."*和*"重复间隔..."*这两个选项）。

结束于...
输入希望结束更新检查事件的时间。时间值必须采用 24 小时的格式，从 00:00 直到 23:59，且必须大于*"开始于..."*值。例如，如果*开始于...*时间值为"10:00"，那么该时间值可以是"10:01"到"23:59"。如果希望它是单次事件而不是重复发生的事件，请留空该选项。

每隔 [xx]分钟循环
这是 AntiVirus 在指定的*开始于...*和*结束于...*时间之间检查更新的间隔时间。如果希望它是单次事件而不是重复发生的事件，请留空该选项。

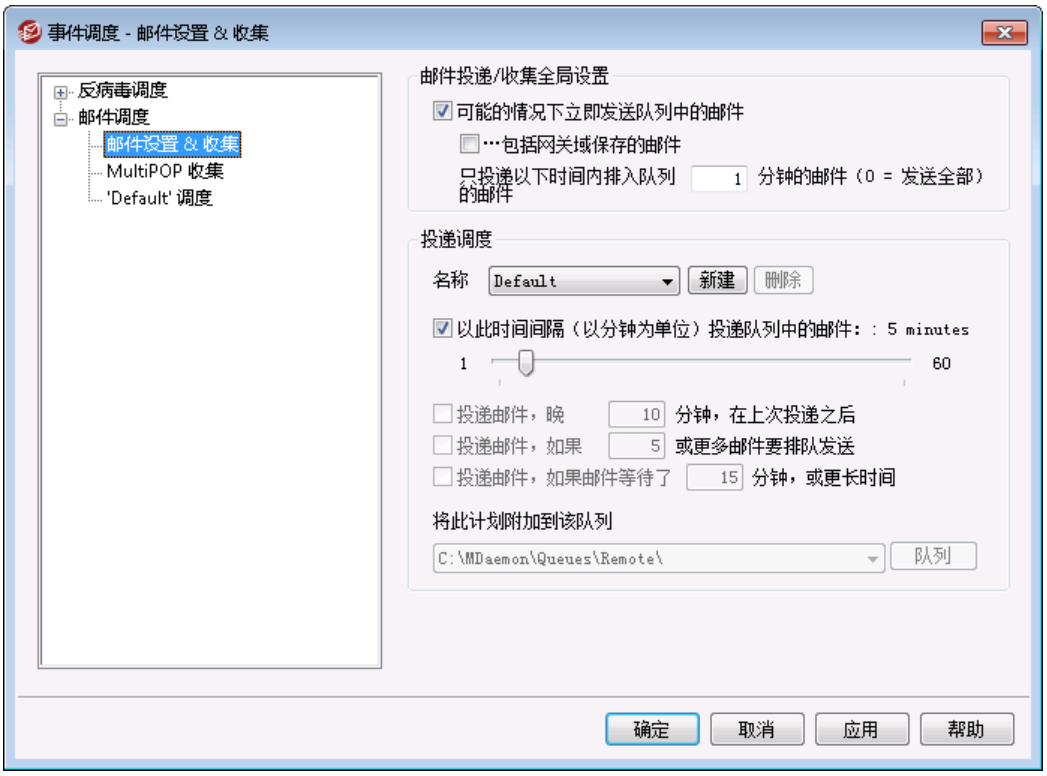
添加
一旦指定了*日子*和*开始于...*时间，以及可选的*结束于...*时间和*重复间隔...*值，可点击该按钮将事件添加到调度安排中。

还请参阅：

反病毒更新
AntiVirus 558
反病毒更新程序 562

3.7.2 邮件调度

3.7.2.1 邮件发送 & 收集



请点击 "设置» 事件调度"来打开 MDaemon的 "事件调度程序"。利用这个屏幕，您便能选择详尽地或简单地调度 MDaemon的远程邮件处理事件。您可使用计数器定期处理邮件，或使用 "邮件调度[321]"屏幕 "来安排邮件投递和收集的确切时间。还可设置在非预订时间触发邮件处理的条件，比如当有一定数量的邮件在等待发送时，或者邮件已经等待了指定时间时。另外，您可创建定制调度以分配给定制远程邮件队列。定制调度使您能为不同类型的邮件设置不同调度。例如，可为大型邮件、列表邮件、特定域等分别创建调度。

请使用 "事件调度程序"的 AntiVirus 更新[315]部分来调度 MDaemon 检查 AntiVirus[539] 更新的频率。

邮件投递/收集全局设置

尽可能立即发送队列中的邮件
启用该选项时，若有邮件到达并等待远程投递，MDaemon 将立即处理并投递在下述 *"只投递在最近 [xx] 分钟内排入队列的邮件"*选项中指定分钟数内排入队列的所有远程邮件，而不是等待下一个调度处理间隔或其他事件触发邮件处理。

…包括存储的网关域邮件
如果希望域网关的邮件也被立即投递，请点击该复选框。不过，这只适用于在 *"网关编辑器"*的 "网关[212]屏幕上启用了 "每当 MDaemon 处理远程邮件时投递所存储的邮件"这一选项的网关。

只投递在最近 [xx]分钟内排入队列的邮件 (0 = 全部发送)
该选项管理在上述 *"尽可能立即投递队列中的邮件"*选项后台处理邮件以作投递之前邮件必须已排入队列的最早时间。当该选项触发远程邮件处理，MDaemon 将仅处理在指定分钟数内排列的邮件而不是尝试投递队列中的每封邮件。但当按下 *处理...队列*工具栏按钮或任何其他触发远程邮件处理的普通调度程序是，整个队列仍将得以处理。默认情况下，该选项设置为 1 分钟。如果希望在每次触发远程邮件处理时处理整个队列，可以将该选项设置为 "0"，但这并非推荐操作，因为它的效率会低很多。

以上选项只适用于默认调度。它们不适用于定制调度 (参见下面的 *"名称..."*选项)。

投递调度

名称...
使用该下拉列表框选择要编辑的调度。默认调度总是用于常规、远程邮件队列以及通过 DomainPOP 和 MultiPOP 收集的邮件。对于使用拨号服务的配置，默认调度也将用于 LAN (局域网)域，此域是您指定为位于本地区域网络的远程域，因此不需要 RAS 拨号。可以将其他调度分配给自定义远程邮件队列，并将邮件自动路由到这些自定义队列 736 (通过使用内容过滤器 540 实现)。完成调度选项的编辑后，点击 "确定"或选择其他调度进行编辑。更改调度后若选择其他调度，将显示确认框询问在切换到其他调度之前是否希望保存或放弃对当前所选调度的更改。

新建
点击该选项创建新的调度。将会显示对话框以便您为其指定名称。指定调度名称后，将在左侧菜单中创建相应的邮件调度 322 屏幕。使用该屏幕为调度分配时间。

删除
要删除定制调度，首先在 *"名称..."*下拉列表中将其选中，然后点击 *"删除"*。将打开一个确认框询问是否确定要进行删除。删除自定义调度不会删除任何自定义远程队列或与之关联的内容过滤器规则。然而，如果删除定制队列，则与之相关联的任何调度以及内容过滤器规则都将被删除。

在此间隔投递排队的邮件 (单位是分钟)
点击该复选框并且向左或者向右移动滑块，可以指定邮件处理会话之间的时间间隔。它可以配置为从 1 到 60 分钟的取值范围内向下倒计数。在此时间段后，MDaemon 将会处理远程邮件，然后再次开始倒计数。当清除该复选框时，*"远程邮件"*处理间隔将由其他调度选项决定。

在上次投递后过 [xx]分钟投递邮件
当希望在上次会话发生后以一定的时间间隔发生远程邮件处理会话，而不去考虑启动会话的触发事件时，可使用该选项。不同于在设置特定时间或使用 *以此时间间隔投递队列中的邮件*滑块时所采用的硬性固定间隔，每次处理邮件时将重置该选项的时间间隔。

当队列中有 [xx]或更多邮件时投递邮件
启用该选项时，每当在远程队列中等待投递的邮件数量达到或者超过了此处指定的数目，MDaemon 将会触发邮件会话。这些邮件会话是任何其它正常调度会话的补充。

投递等待时间超过 [xx]分钟的邮件
当选中该复选框时，每当有邮件在队列中等待了指定分钟后，MDaemon 将会触发一个邮件会话。这些会话是任何其它正常调度会话的补充。

队列

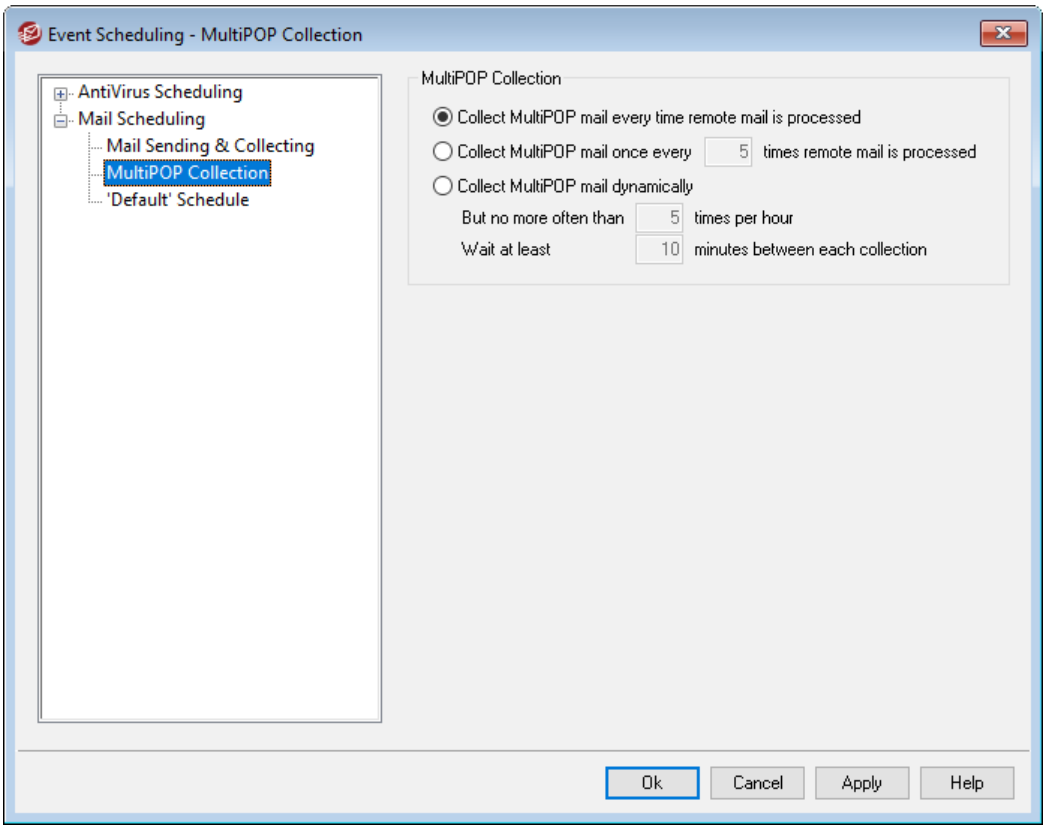
将该调度附加到该队列
使用该选项可将选定调度与特定定制远程邮件队列相关联。然后可使用内容过滤器来创建规则以将某些邮件放入该队列。例如，如果希望调度发往远程地址的邮件列表邮件在指定时间进行投递，那么可以为这些邮件创建定制队列，然后创建一条规则以将它们全部放入定制队列，最后创建定制调度并将它指派给该队列。

队列
点击该按钮可打开定制队列 736 屏幕，在其上可创建定制远程队列以用于事件调度程序。

还请参阅：

邮件调度 322
反病毒更新 315

3.7.2.2 MultiPOP 收集



MultiPOP 收集

每次处理远程邮件时收集 MultiPOP 邮件
如果希望每次处理远程邮件时，MDaemon 会收集所有 MultiPOP 邮件，请点击该选项。

每当处理 XX 次远程邮件后收集 MultiPOP 邮件
如果希望 MultiPOP 邮件的收集频率低于远程邮件的处理频率，请点击该选项并在框中指定一个数字。该数字表示在收集 MultiPOP 邮件前远程邮件的处理次数。

动态收集 MultiPOP 邮件
如果希望动态收集 MultiPOP 邮件，请点击该选项。通常，每隔一次或 *x* 次远程邮件处理间隔，即在同一时间为所有用户收集 MultiPOP 邮件。如果是动态收集，则当个别用户通过 POP、IMAP 或者 Webmail查看其本地邮件时，将为该个别用户而不是一次性为所有用户收集 MultiPOP 邮件。然而，由于 MultiPOP 收集是由用户查看其邮件触发的，所以该用户看不到任何新收集的 MultiPOP 邮件，直到他*再次*查看邮件为止。因此，用户需要查看邮件两次才能看到新的 MultiPOP 邮件。第一次会触发 MultiPOP 收集，第二次会看到所收集的邮件。

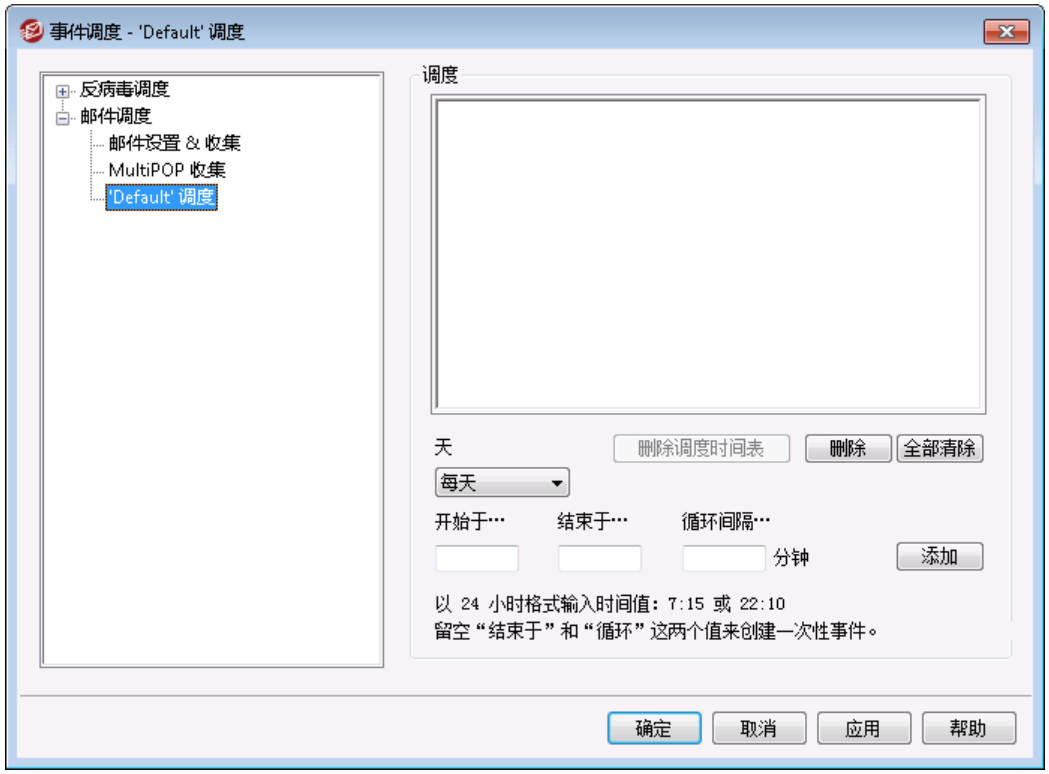
但不超过 XX 次/小时
为了减轻大量使用 MultiPOP 可能对 MDaemon 造成的压力负荷，可使用该控件指定每小时内可为每个用户收集 MultiPOP 邮件的最大次数。

在每次收集之间最少等待 XX 分钟
该选项通过限制每个用户收集 MultiPOP 邮件的频率有助于减轻邮件服务器的压力。它将限制每个用户每隔这么些分钟收集一次 MultiPOP 邮件。指定您希望用户在被允许再次查看 MultiPOP 之前必须等待的分钟数。

还请参阅：

MultiPOP
账户编辑器 | MultiPOP

3.7.2.3 邮件调度



每个邮件调度对应于*“名称”*下拉列表（位于邮件发送 & 收集[318]）屏幕中所列的同名调度。使用每个“邮件调度”可指定该调度安排中处理远程邮件的特定时间。“邮件调度”位于：设置 » 事件调度 » 邮件调度。调度名调度。

调度

删除调度时间表
该按钮将删除定制的“邮件调度”。调度将被删除，并从邮件发送 & 收集[318]屏幕上的*名称*下拉列表中移去相应条目。点击该按钮后，会打开确认框询问您是否确实要删除该调度。只有定制调度才能使用该选项—默认调度无法删除。

删除

要从列表中删除一个条目，请选择该条目然后点击该按钮。

全部删除
该按钮从调度事件列表中删除所有条目。

创建调度事件

天
创建新的调度事件时，首先选择该调度事件发生的日子。您可选择：每天、工作日（星期一到星期五）、周末（星期六和星期天）、或一周中的特定日子。

开始于...
输入您希望事件开始的时间。时间值必须采用 24 小时的格式，从 00:00 直到 23:59。如果希望它是单次事件而不是重复发生的事件，您只需输入该时间值（留空*"结束于..."*和*"重复间隔..."*这两个选项）。

结束于...
输入希望事件结束的时间。时间值必须采用 24 小时的格式，从 00:00 直到 23:59，且必须大于*"开始于..."*值。例如，如果*开始于...*时间值为"10:00"，那么该时间值可以是"10:01"到"23:59"。如果希望它是单次事件而不是重复发生的事件，请留空该选项。

重复间隔为 [xx] 分钟
这是在指定的*"开始于..."*和*"结束于..."*时间之间处理邮件的时间间隔。如果希望它是单次事件而不是重复发生的事件，请留空该选项。

添加
一旦指定了*日子*和*开始于...*时间，以及可选的*结束于...*时间和*重复间隔...*值，可点击该按钮将事件添加到调度安排中。

根据您的需要，使用邮件发送 & 收集[318]屏幕上的简单调度选项可能已足以控制邮件处理间隔。例如，当您只需将"调度 & 收集"屏幕上的滑块设置为间隔一分钟，即可完成每天每隔一分钟的事件调度时，就无需制定特殊调度来实现同样目的。另一方面，如果希望处理时间间隔超过一小时，或只在某些日子发生，则可结合使用调度选项和特定时间。

还请参阅：

邮件发送 & 收集[318]
反病毒更新[315]
反垃圾邮件更新[582]

3.8 MDaemon Connector

MDaemon Connector（MC）的技术支持是 MDaemon Technologies 提供的一个授权功能。在部署了 MC 时，希望将 Microsoft Outlook 用作其首选邮件客户端的任何用户都能实现这一点。该程序通过用户的 Outlook 客户端连接到 MDaemon 服务器来提供群件和协作功能，并使用 Outlook 的电子邮件、具有空闲 / 忙碌安排的日历、地址簿、分发列表、任务和便签等

当您已激活了对于 MC 的技术支持，MDaemon Connector 屏幕就可以在 MDaemon 的菜单栏里获得，其位于：设置» MDaemon Connector。该对话框用于启用和配置 MC，以及授权特定的账户来使用它。

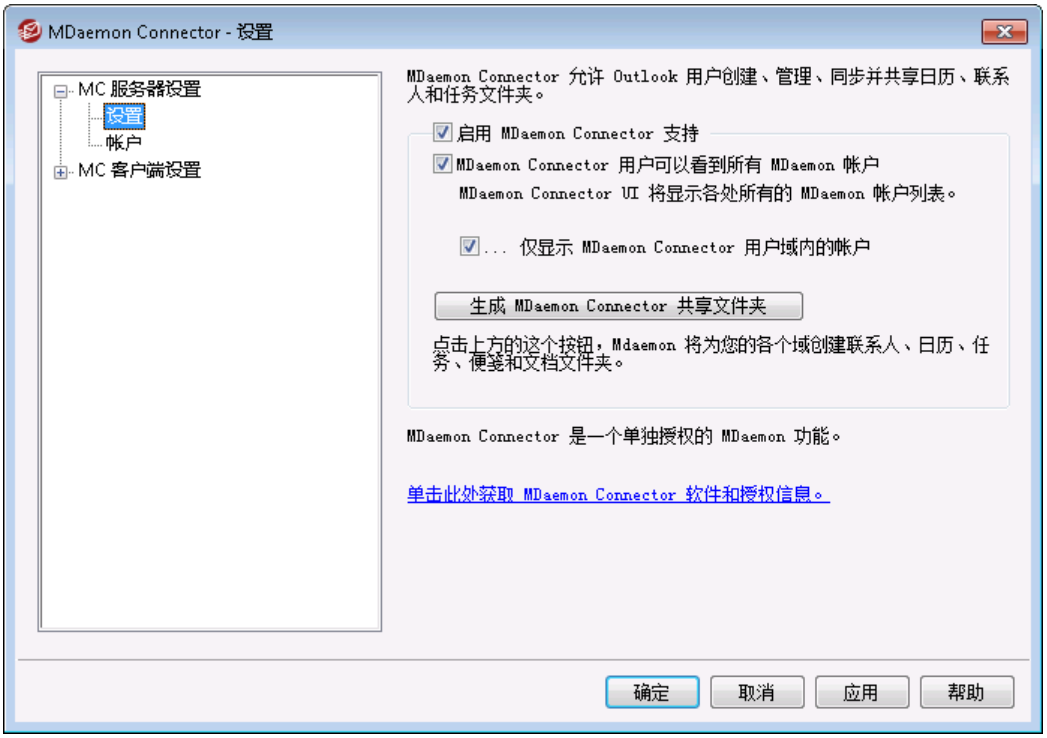
要了解更多信息或获取 MDaemon Connector 功能，请访问 MDaemon Connector 页面，位于 www.mdaemon.com.

还请参阅：

MC 服务器设置 » 设置 324
MC 服务器设置 » 账户 325
MC 客户端设置 326

3.8.1 MC 服务器设置

3.8.1.1 设置



MDaemon Connector

启用 MDaemon Connector 支持
点击此勾选框来启用针对 MDaemon Connector (MC) 的技术支持。您的用户将不能使用 MC 的功能除非选中这个选项。

MDaemon Connector 用户可以看到所有 MDeamon 账户
如果您希望授权所有 MDaemon 账户通过 MC 进行连接，并在用户客户端上的 MDaemon Connector 内的 *"权限"*列表上可见，请点击此项。从该列表中，MC 用户可以选择他们希望授予共享 Outlook 项目权限的账户。禁用此项时，MDaemon Connector 的 *"权限"*列表会清空，且用户必须手动输入邮件地址。只有被授权通过 MC 进行连接的账户的地址才能共享 Outlook 项目。如果用户输入一个未被授权的邮件地址，那么这个项目将不被共享，除非它以后被授权通过 MC 进行连接。

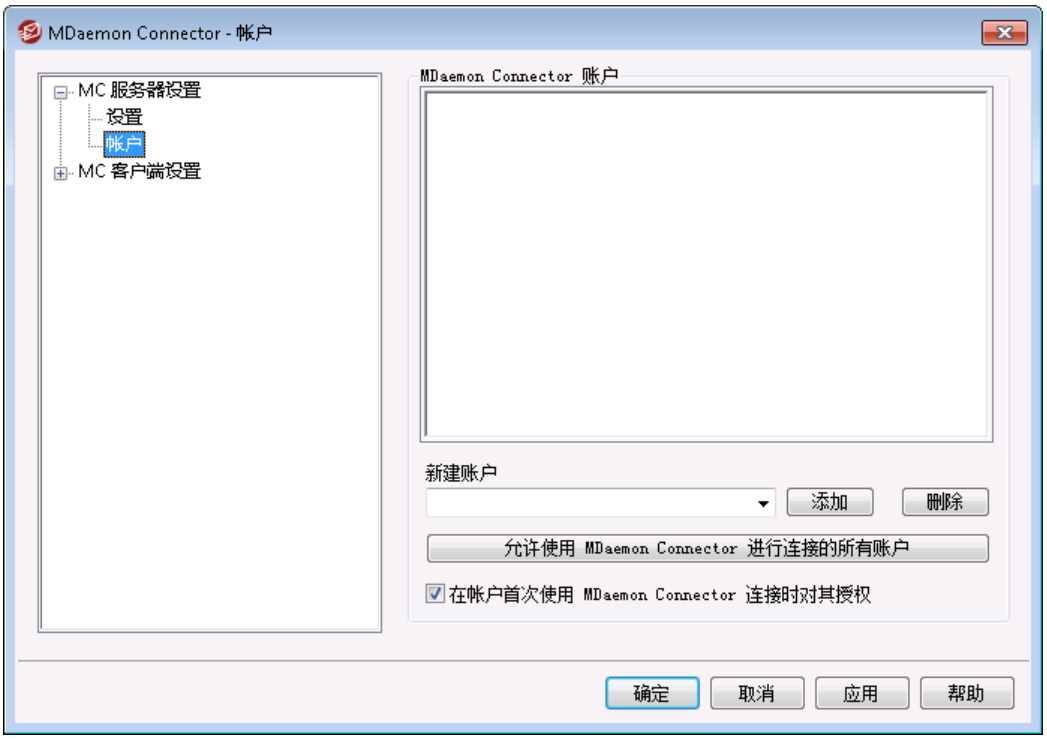
...仅显示 MDaemon Connector用户域内的账户
只有当以上的 *MDaemon Connector用户可以看到所有 MDaemon 账户*选项启用时，该选项才能获得。如果您希望授权通过 MC 连接的用户和属于相同域的用户在 MDaemon Connector 中的 *"权限"*列表上显示，请勾选此框。即使他们被授权通过 MC 连接，属于不同域的账户也不会被列出。

生成 MDaemon Connector共享文件夹
点击这个按钮来为每个域生成一个 MC 文件夹。它将生成如下文件夹：联系人、约会、日志、任务和便笺。

还请参阅：

MC 服务器设置 » 账户 325
MC 客户端设置 326

3.8.1.2 账户



MDaemon Connector账户

这是被授权通过 MDaemon Connector来共享他们的 Outlook 文件夹、日历、联系人、便签等信息的 MDaemon 账户列表。您能通过如下列出的选项来添加账户到该列表。

新建帐户
要添加一个新的 MDaemon 账户到授权的 MDaemon Connector账户列表，请从这个下拉列表中选择目标账户并点击 *"添加"*。要删除一个账户，选定此账户后点击 *"删除"*即可。

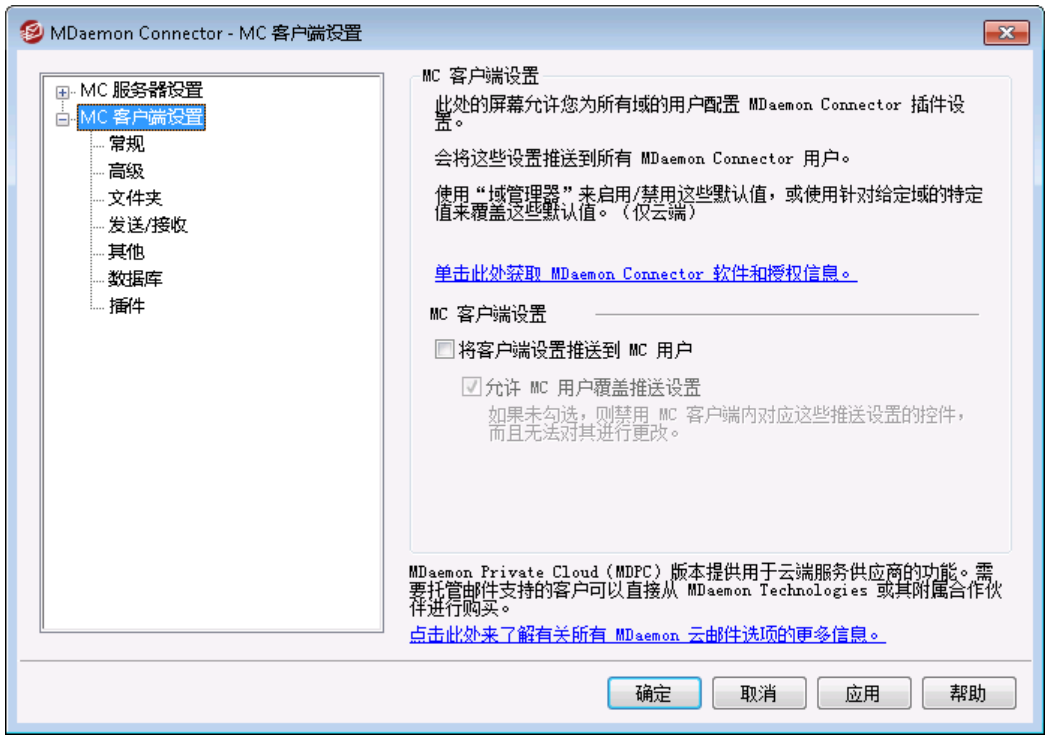
允许所有账户使用 MDaemon Connector连接
要立即授权所有的 MDaemon 帐户通过 MDaemon Connector连接，请单击该按钮则所有的 MDaemon 帐户将被添加到 *MDaemon Connector用户*列表。

在账户首次使用 MDaemon Connector连接时对其授权
如果您希望在每个连接账户第一次使用 *MDaemon Connector* 时，将个别账户添加到 MDaemon Connector账户列表，请点击该复选框。**请注意：** 如果您启用这个选项，那么您就有效地授权了所有 MDaemon 账户使用 请勾选此框。账户本身并不会被添加到列表，直到用户首次使用以后才进行添加。

还请参阅：

MC 服务器设置 » 设置 324
MC 客户端设置 326

3.8.2 MC 客户端设置



使用 “MC 客户端设置”对话框来集中管理您 MDaemon Connector用户的客户端设置。使用您需要的客户端设置来配置各个屏幕，这样 MDaemon 会将这些设置推送到相应的客户端屏幕，每次将一名 MC 用户连接到服务器。自上次 MC 客户端连接和接收设置以来，只有在更新和改变设置时，才发送最新设置。如果您启用了下方的选项来 *“允许 MC 用户覆盖推送的设置”*时，用户可以在其个别客户端上覆盖任何推送的设置。如果禁用了此项，将锁定所有客户端屏幕；MC 用户可以不做任何变更。

要允许必须不同于各名用户或域的特定设置，MC 客户端设置支持以下宏，例如 $USERNAME$、$EMAIL$ 和 $DOMAIN$。在将设置推送到一个客户端时，会将这些宏转换成视

用户或域而定的数据。注意不要将任何静态值放入应该使用宏的任何字段，例如不要将 "Frank Thomas"这样的信息放入您的 "姓名"字段。这会使每名连接到 MDaemon 的 MC 用户将其姓名设置成 "Frank Thomas"。方便起见，在常规 328屏幕上存在一个 "宏引用"按钮，它显示所支持宏的一个列表。

对于使用 MDaemon Private Cloud (MDPC) 的用户，在域管理器 149上的另一个 "MC 客户端设置"对话框用来按域控制 MDaemon Connector 客户端设置。

此功能在默认情况下处于禁用状态，仅在 MDaemon Connector 客户端 4.0.0 或更高版本中受支持。

MC 客户端设置

将客户端设置推送到 MC 用户
如果您希望每当 MC 用户进行连接时，将 "MC 客户端设置"屏幕上预配置的设置推送到这些用户，请启用此项。自上次 MC 客户端连接和接收设置以来，只有在更新和改变设置时，才发送最新设置。默认情况下，禁用该选项。

允许 MC 用户覆盖推送设置
如果启用此项，用户可以覆盖其个别客户端上的任何推送设置。如果禁用了此项，将锁定所有客户端屏幕；MDaemon Connector 用户可以不做任何变更。

允许用户覆盖设置不会阻止服务器将以后的变更推送到这些客户端，例如，如果用户更改了其中一个 MDaemon Connector 设置，然后管理员对这个服务器上的 "MC 客户端设置"屏幕做出一些变更，那么在下一次与上述服务器建立连接时，会将所有 MC 客户端设置推送到该用户的客户端。因此甚至会将用户以前覆盖的设置进行更改来匹配服务器上的这些设置。

自动发现 MC 设置

首次配置 客户端上的 MDaemon Connector 插件时，用户可以点击 "常规"屏幕上的 *"文本 & 获取账户设置"*按钮后，输入其 *"用户名"*和 *"密码"*。这会使 MDaemon Connector 尝试验证凭证并自动检索该账户的服务器信息。

要连接到这台服务器，客户端将先尝试常规的 FQDN 值。对于 IMAP，它将尝试依次使用专用的 SSL 端口、使用 TLS 的非 SSL 端口来验证 mail.<domain> (例如 mail.example.com)。如果没有成功，它将依次为 imap.<domain>、<domain> 和 imap.mail.<domain> 重复相同的过程。如果所有尝试都失败了，将为这些相同的位置尝试未加密的登录。

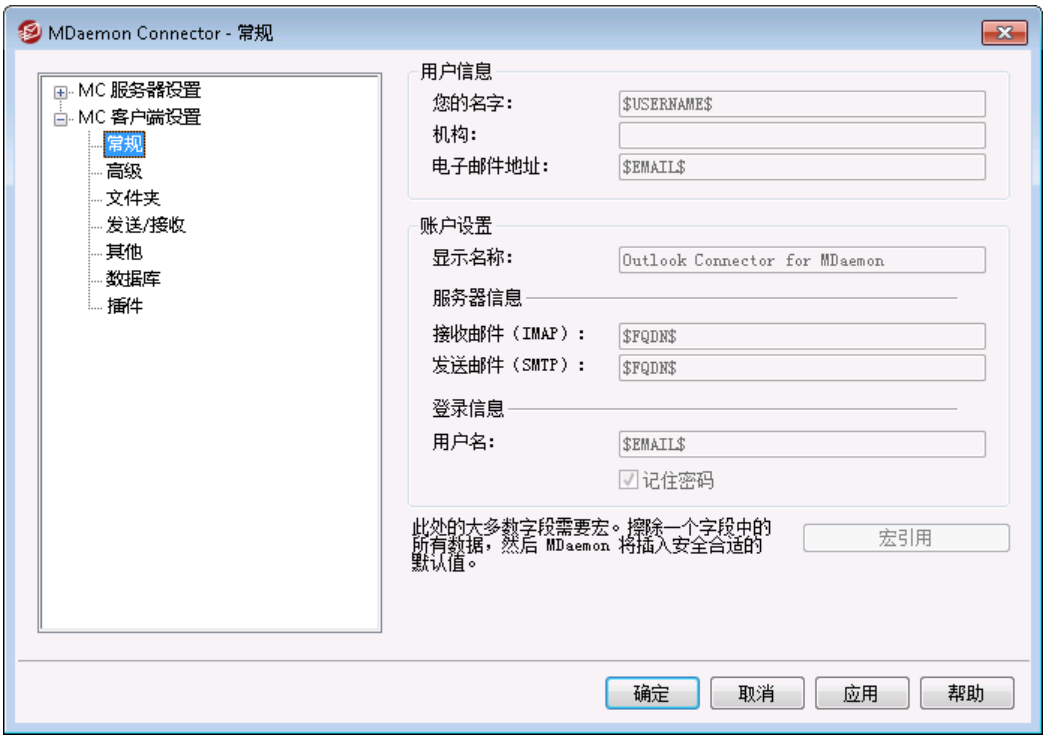
对于 SMTP，它将依次使用 587、25 和 465 端口 (先 SSL 再 TLS)尝试mail.<domain>。然后依次为 smtp.<domain>、<domain> 和 smtp.mail.<domain> 重复这些步骤。如果所有尝试都失败了，将为这些相同的位置尝试未加密的登录。

如果 MDaemon Connector 可以成功验证，那么将自动配置入站和出站服务器信息和 SSL/TLS 信息。

还请参阅：

MC 服务器设置 » 设置 324
MC 服务器设置 » 账户 325
MC 客户端设置 » 常规 328

3.8.2.1 常规



当您启用 *"将客户端设置推送至 MC 用户"*这个选项时，（位于 MC 客户端设置 326屏幕），每当 MDaemon Connector用户连接到服务器时，会将此屏幕上的设置推送至 MDaemon Connector客户端中相应的屏幕。自上次 MC 客户端连接和接收设置以来，只有在更新和改变设置时，才发送最新设置。这个屏幕上的大多数字段应包含宏而不是静态值。还请参阅下方的宏引用 329。

用户信息

您的姓名
默认情况下此项使用 $USERNAME$ 宏，这会插入用户的姓和名。这会在用户邮件的 "发件人"报头出现。

组织
这个可选字段用于您的公司或组织名称。

电子邮件地址
默认情况下此项使用 $EMAIL$ 宏，这会插入用户的邮件地址。这会在用户邮件的 "发件人"报头出现。

账户设置

显示姓名
该姓名在 Outlook 中显示，这样用户便能识别正在使用哪个账户。这在用户在其配置文件中拥有多个账户时很有用。只有该用户看得见这条信息。默认情况下将此设置成 "MDaemon Connector"。

服务器信息

入站邮件 (IMAP)：
这是 MC 客户端将访问的服务器，以便收集和管理每名用户的电子邮件。默认情况下将此值设置成 $FQDN$。

出站邮件 (SMTP)：
这是 MC 客户端用来连接并发送您用户出站邮件的服务器。通常这与上方的入站邮件 (IMAP) 服务器相同。默认情况下将此值设置成 $FQDN$。

登录信息

用户名
这是访问和管理每名用户的 MDaemon 邮件账户所需的用户名。这通常与上方的 *"电子邮件地址"*相同。默认情况下将此项设置成 $EMAIL$。

记住密码
默认情况下将 MDaemon Connector 客户端设置成保存用户密码，这样一来在启动 Outlook 时，它将自动登录邮件账户，无需请求凭证。如果您希望在启动 Outlook 时要求用户输入其密码，请禁用此项。

宏引用

要允许必须不同于各名用户或域的特定设置，MC 客户端设置支持以下宏，例如 $USERNAME$、$EMAIL$ 和 $DOMAIN$。在将设置推送到一个客户端时，会将这些宏转换成视用户或域而定的数据。注意不要将任何静态值放入应该使用宏的任何字段，例如不要将 "Frank Thomas"这样的信息放入 *"您的姓名"*字段。这会使每名连接到 MDaemon 的 MC 用户将其姓名设置成 "Frank Thomas"。请点击 "宏引用"按钮来查看可用宏的列表：

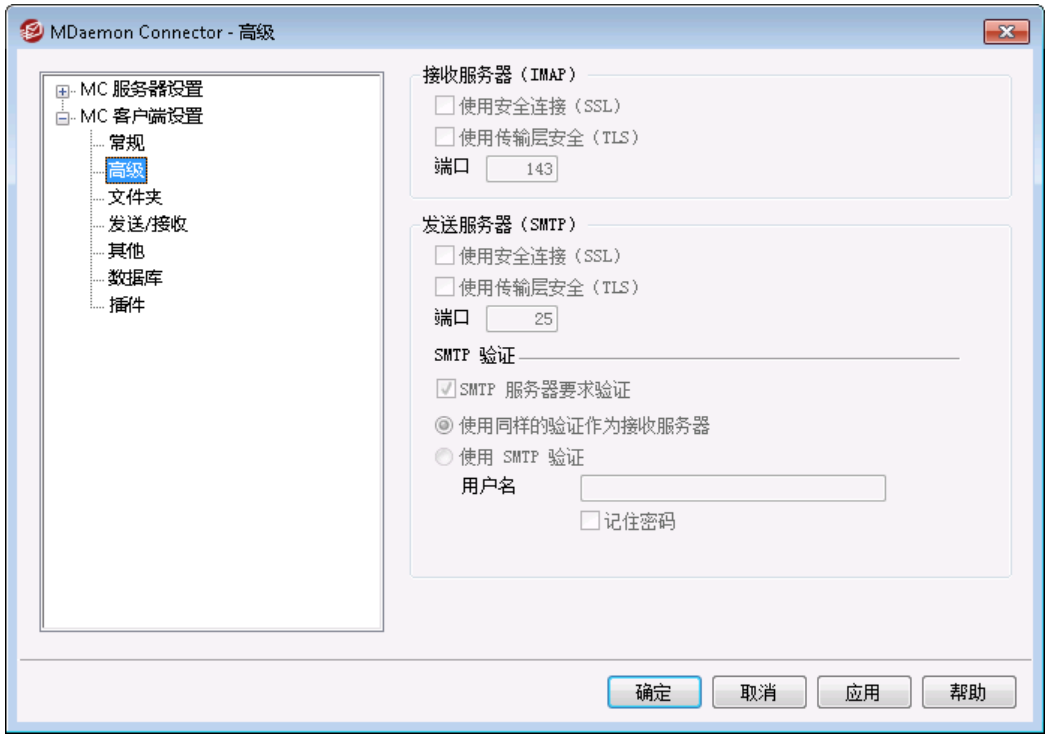
$USERNAME$	此宏插入 *"姓名"*选项的值，位于用户的账户详细信息 598 屏幕下方。它等同于："$USERFIRSTNAME$ $USERLASTNAME$"
$EMAIL$	插入用户的电子邮件地址。这等同于：$MAILBOX$@ $DOMAIN$。
$MAILBOX$	此宏插入账户的邮箱名称 598。

$MAILDIR$	插入用户的根邮件文件夹[601]。
$USERFIRSTNAME$	此宏解析账户持有者的名字。
$USERFIRSTNAMELC$	此宏以小写字母解析账户持有人的名。
$USERLASTNAME$	此宏解析账户持有者的姓氏。
$USERLASTNAMELC$	此宏以小写字母解析账户持有人的姓。
$USERFIRSTINITIAL$	此宏解析账户持有人名的第一个字母。
$USERFIRSTINITIALLC$	此宏以小写字母解析账户持有人名的第一个字母。
$USERLASTINITIAL$	此宏解析账户持有人姓的第一个字母。
$USERLASTINITIALLC$	此宏以小写字母解析账户持有人名的第一个字母。
$MAILBOXFIRSTCHARSn$	此处的 "n"是 1 到 10 之间的数。它将随着邮件箱名称中第一个 "n"字符而扩展。
$DOMAIN$	插入账户的邮箱域[598]。
$DOMAINIP$	此宏解析与账户所属域相关联的 IPv4 地址[151]。
$DOMAINIP6$	此宏解析与账户所属域相关联的 IPv6 地址[151]。
$FQDN$	插入账户所属域的全称域名或 SMTP 主机名[151]。
$PRIMARYDOMAIN$	此宏解析 MDaemon 的默认域[149]名。
$PRIMARYIP$	此宏解析 IPv4 地址[151]，该地址与 MDaemon 的默认域[149]相关联。
$PRIMARYIP6$	此宏解析 IPv6 地址[151]，该地址与 MDaemon 的默认域[149]相关联。

还请参阅：

MC 客户端设置[326]
MC 服务器设置 » 设置[324]
MC 服务器设置 » 账户[325]

3.8.2.2 高级



当您启用 *"将客户端设置推送至 MC 用户"*这个选项时，（位于 MC 客户端设置 326屏幕），每当 MDaemon Connector 用户连接到服务器时，会将此屏幕上的设置推送至 MDaemon Connector 客户端中相应的屏幕。MC 客户端连接和接收设置以来，只有在更新和改变设置时，才发送最新设置。

接收服务器（IMAP）

使用安全连接（SSL）
如果您希望客户端在连接到入站邮件（IMAP）服务器时使用安全的 SSL 连接，请勾选此框。启用此项会将 "端口"设置自动更改成 "993"，这是默认的 SSL 端口。

使用传输层安全（TLS）
如果您希望客户端在连接到入站邮件（IMAP）服务器时使用安全的 TLS 连接，请勾选此框。

端口
这是 MC 客户端用来连接到您入站邮件（IMAP）服务器的端口。默认情况下，将其设置成 143 用于 IMAP 连接，或 993 用于 SSL 加密 IMAP 连接。

发送服务器（SMTP）

使用安全连接（SSL）
如果您希望 MC 客户端在连接到出站邮件（SMTP）服务器时使用安全的 SSL 连接，请勾选此框。启用此项会将 "端口"设置自动更改成 "465"，这是默认的 SSL 端口。

使用传输层安全 (TLS)
如果您希望 MC 客户端在连接到出站邮件 (SMTP) 服务器时使用安全的 TLS 连接，请勾选此框。

端口
这是 MC 客户端用来连接到您出站邮件 (SMTP)服务器的端口。默认情况下，将其设置成 25 用于 SMTP 连接，或 465 用于 SSL 加密 SMTP 连接。

SMTP 验证

SMTP 服务器要求验证
默认情况下，在用户连接到出站服务器 (SMTP) 来发送邮件时，必须使用有效的登录凭证来验证自身。

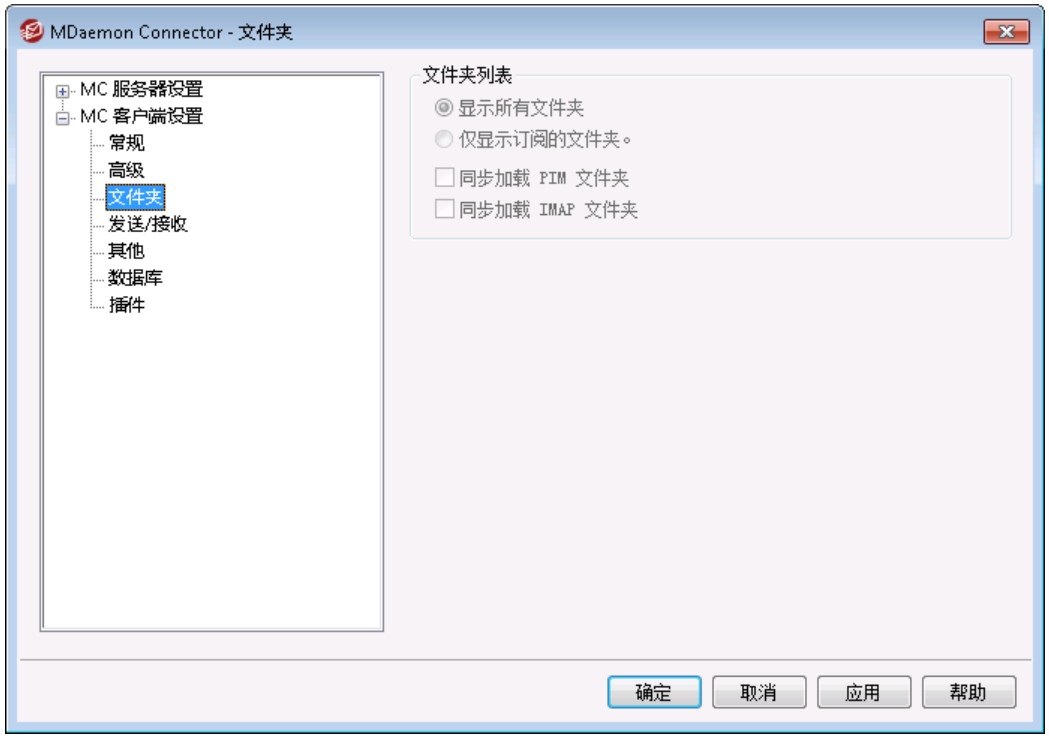
使用同样的验证作为接收服务器
默认情况下 MC 客户端将使用针对出站邮件 (SMTP) 服务器的相同的登录凭证来验证自身。

使用 SMTP 验证
如果您希望要求 MC 用户在发送邮件时使用不同的验证凭证 (这在为出站邮件使用不同的邮件服务器时很必要)，请使用此项。

还请参阅：

MC 客户端设置 326
MC 服务器设置 » 设置 324
MC 服务器设置 » 账户 325

3.8.2.3 文件夹



当您启用 *"将客户端设置推送至 MC 用户"*这个选项时，（位于 MC 客户端设置 326屏幕），每当 MDaemon Connector用户连接到服务器时，会将此屏幕上的设置推送至 MDaemon Connector客户端中相应的屏幕。自上次 MC 客户端连接和接收设置以来，只有在更新和改变设置时，才发送最新设置。

文件夹列表

显示所有文件夹
默认情况下 Outlook 中的文件夹列表将显示 MDaemon Connector用户在邮件服务器上有权访问的所有文件夹。

仅显示订阅的文件夹。
如果您希望 Outlook 文件夹列表仅显示用户已订阅的这些文件夹，请选择此项。

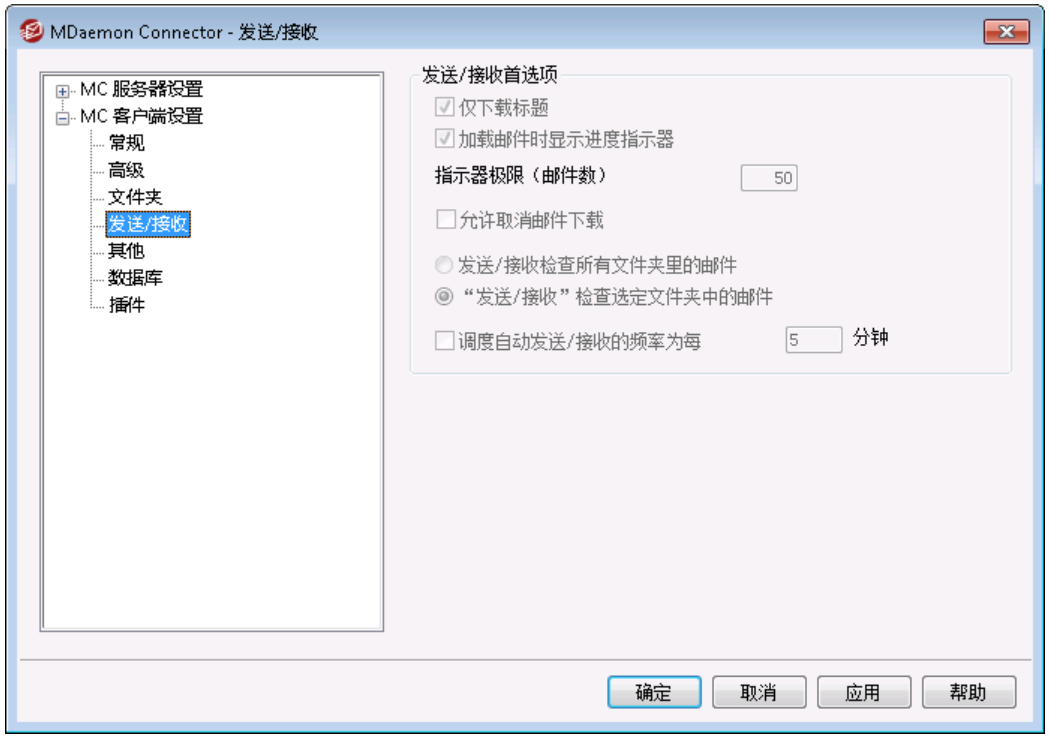
同步加载 PIM 文件夹
在大多数情况下将不勾选此项，表示在 MDaemon Connector加载 PIM 文件夹的内容（例如非邮件文件夹：联系人、日历和任务等）时，MDaemon Connector用户可以继续使用 Outlook。如果您勾选了此框，那么直到加载完所有数据，才能使用 Outlook。通常只有在用户拥有用来访问 PIM 文件夹内容的第三方应用程序时才需要此项。

同步加载 IMAP 文件夹
在大多数情况下将不勾选此项，表示在 MDaemon Connector加载用户的 IMAP 邮件文件夹的内容时，MDaemon Connector用户可以继续使用 Outlook。如果您勾选了此框，那么直到加载完所有数据，才能使用 Outlook。通常只有在用户拥有用来访问邮件文件夹内容的第三方应用程序时才需要此项。

还请参阅：

MC 客户端设置 326
MC 服务器设置 » 设置 324
MC 服务器设置 » 账户 325

3.8.2.4 发送/接收



当您启用了*“推送客户端设置到 MC 用户”*选项（位于MC 客户端设置 326屏幕），每当 MDaemon Connector用户连接到该服务器，便会将这个屏幕上的这些设置推送到 MDaemon Connector客户端相应的屏幕上。自上次 MC 客户端连接和接收设置以来，只有在更新和改变设置时，才发送最新设置。

发送/接收首选项

仅下载标题
默认情况下在 MDaemon Connector在执行 *“发送/接收”*操作并查找新邮件时，它将仅下载邮件报头（例如 *“收件人”*、*“发件人”*和 *“主题”*）显示于邮件列表中。直到查看该邮件时才会下载完整的邮件。

加载邮件时显示进度指示器
MDaemon Connector在下载大量邮件时将显示进度提示器。如果您不希望显示进度提示器，请清除该复选框。

指示器极限（邮件数）
启用了*“显示进度提示器...”*选项时，将在下载大量邮件时显示 *“进度提示器”*。

启用邮件下载取消
如果您希望在 MDaemon Connector 下载大邮件时，您的 MDaemon Connector 用户可以取消下载，请勾选此框。

发送/接收检查所有文件夹里的邮件
如果您希望在 MDaemon Connector 为用户账户执行 "发送/接收"操作时检查各个邮件文件夹是否存在新邮件，请选择此项。

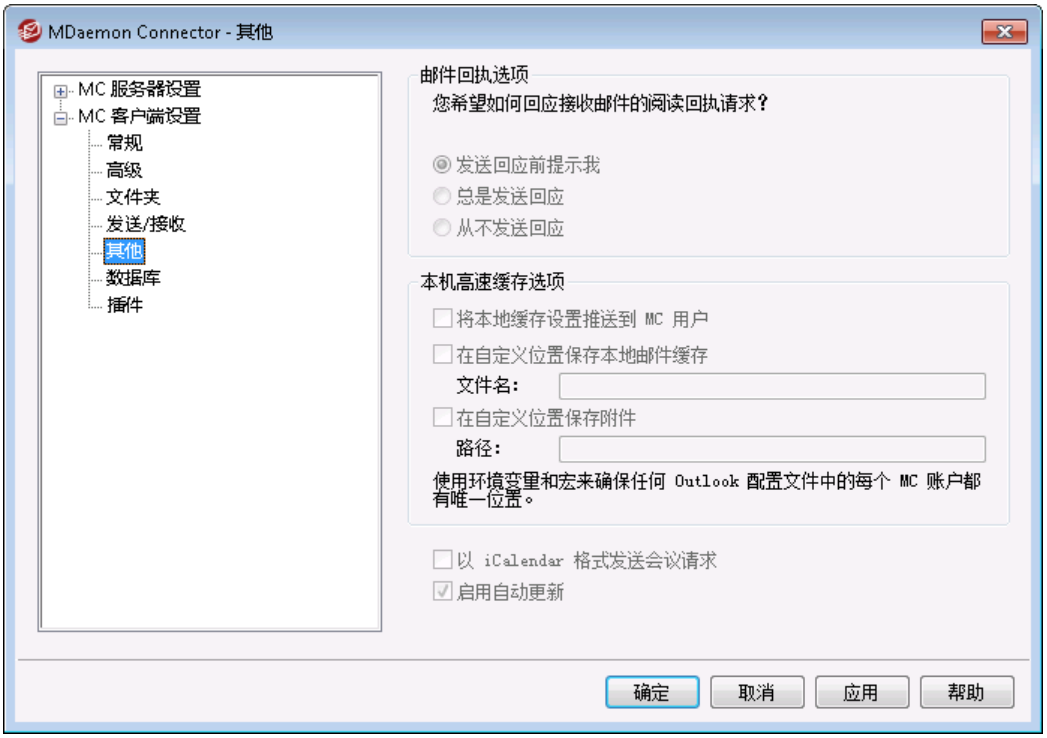
发送/接收检查选定文件夹里的邮件
如果您希望在 MDaemon Connector 对账户执行 "发送/接收"操作时检查用户指定的文件夹中是否存在新邮件，请选择此项。

每隔 [xx]分钟调度自动发送/接收
如果您希望以指定的间隔进行发送/接收，请使用此选项。

还请参阅：

MC 客户端设置 326
MC 服务器设置 » 设置 324
MC 服务器设置 » 账户 325

3.8.2.5 其他选项



当您启用 *"将客户端设置推送至 MC 用户"*这个选项时，位于 MC 客户端设置 326 屏幕），每当 MDaemon Connector 用户连接到服务器时，会将此屏幕上的设置推送至 MDaemon Connector 客户端中相应的屏幕。自上次 MC 客户端连接和接收设置以来，只有在更新和改变设置时，才发送最新设置。

管理回执选项

有时入站邮件包含特殊报头，要求向发件人发送自动邮件请求，以让其了解您何时阅读了该邮件。设置该选项来指定您希望 MDaemon Connector 如何处理要求已读确认的邮件。

发送回应前提示我
如果您希望每当用户打开要求已读确认的邮件时，询问用户是否发送已读确认邮件，请选择此项。

总是发送回应
如果您希望每当用户打开要求已读确认的邮件时，自动发送已读确认邮件，请选择此项。

从不发送回应
如果您不希望 MDaemon Connector 响应已读确认请求，请选择此项。

本地缓存选项

本节中的选项管理 MDaemon Connector 用户的本地邮件缓存的特定位置以及附件的保存位置。

这些选项需要用户的 MDaemon Connector to be version 4.5.0 or newer.

将本地缓存设置推送到 MC 用户
默认情况下，MDaemon 不会将这些设置推送到 MDaemon Connector 客户端。如果您希望将这些设置推送到那里，请选中此框。MC 客户端会将本地文件从当前位置移动到默认位置，如果您在下面的自定义选项中指定了一个，则移动至自定义位置。

将本地邮件缓存保存到自定义位置 |文件名
如果希望 MC 客户端将本地文件移动到自定义位置，请指定缓存的本地路径和文件名。应使用环境变量和宏来确保每个用户的唯一位置。例如：

```
%APPDATA%\Alt-N\Outlook Connector 2.0\Accounts\%OUTLOOKPROFILE%\%
  OUTLOOKEMAIL%\LocalCache.db
```

将附件保存到自定义位置 |路径
如果要自定义 MC 客户端保存文件附件的文件夹位置，请在此处指定路径。应使用环境变量和宏来确保每个用户的唯一位置。

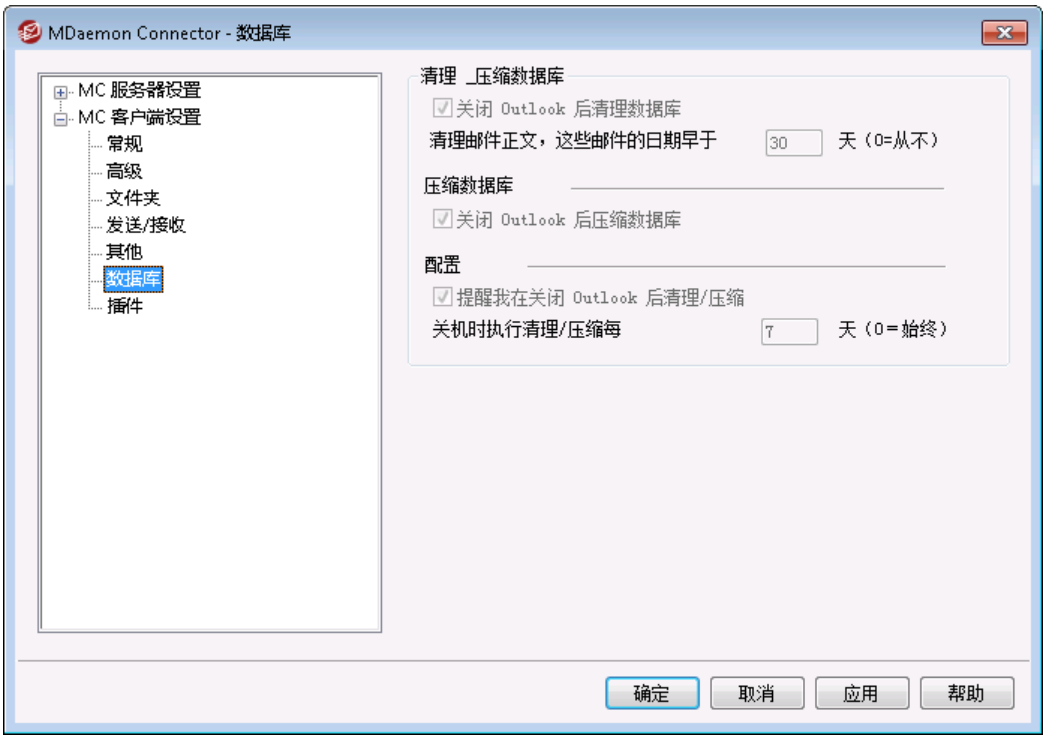
以 iCalendar 格式发送会议请求
如果您希望 MC 以 iCalendar (iCal) 会议格式发送会议请求，请勾选此框。

启用自动更新
默认情况下，每当存在可用的新版本时将自动更新 MC。如果您不希望自动更新，请清除该复选框。

还请参阅：

MC 客户端设置 326
MC 服务器设置 » 设置 324
MC 服务器设置 » 账户 325

3.8.2.6 数据库



当您启用 *"将客户端设置推送至 MC 用户"*这个选项时，（位于 MC 客户端设置 326屏幕），每当 MDaemon Connector 用户连接到服务器时，会将此屏幕上的设置推送至 MDaemon Connector 客户端中相应的屏幕。自上次 MC 客户端连接和接收设置以来，只有在更新和改变设置时，才发送最新设置。

清理 & 压缩数据库

在 Outlook 关闭时清理数据库
默认情况下将 MDaemon Connector 设置成在您关闭 Outlook 时清理/删除旧邮件的邮件正文，以便维护磁盘空间并提高性能。这既不会删除邮件报头，也不会影响保存在服务器上的原始邮件，该操作只是删除本地缓存的邮件正文。每当您打开一封在过去清理过的旧邮件，会再次将邮件正文下载到您的计算机。此外只清理邮件正文，该操作不影响联系人、日历、任务、日志或便笺。如果您不希望在关机时清理数据库，请禁用此项。

清理存在时间长于 XX 天的邮件正文 (0=从不)
使用此项来指定在关闭 Outlook 时，要清理存在时间多长的邮件正文。默认情况下，待清理的邮件的存在时间必须超过 30 天。其存在时间基于邮件修改日期。如果您不希望执行清理操作，请在此项中使用 "0"。

压缩数据库

在 Outlook 关机时压缩数据库
默认情况下将 MDaemon Connector 设置成在用户关闭 Outlook 时，对缓存在本地的邮件数据库文件进行压缩和磁盘碎片清理，以便维护磁盘空间并提高性能。不过必须明确关闭 Outlook 来触发压缩操作，如果 Outlook 崩溃或者您使用 "任务管理器"来 "结束任务"，则不会压缩数据库。您可以使用下方 "配置"部分中的一些选项来指定该操作的发生频率，以及是否在执行前向您发送提示。

配置

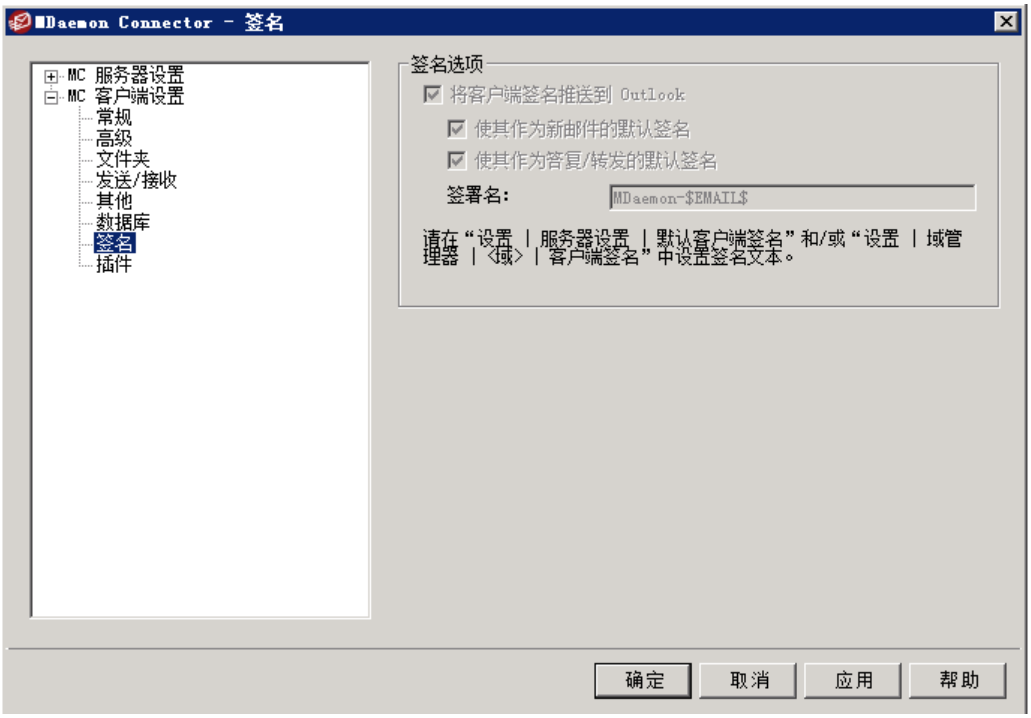
在 Outlook 关闭时执行清理/压缩操作时向我发送提示
如果您希望 MDaemon Connector 在 Outlook 关闭时开始执行数据库清理或压缩操作前向您发送提示，请使用此项。如果用户点击 "是"，它将执行压缩或清理操作，并显示进度提示器。如果您不希望用户接收提示，请清理此勾选框；MDaemon Connector 将在 Outlook 关闭时自动开始清理或压缩数据库，并同时显示进度提示器。

每隔 XX 天在关闭时运行清理/压缩 (0=始终)
此项控制 MDaemon Connector 在 Outlook 关闭时执行数据库清理或压缩操作的频率。默认情况下将此项设置成 7 天，表示每隔 7 天就在 Outlook 关闭时执行数据库清理或压缩操作。如果您希望在用户每次关闭 Outlook 时都清理/压缩数据库，请将此项设置成 "0"。

还请参阅：

MC 客户端设置 326
MC 服务器设置 » 设置 324
MC 服务器设置 » 账户 325

3.8.2.7 签名



当您启用了*"推送客户端设置到 MC 用户"*选项（位于MC 客户端设置 326屏幕），每当 MDaemon Connector用户连接到该服务器，便会将这个屏幕上的这些设置推送到"签名"(位于 Outlook 中"**文件 » 选项 » 邮件 » 签名**"下）屏幕上。此功能需要 MDaemon Connector6.5.0 或更高版本。

签名选项

将客户端签名推送到 Outlook
如果您希望将默认的客户端签名 113（或已经创建的是域而定的客户端签名 170）推送到您的 MDaemon Connector用户，请启用此项。在下方的*"签名名称"*选项中指定名称。

使其成为新邮件的默认签名
如果您希望使客户端签名成为用于新邮件的默认签名，请选中此框。

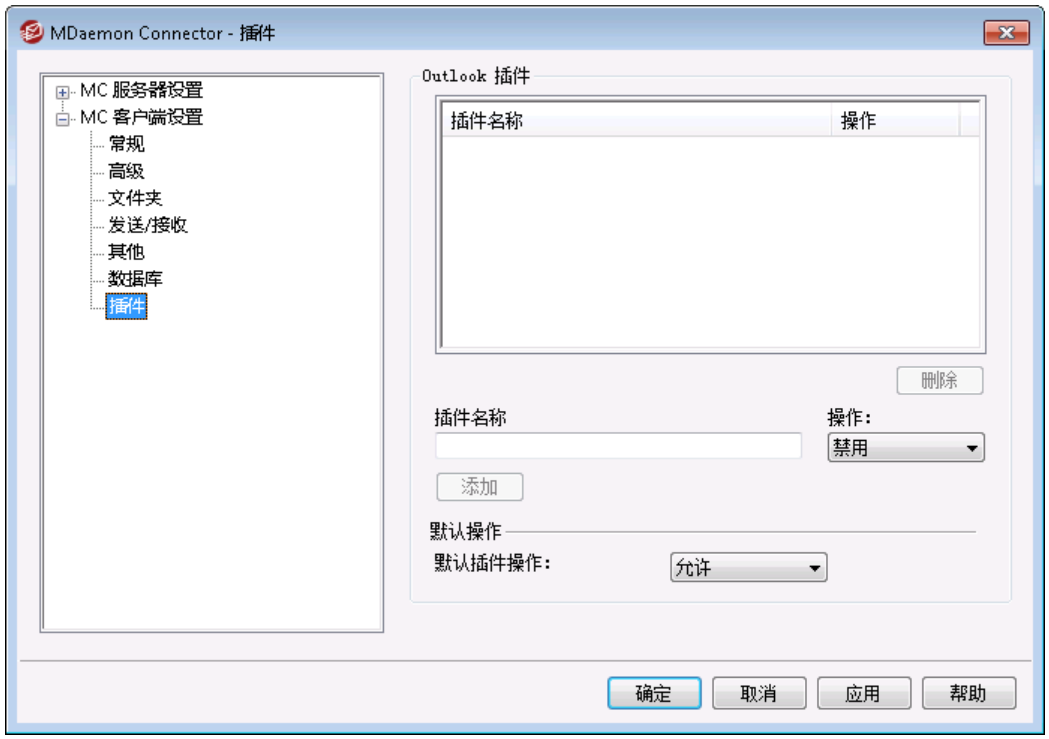
使其成为答复/转发的默认签名
如果您希望使客户端签名成为用于答复/转发的默认签名，请选中此框。

签名名称：
这是推送给 MDaemon Connector用户在 Outlook 中的电子邮件账户的签名名称。默认情况下将此签名的名称设置成："MDaemon-$EMAIL$"。会将 $EMAIL$ 宏转换成用户的邮件地址。例如：MDaemon-Frank.Thomas@company.test。

还请参阅：

MC 客户端设置 326
MC 服务器设置 » 设置 324
MC 服务器设置 » 账户 325
默认客户端签名 113
域管理器 » 客户端签名 170

3.8.2.8 插件



使用插件屏幕，您可以管理 MDaemon Connector (MC)用户使用的 Outlook 插件的状态。您可以允许任何或全部插件被正常使用，或者禁用任何您选择的插件。当您知道与 MDaemon Connector 客户端发生冲突的特定插件时，此功能可能特别有用，从而允许您禁用该插件来避免问题。上述插件功能需要 MDaemon Connector 5.0 或更高版本。

Outlook 插件

此框包含用户的 Outlook 插件列表和分配给每个用户的操作：*禁用*、*允许*或*默认值*。当 MC 用户启动 Outlook 时，MC 客户端将用户插件列表发送至 MDaemon，然后禁用 被设置成 *"禁用"*的任何插件。任何设置成 *"允许"*的插件不会发生变化。被设置成 *"默认值"*值的插件将使用下方分配的 *"插件默认操作"*。

MDaemon Connector 可以仅为将其 MDaemon Connector 账户设置成 Microsoft Outlook 默认账户的用户管理 Outlook 插件。

添加、删除和修改插件

添加插件
要将插件添加到列表，请输入在 Outlook 中显示的*插件名称*，设置*操作*并点击**添加**。如果您知道您希望管理的插件，但是安装了该插件的用户尚未连接，则此选项非常有用。

删除插件
要从列表中删除插件，请选择这个插件并点击 *"删除"*。

设置插件的操作
要修改插件，将其选定，然后使用下拉列表来设置其*操作*并点击**添加**。

默认操作

插件的默认操作
将此项设置成*允许*或*禁用*。设置成*允许*时，默认情况下 Outlook Connector 将仅禁用您专门设置成 *"禁用"*的插件。所有其他插件保持原样。设置成 *"禁用"*时，Outlook Connector 将自动禁用所有插件，除非您专门将其设置成 *"允许"*。默认情况下，将此项设置为 *"允许"*。

还请参阅：

MC 客户端设置 326
MC 服务器设置 » 设置 324
MC 服务器设置 » 账户 325

3.9 集群服务

MDaemon 的集群服务的设计旨在：在网络上的两个或多个 MDaemon 服务器之间共享您的配置。这使您可以使用负载均衡硬件或软件，在多个 MDaemon 服务器之间分配电子邮件负载，从而可以通过减少网络拥塞和过载，并最大化电子邮件资源来提高速度和效率。如果一台服务器发生硬件或软件故障，该功能还有助于确保电子邮件系统中的冗余。

在决定是否在网络上设置 MDaemon 集群时，需要考虑以下几点：

节点

一个 MDaemon 集群将具有一个主节点和一个次节点。一台 MDaemon 服务器将被指定为主服务器，而其他所有服务器将被指定为次服务器。

- 用作主节点的 MDaemon 服务器将其配置复制到所有其他节点上。因此，主节点是唯一可用于进行配置更改的节点。如果您访问次节点并进行配置变更，则这些变更将被覆盖。因此，大多数配置选项在次节点上的用户界面中均不可用。
- 集群服务不会跨节点复制邮箱文件夹或公共文件夹；所有节点共享同一组邮件文件夹。用户邮件文件夹和公共文件夹必须位于网络上所有节点均可访问的位置。
- 在次节点上发生的任何电子邮件变更都将发送到主节点，然后将所有变更通知所有其他节点。
- 次节点上的 XML-API 仅可读。

- 集群上的每个节点应位于同一个网络。我们不建议使用集群服务来群集位于不同位置的服务器。
- 集群中的每个节点需要运行相同版本的 MDaemon。
- 集群中的每个节点都需要自己的 MDaemon 密钥。

路由

MDaemon 不处理去往或来自特定节点的任何流量的路由。我们建议您使用第三方负载均衡器来处理流量路由。

负载均衡器中的粘滞 (Sticky)会话是必需的，以便来自同一 IP 的所有流量都路由到同一主机。对于 MDRA、Webmail和 XMPP 流量而言，粘滞会话最重要，因为它们尚不支持集群，这意味着会话信息不会在节点之间传递。要消除这个限制：

- 所有 MDRA 连接必须路由到主节点。
- 当某人登录到特定服务器上的 Webmail时，该会话的所有流量都必须路由到这个同一服务器。
- Webmail和 XMPP 通信需要路由到同一服务器，以便 Webmail的内置聊天功能正常工作。
- 所有 XMPP 通信都必须路由到同一节点，否则连接到不同服务器的用户将无法彼此聊天。
- 考虑到以上几点，我们建议将所有 HTTP 和 XMPP 通信都路由到主节点，因为这是最简单的配置，并且几乎不会引起任何问题。但是，如果您不使用其中某些功能，则可以更改配置 (尽管仍然需要粘滞会话)。

邮箱和文件夹

邮箱、公共文件夹和其他一些文件夹必须保存在共享路径中，集群中的每个节点都可以访问该共享路径。请记住，如果您使用的是 UNC 路径，则需要以有权访问网络位置的用户身份运行 MDaemon 服务。

- 您必须手动更新您的邮箱和文件夹路径，并将文件夹的内容移至集群可访问的位置。这不是在设置集群时 MDaemon 可为您执行的自动功能。集群服务将使用您在集群服务配置中提供的邮箱和公共文件夹的网络文件夹路径，更新 MDaemon.ini 文件。
- 必须将 Lockfiles 目录移动到共享位置。您可以允许 "集群服务"自动执行此操作，也可以通过编辑 LockFiles 密钥 (位于 [Directories] 部分，在 MDaemon.ini 文件中)。如果您允许集群服务为您执行此操作，则 LockFiles 目录将位于 "网络邮箱"路径下。
- 还必须将 PEM 目录移动到共享位置。要实现这个目的，请将 MDaemon\PEM\ 文件夹复制到新的共享位置，并编辑 PEM 密钥，位于 [Directories] 部分，在 MDaemon.ini 文件中，然后重启 MDaemon。
- 新账户模板将使用集群服务配置中提供的邮箱路径进行更新。

动态屏蔽

- 动态屏蔽 510 将所有请求发送到主服务器节点，主节点中的数据被复制到次节点。

- 如果主节点处于离线状态，则次节点将使用其自己的动态屏蔽配置，该配置应与主节点离线时的配置相同。当主服务器联机时，次服务器对动态屏蔽所做的任何变更都将被覆盖。

证书

- SSL证书会自动从主节点复制到从节点。
- MDaemon 还复制其证书设置[481]，因此每个集群中的节点/服务器都将尝试使用相同的证书。如果节点没有正确的证书，则所有 SSL/TLS/HTTPS 通信都将在该节点上失败。
- MDaemon 的 LetsEncrypt 选项目前不支持次节点。

其他

- 附件链接[305]无法在集群中使用 因此在您启用集群中将其禁用。
- 自动更新安装[420]必须禁用。
- 域名至 IP 地址绑定[151]必须禁用。
- 集群中的所有节点应设置为相同的时区，并设置为完全相同的时间。如果时区不同，或者时间间隔超过1秒，则会在集群日志中记录一条警告。

配置集群服务

请按照以下步骤来设置集群服务：

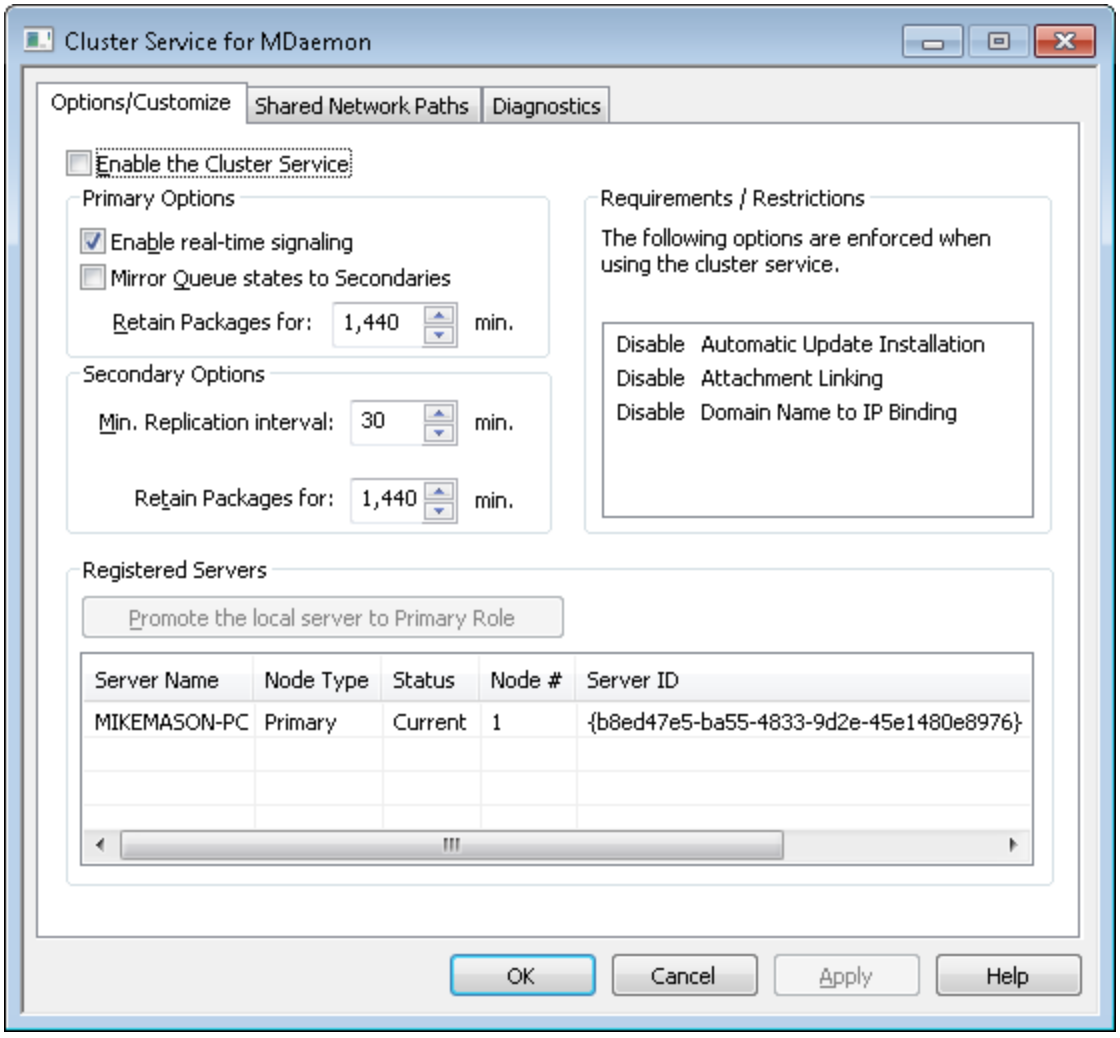
1. 请确保已更新所有邮箱路径并调整了公共文件夹路径。主服务器应使用该数据的网络存储位置，并且应该能够在继续操作之前毫无问题地访问数据。
2. 所有适当的证书应安装在每个节点上。
3. 使用唯一密钥在次节点上安装 MDaemon。
4. 在主节点上，前往 **"设置 » 集群服务"**。
5. 右键单击 "受限制服务器"列表，然后点击 **"将新的 MDaemon 服务器添加到集群"**（这可能很慢，因为它正在网络中搜索可用的服务器）。
6. 在 *"服务器名称"*中，输入安装了 MDaemon 的从节点的 NETBIOS 名称、IP 地址或 DNS 名称，或从下拉列表选择服务器，可能会有延迟，因为它正在网络中搜索可用的服务器。
7. 点击 **"确定"**。
8. 检查 "插件/集群"日志，以确保两个服务器已连接并且正在复制。
9. 前往次节点上的 **"设置 » 集群服务"**来确认它现在还在 "已登记服务器"下列出了主节点和次节点。
10. 如上所述，配置负载均衡硬件或软件来将流量路由到集群。

还请参阅：

集群服务 | 选项/自定义 344
集群服务器 | 共享网络路径 345
集群服务 | 诊断 347

3.9.1 选项/定制

选项/定制



启用集群服务

点击启用“集群服务”。

主节点选项

启用实时信令
默认情况下，无论何时在主节点上发生变更，它都会向从节点发送一个复制信号，以通知它们需要进行复制请求，以在节点之间同步设置。

将队列状态镜像到从节点
如果您希望确保在主节点上更改邮件队列的状态（即冻结或解冻），请选中此框，该状态也将在从节点上进行更改。

从节点选项

复制间隔 [xx]分钟
此选项确定从节点在发出复制请求之前将等待来自主节点的复制信号的时间。默认情况下将此项设置成 30 分钟。

已登记服务器

这将显示 MDaemon 服务器集群中的所有节点。

将本地服务器提升到主节点角色
要将从节点更改为主节点，请在要提升的从节点上，选择列表中的节点，然后点击 **"提升"**。新的主节点应通知旧的主节点，作为从节点重新加入该集群。对于具有多个从节点的设置，则需删除其他从节点，并将其重新添加到集群中。

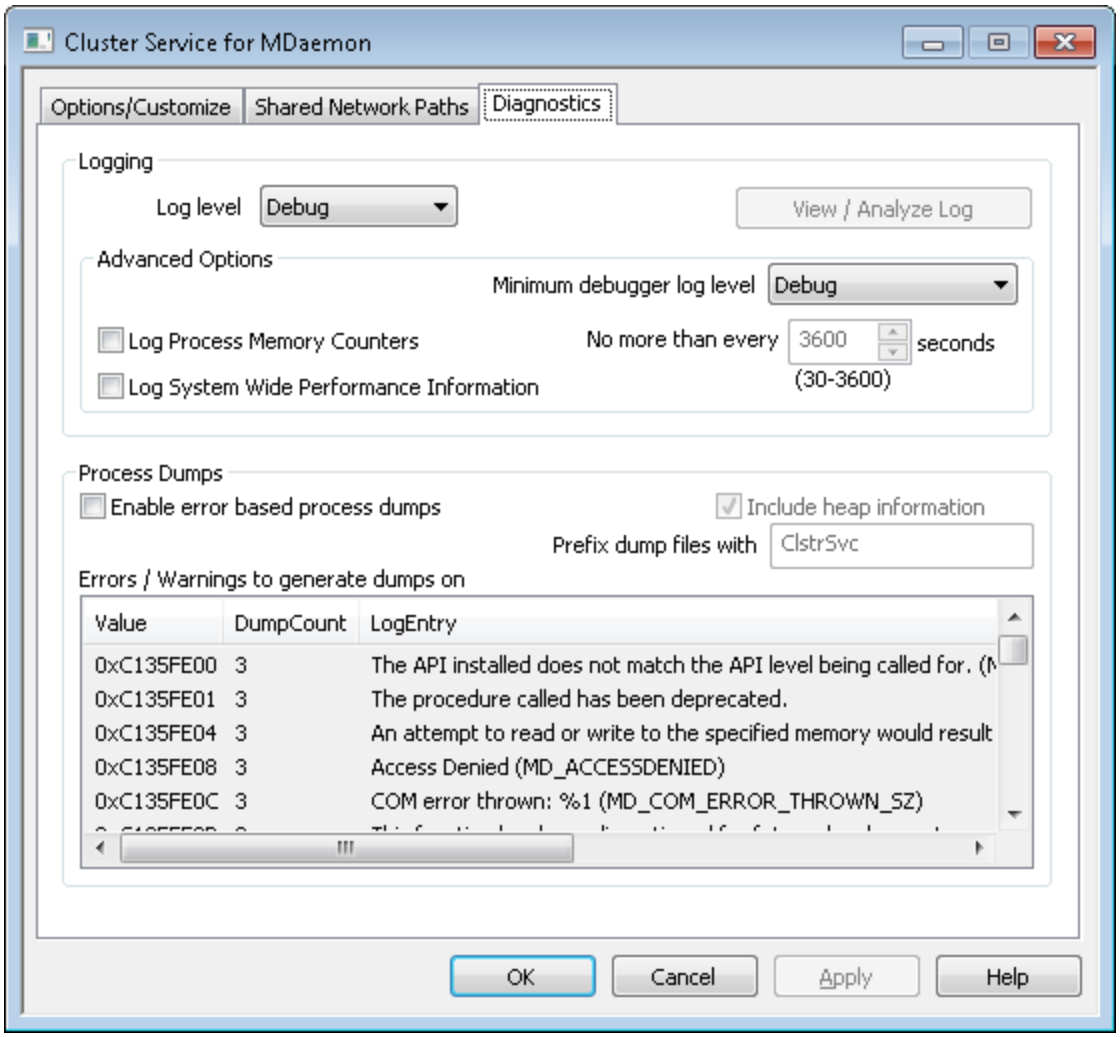
将新的 MDaemon 服务器添加到集群
要将新的 MDaemon 服务器添加到集群，请右键单击服务器列表并点击 **"将新的 MDaemon 服务器添加到集群"**。在打开的屏幕上，输入安装了 MDaemon 的服务器的 NETBIOS 名称、IP 地址或 DNS 名称，或从下拉列表中选择它。起初可能会有延迟，因为它正在网络中搜索可用的服务器。

还请参阅：

集群服务 341
集群服务器 | 共享网络路径 345
集群服务 | 诊断 347

3.9.2 共享网络路径

共享网络路径



启用共享网络路径编辑（如果这是集群的第一个节点，则是必需的）

使用此屏幕上的选项来设置 MDaemon 集群将使用的共享网络路径。这在集群的首个节点上是必需的，以便可以在其他节点上复制共享的网络路径。

设置所有网络路径都使用常规的公共 MDaemon 网络共享
如果您希望将所有共享的网络路径定位在一个公共网络共享下，请选择此选项。此项导致所有路径均设置为默认值，并且所有路径控件均为只读。

分别设置所有网络路径
如果您希望分别设置每个共享网络路径，请选择此选项。例如，如果您希望在不同的网络位置保存邮件文件夹和邮件归档，请按上述设置。

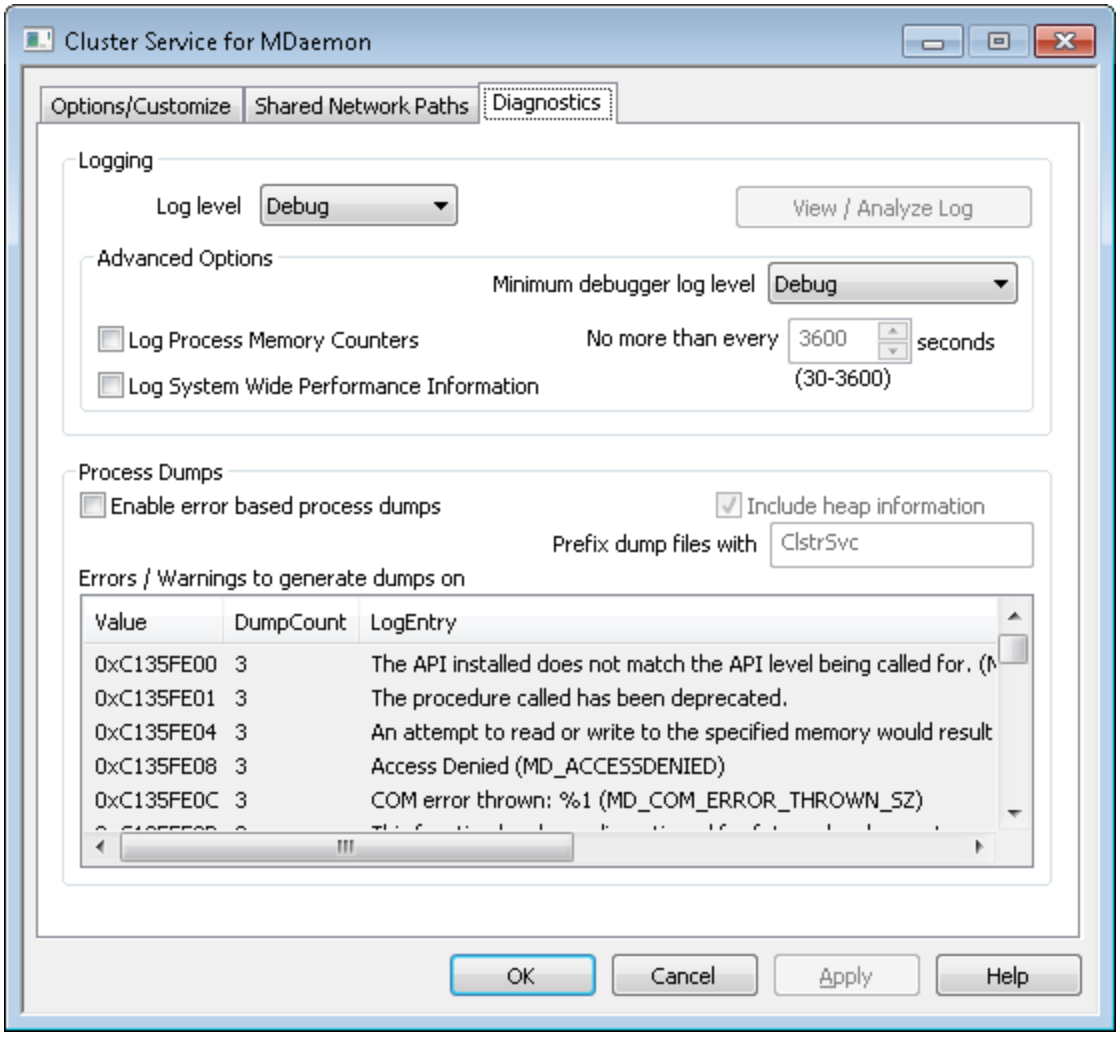
启用多节点邮件路由
如果您希望在集群的节点之间共享邮件队列，请使用“多节点邮件路由”功能。会使用多个服务器来处理和投递邮件，允许它们更平均地分配工作，并防止邮件被卡在任何发生故障的服务器的队列中。

还请参阅：

集群服务 341
集群服务 | 选项/自定义 344
集群服务 | 诊断 347

3.9.3 故障诊断

故障诊断



日志

日志级别

支持 6 种日志级别，将按记录的数据量由高到低进行说明：

调试 这是最丰富的日志级别。记录所有可用条目，通常仅在诊断问题或管理员需要详细信息时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

查看/分析日志文件
点击此按钮来打开 MDaemon 高级系统日志查看器。默认情况下，将日志保存在："..\MDaemon\Logs\"

高级选项

最小化调试器日志级别
这是发送至调试器的日志最小级别。可用的日志级别与上述相同。

记录进程内存计数器
选中此框可将特定于进程的内存、句柄和线程信息记录到日志文件中。这对于发现潜在的故障和资源分配问题很有用。仅当数据自上次记录以来发生变更时，才会发出日志条目。

记录系统范围的性能信息
如果您希望将系统范围的性能信息记录到日志文件中，请选中此框。这对于发现潜在的故障和资源分配问题很有用。仅当数据自上次记录以来发生变更时，才会发出日志条目。

不大于每隔 [xx]秒
使用此选项可以设置对于进程和性能信息的记录频率的限制。

进程转储

启用基于进程转储的错误
如果您希望在发生您于下方指定的特定警告或错误时生成进程转储，请启用此项。

在转储中包含堆信息
默认情况下，在进程转储中包含堆信息。如果您不希望包含这个信息，请清除该复选框。

为转储文件使用前缀
进程转储文件名将使用这个文本开头。

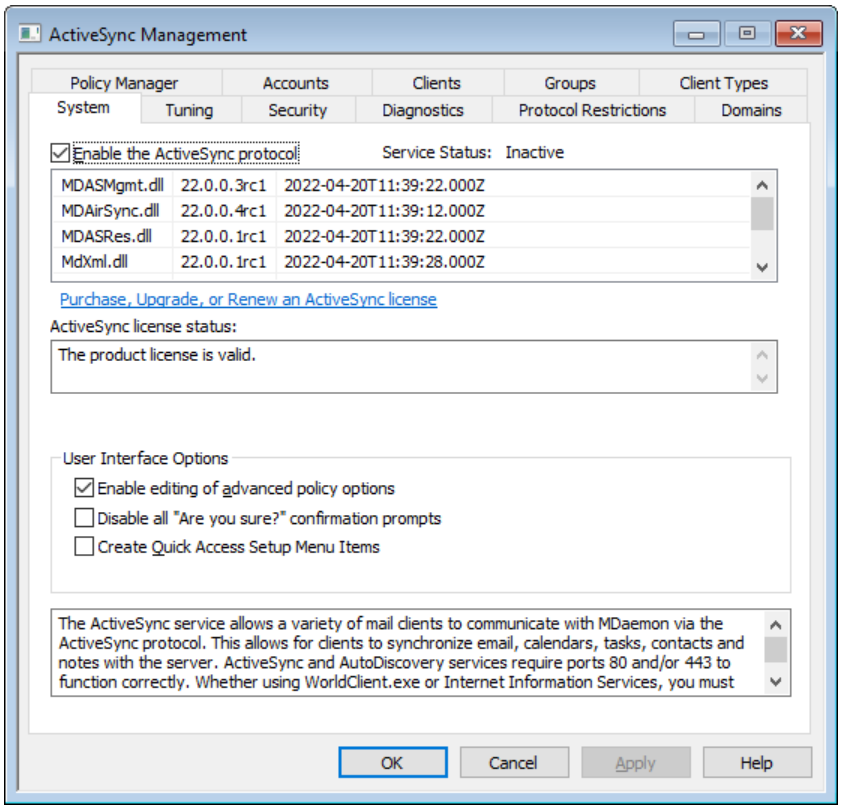
出错/警告时生成转储
右键单击此区域并使用 *"添加/编辑/删除条目..."* 选项来管理将触发进程转储的错误或警告列表。对于每个条目，您可以指定取消激活前进程转储数量。

还请参阅：

集群服务 341
集群服务 | 选项/自定义 344
集群服务器 | 共享网络路径 345

3.10 ActiveSync

3.10.1 系统



现在 MDaemon 中包含了 "ActiveSync for MDaemon"支持，它是单独授权的空中 (OTA) ActiveSync 服务器。该服务器能够同步用户 MDaemon/Webmail账户和设备 (具备 ActiveSync 功能)之间的用户邮件和 PIM 数据 (例如联系人、日历和任务)。

如果您在首次启用 ActiveSync for MDaemon 时使用试用密钥，该程序将有效运行 30 天。60天过后，如果您希望继续使用该软件，您可以从 www.mdaemon.com 或您的本地分销商/经销商那里购买许可证密钥。

ActiveSync 是 web 服务的扩展，只能在 **80** 端口 (用于 http)以及 **443** 端口 (用于 https)上进行作业。这是 ActiveSync 的实施要求。如果启用了 ActiveSync，而且您正在使用 Webmail内置的 web 服务器 (但其未在 80 或 443 端口运行)，那么除了您已在 Web 服务器 270和 SSL & HTTPS 274 屏幕上配置的其他端口之外，它将自动开始在 80 端口运行。如

果您为 Webmail使用其他服务器 (例如 IIS),那么您必须手动配置其使用 80 或 443 端口。

如果您打算在 IIS 下运行 ActiveSync,在要求"/Microsoft-Server-ActiveSync"时您必须调用 ActiveSync DLL (MDAirSync.dll)。所有的 ActiveSync 客户端都会使用该请求。有些版本的 IIS 在不下载、安装和配置第三方软件的情况下不具备此项功能。

使用 ActiveSync 进行的所有初次同步化都是单程的,从服务器同步化到设备。当您初次使用 ActiveSync 执行同步化时,您会丢失该设备上的相关数据。这是 ActiveSync 的实施要求。因此,在您初次使用 ActiveSync 之前请备份您的数据。支持 ActiveSync 的大部分设备警告用户 **将会丢失设备数据**",不过有些设备不会这样做。

启用/禁用 ActiveSync

点击 *"启用 ActiveSync 协议"*来启用 ActiveSync for MDaemon。然后您可以使用 "域 365"选项来控制该程序是对您的所有域可用还是对您的部分域可用。

用户界面选项

启用编辑高级策略选项
如果您希望在 "ActiveSync 策略编辑器 373"上看见 "高级设置"选项卡,请启用此项。它包含在大多数情况下无需变更的各种高级策略设置。默认情况下,禁用该选项。

禁用所有 "您确定吗"确认提示
默认情况下,当您更改某些 ActiveSync 设置时,会出现提示,询问您是否确定要进行更改。如果您希望禁用这些提示,可点击此复选框。

创建快速访问 "设置"菜单项目
如果启用此项,将更改 MDaemon 应用程序界面中的 "设置 » ActiveSync"菜单,并添加指向 "ActiveSync 连接"监视器和 "日志查看器/分析器"的链接。**请注意:** 禁用此项后,仍可以通过右键单击 "统计"窗格内 "服务器"下的 **ActiveSync** 来访问这些工具。

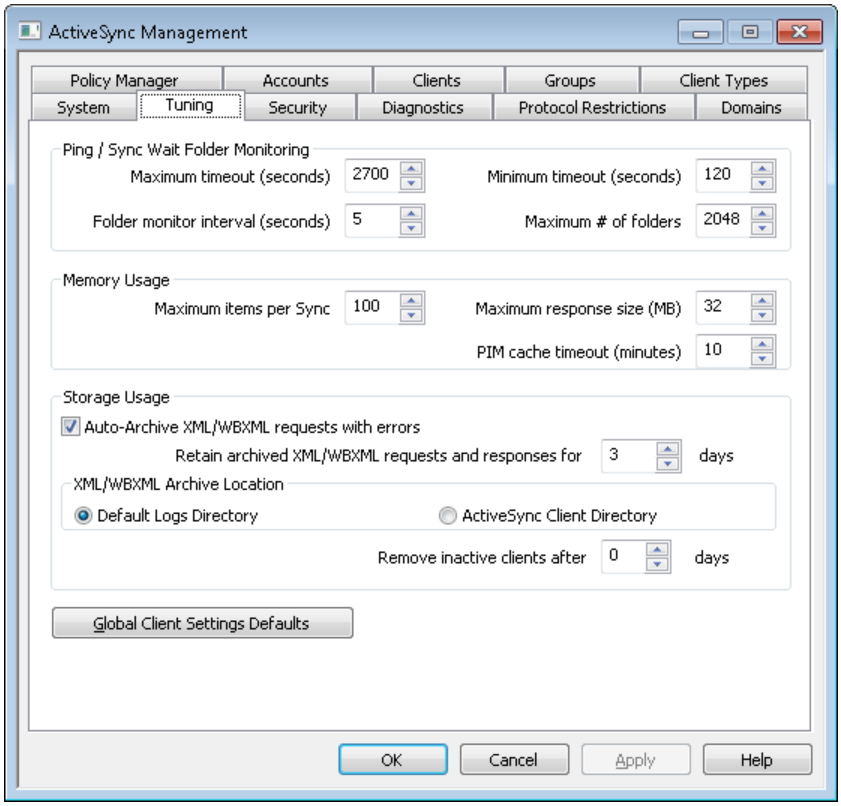
自动发现服务 62

MDaemon 现在支持 自动发现服务 62,这允许用户只需使用其电子邮件地址和密码即可设置 ActiveSync 账户,无需知道 ActiveSync 服务器的主机名。自动发现需要启用 HTTPS 274。

还请参阅:

账户编辑器 » ActiveSync 642
ActiveSync » 域 365
SSL & HTTPS 274
Web 服务器 270

3.10.2 微调



此屏幕包含高级选项，在大多数情况下无需调整，它包含一个按钮来打开全局客户端设置默认值 353 对话框来调整 ActiveSync 客户端使用的默认设置。

Ping/同步等待文件夹监控

超时最大值 (1200-7200 秒)
这是 MDaemon ActiveSync Service (MDAS) 在向客户端返回响应前监控文件夹时将等候的时长最大值。默认值是 2700 秒 (例如：45 分钟)。

超时最小值 (120-480 秒)
这是 MDAS 在向客户端返回响应前监控文件夹时将等候的时长最小值。默认值是 120 秒。您可以在必要时通过增加此值来减少与服务器建立的连接数，因为由于等候时间变长，它将使客户端建立连接的频率变小。

文件夹监控间隔 (3-50 秒)
这是 ActiveSync 服务在文件夹监控发生事件之间将等候的秒数。默认情况下将此值设置成 5。

至多 # 文件夹
这是每个 ActiveSync 客户端被允许监控变更的文件夹数量的最大值。默认值为 2048。

内存使用情况

每次同步的项目数量最大值
这是 ActiveSync 服务响应 Sync 请求时返回客户端的项目数最大值。在此项中使用一个较低的值可以在一个忙碌的服务器上减少内存使用，不过这将需要更多连接和带宽。这还会缩短电池寿命，因为这些设备可能在同步期间发送更多请求来获取所有变更。在此项中使用较高的值将增加内存使用，而且更容易发生通信错误。默认值 100 是一个折中的选择。不过这些客户端将指定它们首选的值，这将有效地为某些客户端降低此值。如果客户端请求了大于最大值的值，将使用这个最大值。

响应大小最大值 (MB)
这是针对来自客户端的 Sync 请求所允许的响应大小最大值。在处理用来进行服务器至客户端同步的指定项目前，将检查响应的当前大小。如果它大于等于此值，就会将这个集合标记成存在更多可用变更，而且不会向这个响应添加更多项目。这对定期在其电子邮件中包含大量大附件的服务器而言极有用处。

PIM 缓存超时 (5-60 分钟)
由于“联系人”、“文档”、“事件”和其他 PIM 数据通常是静态的，只会偶尔从客户端获取更新，MDAS 将缓存这个数据来减少磁盘活动。不过每当磁盘上的数据变化时它将自动重新加载。此值控制自上次被访问后隔多长时间缓存用户的数据。

存储使用

出错时自动归档 XML/WBXML 请求
如果您关闭了用来*归档 [XML / WBXML] 请求和响应*的选项 (位于客户端设置 353 屏幕)，该选项仍然归档存在问题的 XML 或 WBXML 请求。仅归档出错的请求。默认情况下启用此项。

保留已归档的 XML/WBXML 请求和响应长达 [xx] 天
这是自动归档的响应将被保存的天数。默认情况下保留3天。

XML/WBXML 归档位置

默认日志目录
默认情况下，自动归档的 XML/WBXML 请求和错误文件将存储在 MDaemon 的日志目录中。

ActiveSync 客户端目录
如果您希望将文件保存在用户的 ActiveSync Client Debug 目录中，请选择此选项。

在 [xx] 天后删除闲置的客户端
这是在 ActiveSync 设备 388 被删除前可以不连接到 MDAS 的天数。当删除此设备时，将丢弃其配置和访问权限设置。如果此设备再次连接，MDaemon 会将其视为未曾在这个服务器上使用过的新设备。如果此域 365 或账户 380 存在一个策略，会向这个设备强制执行该策略，执行初始文件夹同步并重新同步所有已订阅的文件夹。此选项使服务器不必为旧设备和无用设备维护和保留信息。默认情况下，将此项设置为 31 天。设置为“0”时，无论设备处于闲置状态长达多久，设备都不会被移除。

全局客户端设置默认值

点击此按钮来打开“全局 ActiveSync 客户端设置 353”对话框，用来配置 ActiveSync 客户端所使用的默认设置。

ActiveSync 通知

同步回滚通知

如果客户端在同步操作中重复/频繁地发送过期的同步密钥，ActiveSync Service 可以告知管理员这个事件。

这些通知仅告诉管理员：因为客户端使用最近过期的同步密钥发出同步请求，致使服务器为给定的集合发送回滚。通知的主题为“ActiveSync 客户端使用过期的同步密钥”。发生这个问题的原因可能是网络问题，或者之前发送至这个集合中的客户端的内容存在一些问题。在某些情况下，取决于之前的集合同步是否发送了任何项目，那里将存在一些项目 id。

回滚警报不表示客户端没有同步，而是意味着客户端可能无法完成同步，而且我们的内部系统已检测到这个可能性。为集合发出的回滚警告的频率不超过 24 小时。可以在 \MDaemon\Data\AirSync.ini 文件中的 [System] 报头下编辑以下键值：

- [System] SendRollbackNotifications=[0|1|Yes|No|True|False]（默认值是禁用）
- [System] RollbackNotificationThreshhold=[1-254]：在将通知发送至管理员之前，在给定的集合上必须发生的回滚数量。我们建议此处的值至少是 5，因为这里会存在一些网络问题。（默认值是 10）
- [System] RollbackNotificationCCUser=[0|1|Yes|No|True|False]：是否抄送给客户端发送了过期同步密钥的用户。（默认值是禁用）

ActiveSync 邮件受损通知

如果无法处理特定的邮件，ActiveSync Service 可以告诉管理员这件事。这些邮件都是实时发送的，以便通知管理员无法解析邮件项目，因此关于该项目的后续操作无法执行。这些邮件的主题为“受损邮件通知”。这些项目在早期版本中会导致软件崩溃。在大多数情况下，msg 文件的内容不会是 MIME 数据。不过如果它是 MIME 数据，便可能受损。您可以使用 CMNCCUser 键来选择将这些通知抄送给受影响的用户，这样他们便能知道抵达他们邮箱的邮件不可读。对于这些邮件采取的适当措施应为移动用户邮箱中指定的 msg 文件，并对其进行分析来确定无法解析的原因和造成其处于这种存在状态的原因。可以在 \MDaemon\Data\AirSync.ini 文件中的 [System] 报头下编辑以下键值：

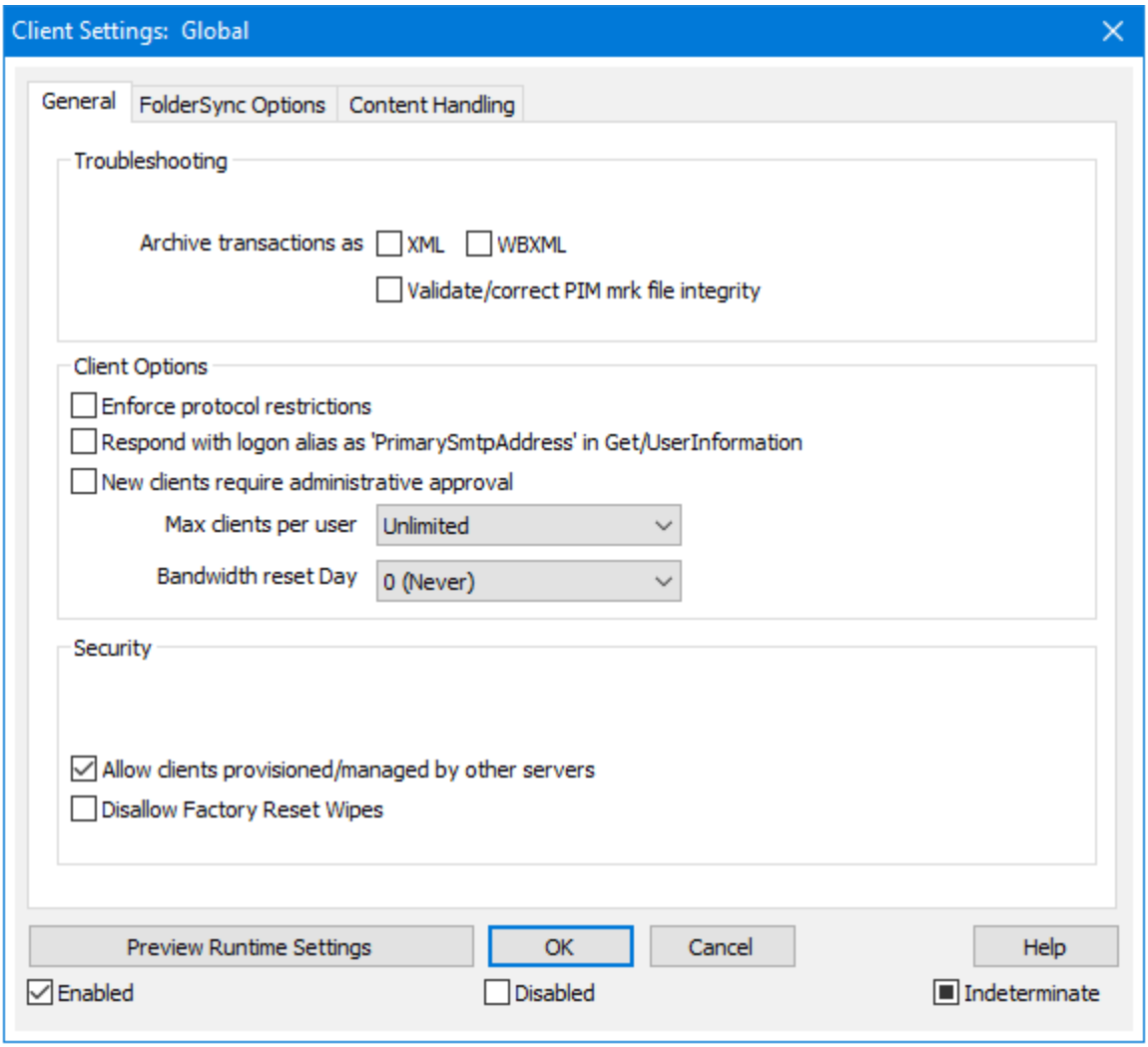
- [System] SendCorruptMessageNotifications=[Yes|No|1|0|True|False]（默认值是启用）
- [System] CMNCCUser==[0|1|Yes|No|True|False]（默认值是启用）

还请参阅：

ActiveSync » 诊断 361

3.10.2.1 客户端设置

“客户端设置”页面列出了已为 ActiveSync 配置的默认 ActiveSync 设置的配置文件。您可以为以下项创建和编辑客户端设置的配置文件：全局、域 170、群组 396、账户 380、客户端类型 402和客户端 388（例如设备）都位于其各自的对话框中。



此屏幕包含用来管理 ActiveSync 客户端的全局设置。ActiveSync 的其他页面下有对应的客户端设置，例如域 365、账户 380和客户端 388，用于按域、按账户和按客户端来分别设置这些选项。全局设置被设置成特定值，不过默认情况下将域、账户、客户端和其他设置成从其各自的父选项 *"继承"*其设置。因此更改此屏幕上的任何设置将有效更改所有子屏幕上相同的设置，允许您在默认情况下通过更改这一个屏幕上的设置来管理服务器上的所有客户端。反之亦然，更改子屏幕上的设置将覆盖其父设置，允许您在必要时以域、账户或其他r级别更改设置。

与策略 372 (将其分配到设备并规定设备可以执行的操作)类似，"客户端设置"规定服务器可以使用哪些相关客户端的选项执行操作，例如：规定一个账户可以使用多少单独的 ActiveSync 客户端、"公共文件夹"是否可以和账户的个人文件夹一起同步到设备、是否可以包含用户的已允许发件人文件夹等。

常规

故障诊断

日志级别

ActiveSync for MDaemon 支持 6 种日志级别，按所记录数据数量的多少分级，以下是从

高到低的级别一览：

调试 这是最丰富的日志级别。记录所有可用条目，而且通常只在诊断问题时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

Inherit 默认情况下，"日志级别"设置是从"客户端设置"层次结构继承的。因此，客户端从客户端类型继承，账户从客户端类型继承，群组从账户等继承其设置。此选项的"全局客户端设置"由故障诊断[361]对话框上的"日志级别"设置确定。

归档处理为 [XML | WBXML]
如果您希望保存此数据，请使用*"归档 XML..."*和*"WBXML"*选项，而且有时这些数据对调试很有帮助。默认情况下，禁用这些全局选项。

验证/修复 PIM mrk 文件完整性
该选项对客户端的 PIM 数据运行验证和修复进程来查询有碍正确同步的已知问题，例如重复的 iCalUID 或空的必填字段。默认情况下，禁用这个全局选项。

客户端选项

强制执行协议限制
如果有连接来自尝试使用指定的*"允许的协议版本"*以外的其他协议的客户端，您希望拒绝这些连接时请启用此项。默认情况下禁用此项，这就表示协议限制不防止客户端使用不同的协议：它们只是告诉客户端使用哪些协议。如果客户端无论如何都要尝试使用限制的协议，MDaemon 仍然允许这个连接。还请参阅：协议限制[363]来了解更多信息。

使用登录别名响应，作为 GetUserInformation 中的"PrimarySmtpAddress"
这允许该服务返回别名/次要地址作为主要地址来响应"设置/获取/用户信息"请求。这有助于解决 iOS9.x 更新所引起的一个问题：即导致客户端无法使用别名发送邮件。使用此项将导致对于"设置/获取/用户信息"不规范的响应。

新建客户端需要管理批准
如果您希望要求新的客户端必须先由管理员授权，才能开始与账户同步，请启用此选项。The 客户端[388]列表指示等候授权的任何客户端，管理员可以从相同的屏幕对其进行授权。默认情况下，禁用该设置。

每用户的客户端最大值
如果您希望限制 MDaemon 账户可以关联的 ActiveSync 客户端或设备的数量，请在此项中指定所需数量。默认情况下将这个全局选项设成"无限"。"全局"、"域"和"账户"客户端设置屏幕提供此项，但是个别客户端屏幕不提供此项。

带宽重置日期
如果您希望在每个月指定的一天为 ActiveSync 设备重置带宽使用统计，请使用此项。重置事件作为常规夜间维护过程的一部分进行，而且像其他维护例程一样被记录到系统日志中。默认情况下将这个全局选项设置成 "0"（从不），这就意味着从不重置使用统计。如果您希望重置的那一天与用户或客户端无线运营商计费的重置日期一致，请将子项设置成不同的一天。

安全

从"位置屏蔽"豁免
启用此项（位于 ActiveSync 客户端的设置屏幕）允许您将设备绕过位置屏蔽[477]。这使得有效的用户有可能通过 ActiveSync 继续访问他或她的账户，例如当前往一个阻止验证尝试的位置时。为了免除设备，它必须使用 ActiveSync 在配置的时间范围内进行连接和验证，请在位于"微调"屏幕的这些天后删除闲置的客户端[351]这个设置中进行配置。

动态允许远程地址
当从"位置屏蔽"豁免设备时，如果您还希望允许其连接的远程 IP 地址，请启用此选项。这对允许其他可能从相同 IP 地址连接的客户端很有用。

允许由其他服务器配置/管理的客户端
默认情况下，当 ActiveSync 服务器向特定客户端发送数据/策略，并报告它也受其他 ActiveSync 服务器管理时，也允许那个客户端连接到 MDaemon。不过在这种情况下，无法确保在与其他 ActiveSync 服务器的策略发生冲突时将应用您的策略。通常默认客户端在策略冲突时使用最具有限制性的选项。如果您不希望允许这些客户端进行连接，请禁用此项。

不允许出厂重置擦除
如果将其设置成启用/是，就不提供**完全擦除** ActiveSync 客户端的功能。如果您希望能够完全远程擦除客户端，您必须先禁用此项。默认情况下，禁用该选项。要了解更多详情，请参阅："客户端"页面上的完全擦除 ActiveSync 客户端[388]。

FolderSync 选项

FolderSync 选项

例外

已允许/已阻止发件人文件夹
默认情况下，无法和设备同步用户的"已允许发件人和已阻止发件人"联系人文件夹。它们通常只能由 MDaemon 用来吸住自动防止垃圾邮件。出于这个原因，它们无需在设备上显示为联系人。

非默认邮件文件夹
默认情况下能与设备同步所有由用户创建和默认的邮件文件夹。如果您仅希望允许同步默认的邮件文件夹（例如收件箱、已发送项目、已删除项目和草稿等），请启用此项。不会包含由用户创建的文件夹。默认情况下，禁用该选项。

非默认 PIM 文件夹
默认情况下，将与设备同步用户的所有 PIM 文件夹（例如联系人、日历、便笺和任务等）。如果您希望仅允许同步默认的 PIM 文件夹，请启用此项。例如，如果启用此项，

而且用户拥有多个日历文件夹，将仅同步默认的日历。默认情况下，禁用该选项。

包括

公告文件夹层次结构

如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的公共文件夹[258]，则勾选此框。默认启用此项。

允许屏蔽

允许客户端搜索它有权访问的公共文件夹[258]。默认情况下允许搜索操作。

公共文件夹遍历（显示文件夹名称）

默认情况下，为了让客户端同步/访问公共子文件夹，该账户必须拥有查询权限[260]，而且必须对子文件夹和所有父代公共文件夹[258]拥有该权限。如果该账户没有权限查看父文件夹，那么该账户也不能查看子文件夹，即使该账户有查看子文件夹的权限也是如此。如果您希望允许客户端访问这些子文件夹，请启用此项。**请注意：**启用此项必须向客户端显示父文件夹的名称，这会被视为安全风险。默认情况下，禁用该选项。

允许的公共文件夹数量最大值

如果您希望限制在设备上允许的“公共文件夹”的数量，请使用此项。在设置了限制时，该服务器遍历文件夹列表，直到达到这个限制为止，不会再将更多项目发送到设备。无法确保以何顺序处理这些文件夹。默认情况下未设置全局限制。

共享文件夹

如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的共享文件夹[97]，则勾选此框。默认启用此项。

允许屏蔽

允许客户端搜索它有权访问的共享文件夹[623]。默认情况下允许搜索操作。

内容处理

内容处理选项

在被客户端标记时为邮件项目创建任务/提醒

该选项可以在客户端请求时，使 MDaemon 通过为各个已标记的邮件创建任务项目来向用户提醒已标记的项目。。默认情况下，此控件的全局选项处于启用状态。

在事件被修改时始终发送会议更新

某些客户端在修改会议时未正确发送会议更新电子邮件。这指示 ActiveSync 服务在组织者更新会议项目时发送会议更新。这仅能在客户端[388]和无法恰当发送会议更新的客户端类型[402]上设置，否则将导致发送重复的会议更新。因此，此选项仅在“客户端”和“客户端类型”的设置页面上可用。

对所有已发送邮件请求已读回执

如果您希望服务器为客户端发送的所有邮件请求已读确认，请启用此项。默认情况下，禁用该选项。

当邮件被标记为已读时，以及发件人请求时，从服务器发送已读回执
如果您希望服务器支持已读确认请求，并在客户端将邮件标记为已读时发送已读回执，请启用此项。默认情况下，禁用该选项。

发送为在 ReplyTo 地址中指定的别名
某些客户端可能不允许发件人使用别名发送邮件。已在 Exchange ActiveSync (EAS) 协议 363 16.x 中添加该功能，不过一些客户端不支持 16.x。例如，Windows 版的 Outlook 仅使用 EAS 14.0，虽然它允许用户指定要发送的备用地址，但生成的邮件并不能正确反映用户的选择。该选项允许使用 ReplyTo (答复) 字段来发送电子邮件，只要 ReplyTo 地址是该用户的有效别名 699 即可。默认情况下启用这个全局选项。

虚拟地将公共联系人合并为默认联系人
如果您希望将设备上的公共联系人与用户的默认联系人合并在一起，请启用此项。这仅仅是一个虚拟合并，实际上未将它们复制到用户的联系人文件夹。这对不支持 "全局地址列表" (GAL) 搜索的客户端而言极其有用。默认情况下，禁用该选项。

在将邮件移入垃圾邮件文件夹时阻止发件人
启用后，当客户端将电子邮件移动到账户的垃圾邮件文件夹时，该服务将该电子邮件的发件人或从地址添加到阻止的发件人联系人文件夹。

在会议请求被接受/拒绝等时强制发送会议请求。
启用后，当客户端接受、拒绝或以其他方式选择响应会议请求的操作时，服务将向会议组织者发送会议响应。这是针对没有正确发送这些更新本身的特定客户端。

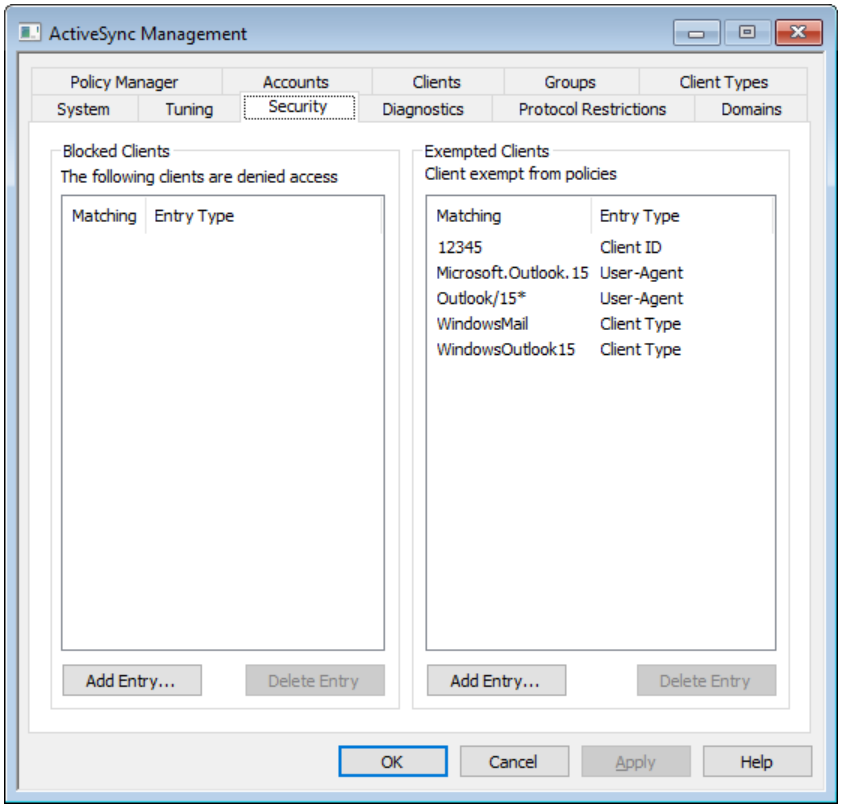
预览有效设置

该按钮在所有子 "客户端设置" 屏幕上可用 (例如域 365、账户 380 和客户端 388)。由于默认情况下，已将这些屏幕上的选项都设置成从父屏幕继承其设置，使用该功能来查看当前向显示的屏幕应用了什么设置。

还请参阅：

ActiveSync » 域 365
ActiveSync » 账户 380
ActiveSync » 客户端 388

3.10.3 安全

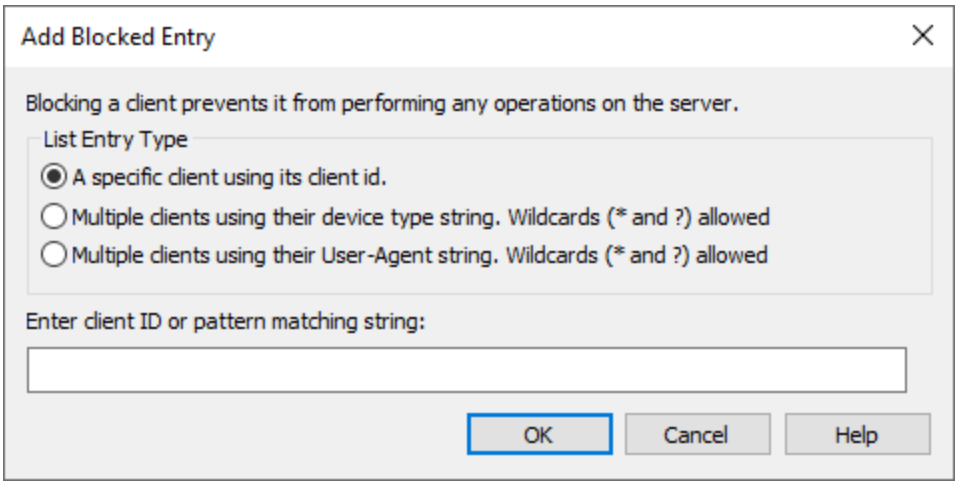


已阻止客户端

使用此项来防止特定的设备类型、客户端 ID、或用户代理访问 MDaemon 的 ActiveSync 服务器。

添加已阻止条目

要向此列表添加一个条目，请点击**添加条目**，指定设备信息并点击**确定**。如果该设备已连接到 MDaemon 的 ActiveSync 服务器，您可以从设备自身或 ActiveSync 日志文件获取设备信息。



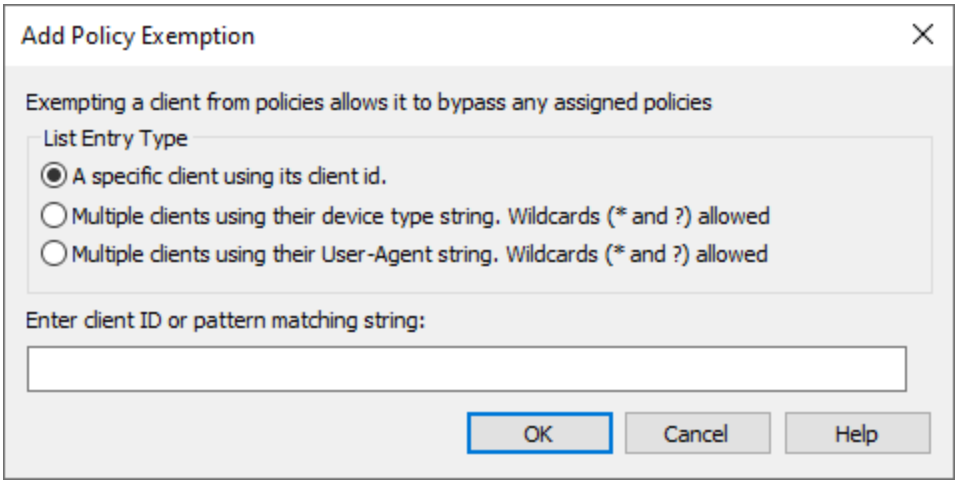
您可以从客户端[388]对话框轻松地阻止一个设备。右键点击列表中的一个客户端，然后点击 **阻止该客户端**”。

删除已阻止条目
要删除条目，请从此列表中选定一个或多个条目，并点击 **删除条目**”。在删除这些条目前将询问您是否确定要执行该操作。

已豁免客户端

使用此项来使特定的设备类型、客户端 ID、或用户代理免于策略[372]限制。

添加已豁免客户端
要向此列表添加一个条目，请点击**添加条目**，指定设备信息并点击**确定**。如果该设备已连接到 MDaemon 的 ActiveSync 服务器，您可以从设备自身或 ActiveSync 日志文件获取设备信息。



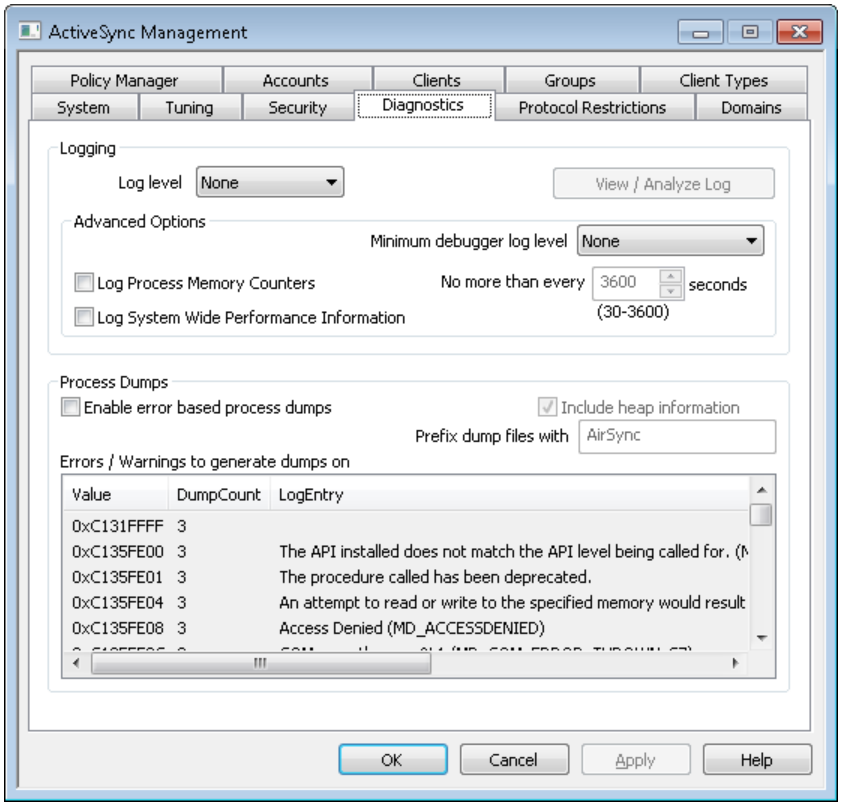
您可以从客户端[388]对话框轻松地豁免一个设备。右键点击列表中的一个客户端，然后点击 **从策略豁免该客户端**”。

删除已豁免条目
要删除条目，请从此列表中选定一个或多个条目，并点击 **删除条目**”。在删除这些条目前将询问您是否确定要执行该操作。

还请参阅：

ActiveSync » 客户端[388]

3.10.4 故障诊断



该屏幕包含高级选项，在大多数情况下，除非您尝试诊断问题或寻求技术支持，否则不需要使用这些选项。

日志记录和归档

这一部分包含 ActiveSync 的全局 "日志级别"设置。如果将动态客户端设置[178]中的 "日志级别"设置成 "使用继承或默认值"，则将从此处来继承该设置。

日志级别

支持 6 种日志级别，将按记录的数据量由高到低进行说明：

调试 这是最丰富的日志级别。记录所有可用条目，通常仅在诊断问题或管理员需要详细信息时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

查看/分析日志文件
点击此按钮来打开 MDaemon 高级系统日志查看器。默认情况下，将日志保存在："..\MDaemon\Logs\"

高级选项

最小化调试器日志级别
这是发送至调试器的日志最小级别。可用的日志级别与上述相同。

记录进程内存计数器
选中此框可将特定于进程的内存、句柄和线程信息记录到日志文件中。这对于发现潜在的故障和资源分配问题很有用。仅当数据自上次记录以来发生变更时，才会发出日志条目。

记录系统范围的性能信息
如果您希望将系统范围的性能信息记录到日志文件中，请选中此框。这对于发现潜在的故障和资源分配问题很有用。仅当数据自上次记录以来发生变更时，才会发出日志条目。

不大于每隔 [xx]秒
使用此选项可以设置对于进程和性能信息的记录频率的限制。

进程转储

启用基于进程转储的错误
如果您希望在发生您于下方指定的特定警告或错误时生成进程转储，请启用此项。

在转储中包含堆信息
默认情况下，在进程转储中包含堆信息。如果您不希望包含这个信息，请清除该复选框。

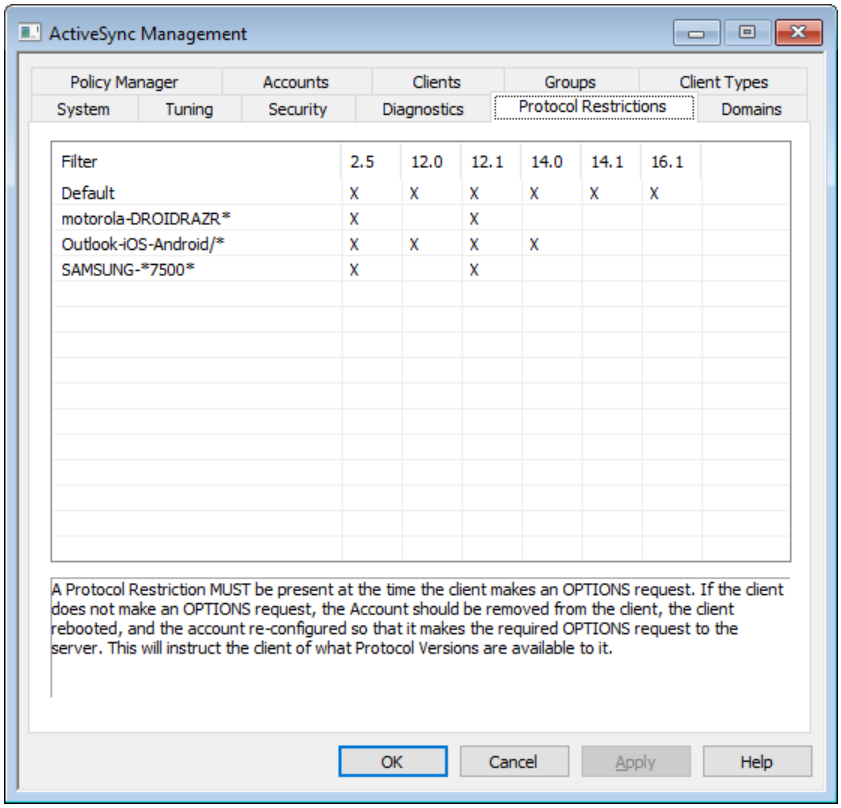
为转储文件使用前缀
进程转储文件名将使用这个文本开头。

出错/警告时生成转储
右键单击此区域并使用 *"添加/编辑/删除条目..."* 选项来管理将触发进程转储的错误或警告列表。对于每个条目，您可以指定取消激活前进程转储数量。

还请参阅：

ActiveSync » 微调 351

3.10.5 协议限制



设备协议限制

使用位于“ActiveSync » 协议限制”下的选项来告知某些客户端和设备，它们受限于特定的 ActiveSync 协议。在发现某个类型的设备不能十分可靠地支持一种协议但能出色支持其他协议时，这很有用。使用“添加/编辑协议限制”[364]对话框，您可以基于用户代理程序或设备类型来定义限制，并将设备限制到以下任何一个 ActiveSync 协议版本：2.5, 12.0, 12.1, 14.0, 14.1 和 16.1。

默认情况下，协议限制不防止客户端尝试使用不同的协议，它们告诉客户端使用哪些协议。如果客户端无论如何都要尝试使用限制的协议，MDaemon 仍然允许这个连接。如果您希望拒绝尝试使用受限协议的协议，请使用“*强制协议限制*”选项，位于客户端设置[353]对话框上。

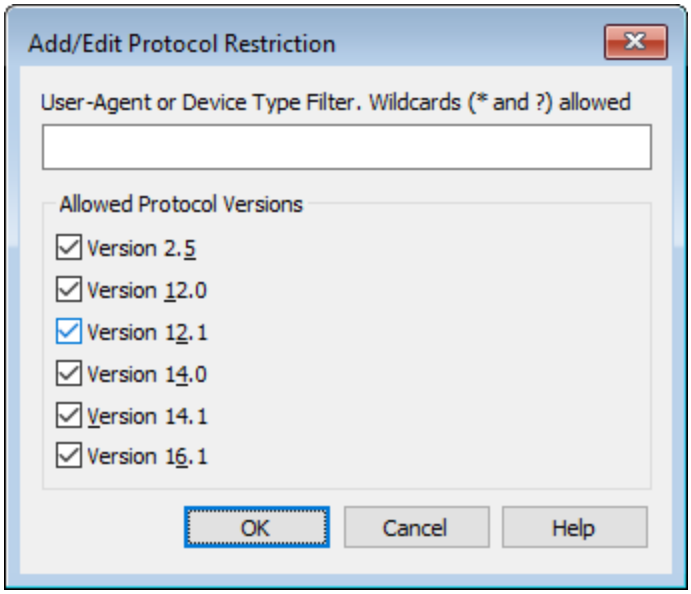
右键点击该列表中的条目来打开一个含有以下选项的菜单：

创建协议限制
点击此选项来打开“添加/编辑协议限制”[364]对话框（见下方），用于添加您的协议限制。

编辑协议限制
要编辑一个协议限制，请从列表中双击一个条目（或右键单击该条目并选择“**编辑协议限制**”）。在限制编辑器中完成了所需更改后，请点击“**确定**”。

删除协议限制
要删除一个协议限制，请从列表中双击一个条目（或右键单击该条目并选择 **删除协议限制**”）。点击 **是**”来确认您准备删除此限制的决定。

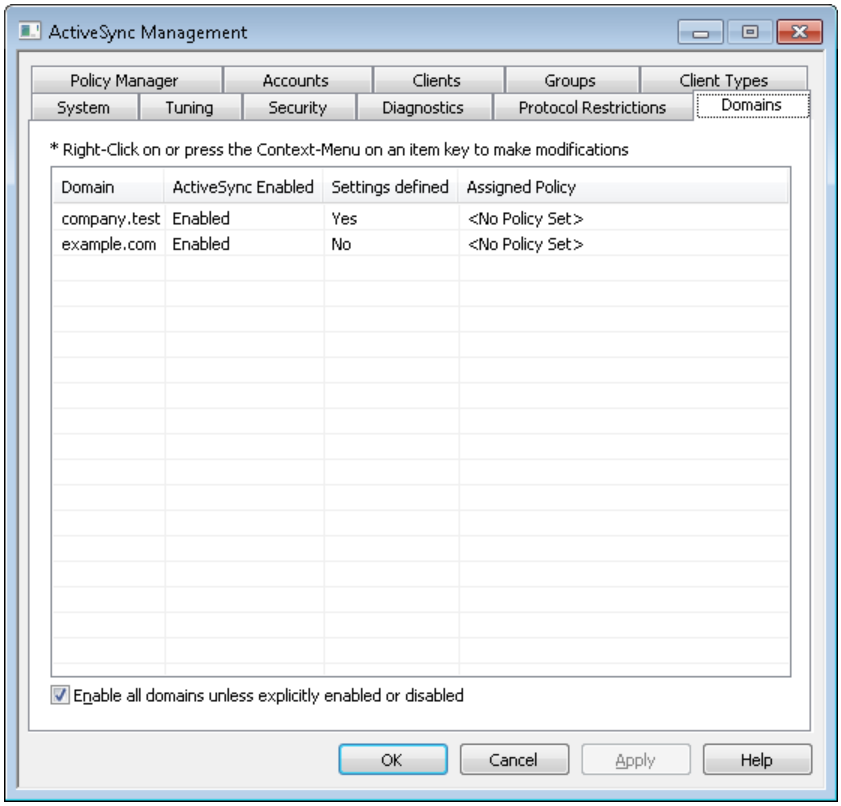
添加/编辑协议限制



用户代理程序或设备类型过滤器
输入将应用限制的 **用户代理程序**”或 **设备类型**”。在识别代理程序时，MDaemon 使用多达并包括字符串中第一个 **/**”字符（若存在）。若不存在则使用整个字符串。如果您不知道 **用户代理程序**”或 **设备类型**”的具体名称，一旦客户端连接到 MDaemon ActiveSync (MDAS)，您可以前往客户端 388 屏幕，选择列表中的客户端并点击 **详细信息**”。您也可以通过直接检查 MDAS 日志文件来查找这个信息。

允许的协议版本
点击您希望设备或代理程序支持的各个协议。当指定的客户端连接到 MDaemon，就会告诉此客户端仅使用您选定的协议。

3.10.6 域



使用此屏幕来为您的域[149]管理 ActiveSync 设置。您可以为每个域启用或禁用 ActiveSync，分配默认的 "ActiveSync 策略[372]"，管理默认的客户端设置，并管理与此域相关联的设备。

为特定域启用/禁用 ActiveSync

要为特定的域设置 ActiveSync 状态：

1. 右键单击此列表中的一个域。
2. 点击 **启用**"、"**禁用**"或 **默认**"。如果您选择 *"默认"*，则 *"启用所有域，除非明确启用或禁用"*下的选项将确定该域的 ActiveSync 是否处于活动状态。

要使用 ActiveSync，您需要在该用户设备上正确配置 ActiveSync 客户端。要获得操作指示，请参阅*购买、升级或审核 ActiveSync for MDaemon* 链接，位于 ActiveSync for MDaemon[349] 屏幕并滚动至设备设置指示。

设置默认的 ActiveSync 状态

在将其 *"已启用 ActiveSync"*列设置成 **启用/禁用（默认）**"的域将从以下选项的状态获取其 ActiveSync 设置：**启用所有域，除非明确启用或禁用**。启用此项时，默认情况下所有域将启用 ActiveSync。禁用此项时，默认情况下将禁用 ActiveSync。将一个域专门设置成 **启用**"或 **禁用**"将覆盖默认设置。

如果您将一个域的“*已启用 ActiveSync*”设置更改成“**禁用**”，将打开一个确认框，询问您是否希望为该域的所有用户撤销 ActiveSync 访问权限。如果您希望允许当前使用 ActiveSync 的任何域用户继续使用它，请选择“**否**”。如果您选择“**是**”，将为该域的所有用户禁用 ActiveSync。

更改域的客户端设置

右键单击一个域来管理其“客户端设置”。默认情况下这些设置将从“全局客户端设置 353”屏幕继承。还请参阅下方的管理域的客户端设置 366。

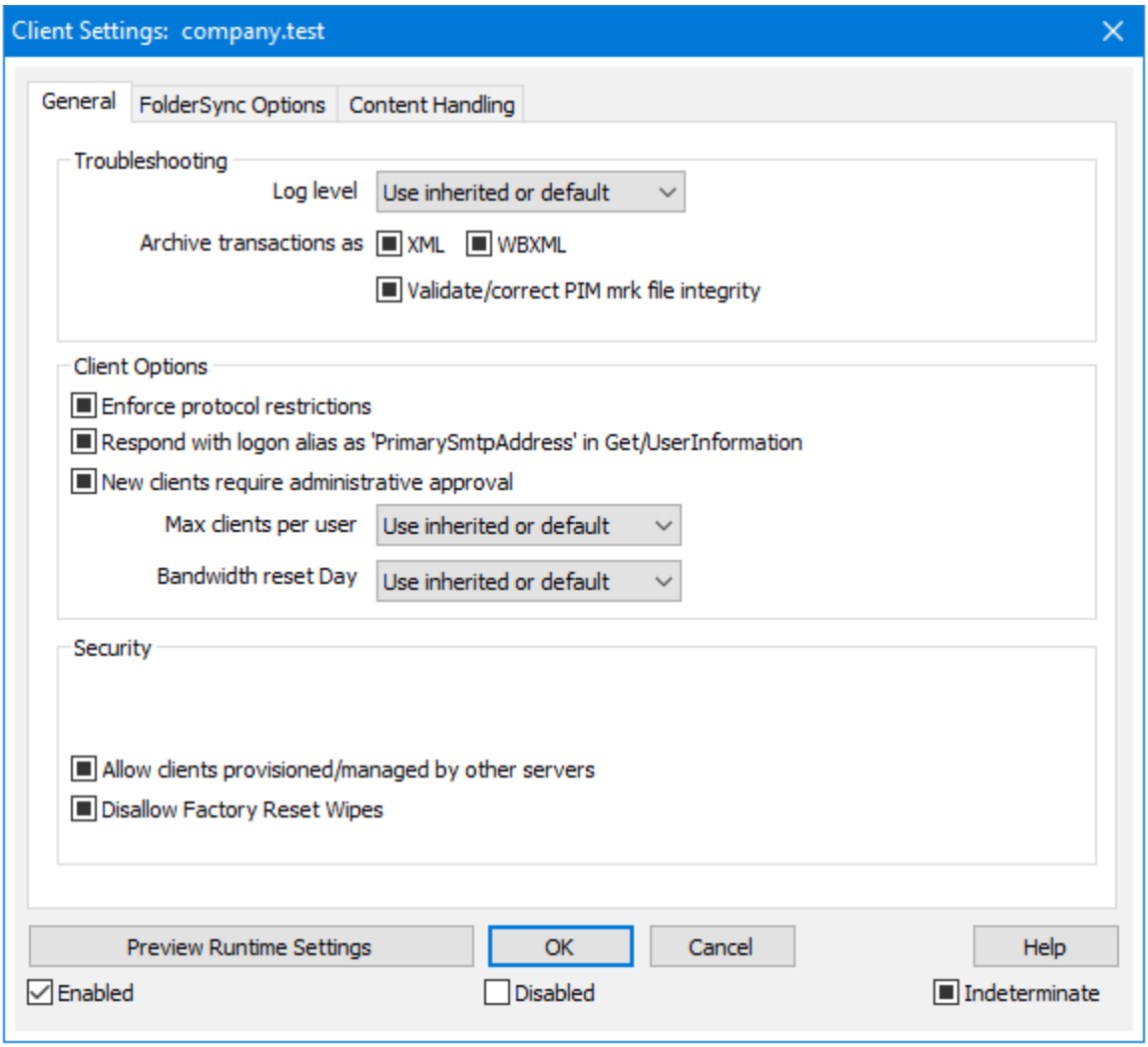
分配默认的 ActiveSync 策略

要将默认的 ActiveSync 策略分配给一个域：

1. 右键单击此列表中的一个域。
2. 点击“**分配策略**”。
3. 在“要分配的策略”下，从下拉列表中选择所需的策略（要管理可用策略，请参阅策略管理器 372）。
4. 点击“**确定**”。

管理域的客户端设置

此域的“客户端设置”屏幕允许您为与此域相关联的账户和客户端管理默认设置。



默认情况下，此屏幕上的所有选项都被设置为 "使用继承或默认值"，表示每个选项都会从全局客户端设置[353]屏幕上的相应选项中获取其设置。类似的，此域 "账户[380]"的客户端设置屏幕将继承此屏幕的设置，因为此域的 "客户端设置"屏幕是其父屏幕。在此屏幕上对这些选项做出的任何变更都将在屏幕上反映。在此下方，"客户类型"具有设置屏幕，可从账户级别的设置继承其设置，个别客户端[388]也拥有其自身的设置。该配置帮助您通过对这一个屏幕做出变更来对一个域的所有账户做出变更，还帮助您按需求为任何账户或客户端覆盖这些设置。

常规

故障诊断

日志级别

ActiveSync for MDaemon 支持 6 种日志级别，按所记录数据数量的多少分级，以下是从高到低的级别一览：

调试 这是最丰富的日志级别。记录所有可用条目，而且通常只在诊断问题

时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

Inherit 默认情况下，"日志级别"设置是从"客户端设置"层次结构继承的。因此，客户端从客户端类型继承，账户从客户端类型继承，群组从账户等继承其设置。此选项的"全局客户端设置"由故障诊断[361]对话框上的"日志级别"设置确定。

归档处理为 [XML | WBXML]
如果您希望保存此数据，请使用*"归档 XML..."*和*"WBXML"*选项，而且有时这些数据对调试很有帮助。默认情况下，禁用这些全局选项。

验证/修复 PIM mrk 文件完整性
该选项对客户端的 PIM 数据运行验证和修复进程来查询有碍正确同步的已知问题，例如重复的 iCalUID 或空的必填字段。默认情况下，禁用这个全局选项。

客户端选项

强制执行协议限制
如果有连接来自尝试使用指定的*"允许的协议版本"*以外的其他协议的客户端，您希望拒绝这些连接时请启用此项。默认情况下禁用此项，这就表示协议限制不防止客户端使用不同的协议：它们只是告诉客户端使用哪些协议。如果客户端无论如何都要尝试使用限制的协议，MDaemon 仍然允许这个连接。还请参阅：协议限制[363]来了解更多信息。

使用登录别名响应，作为 GetUserInformation 中的 "PrimarySmtpAddress"
这允许该服务返回别名/次要地址作为主要地址来响应"设置/获取/用户信息"请求。这有助于解决 iOS9.x 更新所引起的一个问题：即导致客户端无法使用别名发送邮件。使用此项将导致对于"设置/获取/用户信息"不规范的响应。

新建客户端需要管理批准
如果您希望要求新的客户端必须先由管理员授权，才能开始与账户同步，请启用此选项。The 客户端[388]列表指示等候授权的任何客户端，管理员可以从相同的屏幕对其进行授权。默认情况下，禁用该设置。

每用户的客户端最大值
如果您希望限制 MDaemon 账户可以关联的 ActiveSync 客户端或设备的数量，请在此项中指定所需数量。默认情况下将这个全局选项设成"无限"。"全局"、"域"和"账户"客户端设置屏幕提供此项，但是个别客户端屏幕不提供此项。

带宽重置日期
如果您希望在每个月指定的一天为 ActiveSync 设备重置带宽使用统计，请使用此项。

重置事件作为常规夜间维护过程的一部分进行，而且像其他维护例程一样被记录到系统日志中。默认情况下将这个全局选项设置成 "0"（从不），这就意味着从不重置使用统计。如果您希望重置的那一天与用户或客户端无线运营商计费的重置日期一致，请将子项设置成不同的一天。

安全

从"位置屏蔽"豁免

启用此项（位于 ActiveSync 客户端的设置屏幕）允许您将设备绕过位置屏蔽 477。这使得有效的用户有可能通过 ActiveSync 继续访问他或她的账户，例如当前往一个阻止验证尝试的位置时。为了免除设备，它必须使用 ActiveSync 在配置的时间范围内进行连接和验证，请在位于"微调"屏幕的这些天后删除闲置的客户端 351 这个设置中进行配置。

动态允许远程地址

当从"位置屏蔽"豁免设备时，如果您还希望允许其连接的远程 IP 地址，请启用此选项。这对允许其他可能从相同 IP 地址连接的客户端很有用。

允许由其他服务器配置/管理的客户端

默认情况下，当 ActiveSync 服务器向特定客户端发送数据/策略，并报告它也受其他 ActiveSync 服务器管理时，也允许那个客户端连接到 MDaemon。不过在这种情况下，无法确保在与其他 ActiveSync 服务器的策略发生冲突时将应用您的策略。通常默认客户端在策略冲突时使用最具有限制性的选项。如果您不希望允许这些客户端进行连接，请禁用此项。

不允许出厂重置擦除

如果将其设置成启用/是，就不提供**完全擦除** ActiveSync 客户端的功能。如果您希望能够完全远程擦除客户端，您必须先禁用此项。默认情况下，禁用该选项。要了解更多详情，请参阅："客户端"页面上的完全擦除 ActiveSync 客户端 388。

FolderSync 选项

FolderSync 选项

例外

已允许/已阻止发件人文件夹

默认情况下，无法和设备同步用户的"已允许发件人和已阻止发件人"联系人文件夹。它们通常只能由 MDaemon 用来吸住自动防止垃圾邮件。出于这个原因，它们无需在设备上显示为联系人。

非默认邮件文件夹

默认情况下能与设备同步所有由用户创建和默认的邮件文件夹。如果您仅希望允许同步默认的邮件文件夹（例如收件箱、已发送项目、已删除项目和草稿等），请启用此项。不会包含由用户创建的文件夹。默认情况下，禁用该选项。

非默认 PIM 文件夹

默认情况下，将与设备同步用户的所有 PIM 文件夹（例如联系人、日历、便笺和任务等）。如果您希望仅允许同步默认的 PIM 文件夹，请启用此项。例如，如果启用此项，而且用户拥有多个日历文件夹，将仅同步默认的日历。默认情况下，禁用该选项。

包括

公告文件夹层次结构
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的公共文件夹[258]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的公共文件夹[258]。默认情况下允许搜索操作。

公共文件夹遍历（显示文件夹名称）
默认情况下，为了让客户端同步/访问公共子文件夹，该账户必须拥有查询权限[260]，而且必须对子文件夹和所有父代公共文件夹[258]拥有该权限。如果该账户没有权限查看父文件夹，那么该账户也不能查看子文件夹，即使该账户有查看子文件夹的权限也是如此。如果您希望允许客户端访问这些子文件夹，请启用此项。**请注意：**启用此项必须向客户端显示父文件夹的名称，这会被视为安全风险。默认情况下，禁用该选项。

允许的公共文件夹数量最大值
如果您希望限制在设备上允许的“公共文件夹”的数量，请使用此项。在设置了限制时，该服务器遍历文件夹列表，直到达到这个限制为止，不会再将更多项目发送到设备。无法确保以何顺序处理这些文件夹。默认情况下未设置全局限制。

共享文件夹
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的共享文件夹[97]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的共享文件夹[623]。默认情况下允许搜索操作。

内容处理

内容处理选项

在被客户端标记时为邮件项目创建任务/提醒
该选项可以在客户端请求时，使 MDaemon 通过为各个已标记的邮件创建任务项目来向用户提醒已标记的项目。。默认情况下，此控件的全局选项处于启用状态。

在事件被修改时始终发送会议更新
某些客户端在修改会议时未正确发送会议更新电子邮件。这指示 ActiveSync 服务在组织者更新会议项目时发送会议更新。这仅能在客户端[388]和无法恰当发送会议更新的客户端类型[402]上设置，否则将导致发送重复的会议更新。因此，此选项仅在“客户端”和“客户端类型”的设置页面上可用。

对所有已发送邮件请求已读回执
如果您希望服务器为客户端发送的所有邮件请求已读确认，请启用此项。默认情况下，禁用该选项。

当邮件被标记为已读时，以及发件人请求时，从服务器发送已读回执
如果您希望服务器支持已读确认请求，并在客户端将邮件标记为已读时发送已读回执，请启用此项。默认情况下，禁用该选项。

发送为在 ReplyTo 地址中指定的别名
某些客户端可能不允许发件人使用别名发送邮件。已在 Exchange ActiveSync (EAS) 协议[363] 16.x 中添加该功能，不过一些客户端不支持 16.x。例如，Windows 版的 Outlook 仅使用 EAS 14.0，虽然它允许用户指定要发送的备用地址，但生成的邮件并不能正确反映用户的选择。该选项允许使用 ReplyTo（答复）字段来发送电子邮件，只要 ReplyTo 地址是该用户的有效别名[699]即可。默认情况下启用这个全局选项。

虚拟地将公共联系人合并为默认联系人
如果您希望将设备上的公共联系人与用户的默认联系人合并在一起，请启用此项。这仅仅是一个虚拟合并，实际上未将它们复制到用户的联系人文件夹。这对不支持“全局地址列表”(GAL)搜索的客户端而言极其有用。默认情况下，禁用该选项。

在将邮件移入垃圾邮件文件夹时阻止发件人
启用后，当客户端将电子邮件移动到账户的垃圾邮件文件夹时，该服务将该电子邮件的发件人或从地址添加到阻止的发件人联系人文件夹。

在会议请求被接受/拒绝等时强制发送会议请求。
启用后，当客户端接受、拒绝或以其他方式选择响应会议请求的操作时，服务将向会议组织者发送会议响应。这是针对没有正确发送这些更新本身的特定客户端。

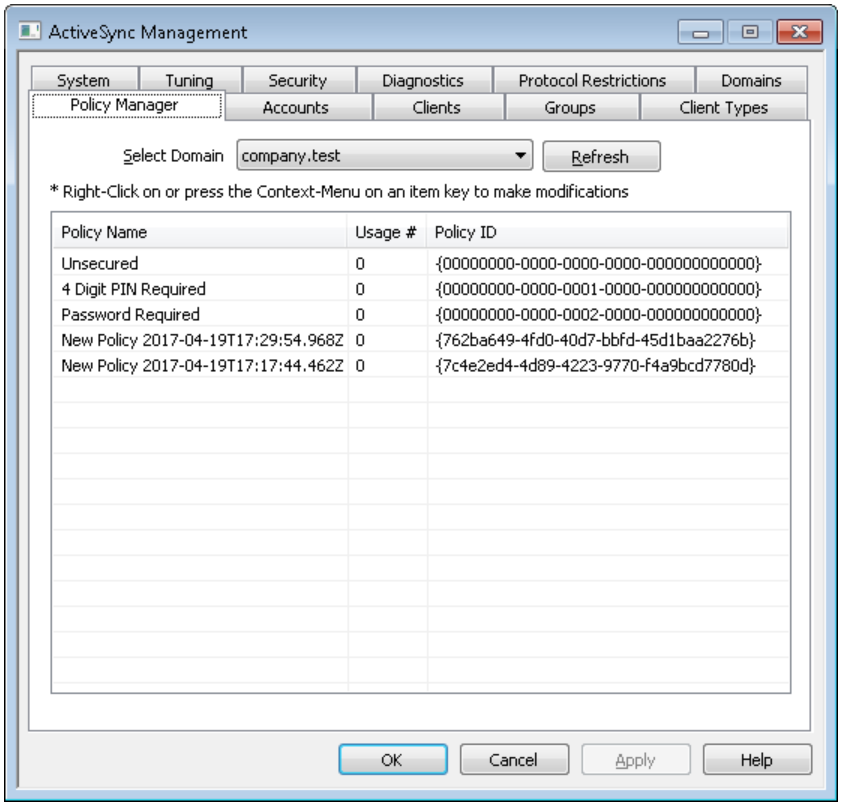
预览有效设置

该按钮在所有子“客户端设置”屏幕上可用（例如域[365]、账户[380]和客户端[388]）。由于默认情况下，已将这些屏幕上的选项都设置成从父屏幕继承其设置，使用该功能来查看当前向显示的屏幕应用了什么设置。

还请参阅：

域管理器 » ActiveSync 客户端设置[178]
域管理器 | ActiveSync 客户端[199]
ActiveSync » 策略管理器[372]

3.10.7 策略管理器



使用此屏幕来管理 "ActiveSync 策略"，可以将这些策略分配给用户设备来管理各种选项。既提供预定义策略，您也可以创建、编辑和删除您自己的策略。可以按域[365]和按账户[380]分配默认的策略，也可以将这些策略分配至特定的客户端[199]。

> 并非所有的 ActiveSync 设备都识别这些策略或按设置应用策略。有些设备可能忽略这些策略或一些策略元素，有些设备可能必须在重启后才能使策略设置生效。此外，在尝试将新策略分配到一个设备时，只有在该设备自身下一次连接到 ActiveSync 服务器时才会应用这个策略；而且只有在建立连接时才能将这些策略 "推送"到设备。

ActiveSync 策略

右键单击列表以打开快捷菜单，其中包含以下选项：

创建策略
点击此选项打开 ActiveSync 策略编辑器来创建和编辑您的策略。

删除
要删除策略，请从列表中选择一个自定义策略并点击 "**删除**"。点击 "**是**"来确认这个操作。预定义策略是无法删除的。

编辑策略
要编辑策略，请从列表中右键单击一个自定义策略并点击 "**编辑策略**"。在策略编辑器中

完成了所需更改后，请点击 **确定**”。预定义策略是无法进行编辑的。

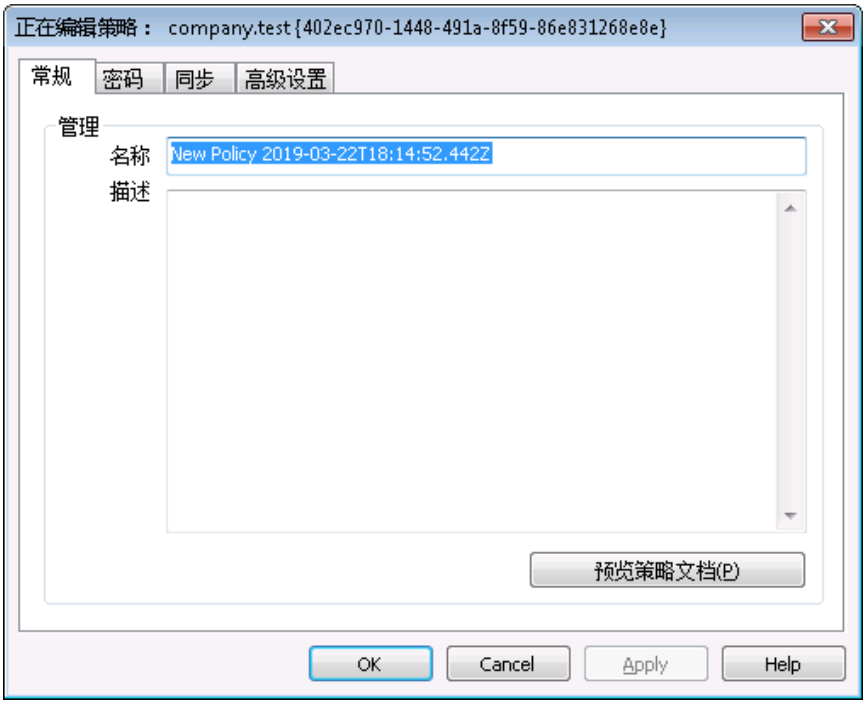
查看策略使用情况
右键单击策略，然后选择此选项来查看被设置成使用此策略的所有域、账户和客户端的列表。

ActiveSync 策略编辑器

ActiveSync 策略编辑器拥有四个选项卡：常规、密码、同步和高级设置。除非您激活了“*启用高级策略选项编辑*349”(位于 ActiveSync 系统屏幕)，否则将隐藏 高级设置”选项卡。

常规

使用这个屏幕来指定您策略的名称和描述。您也可以预览 XML 策略文档。



管理

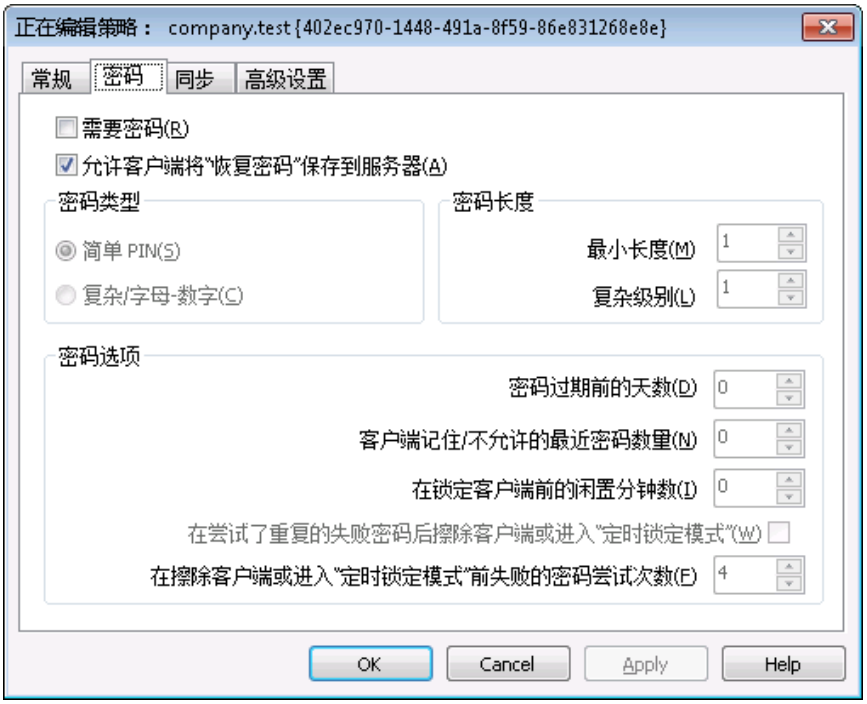
名称
请在此处为您的自定义策略指定一个名称。

描述
使用此区域来描述您的自定义策略。在选择要应用至域、账户或客户端的策略时，在“应用策略”对话框上显示的描述。

预览策略文档
点击此按钮来预览这个策略的 XML 策略文档。

密码

在这个选项卡上指定密码选项和策略要求。



需要密码
如果您希望在设备上需要密码，请勾选此框。默认情况下，禁用该选项。

允许设备将"恢复密码"保存到服务器
如果您希望允许客户端使用 ActiveSync 的"恢复密码"选项，这将允许设备将临时恢复密码保存到服务器，以便在忘记密码时解锁设备，请启用此项。管理员可以在客户端的"详细信息 388"下找到这个恢复密码。大多数设备不支持此功能。

密码类型

简单 PIN
此项如何实施在很大程度上取决于设备，不过将*"Simple PIN"*选为密码类型通常意味着对设备密码不施加任何限制或复杂要求，不像下方的*"密码长度最小值"*选项。这允许如下所示的简单密码："111"、"aaa"、"1234"、"ABCD"等。

复杂/字母-数字
如果您需要比*"简单 PIN"*选项更复杂更安全的设备密码，请使用这个策略选项。使用下方的*"复杂级别"*选项来定义这个密码必须拥有的复杂性。在策略请求密码时，这是默认选项。

密码强度

最小长度
使用此项来设置设备密码必须包含的字符数最小值，从 1-16。默认情况下将此项设置成"1"。

复杂级别
使用此项来为 *"复杂/字母-数字"*设备密码设置复杂级别要求。这个级别是密码必须包含的字符的不同类型数量：大写字母、小写字母、数字、非字母数字字符 (例如句号或特殊字符)。您可以要求 1-4 种字符类型。例如，如果将此项设置成 "2"，那么这个密码必须包含至少以下四种字符类型的两种：大写字母和数字、大写字母和小写字母、数字和符号等。默认情况下将此项设置成 "1"。

密码选项

密码过期前的天数 (0=从不)
这是在必须更改设备密码前允许的天数。默认情况下，禁用该选项 (设置成 "0")。

设备记住/不允许的最近密码数 (0=无)
如果您希望防止设备重复使用指定数量的旧密码，请使用此项。例如，如果将此项设置成 "2"而且您更改了您的设备密码，那么您无法将密码更改成上两个已使用过的密码。默认情况下，禁用该选项 (设置成 "0")。

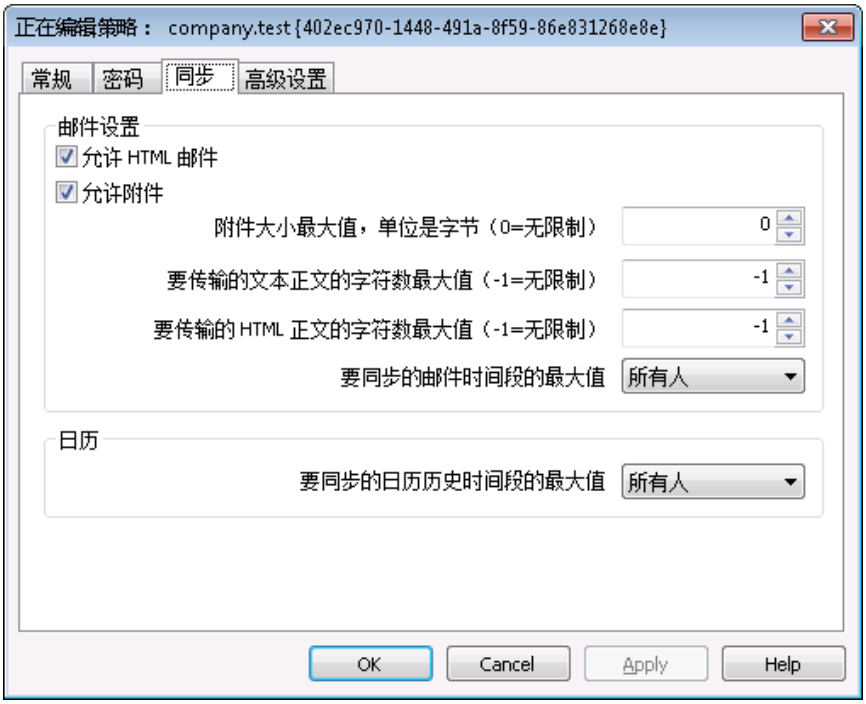
设备锁定之前闲置的分钟数 (0=从不)
这是设备在自我锁定前无需任何用户输入仍然能够正常运行的分钟数。默认情况下，禁用这个密码选项 (设置成 "0")。

反复尝试失败的密码后，擦除设备或进入 "定时锁定模式"
启用此项时，当用户达到指定次数的失败密码尝试后，设备将按照设置自我锁定一段时间或擦除所有数据。默认情况下，禁用该选项。

设备擦除或进入 "定时锁定模式"前失败的密码尝试次数
在启用上方的 *"擦除设备.."*选项，而且用户达到了指定的失败密码尝试次数时，该设备将按照设置进行擦除或进入 "定时锁定模式"。

同步

该屏幕含有各种设置，包括管理 HTML 邮件、允许附件、限制要传输的字符数、待同步的邮件数最大值和日历框架。



邮件设置

允许 HTML 邮件

默认情况下，可以向 ActiveSync 客户端同步/发送 HTML 格式的电子邮件。如果您希望仅发送纯文本，请取消勾选此框。

允许附件

允许设备下载文件附件。默认情况下启用此项。

附件大小最大值，单位是字节（0=无限制）

这是将自动下载到设备的附件的最大大小。默认情况下未为此项设置任何大小限制（设置成“0”）。

待传输的文本正文字符数最大值（-1=无限制）

这是将发送至客户端的纯文本格式正文中字符数的最大值。如果邮件正文包含的字符数大于允许的值，会将正文截短到指定限制。默认情况下没有限制设置（将此项设置成“-1”）。如果您将此项设置成“0”，将仅发送邮件报头。

待传输的 HTML 正文字符数最大值（-1=无限制）

这是将发送至客户端的 HTML 格式正文中字符数的最大值。如果邮件正文包含的字符数大于允许的值，会将正文截短到指定限制。默认情况下没有限制设置（将此项设置成“-1”）。如果您将此项设置成“0”，将仅发送邮件报头。

待同步的邮件时间框架的最大值

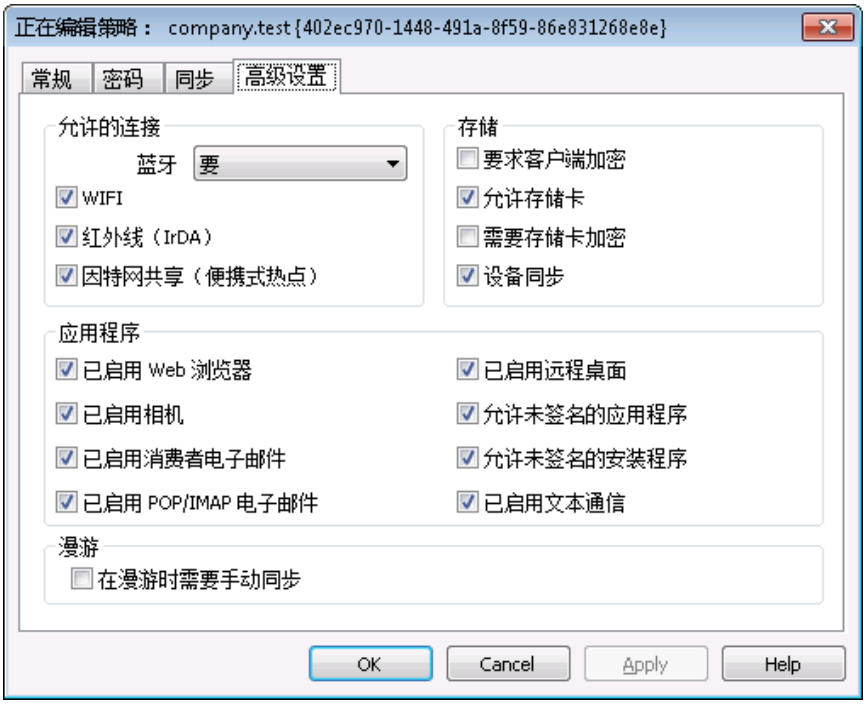
这是可以被设备同步的从今天开始到之后一段日期范围内的以往电子邮件的数量。默认情况下将此项设置成“所有”，这就意味着无论邮件的存在时间有多久，将会同步所有邮件。

日历

待同步的日志历史时间框架的最大值
这是从今天起此设备可以同步过去多久之前的日历条目。默认情况下将此项设置成 "所有"，这就意味着无论这些条目的存在时间有多久，都会同步所有过去的条目。

高级设置

"高级设置"选项卡包含各种选项管理，包括允许的连接类型、是否能够启用特定的应用程序、存储、加密和漫游。



除非您激活了 "*启用高级策略选项编辑*[349]" (位于 ActiveSync for MDaemon屏幕)，否则将隐藏 "高级设置"选项卡。

允许的连接

蓝牙
使用此项来指定是否在设备上允许蓝牙连接。您可以选择 "是"来允许 "蓝牙"连接，选择 "否"来进行阻止，或选择 "免提"将 "蓝牙"限制成仅在免提时使用。默认情况下将此项设置成 "是"。

WIFI
允许 WIFI连接。默认情况下启用此项。

红外线 (IrDA)
允许红外线 (IrDA)连接。默认情况下启用此项。

互联网共享（移动热点）
此项允许设备使用互联网共享（移动热点）。默认情况下，启用该选项。

存储

需要设备加密
如果您希望在设备上需要加密，请点击此项。并非所有设备要强制加密。默认情况下，禁用该选项。

允许存储卡
允许在设备中使用存储卡。默认启用此项。

需要存储卡加密
如果您希望在存储卡上需要加密，请使用此项。默认情况下，禁用该选项。

桌面同步
在设备上允许桌面同步。默认情况下启用此项。

应用程序

启用 web 浏览器
允许在设备上使用浏览器。某些设备不支持此项，而且无法应用到第三方浏览器。默认情况下，启用该选项。

启用相机
允许在设备上使用相机。默认情况下启用此项。

启用消费者电子邮件
设备允许用户配置个人邮件账户。禁用时，将取决于特定的 ActiveSync 客户端完全禁用邮件账户或服务类型。默认情况下启用此项。

启用 POP/IMAP 邮件
允许访问 POP 或 IMAP 电子邮件。默认情况下启用此项。

启用远程桌面
允许客户端使用远程桌面。默认情况下启用此项。

允许未签名的应用程序
此项允许在设备上使用未签名的应用程序。默认启用此项。

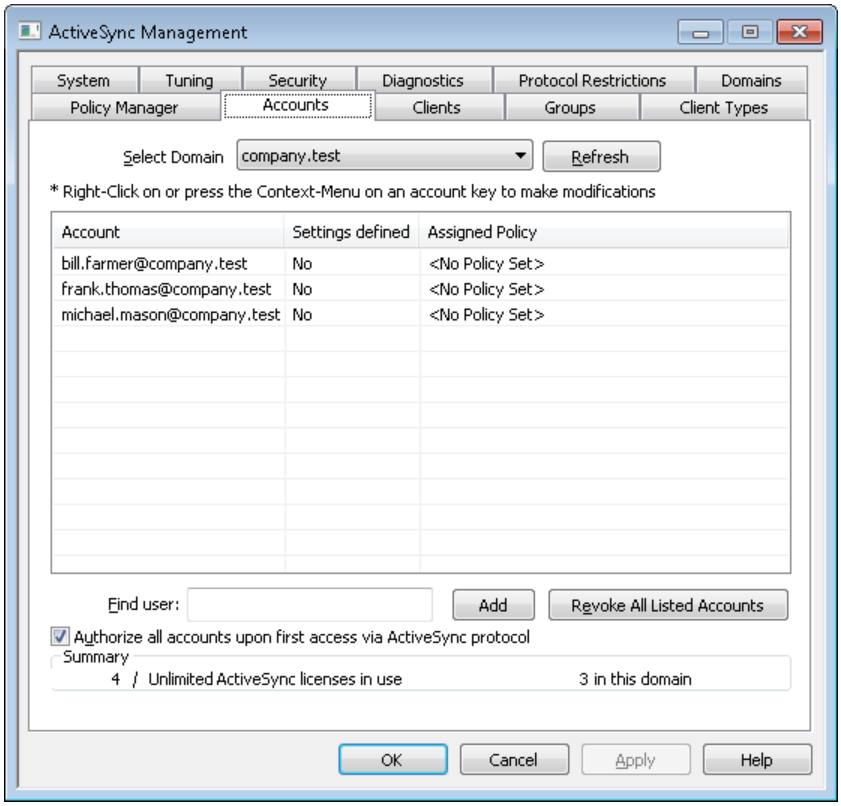
允许未签名的安装程序
此项允许在设备上运行未签名的安装程序。默认启用此项。

启用文本消息
此项允许在设备上进行文本通信。默认情况下启用文本通信。

漫游

漫游时需要手动同步
如果您希望在设备漫游时对其进行手动同步，请使用这个策略选项。取决于设备运营商和数据规划项目，允许在漫游时自动同步可能增加设备的数据费用。默认情况下，禁用该选项。

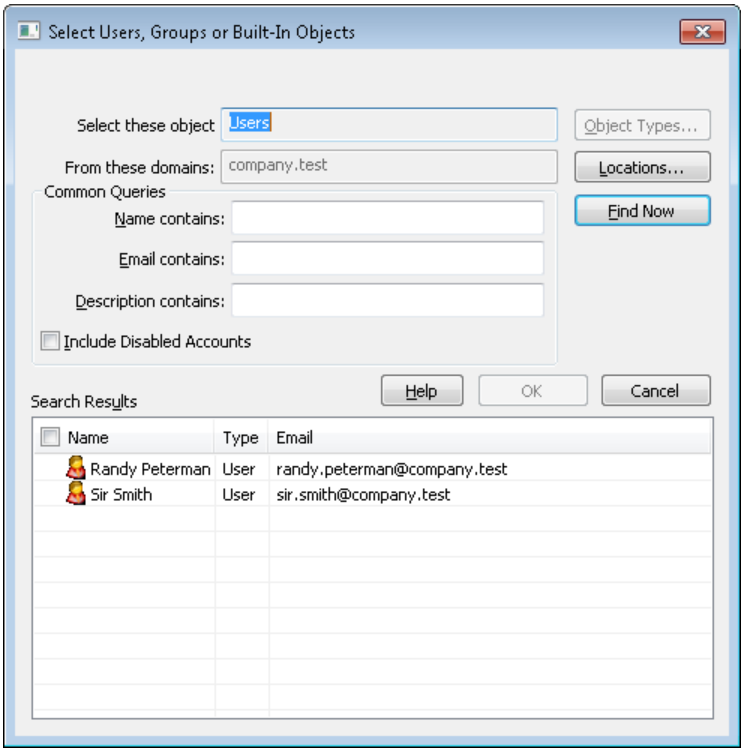
3.10.8 账户



使用此屏幕来指定授权使用 ActiveSync 的账户。您可以手动授权或撤销账户、或者设置 MDaemon 在每个账户使用 ActiveSync 进行连接时自动为其授权。

手动授权账户

在"账户"屏幕上，从"选择域"下拉列表中选择一个域，然后点击"添加"来手动授权一个或多个账户使用 ActiveSync。这将打开"选择用户"对话框来查找和选择账户。



从这些域
这列出了您在 "账户"屏幕的 *"选择域"*选项中选择的域。您可以搜索此域中的用户。

常规查询
使用这一部分的这些选项，通过指定所有或部分用户名、邮件地址或账户描述[598]的内容来缩小您的搜索范围。如果您希望搜索结果包含每个选定域的用户，请将这些字段留空。

包含"禁用账户"
如果您希望在搜索中包含"禁用账户[598]"，请勾选此框。

立即查找
在您指定了所有搜索条件之后，请点击"**立即查找**"来执行搜索。

搜索结果
执行完搜索后，请在"搜索结果"中选择任何所需用户，并点击"**确定**"来将其添加到授权账户的列表。

撤销账户

要撤销账户的 ActiveSync 使用授权，请右键单击这个账户并点击"**撤销选 ActiveSync 权限**"。如果您希望撤销所有账户，请点击"**撤销所有账户**"这个按钮。

如果您已启用了此项，以便在 *"通过 ActiveSync 协议初次访问时授权所有账户"*，撤销一个账户的访问权限会将其从列表删除，不过在设备下次连接账户时将再次授权。

通过 ActiveSync 协议初次访问时授权所有账户

如果您希望每当账户使用 ActiveSync 连接到 MDaemon 时自动为账户授权（一次一个），请勾选此框。

分配 ActiveSync 策略

要向账户分配一个策略[372]：

1. 右键单击列表中的一个账户。
2. 点击 **"分配策略"**。
3. 在 **"要分配的策略"**下，从下拉列表中选择所需的策略（要管理可用策略，请参阅策略管理器[372]）。
4. 点击 **"确定"**。

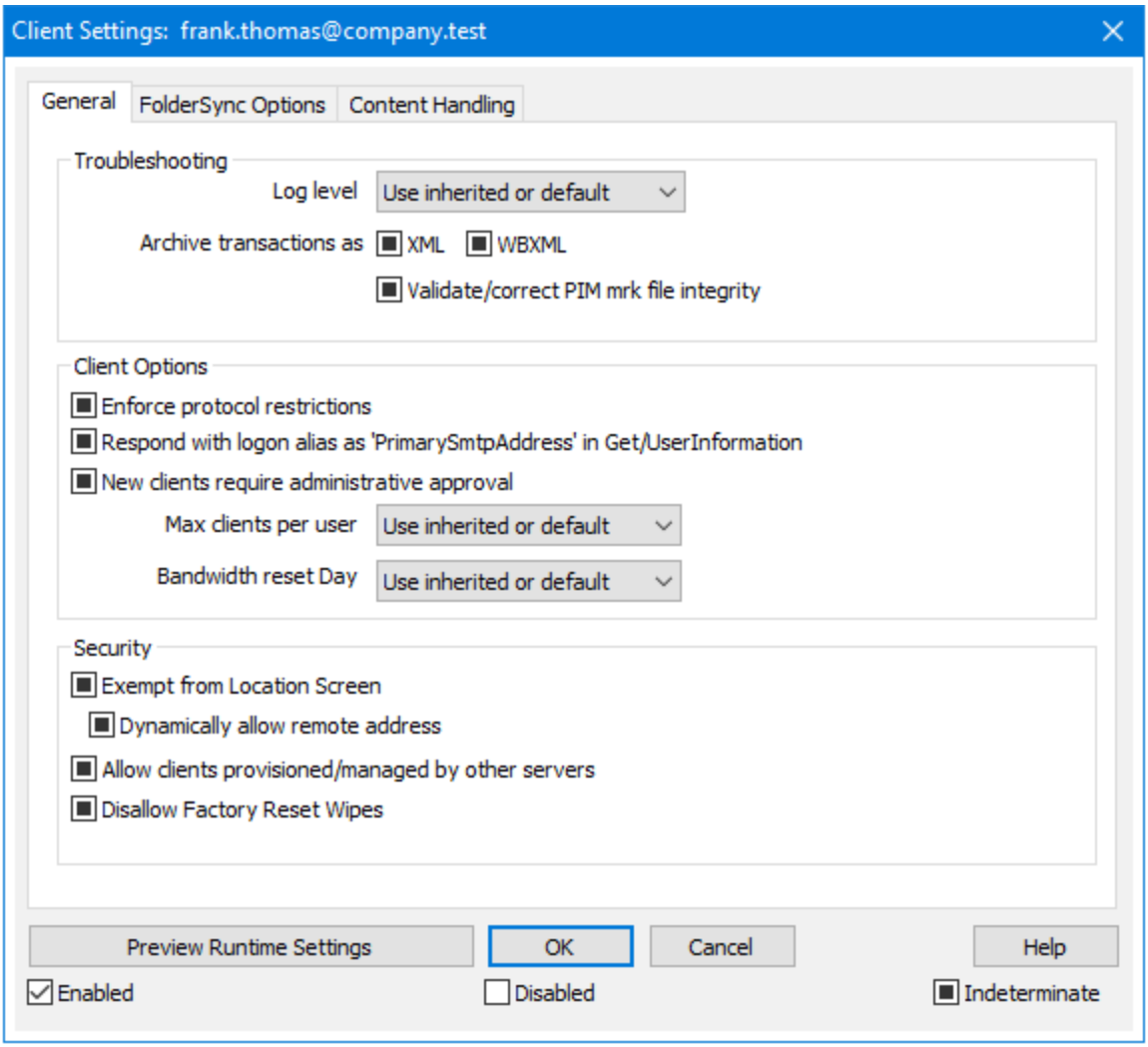
会将该策略分配给连接此账户的任何新设备。

搜索授权账户列表

如果您有许多被授权使用 ActiveSync 的账户，您可以使用 **"查找用户"**框来搜索特定账户列表。只需输入账户邮件地址的开头几个字母即可选择用户。

账户客户端设置

"右键点击一个账户并点击 **"自定义客户端设置"**来管理该账户的 **"客户端设置"**。会将这些设置应用至连接此账户的任何 ActiveSync 客户端。



默认情况下，该屏幕上的所有选项都被设置成 "使用继承或默认值"，这就意味着如果该账户是群组[396]的成员，则将从该群组的 "客户端设置"获取每个选项的设置。如果该账户不在群组中，或者没有为该群组配置 "客户端设置"，则每个选项将从此域的 "客户端设置"[178]屏幕上的相应选项中获取其设置。在此屏幕上对设置做出的任何变更都将在屏幕上反映。反之亦然，您在此屏幕上做出的任何变更将覆盖此账户的群组或域级别的设置。

常规

故障诊断

日志级别

ActiveSync for MDaemon 支持 6 种日志级别，按所记录数据数量的多少分级，以下是从高到低的级别一览：

调试 这是最丰富的日志级别。记录所有可用条目，而且通常只在诊断问题时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

Inherit 默认情况下，"日志级别"设置是从"客户端设置"层次结构继承的。因此，客户端从客户端类型继承，账户从客户端类型继承，群组从账户等继承其设置。此选项的"全局客户端设置"由故障诊断 361 对话框上的"日志级别"设置确定。

归档处理为 [XML | WBXML]
如果您希望保存此数据，请使用*"归档 XML..."*和*"WBXML"*选项，而且有时这些数据对调试很有帮助。默认情况下，禁用这些全局选项。

验证/修复 PIM mrk 文件完整性
该选项对客户端的 PIM 数据运行验证和修复进程来查询有碍正确同步的已知问题，例如重复的 iCalUID 或空的必填字段。默认情况下，禁用这个全局选项。

客户端选项

强制执行协议限制
如果有连接来自尝试使用指定的*"允许的协议版本"*以外的其他协议的客户端，您希望拒绝这些连接时请启用此项。默认情况下禁用此项，这就表示协议限制不防止客户端使用不同的协议：它们只是告诉客户端使用哪些协议。如果客户端无论如何都要尝试使用限制的协议，MDaemon 仍然允许这个连接。还请参阅：协议限制 363 来了解更多信息。

使用登录别名响应，作为 GetUserInformation 中的"PrimarySmtpAddress"
这允许该服务返回别名/次要地址作为主要地址来响应"设置/获取/用户信息"请求。这有助于解决 iOS9.x 更新所引起的一个问题：即导致客户端无法使用别名发送邮件。使用此项将导致对于"设置/获取/用户信息"不规范的响应。

新建客户端需要管理批准
如果您希望要求新的客户端必须先由管理员授权，才能开始与账户同步，请启用此选项。The 客户端 388 列表指示等候授权的任何客户端，管理员可以从相同的屏幕对其进行授权。默认情况下，禁用该设置。

每用户的客户端最大值
如果您希望限制 MDaemon 账户可以关联的 ActiveSync 客户端或设备的数量，请在此项中指定所需数量。默认情况下将这个全局选项设成"无限"。"全局"、"域"和"账户"客户端设置屏幕提供此项，但是个别客户端屏幕不提供此项。

带宽重置日期
如果您希望在每个月指定的一天为 ActiveSync 设备重置带宽使用统计，请使用此项。重置事件作为常规夜间维护过程的一部分进行，而且像其他维护例程一样被记录到系统日志中。默认情况下将这个全局选项设置成"0"(从不)，这就意味着从不重置使用统

计。如果您希望重置的那一天与用户或客户端无线运营商计费的重置日期一致，请将子项设置成不同的一天。

安全

从“位置屏蔽”豁免

启用此项（位于 ActiveSync 客户端的设置屏幕）允许您将设备绕过位置屏蔽[477]。这使得有效的用户有可能通过 ActiveSync 继续访问他或她的账户，例如当前往一个阻止验证尝试的位置时。为了免除设备，它必须使用 ActiveSync 在配置的时间范围内进行连接和验证，请在位于“微调”屏幕的这些天后删除闲置的客户端[351]这个设置中进行配置。

动态允许远程地址

当从“位置屏蔽”豁免设备时，如果您还希望允许其连接的远程 IP 地址，请启用此选项。这对允许其他可能从相同 IP 地址连接的客户端很有用。

允许由其他服务器配置/管理的客户端

默认情况下，当 ActiveSync 服务器向特定客户端发送数据/策略，并报告它也受其他 ActiveSync 服务器管理时，也允许那个客户端连接到 MDaemon。不过在这种情况下，无法确保在与其他 ActiveSync 服务器的策略发生冲突时将应用您的策略。通常默认客户端在策略冲突时使用最具有限制性的选项。如果您不希望允许这些客户端进行连接，请禁用此项。

不允许出厂重置擦除

如果将其设置成启用/是，就不提供**完全擦除** ActiveSync 客户端的功能。如果您希望能够完全远程擦除客户端，您必须先禁用此项。默认情况下，禁用该选项。要了解更多详情，请参阅：“客户端”页面上的完全擦除 ActiveSync 客户端[388]。

FolderSync 选项

FolderSync 选项

例外

已允许/已阻止发件人文件夹

默认情况下，无法和设备同步用户的“已允许发件人和已阻止发件人”联系人文件夹。它们通常只能由 MDaemon 用来吸住自动防止垃圾邮件。出于这个原因，它们无需在设备上显示为联系人。

非默认邮件文件夹

默认情况下能与设备同步所有由用户创建和默认的邮件文件夹。如果您仅希望允许同步默认的邮件文件夹（例如收件箱、已发送项目、已删除项目和草稿等），请启用此项。不会包含由用户创建的文件夹。默认情况下，禁用该选项。

非默认 PIM 文件夹

默认情况下，将与设备同步用户的所有 PIM 文件夹（例如联系人、日历、便笺和任务等）。如果您希望仅允许同步默认的 PIM 文件夹，请启用此项。例如，如果启用此项，而且用户拥有多个日历文件夹，将仅同步默认的日历。默认情况下，禁用该选项。

包括

公告文件夹层次结构
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的公共文件夹[258]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的公共文件夹[258]。默认情况下允许搜索操作。

公共文件夹遍历（显示文件夹名称）
默认情况下，为了让客户端同步/访问公共子文件夹，该账户必须拥有查询权限[260]，而且必须对子文件夹和所有父代公共文件夹[258]拥有该权限。如果该账户没有权限查看父文件夹，那么该账户也不能查看子文件夹，即使该账户有查看子文件夹的权限也是如此。如果您希望允许客户端访问这些子文件夹，请启用此项。**请注意：**启用此项必须向客户端显示父文件夹的名称，这会被视为安全风险。默认情况下，禁用该选项。

允许的公共文件夹数量最大值
如果您希望限制在设备上允许的“公共文件夹”的数量，请使用此项。在设置了限制时，该服务器遍历文件夹列表，直到达到这个限制为止，不会再将更多项目发送到设备。无法确保以何顺序处理这些文件夹。默认情况下未设置全局限制。

共享文件夹
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的共享文件夹[97]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的共享文件夹[623]。默认情况下允许搜索操作。

内容处理

内容处理选项

在被客户端标记时为邮件项目创建任务/提醒
该选项可以在客户端请求时，使 MDaemon 通过为各个已标记的邮件创建任务项目来向用户提醒已标记的项目。。默认情况下，此控件的全局选项处于启用状态。

在事件被修改时始终发送会议更新
某些客户端在修改会议时未正确发送会议更新电子邮件。这指示 ActiveSync 服务在组织者更新会议项目时发送会议更新。这仅能在客户端[388]和无法恰当发送会议更新的客户端类型[402]上设置，否则将导致发送重复的会议更新。因此，此选项仅在“客户端”和“客户端类型”的设置页面上可用。

对所有已发送邮件请求已读回执
如果您希望服务器为客户端发送的所有邮件请求已读确认，请启用此项。默认情况下，禁用该选项。

当邮件被标记为已读时，以及发件人请求时，从服务器发送已读回执
如果您希望服务器支持已读确认请求，并在客户端将邮件标记为已读时发送已读回执，请启用此项。默认情况下，禁用该选项。

发送为在 ReplyTo 地址中指定的别名
某些客户端可能不允许发件人使用别名发送邮件。已在 Exchange ActiveSync (EAS) 协议[363] 16.x 中添加该功能，不过一些客户端不支持 16.x。例如，Windows 版的 Outlook 仅使用 EAS 14.0，虽然它允许用户指定要发送的备用地址，但生成的邮件并不能正确反映用户的选择。该选项允许使用 ReplyTo（答复）字段来发送电子邮件，只要 ReplyTo 地址是该用户的有效别名[699]即可。默认情况下启用这个全局选项。

虚拟地将公共联系人合并为默认联系人
如果您希望将设备上的公共联系人与用户的默认联系人合并在一起，请启用此项。这仅仅是一个虚拟合并，实际上未将它们复制到用户的联系人文件夹。这对不支持“全局地址列表”(GAL)搜索的客户端而言极其有用。默认情况下，禁用该选项。

在将邮件移入垃圾邮件文件夹时阻止发件人
启用后，当客户端将电子邮件移动到账户的垃圾邮件文件夹时，该服务将该电子邮件的发件人或从地址添加到阻止的发件人联系人文件夹。

在会议请求被接受/拒绝等时强制发送会议请求。
启用后，当客户端接受、拒绝或以其他方式选择响应会议请求的操作时，服务将向会议组织者发送会议响应。这是针对没有正确发送这些更新本身的特定客户端。

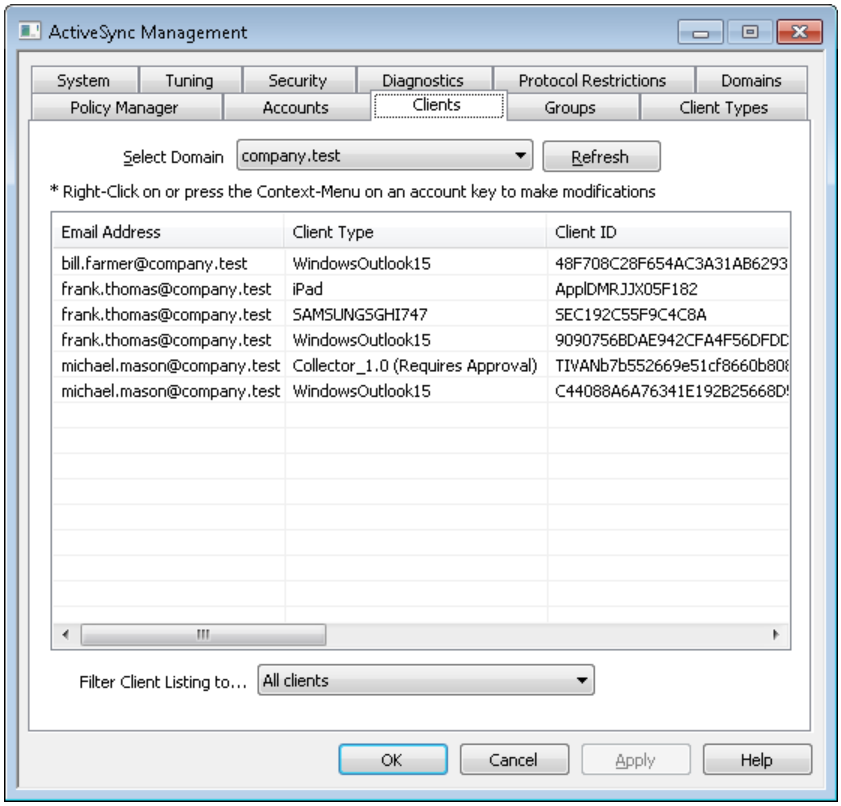
预览有效设置

该按钮在所有子“客户端设置”屏幕上可用（例如域[365]、账户[380]和客户端[388]）。由于默认情况下，已将这些屏幕上的选项都设置成从父屏幕继承其设置，使用该功能来查看当前向显示的屏幕应用了什么设置。

还请参阅：

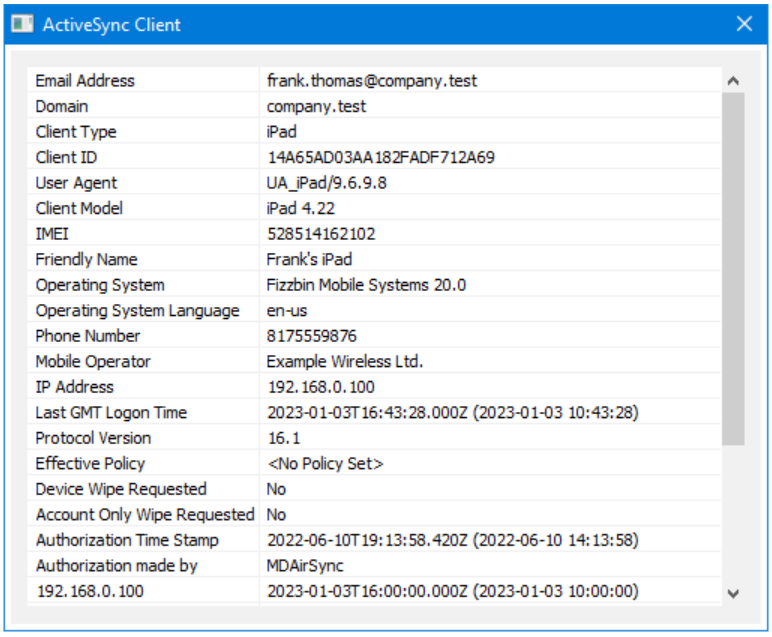
ActiveSync » 客户端设置[353]
ActiveSync » 域[365]
ActiveSync » 客户端[388]
账户 » ActiveSync 客户端设置[643]
账户 » ActiveSync 客户端[649]

3.10.9 客户端



此屏幕包含与所选域关联的每个 ActiveSync 客户端的条目。双击任何条目即可查看有关此客户端的更多详细信息。右键单击一个条目来打开快捷方式菜单，从中可以自定义其客户端设置、查看统计信息并执行其他各种功能。

ActiveSync 客户端详细信息



双击一个条目，或右键单击该条目并点击 **"查看详细信息"**来打开 "客户端详细信息"对话框。此屏幕包含有关客户端的信息，例如其客户端类型、客户端 ID 和上次登录时间等。

客户端设置

右键点击一个客户端并点击 **"自定义客户端设置"**来管理其 "客户端设置"。默认情况下，这些设置是从 "客户端类型"设置继承的，但是可以按需进行调整。请参阅下方的 管理设备的客户端设置 390 。

分配 ActiveSync 策略

要向设备分配一个策略 372:

1. 右键单击此列表中的一个设备。
2. 点击 **"分配策略"**。这会打开 "应用策略"对话框。
3. 点击 **"特分配策略"**下拉列表并选择所需策略。
4. 点击 **"确定"**。

统计

右键点击一个条目，并点击 **"统计"**来打开 "客户端统计"对话框，其中含有关于该客户端的各种使用统计。

重置统计

如果要重置客户端的统计信息，请右键单击该客户端，然后依次点击 **"重置统计"**和 **"确定"**来确认操作。

删除 ActiveSync 客户端

要删除 ActiveSync 客户端，右键单击客户端并点击**删除**，然后点击**是**。这将删除列表中的

客户端，并删除 MDaemon 中与其相关的所有同步信息。因此，如果该账户在未来使用 ActiveSync 来同步相同的客户端，MDaemon 会将该客户端视作从未在这台服务器上使用过的客户端；所有客户端数据必须重新与 MDaemon 进行同步。

完全擦除 ActiveSync 客户端

在将一个策略[372]应用到选定的 ActiveSync 客户端时，并且客户端已应用它并做出响应，则该客户端将有一个可用的 "完全擦除"选项。要进行完全擦除，请右键点击客户端（如果您使用 MDRA，请选择它），并点击 **"完全擦除"**。下次该客户端进行连接时，MDaemon 将告诉它擦除所有数据，或将自身重置成出厂默认状态。取决于该客户端，上述操作可能删除设备上的一切，包括已下载的应用程序。此外，只要客户端的 ActiveSync 条目存在，MDaemon 将在该设备日后进行连接的任何时候继续发送擦除请求。如果有时您希望删除客户端，请确保您先将其添加到阻止列表[359]，这样它以后就无法再次连接。最后，如果擦除的设备被恢复，并且您希望允许它再次连接，您应该选择该设备并点击 **"取消擦除操作"**。您也必须从 阻止列表将其删除。

账户擦除 ActiveSync 客户端

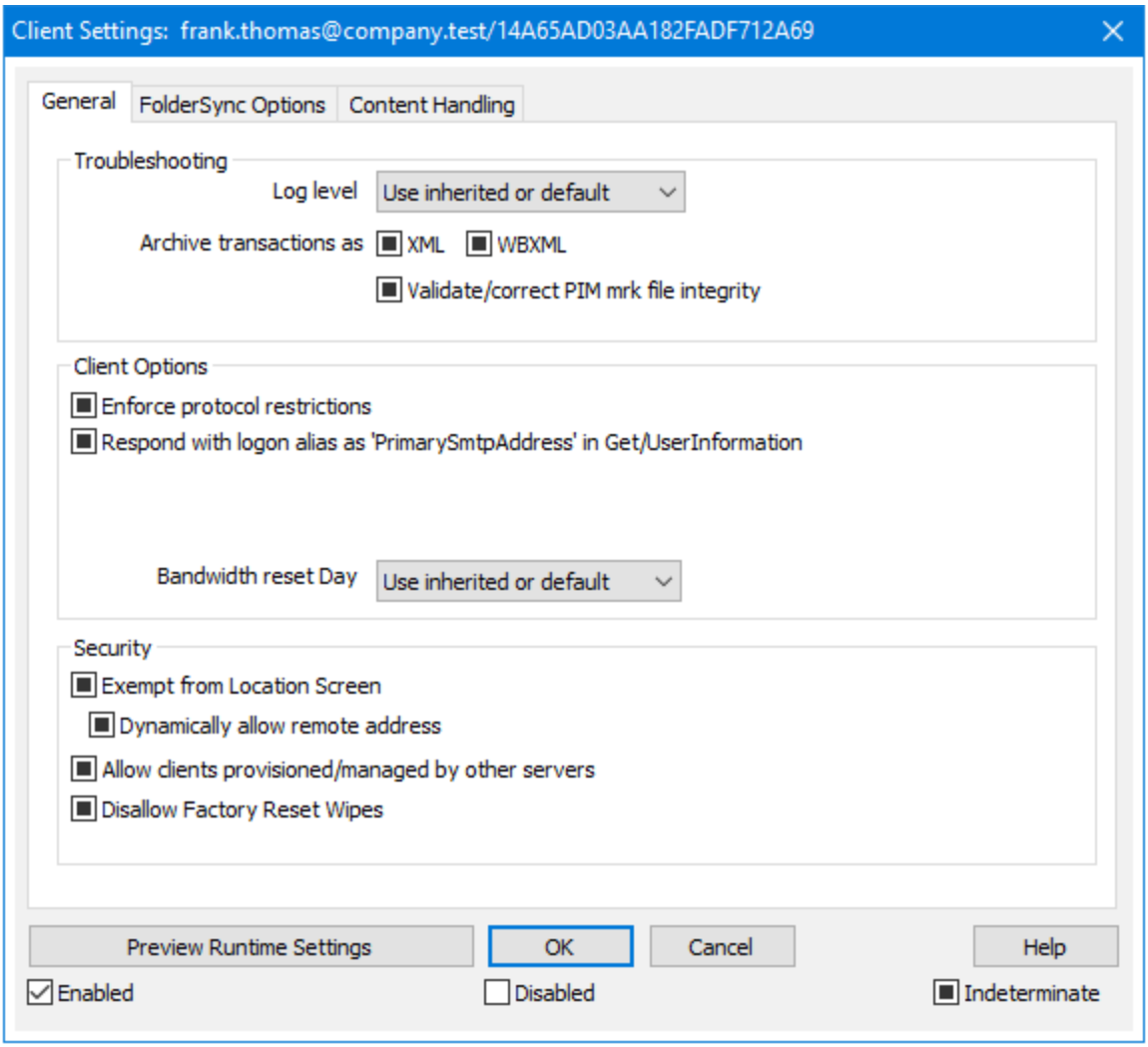
要从客户端或设备中擦除账户的邮件和 PIM 数据，请右键点击并选择 **"从客户端擦除账户邮件和 PIM"**。*"账户擦除"*选项与上述 *"完全擦除"*选项类似，不过该项不擦除所有数据，而是仅擦除这个账户的数据，例如其电子邮件、日历条目和联系人等。保留剩余所有项目，例如应用程序、照片或音乐。

授权客户端

如果将 *"新建客户端需要管理批准"*选项（位于 ActiveSync 客户端设置[353]屏幕）设置成需要批准，选择一个客户端并点击批准客户端进行同步来授权它与服务器进行同步。

管理设备的客户端设置

设备级别的 "客户端设置"屏幕允许您管理特定设备的设置。



默认情况下，此屏幕上的所有选项都被设置为 "使用继承或默认值"，表示每个选项都会从客户端类型客户端设置 402 屏幕上的相应选项中获取其设置。在此屏幕上对设置做出的任何变更都将在屏幕上反映。反之亦然，您在此屏幕上做出的任何变更将覆盖此设备的客户端类型级别的设置。

常规

故障诊断

日志级别

ActiveSync for MDaemon 支持 6 种日志级别，按所记录数据数量的多少分级，以下是从高到低的级别一览：

调试 这是最丰富的日志级别。记录所有可用条目，而且通常只在诊断问题时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

Inherit 默认情况下，"日志级别"设置是从"客户端设置"层次结构继承的。因此，客户端从客户端类型继承，账户从客户端类型继承，群组从账户等继承其设置。此选项的"全局客户端设置"由故障诊断[361]对话框上的"日志级别"设置确定。

归档处理为 [XML | WBXML]
如果您希望保存此数据，请使用*"归档 XML..."*和*"WBXML"*选项，而且有时这些数据对调试很有帮助。默认情况下，禁用这些全局选项。

验证/修复 PIM mrk 文件完整性
该选项对客户端的 PIM 数据运行验证和修复进程来查询有碍正确同步的已知问题，例如重复的 iCalUID 或空的必填字段。默认情况下，禁用这个全局选项。

客户端选项

强制执行协议限制
如果有连接来自尝试使用指定的*"允许的协议版本"*以外的其他协议的客户端，您希望拒绝这些连接时请启用此项。默认情况下禁用此项，这就表示协议限制不防止客户端使用不同的协议：它们只是告诉客户端使用哪些协议。如果客户端无论如何都要尝试使用限制的协议，MDaemon 仍然允许这个连接。还请参阅：协议限制[363]来了解更多信息。

使用登录别名响应，作为 GetUserInformation 中的"PrimarySmtpAddress"
这允许该服务返回别名/次要地址作为主要地址来响应"设置/获取/用户信息"请求。这有助于解决 iOS9.x 更新所引起的一个问题：即导致客户端无法使用别名发送邮件。使用此项将导致对于"设置/获取/用户信息"不规范的响应。

新建客户端需要管理批准
如果您希望要求新的客户端必须先由管理员授权，才能开始与账户同步，请启用此选项。The 客户端[388]列表指示等候授权的任何客户端，管理员可以从相同的屏幕对其进行授权。默认情况下，禁用该设置。

每用户的客户端最大值
如果您希望限制 MDaemon 账户可以关联的 ActiveSync 客户端或设备的数量，请在此项中指定所需数量。默认情况下将这个全局选项设成"无限"。"全局"、"域"和"账户"客户端设置屏幕提供此项，但是个别客户端屏幕不提供此项。

带宽重置日期
如果您希望在每个月指定的一天为 ActiveSync 设备重置带宽使用统计，请使用此项。重置事件作为常规夜间维护过程的一部分进行，而且像其他维护例程一样被记录到系统日志中。默认情况下将这个全局选项设置成"0"(从不)，这就意味着从不重置使用统计。如果您希望重置的那一天与用户或客户端无线运营商计费的重置日期一致，请将子项设置成不同的一天。

安全

从“位置屏蔽”豁免
启用此项（位于 ActiveSync 客户端的设置屏幕）允许您将设备绕过位置屏蔽 477。这使得有效的用户有可能通过 ActiveSync 继续访问他或她的账户，例如当前往一个阻止验证尝试的位置时。为了免除设备，它必须使用 ActiveSync 在配置的时间范围内进行连接和验证，请在位于“微调”屏幕的这些天后删除闲置的客户端 351这个设置中进行配置。

动态允许远程地址
当从“位置屏蔽”豁免设备时，如果您还希望允许其连接的远程 IP 地址，请启用此选项。这对允许其他可能从相同 IP 地址连接的客户端很有用。

允许由其他服务器配置/管理的客户端
默认情况下，当 ActiveSync 服务器向特定客户端发送数据/策略，并报告它也受其他 ActiveSync 服务器管理时，也允许那个客户端连接到 MDaemon。不过在这种情况下，无法确保在与其他 ActiveSync 服务器的策略发生冲突时将应用您的策略。通常默认客户端在策略冲突时使用最具有限制性的选项。如果您不希望允许这些客户端进行连接，请禁用此项。

不允许出厂重置擦除
如果将其设置成启用/是，就不提供完全擦除 ActiveSync 客户端的功能。如果您希望能够完全远程擦除客户端，您必须先禁用此项。默认情况下，禁用该选项。要了解更多详情，请参阅：“客户端”页面上的完全擦除 ActiveSync 客户端 388。

FolderSync 选项

FolderSync 选项

例外

已允许/已阻止发件人文件夹
默认情况下，无法和设备同步用户的“已允许发件人和已阻止发件人”联系人文件夹。它们通常只能由 MDaemon 用来吸住自动防止垃圾邮件。出于这个原因，它们无需在设备上显示为联系人。

非默认邮件文件夹
默认情况下能与设备同步所有由用户创建和默认的邮件文件夹。如果您仅希望允许同步默认的邮件文件夹（例如收件箱、已发送项目、已删除项目和草稿等），请启用此项。不会包含由用户创建的文件夹。默认情况下，禁用该选项。

非默认 PIM 文件夹
默认情况下，将与设备同步用户的所有 PIM 文件夹（例如联系人、日历、便笺和任务等）。如果您希望仅允许同步默认的 PIM 文件夹，请启用此项。例如，如果启用此项，而且用户拥有多个日历文件夹，将仅同步默认的日历。默认情况下，禁用该选项。

包括

公告文件夹层次结构
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的公共文件

夹[258]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的公共文件夹[258]。默认情况下允许搜索操作。

公共文件夹遍历（显示文件夹名称）
默认情况下，为了让客户端同步/访问公共子文件夹，该账户必须拥有查询权限[260]，而且必须对子文件夹和所有父代公共文件夹[258]拥有该权限。如果该账户没有权限查看父文件夹，那么该账户也不能查看子文件夹，即使该账户有查看子文件夹的权限也是如此。如果您希望允许客户端访问这些子文件夹，请启用此项。**请注意：**启用此项必须向客户端显示父文件夹的名称，这会被视为安全风险。默认情况下，禁用该选项。

允许的公共文件夹数量最大值
如果您希望限制在设备上允许的“公共文件夹”的数量，请使用此项。在设置了限制时，该服务器遍历文件夹列表，直到达到这个限制为止，不会再将更多项目发送到设备。无法确保以何顺序处理这些文件夹。默认情况下未设置全局限制。

共享文件夹
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的共享文件夹[97]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的共享文件夹[623]。默认情况下允许搜索操作。

内容处理

内容处理选项

在被客户端标记时为邮件项目创建任务/提醒
该选项可以在客户端请求时，使 MDaemon 通过为各个已标记的邮件创建任务项目来向用户提醒已标记的项目。。默认情况下，此控件的全局选项处于启用状态。

在事件被修改时始终发送会议更新
某些客户端在修改会议时未正确发送会议更新电子邮件。这指示 ActiveSync 服务在组织者更新会议项目时发送会议更新。这仅能在客户端[388]和无法恰当发送会议更新的客户端类型[402]上设置，否则将导致发送重复的会议更新。因此，此选项仅在“客户端”和“客户端类型”的设置页面上可用。

对所有已发送邮件请求已读回执
如果您希望服务器为客户端发送的所有邮件请求已读确认，请启用此项。默认情况下，禁用该选项。

当邮件被标记为已读时，以及发件人请求时，从服务器发送已读回执
如果您希望服务器支持已读确认请求，并在客户端将邮件标记为已读时发送已读回执，请启用此项。默认情况下，禁用该选项。

发送为在 ReplyTo 地址中指定的别名
某些客户端可能不允许发件人使用别名发送邮件。已在 Exchange ActiveSync (EAS) 协议 363 16.x 中添加该功能，不过一些客户端不支持 16.x。例如，Windows 版的 Outlook 仅使用 EAS 14.0，虽然它允许用户指定要发送的备用地址，但生成的邮件并不能正确反映用户的选择。该选项允许使用 ReplyTo（答复）字段来发送电子邮件，只要 ReplyTo 地址是该用户的有效别名 699 即可。默认情况下启用这个全局选项。

虚拟地将公共联系人合并为默认联系人
如果您希望将设备上的公共联系人与用户的默认联系人合并在一起，请启用此项。这仅仅是一个虚拟合并，实际上未将它们复制到用户的联系人文件夹。这对不支持“全局地址列表”(GAL)搜索的客户端而言极其有用。默认情况下，禁用该选项。

在将邮件移入垃圾邮件文件夹时阻止发件人
启用后，当客户端将电子邮件移动到账户的垃圾邮件文件夹时，该服务将该电子邮件的发件人或从地址添加到阻止的发件人联系人文件夹。

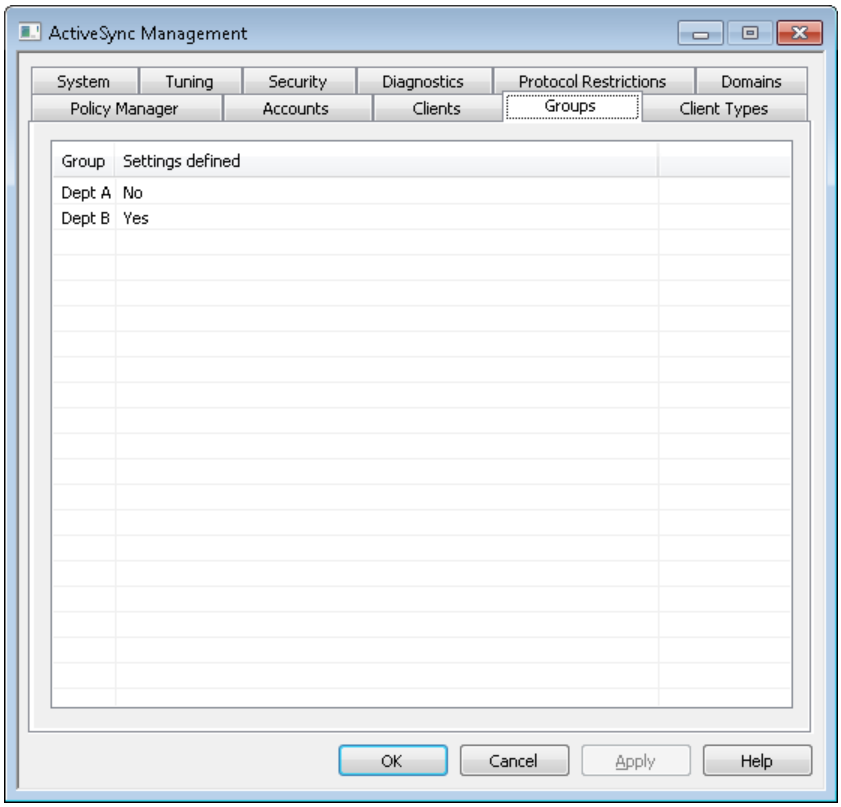
在会议请求被接受/拒绝等时强制发送会议请求。
启用后，当客户端接受、拒绝或以其他方式选择响应会议请求的操作时，服务将向会议组织者发送会议响应。这是针对没有正确发送这些更新本身的特定客户端。

预览有效设置
该按钮在所有子“客户端设置”屏幕上可用（例如域 365、账户 380 和客户端 388）。由于默认情况下，已将这些屏幕上的选项都设置成从父屏幕继承其设置，使用该功能来查看当前向显示的屏幕应用了什么设置。

还请参阅下方的：

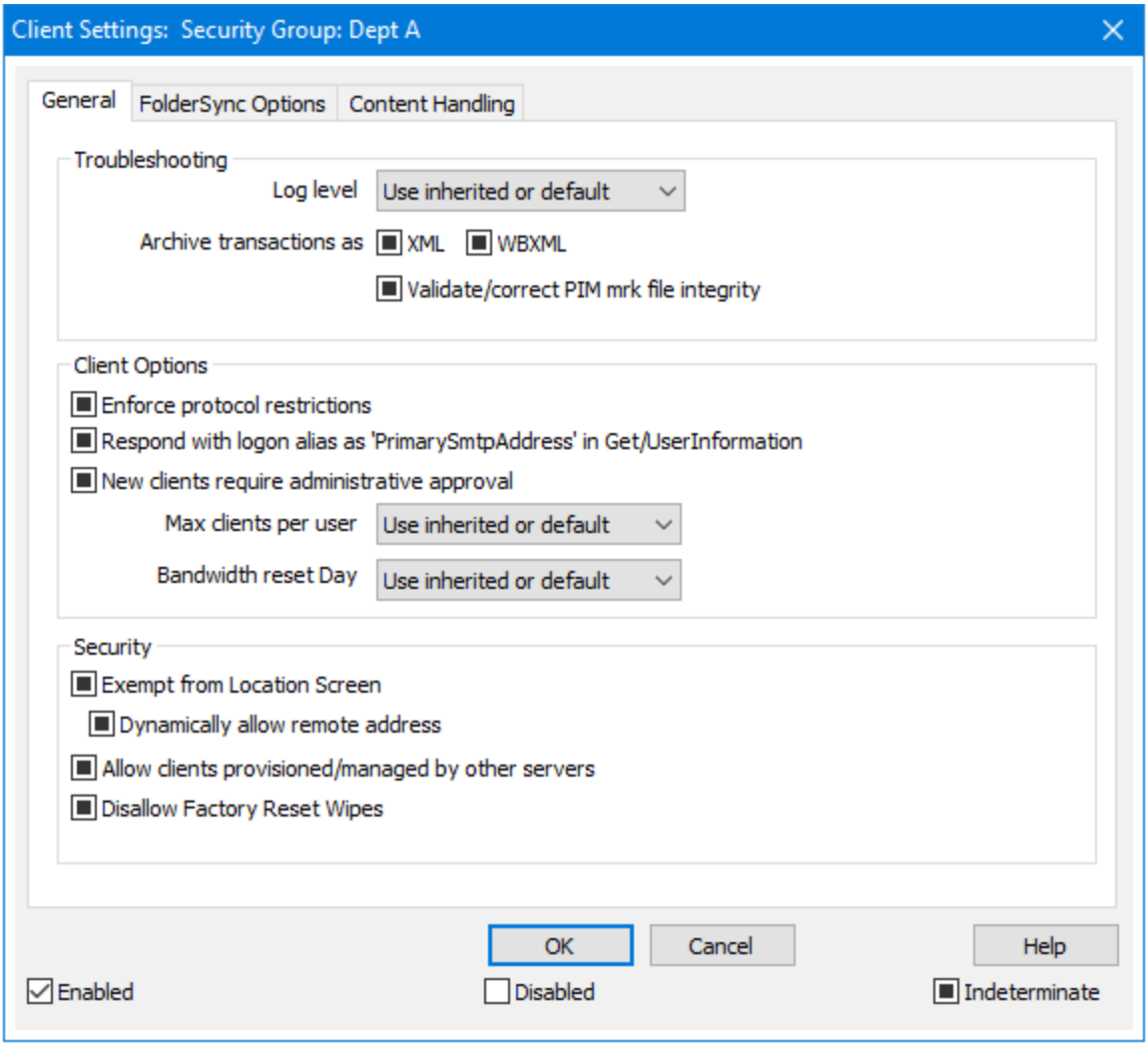
ActiveSync » 客户端设置 353
ActiveSync » 域 365
ActiveSync » 账户 380

3.10.1 群组
0



如果您希望为一个账户群组[657]定义定制的 "ActiveSync 客户端设置"，请使用此屏幕来管理那些设置。此处列出了所有群组，每个群组的条目指示其设置是否被定义。要编辑一个 "群组"的 "客户端设置"，请双击该群组，或右键单击这个群组并点击 **"自定义客户端设置"**。

群组客户端设置



默认情况下，每个"群组"的客户端设置都被设置成从"域客户端设置 178"继承其状态。更改群组设置将覆盖属于该组成员的任何账户的域设置。如果您不希望"群组客户端设置"应用于特定的群组成员或设备，则可以通过编辑账户 380、客户端类型 402或客户端 388的"客户端设置"来覆盖群组设置。

常规

故障诊断

日志级别

ActiveSync for MDaemon 支持 6 种日志级别，按所记录数据数量的多少分级，以下是从高到低的级别一览：

调试 这是最丰富的日志级别。记录所有可用条目，而且通常只在诊断问题时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

Inherit 默认情况下，"日志级别"设置是从"客户端设置"层次结构继承的。因此，客户端从客户端类型继承，账户从客户端类型继承，群组从账户等继承其设置。此选项的"全局客户端设置"由故障诊断[361]对话框上的"日志级别"设置确定。

归档处理为 [XML | WBXML]
如果您希望保存此数据，请使用*"归档 XML..."*和*"WBXML"*选项，而且有时这些数据对调试很有帮助。默认情况下，禁用这些全局选项。

验证/修复 PIM mrk 文件完整性
该选项对客户端的 PIM 数据运行验证和修复进程来查询有碍正确同步的已知问题，例如重复的 iCalUID 或空的必填字段。默认情况下，禁用这个全局选项。

客户端选项

强制执行协议限制
如果有连接来自尝试使用指定的*"允许的协议版本"*以外的其他协议的客户端，您希望拒绝这些连接时请启用此项。默认情况下禁用此项，这就表示协议限制不防止客户端使用不同的协议：它们只是告诉客户端使用哪些协议。如果客户端无论如何都要尝试使用限制的协议，MDaemon 仍然允许这个连接。还请参阅：协议限制[363]来了解更多信息。

使用登录别名响应，作为 Get/UserInformation 中的 "PrimarySmtpAddress"
这允许该服务返回别名/次要地址作为主要地址来响应"设置/获取/用户信息"请求。这有助于解决 iOS9.x 更新所引起的一个问题：即导致客户端无法使用别名发送邮件。使用此项将导致对于"设置/获取/用户信息"不规范的响应。

新建客户端需要管理批准
如果您希望要求新的客户端必须先由管理员授权，才能开始与账户同步，请启用此选项。The 客户端[388]列表指示等候授权的任何客户端，管理员可以从相同的屏幕对其进行授权。默认情况下，禁用该设置。

每用户的客户端最大值
如果您希望限制 MDaemon 账户可以关联的 ActiveSync 客户端或设备的数量，请在此项中指定所需数量。默认情况下将这个全局选项设成"无限"。"全局"、"域"和"账户"客户端设置屏幕提供此项，但是个别客户端屏幕不提供此项。

带宽重置日期
如果您希望在每个月指定的一天为 ActiveSync 设备重置带宽使用统计，请使用此项。重置事件作为常规夜间维护过程的一部分进行，而且像其他维护例程一样被记录到系统日志中。默认情况下将这个全局选项设置成"0"（从不），这就意味着从不重置使用统计。

如果您希望重置的那一天与用户或客户端无线运营商计费的重置日期一致，请将子项设置成不同的一天。

安全

从“位置屏蔽”豁免
启用此项（位于 ActiveSync 客户端的设置屏幕）允许您将设备绕过位置屏蔽 477。这使得有效的用户有可能通过 ActiveSync 继续访问他或她的账户，例如当前往一个阻止验证尝试的位置时。为了免除设备，它必须使用 ActiveSync 在配置的时间范围内进行连接和验证，请在位于“微调”屏幕的这些天后删除闲置的客户端 351这个设置中进行配置。

动态允许远程地址
当从“位置屏蔽”豁免设备时，如果您还希望允许其连接的远程 IP 地址，请启用此选项。这对允许其他可能从相同 IP 地址连接的客户端很有用。

允许由其他服务器配置/管理的客户端
默认情况下，当 ActiveSync 服务器向特定客户端发送数据/策略，并报告它也受其他 ActiveSync 服务器管理时，也允许那个客户端连接到 MDaemon。不过在这种情况下，无法确保在与其他 ActiveSync 服务器的策略发生冲突时将应用您的策略。通常默认客户端在策略冲突时使用最具有限制性的选项。如果您不希望允许这些客户端进行连接，请禁用此项。

不允许出厂重置擦除
如果将其设置成启用/是，就不提供**完全擦除** ActiveSync 客户端的功能。如果您希望能够完全远程擦除客户端，您必须先禁用此项。默认情况下，禁用该选项。要了解更多详情，请参阅：“客户端”页面上的完全擦除 ActiveSync 客户端 388。

FolderSync 选项

FolderSync 选项

例外

已允许/已阻止发件人文件夹
默认情况下，无法和设备同步用户的“已允许发件人和已阻止发件人”联系人文件夹。它们通常只能由 MDaemon 用来吸住自动防止垃圾邮件。出于这个原因，它们无需在设备上显示为联系人。

非默认邮件文件夹
默认情况下能与设备同步所有由用户创建和默认的邮件文件夹。如果您仅希望允许同步默认的邮件文件夹（例如收件箱、已发送项目、已删除项目和草稿等），请启用此项。不会包含由用户创建的文件夹。默认情况下，禁用该选项。

非默认 PIM 文件夹
默认情况下，将与设备同步用户的所有 PIM 文件夹（例如联系人、日历、便笺和任务等）。如果您希望仅允许同步默认的 PIM 文件夹，请启用此项。例如，如果启用此项，而且用户拥有多个日历文件夹，将仅同步默认的日历。默认情况下，禁用该选项。

包括

公告文件夹层次结构
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的公共文件夹[258]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的公共文件夹[258]。默认情况下允许搜索操作。

公共文件夹遍历（显示文件夹名称）
默认情况下，为了让客户端同步/访问公共子文件夹，该账户必须拥有查询权限[260]，而且必须对子文件夹和所有父代公共文件夹[258]拥有该权限。如果该账户没有权限查看父文件夹，那么该账户也不能查看子文件夹，即使该账户有查看子文件夹的权限也是如此。如果您希望允许客户端访问这些子文件夹，请启用此项。**请注意：**启用此项必须向客户端显示父文件夹的名称，这会被视为安全风险。默认情况下，禁用该选项。

允许的公共文件夹数量最大值
如果您希望限制在设备上允许的“公共文件夹”的数量，请使用此项。在设置了限制时，该服务器遍历文件夹列表，直到达到这个限制为止，不会再将更多项目发送到设备。无法确保以何顺序处理这些文件夹。默认情况下未设置全局限制。

共享文件夹
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的共享文件夹[97]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的共享文件夹[623]。默认情况下允许搜索操作。

内容处理

内容处理选项

在被客户端标记时为邮件项目创建任务/提醒
该选项可以在客户端请求时，使 MDaemon 通过为各个已标记的邮件创建任务项目来向用户提醒已标记的项目。。默认情况下，此控件的全局选项处于启用状态。

在事件被修改时始终发送会议更新
某些客户端在修改会议时未正确发送会议更新电子邮件。这指示 ActiveSync 服务在组织者更新会议项目时发送会议更新。这仅能在客户端[388]和无法恰当发送会议更新的客户端类型[402]上设置，否则将导致发送重复的会议更新。因此，此选项仅在“客户端”和“客户端类型”的设置页面上可用。

对所有已发送邮件请求已读回执
如果您希望服务器为客户端发送的所有邮件请求已读确认，请启用此项。默认情况下，禁用该选项。

当邮件被标记为已读时，以及发件人请求时，从服务器发送已读回执
如果您希望服务器支持已读确认请求，并在客户端将邮件标记为已读时发送已读回执，

请启用此项。默认情况下，禁用该选项。

发送为在 ReplyTo 地址中指定的别名
某些客户端可能不允许发件人使用别名发送邮件。已在 Exchange ActiveSync (EAS) 协议[363] 16.x 中添加该功能，不过一些客户端不支持 16.x。例如，Windows 版的 Outlook 仅使用 EAS 14.0，虽然它允许用户指定要发送的备用地址，但生成的邮件并不能正确反映用户的选择。该选项允许使用 ReplyTo (答复) 字段来发送电子邮件，只要 ReplyTo 地址是该用户的有效别名[699]即可。默认情况下启用这个全局选项。

虚拟地将公共联系人合并为默认联系人
如果您希望将设备上的公共联系人与用户的默认联系人合并在一起，请启用此项。这仅仅是一个虚拟合并，实际上未将它们复制到用户的联系人文件夹。这对不支持 "全局地址列表" (GAL) 搜索的客户端而言极其有用。默认情况下，禁用该选项。

在将邮件移入垃圾邮件文件夹时阻止发件人
启用后，当客户端将电子邮件移动到账户的垃圾邮件文件夹时，该服务将该电子邮件的发件人或从地址添加到阻止的发件人联系人文件夹。

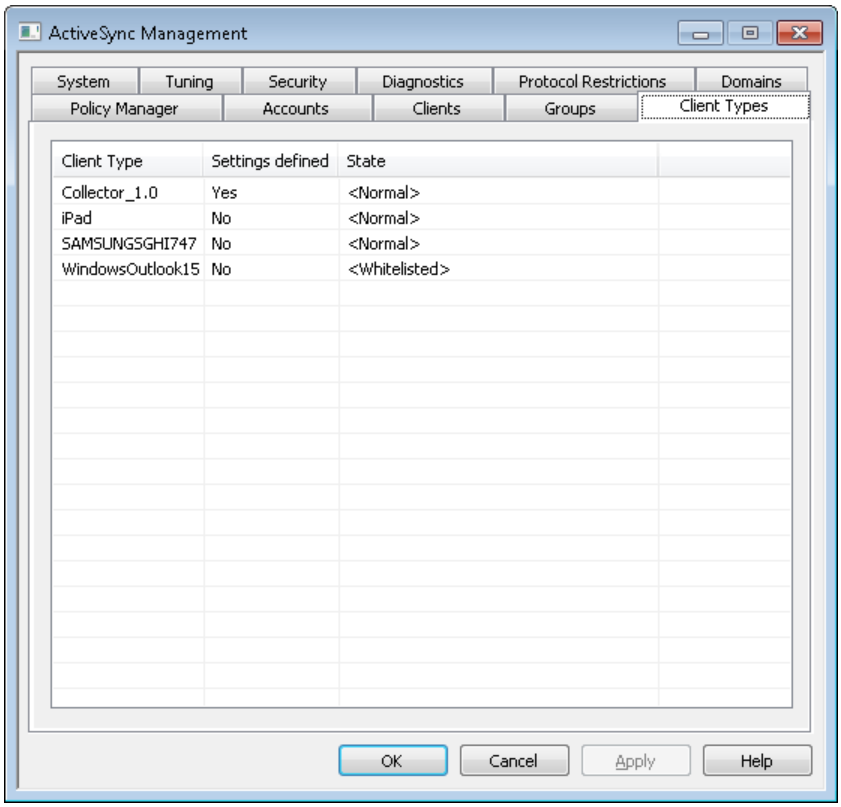
在会议请求被接受/拒绝等时强制发送会议请求。
启用后，当客户端接受、拒绝或以其他方式选择响应会议请求的操作时，服务将向会议组织者发送会议响应。这是针对没有正确发送这些更新本身的特定客户端。

预览有效设置
该按钮在所有子 "客户端设置" 屏幕上可用 (例如域[365]、账户[380]和客户端[388])。由于默认情况下，已将这些屏幕上的选项都设置成从父屏幕继承其设置，使用该功能来查看当前向显示的屏幕应用了什么设置。

还请参阅：

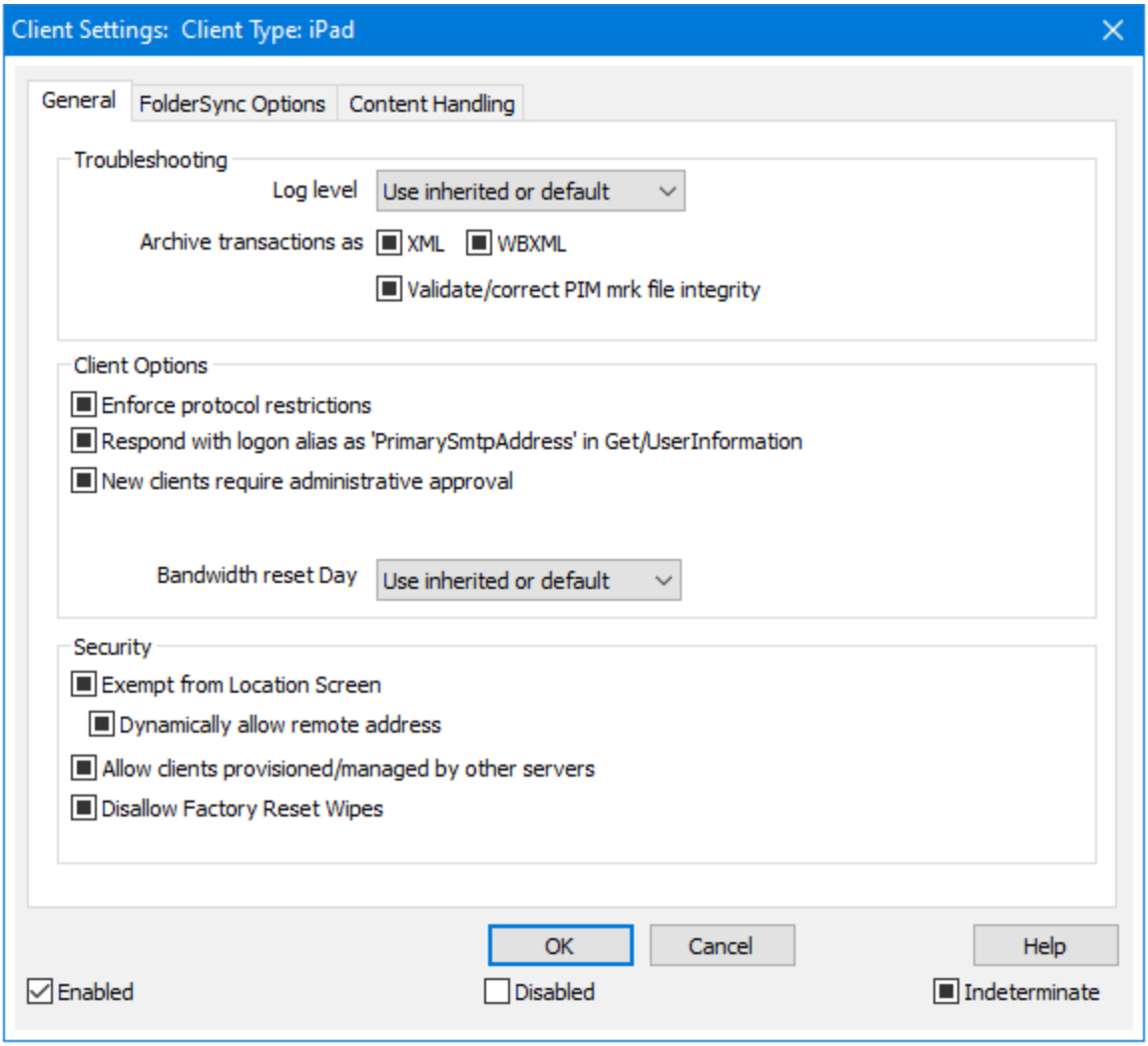
ActiveSync » 域[365]
ActiveSync » 账户[380]
ActiveSync » 客户端[388]

3.10.1 客户端类型
1



如果您希望为特定类型的 ActiveSync 客户端定义定制的 ActiveSync 客户端设置，请使用此屏幕来管理那些设置。当前被授权使用 ActiveSync 的所有客户端388的客户端类型都列于此处，而且每个 "客户端类型"条目都指示其设置是否已被定义。要编辑 "客户端类型"的 "客户端设置"，请双击该条目，或右键单击它并点击 **"自定义客户端设置"**。您也能右键单击一个条目来删除自定义设置，或者从 ActiveSync 允许列表或豁免列表359添加或删除 "客户端类型"。

客户端类型的客户端设置



默认情况下，每个 "客户端类型"的客户端设置都被设置成从 "账户客户端设置 643"继承其状态。更改 "客户端类型"设置将覆盖使用该类型客户端的任何账户的账户设置。如果您不希望将 "客户端类型的客户端设置"应用于特定的客户端，则可以通过编辑那个客户端的 "客户端设置" 388来覆盖 "客户端类型"设置。

常规

故障诊断

日志级别

ActiveSync for MDaemon 支持 6 种日志级别，按所记录数据数量的多少分级，以下是从高到低的级别一览：

调试 这是最丰富的日志级别。记录所有可用条目，而且通常只在诊断问题时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

Inherit 默认情况下，"日志级别"设置是从"客户端设置"层次结构继承的。因此，客户端从客户端类型继承，账户从客户端类型继承，群组从账户等继承其设置。此选项的"全局客户端设置"由故障诊断 361 对话框上的"日志级别"设置确定。

归档处理为 [XML | WBXML]
如果您希望保存此数据，请使用*"归档 XML..."*和*"WBXML"*选项，而且有时这些数据对调试很有帮助。默认情况下，禁用这些全局选项。

验证/修复 PIM mrk 文件完整性
该选项对客户端的 PIM 数据运行验证和修复进程来查询有碍正确同步的已知问题，例如重复的 iCalUID 或空的必填字段。默认情况下，禁用这个全局选项。

客户端选项

强制执行协议限制
如果有连接来自尝试使用指定的*"允许的协议版本"*以外的其他协议的客户端，您希望拒绝这些连接时请启用此项。默认情况下禁用此项，这就表示协议限制不防止客户端使用不同的协议：它们只是告诉客户端使用哪些协议。如果客户端无论如何都要尝试使用限制的协议，MDaemon 仍然允许这个连接。还请参阅：协议限制 363 来了解更多信息。

使用登录别名响应，作为 Get/UserInformation 中的 "PrimarySmtpAddress"
这允许该服务返回别名/次要地址作为主要地址来响应"设置/获取/用户信息"请求。这有助于解决 iOS9.x 更新所引起的一个问题：即导致客户端无法使用别名发送邮件。使用此项将导致对于"设置/获取/用户信息"不规范的响应。

新建客户端需要管理批准
如果您希望要求新的客户端必须先由管理员授权，才能开始与账户同步，请启用此选项。The 客户端 388 列表指示等候授权的任何客户端，管理员可以从相同的屏幕对其进行授权。默认情况下，禁用该设置。

每用户的客户端最大值
如果您希望限制 MDaemon 账户可以关联的 ActiveSync 客户端或设备的数量，请在此项中指定所需数量。默认情况下将这个全局选项设成"无限"。"全局"、"域"和"账户"客户端设置屏幕提供此项，但是个别客户端屏幕不提供此项。

带宽重置日期
如果您希望在每个月指定的一天为 ActiveSync 设备重置带宽使用统计，请使用此项。重置事件作为常规夜间维护过程的一部分进行，而且像其他维护例程一样被记录到系统日志中。默认情况下将这个全局选项设置成"0"（从不），这就意味着从不重置使用统计。

如果您希望重置的那一天与用户或客户端无线运营商计费的重置日期一致，请将子项设置成不同的一天。

安全

从“位置屏蔽”豁免
启用此项（位于 ActiveSync 客户端的设置屏幕）允许您将设备绕过位置屏蔽 477。这使得有效的用户有可能通过 ActiveSync 继续访问他或她的账户，例如当前往一个阻止验证尝试的位置时。为了免除设备，它必须使用 ActiveSync 在配置的时间范围内进行连接和验证，请在位于“微调”屏幕的这些天后删除闲置的客户端 351这个设置中进行配置。

动态允许远程地址
当从“位置屏蔽”豁免设备时，如果您还希望允许其连接的远程 IP 地址，请启用此选项。这对允许其他可能从相同 IP 地址连接的客户端很有用。

允许由其他服务器配置/管理的客户端
默认情况下，当 ActiveSync 服务器向特定客户端发送数据/策略，并报告它也受其他 ActiveSync 服务器管理时，也允许那个客户端连接到 MDaemon。不过在这种情况下，无法确保在与其他 ActiveSync 服务器的策略发生冲突时将应用您的策略。通常默认客户端在策略冲突时使用最具有限制性的选项。如果您不希望允许这些客户端进行连接，请禁用此项。

不允许出厂重置擦除
如果将其设置成启用/是，就不提供**完全擦除** ActiveSync 客户端的功能。如果您希望能够完全远程擦除客户端，您必须先禁用此项。默认情况下，禁用该选项。要了解更多详情，请参阅：“客户端”页面上的完全擦除 ActiveSync 客户端 388。

FolderSync 选项

FolderSync 选项

例外

已允许/已阻止发件人文件夹
默认情况下，无法和设备同步用户的“已允许发件人和已阻止发件人”联系人文件夹。它们通常只能由 MDaemon 用来吸住自动防止垃圾邮件。出于这个原因，它们无需在设备上显示为联系人。

非默认邮件文件夹
默认情况下能与设备同步所有由用户创建和默认的邮件文件夹。如果您仅希望允许同步默认的邮件文件夹（例如收件箱、已发送项目、已删除项目和草稿等），请启用此项。不会包含由用户创建的文件夹。默认情况下，禁用该选项。

非默认 PIM 文件夹
默认情况下，将与设备同步用户的所有 PIM 文件夹（例如联系人、日历、便笺和任务等）。如果您希望仅允许同步默认的 PIM 文件夹，请启用此项。例如，如果启用此项，而且用户拥有多个日历文件夹，将仅同步默认的日历。默认情况下，禁用该选项。

包括

公告文件夹层次结构
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的公共文件夹[258]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的公共文件夹[258]。默认情况下允许搜索操作。

公共文件夹遍历（显示文件夹名称）
默认情况下，为了让客户端同步/访问公共子文件夹，该账户必须拥有查询权限[260]，而且必须对子文件夹和所有父代公共文件夹[258]拥有该权限。如果该账户没有权限查看父文件夹，那么该账户也不能查看子文件夹，即使该账户有查看子文件夹的权限也是如此。如果您希望允许客户端访问这些子文件夹，请启用此项。**请注意：**启用此项必须向客户端显示父文件夹的名称，这会被视为安全风险。默认情况下，禁用该选项。

允许的公共文件夹数量最大值
如果您希望限制在设备上允许的“公共文件夹”的数量，请使用此项。在设置了限制时，该服务器遍历文件夹列表，直到达到这个限制为止，不会再将更多项目发送到设备。无法确保以何顺序处理这些文件夹。默认情况下未设置全局限制。

共享文件夹
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的共享文件夹[97]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的共享文件夹[623]。默认情况下允许搜索操作。

内容处理

内容处理选项

在被客户端标记时为邮件项目创建任务/提醒
该选项可以在客户端请求时，使 MDaemon 通过为各个已标记的邮件创建任务项目来向用户提醒已标记的项目。。默认情况下，此控件的全局选项处于启用状态。

在事件被修改时始终发送会议更新
某些客户端在修改会议时未正确发送会议更新电子邮件。这指示 ActiveSync 服务在组织者更新会议项目时发送会议更新。这仅能在客户端[388]和无法恰当发送会议更新的客户端类型[402]上设置，否则将导致发送重复的会议更新。因此，此选项仅在“客户端”和“客户端类型”的设置页面上可用。

对所有已发送邮件请求已读回执
如果您希望服务器为客户端发送的所有邮件请求已读确认，请启用此项。默认情况下，禁用该选项。

当邮件被标记为已读时，以及发件人请求时，从服务器发送已读回执
如果您希望服务器支持已读确认请求，并在客户端将邮件标记为已读时发送已读回执，

请启用此项。默认情况下，禁用该选项。

发送为在 ReplyTo 地址中指定的别名
某些客户端可能不允许发件人使用别名发送邮件。已在 Exchange ActiveSync (EAS) 协议 363 16.x 中添加该功能，不过一些客户端不支持 16.x。例如，Windows 版的 Outlook 仅使用 EAS 14.0，虽然它允许用户指定要发送的备用地址，但生成的邮件并不能正确反映用户的选择。该选项允许使用 ReplyTo (答复) 字段来发送电子邮件，只要 ReplyTo 地址是该用户的有效别名 699 即可。默认情况下启用这个全局选项。

虚拟地将公共联系人合并为默认联系人
如果您希望将设备上的公共联系人与用户的默认联系人合并在一起，请启用此项。这仅仅是一个虚拟合并，实际上未将它们复制到用户的联系人文件夹。这对不支持 "全局地址列表" (GAL) 搜索的客户端而言极其有用。默认情况下，禁用该选项。

在将邮件移入垃圾邮件文件夹时阻止发件人
启用后，当客户端将电子邮件移动到账户的垃圾邮件文件夹时，该服务将该电子邮件的发件人或从地址添加到阻止的发件人联系人文件夹。

在会议请求被接受/拒绝等时强制发送会议请求。
启用后，当客户端接受、拒绝或以其他方式选择响应会议请求的操作时，服务将向会议组织者发送会议响应。这是针对没有正确发送这些更新本身的特定客户端。

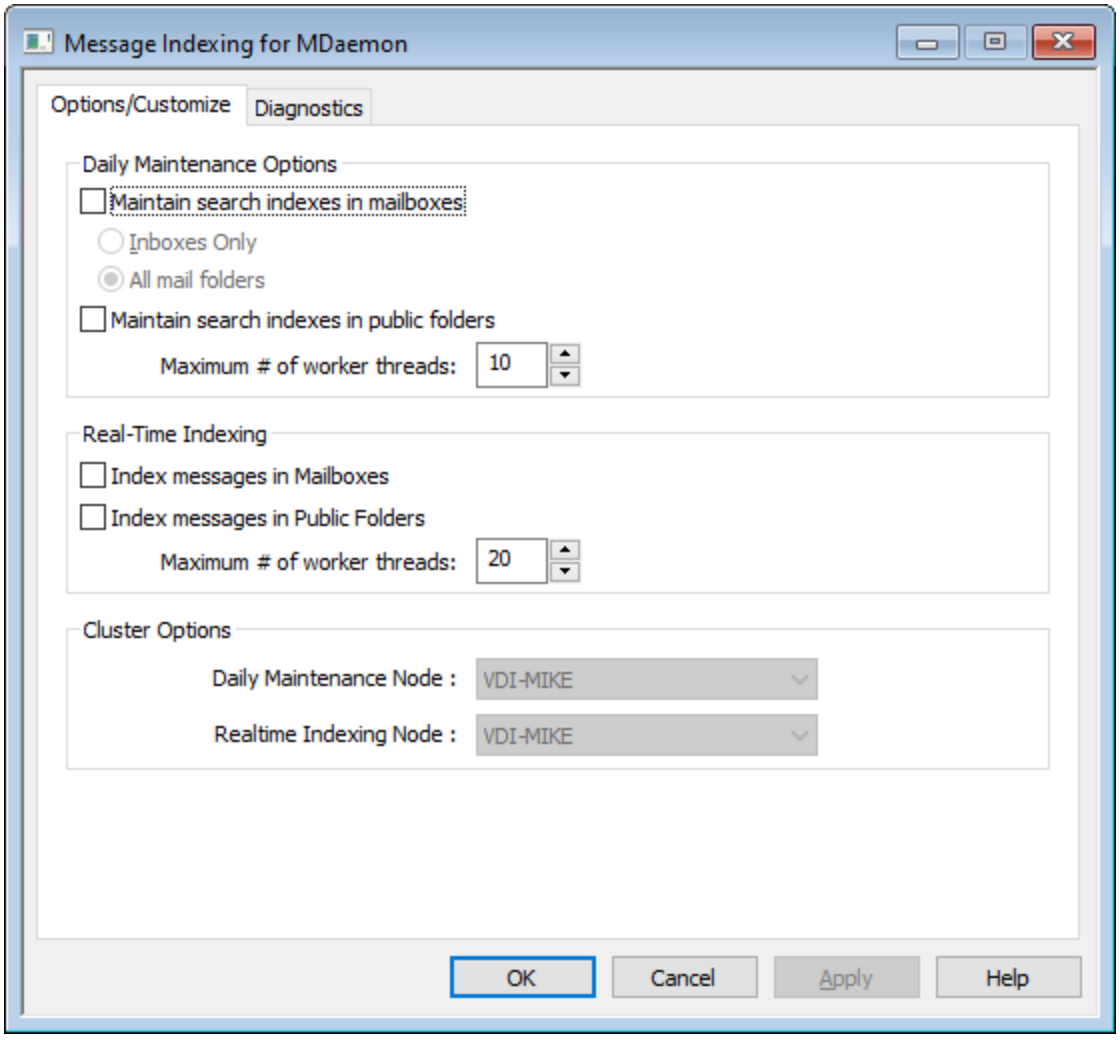
预览有效设置
该按钮在所有子 "客户端设置" 屏幕上可用 (例如域 365、账户 380 和客户端 388)。由于默认情况下，已将这些屏幕上的选项都设置成从父屏幕继承其设置，使用该功能来查看当前向显示的屏幕应用了什么设置。

还请参阅：

ActiveSync » 账户 380
ActiveSync » 客户端 388
ActiveSync » 安全 359

3.11 邮件索引

3.11.1 选项/定制



"邮件索引"对话框用于配置 Webmail、ActiveSync 和 Remote Administration 所使用的搜索索引的实时和夜间维护。

每日维护选项

此部分的选项控制夜间搜索索引。

维护邮箱中的搜索索引

如果您希望维护邮箱文件夹中的搜索索引，请选中此框。您可以选择仅对"收件箱"或所有邮件文件夹进行此操作。

维护公共文件夹中的搜索索引

如果您希望维护公共文件夹[258]中的搜索索引，请选中此项。您还能指定允许同时处理的最大线程数。

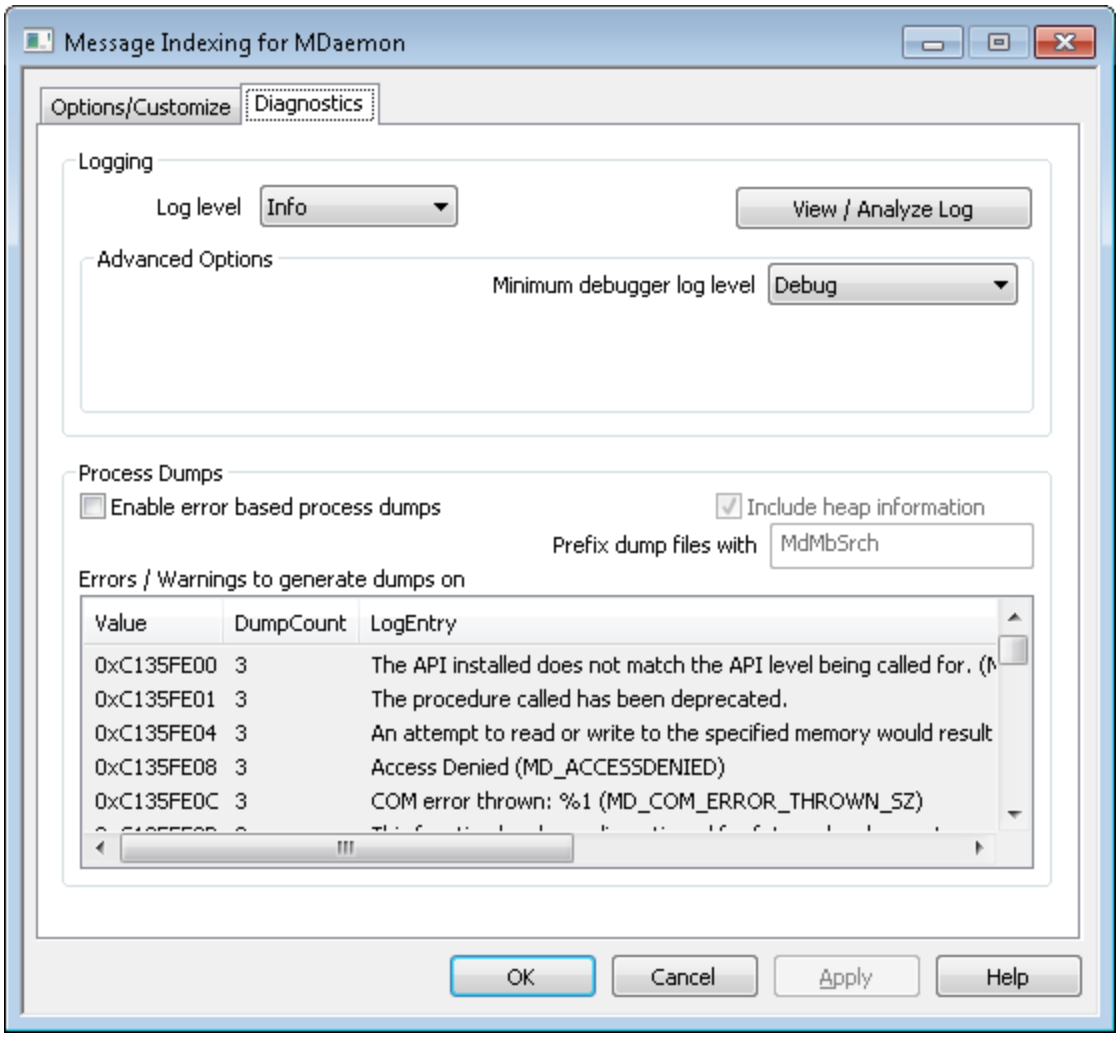
实时索引

索引邮箱中的邮件
如果您希望在邮箱中执行实时搜索索引，请启用此项，以便将搜索索引始终保持最新状态。

索引公共文件夹中的邮件
如果您希望对公共文件夹[258]进行实时搜索索引，请选中此框。

集群选项
如果使用“集群”，请使用这一部分的选项来指定专用于日常索引维护和实时索引的集群节点。

3.11.2 故障诊断



该屏幕包含高级选项，在大多数情况下，除非您尝试诊断“邮件索引”问题或寻求技术支持，否则不需要使用这些选项。

日志

日志级别

支持 6 种日志级别，将按记录的数据量由高到低进行说明：

调试 这是最丰富的日志级别。记录所有可用条目，通常仅在诊断问题或管理员需要详细信息时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

查看/分析日志文件

点击此按钮来打开 MDaemon 高级系统日志查看器。默认情况下，将日志保存在："..\MDaemon\Logs\"

高级选项

最小化调试器日志级别

这是发送至调试器的日志最小级别。可用的日志级别与上面概述的级别相同。

进程转储

启用基于进程转储的错误

如果您希望在发生您于下方指定的特定警告或错误时生成进程转储，请启用此项。

在转储中包含堆信息

默认情况下，在进程转储中包含堆信息。如果您不希望包含这个信息，请清除该复选框。

为转储文件使用前缀

进程转储文件名将使用这个文本开头。

出错/警告时生成转储

右键单击此区域并使用 *"添加/编辑/删除条目..."*选项来管理将触发进程转储的错误或警告列表。对于每个条目，您可以指定取消激活前进程转储数量。

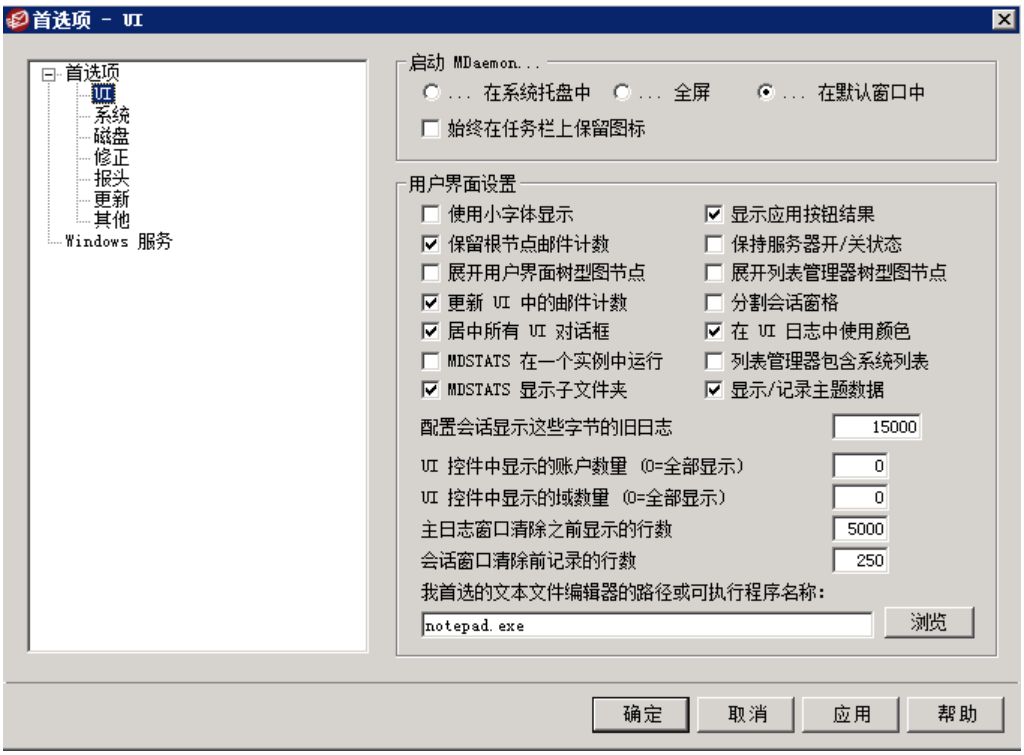
还请参阅：

动态屏蔽 » 选项/自定义 510

3.12 首选项

3.12.1 首选项

3.12.1.1 用户界面



启动 MDaemon...

...在系统托盘中
如果您不希望在启动时显示 MDaemon 的界面，请选择该选项。MDaemon 图标将仍旧在系统托盘显示。

...全屏
如果您希望在启动时将 MDaemon 的界面最大化，请选择该选项。

...在默认窗口中
如果您希望在启动时将 MDaemon 的界面显示在默认窗口中，请选择该选项。

始终在任务栏上保留图标
启用此选项时，MDaemon 将在启动时最小化到任务栏，但最小化时它将同时出现在任务栏和系统托盘中。如果您不希望 MDaemon 在最小化时，出现在任务栏中，清空此选项；那么只有托盘图标可见。

UI 设置

使用小的显示字体
在事件跟踪和会话窗口上，启用小字体。

显示应用按钮结果
默认情况下，每当您点击某一对话框上的“应用”按钮，会打开一个信息框以确认已保存您对此对话框设置所作的更改。如果您希望应用这些更改而不显示此消息，请取消勾选此框。

保留根节点邮件计数
如果您希望在服务器重启后保留根节点计数器，请启用该选项。根节点计数器会在统计窗格的“统计”部分中列出，其位于 MDaemon 的主 GUI。

保留服务器的开/关状态
如果启用此控件，MDaemon 将会确保其服务器（启用或者禁用）状态在重启后保持一致。

扩展 UI树节点
如果您希望自动展开各种对话框左侧窗格的导航树节点，请点击此选框。这不应用于“邮件列表管理器[223]”。如果您希望自动展开邮件列表的树型节点，请使用下方的“*展开列表管理器树型节点*”选项。

扩展列表管理器树节点
如果您希望自动展开左侧窗格中“邮件列表管理器[223]”的导航树型节点，请点击此勾选框。

更新 UI中的邮件计数
该选项控制是否 MDaemon 将检查在邮件队列中计算等待邮件的磁盘。

分割会话窗格
如果您希望将 MDaemon 主界面中的“会话”选项卡从其他选项卡拆分成您自己的窗格，请启用此项。更改这个设置，需要重启 MDaemon UI，Windows 菜单中用来切换窗格的选项也不再可用。

居中所有 UI对话框
默认情况下，所有对话框在打开时都位于屏幕中央，而不是彼此重叠。如果您希望对话框重叠，请清除此复选框，这有时可能会导致它们部分脱离屏幕或超出画面范围。

在 UI日志中使用彩色模式
此项将使 MDaemon 用户界面中若干事件跟踪和日志记录[59]选项卡上显示的文本成为彩色文本。默认情况下启用此项，更改其设置需要重启 MDaemon 界面才能使变更生效。请参阅：彩色会话日志[147]来获得更多信息。

列表管理器包含系统列表
如果您希望在“邮件列表管理器[223]”中显示由 MDaemon 系统生成的邮件列表（例如 Everyone@ 和 MasterEveryone@），请启用此项。系统生成的列表提供用来配置用户的有限项目。禁用此项时，将隐藏系统列表，不过仍然可以使用它。默认情况下，禁用该选项。

MDSTATS 在单实例中运行
如果您不希望一次运行多于一个的 MDaemon 队列和统计管理器[741]，请点击该选择框。当管理器已经在运行中，再尝试启用该管理器将会使得当前运行的实例变成活动窗口。

MDSTATS 显示子文件夹
如果您希望队列与统计管理器[741]显示在不同队列以及用户邮件目录中包含的子文件夹，请点击此选择框。

显示/记录主题数据
默认情况下，主题:行数据显示在 MDaemon UI 选项卡中，并写入日志文件。注意：主题:行可以包含发件人不希望显示的信息，以及不希望被记入日志文件中的信息，此外邮件列表还能具有用户放置在主题:行中的密码 。因此推荐禁用此项。

配置会话显示这些字节的旧日志
在运行一个配置会话时，这是将在事件跟踪和日志记录[59]选项卡中显示的日志数据最大值。默认设置是 15000 字节。

UI控件里显示的账户数 (0=显示所有)
这是将在各种对话框的下拉列表框中显示的最大数量的账户。此外，将该选项中的值设置为低于当前存在的账户数，"编辑账户"与 "删除账户"选项将不再出现在账户菜单上；您只能通过使用账户管理器[596]编辑与删除账户。在对此选项的任何更改生效前，您必须重启 MDaemon。此默认设置是 "0"，将显示所有账户。

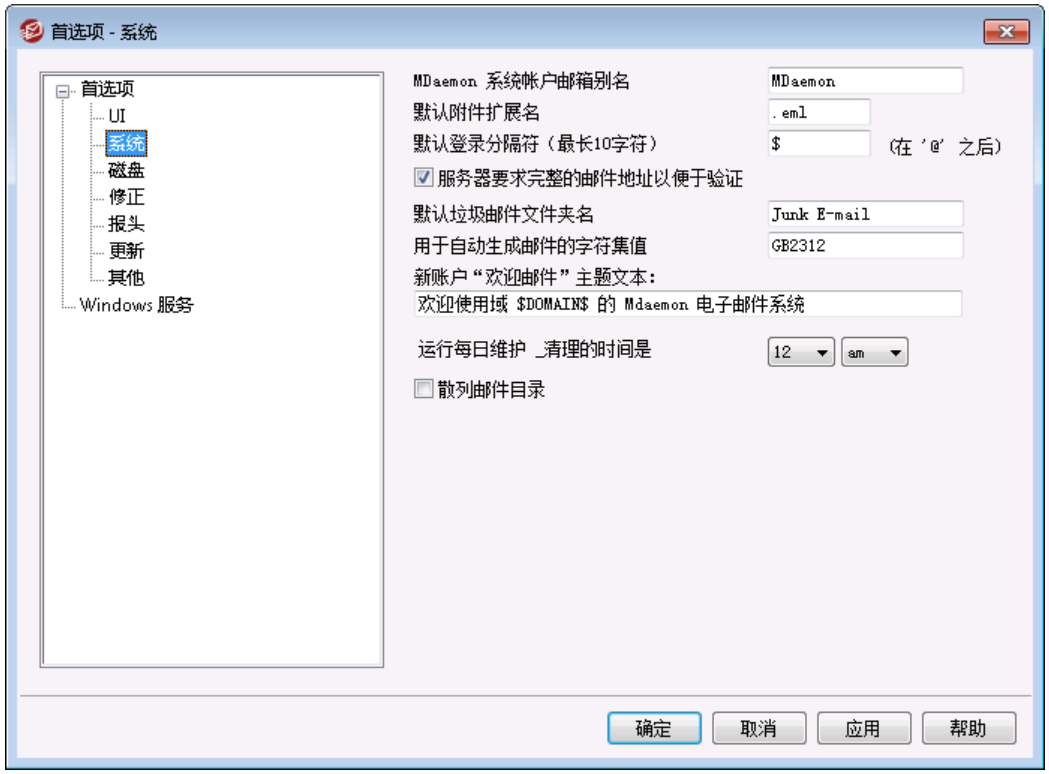
UI控件里显示的域数 (0=显示所有)
这是将在主 GUI 上显示的域的最大数目，不管实际存在多少域。更改完值之后，您必须重启 MDaemon 才更看见这些更改。此默认设置是 "0"，将显示所有域。

主日志窗口清除之前显示的行数
这是在主日志窗口中显示的行数最大值。达到这个行数时，将清空窗口。这并不影响日志文件；只是清除显示屏。

会话窗口清除前记录的行数
这是在每一个会话窗口[69]被清空前，将在其里面出现的行数最大值。这对日志文件没有任何影响。

我首选文本文件编辑器的路径或可执行名称
在需要时，Notepad.exe 是默认情况下 MDaemon UI 将启动的常规文本编辑器。如果您倾向于使用一个不同的文本编辑器，请在此处输入其文件路径或可执行名称。

3.12.1.2 系统



MDaemon 系统账户邮箱别名[地址]
这是系统生成的邮件所来自的电子邮件地址。订阅确认，投递状态通知 (DSN)邮件，各种其他通知邮件等都是系统邮件。

默认附件扩展名
系统生成的邮件将会以此扩展名被创建。这也将是系统生成邮件的附件的扩展名。例如，如果 MDaemon 生成一封关于指定邮件的警告邮件给 postmaster，它会将该值作为邮件的文件扩展名。

默认登录分隔符（最长10字符）
当使用一个电子邮件地址作为账号登录参数时，此字符或者字符串可以被用来作为 “@”的另一个选择。这对某些在登录字段不支持 “@”的邮件客户端的用户来说，可能非常必要。例如，如果您在此字段中使用 “$”，则用户可以使用 “user1@example.com”或者 “user1$example.com”来登录。

服务器要求完整的电子邮件进行验证
MDaemon 的 POP 和 IMAP 服务器要求您在登录到 MDaemon 时，默认情况下使用您的完整邮件地址。如果您希望仅将邮箱作为登录信息 (例如：以 “user1”取代 “user1@example.com”)，然后您可以禁用此选项，不过当 MDaemon 服务于多个域时，仅邮箱的登录信息会产生歧义。

默认垃圾邮件文件夹名
使用此文本框向 MDaemon 为您用户自动创建的垃圾邮件文件夹指定默认名。默认名是 “Junk E-mail”以匹配各种其他广泛分布的产品默认值。

用于自动生成邮件的字符集值
指定您希望用于自动生成邮件的字符集。默认设置是 iso-8859-1。

新账户"欢迎邮件"主题文本：
MDaemon 会典型地向新账户发送一封"欢迎邮件"。在此处指定的文本会作为邮件的"主题"报头显示。欢迎邮件从包含在 …\MDaemon\app\ 文件夹里的 NEWUSERHELP.DAT 文件创建，并且该主题报头可以包含任何在自动响应脚本 707 里允许的宏指令。

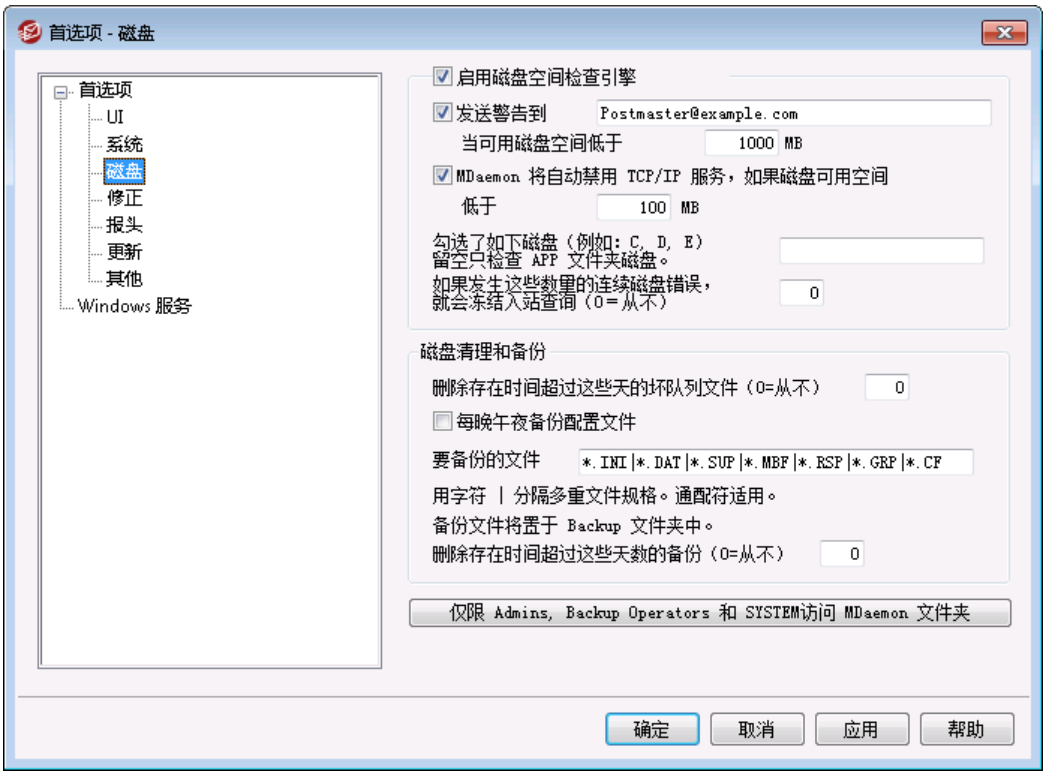
运行每日维护和清理的时间是 [1-12][上午/下午]
使用此项来设置每日维护和清理事件发生的时间。建议的默认设置是"午夜12点"。

无论您在此处如何设置这个选项，有一些每日事件始终在午夜发生（例如日志文件维护）并运行 midnight.bat。

在域或邮箱值发生变化时移动账户邮件文件夹
如果勾选此框，在您更改域名或邮箱时，会将受影响账户的邮件文件夹移动到新的位置。否则，MDaemon 将会继续使用旧邮件的文件夹名称。

散列邮件目录
如果您希望启用散列目录，请点击此选择框——MDaemon 将会通过拼凑最多 65 个子目录来散列某些目录。散列可以为某些高流量站点增加性能，但也可能轻微地降低常规 MDaemon 站点的性能。默认情况下，禁用该选项。

3.12.1.3 磁盘



启用磁盘空间检查引擎
如果您希望 MDaemon 监视 MDaemon.exe 所在驱动上的可用磁盘空间的大小，请激活该选择框。

发送警告到 [用户或者地址] 当磁盘可用空间低于 [xx] MB
通过使用此选项，在磁盘空间下降到某一个级别值时，您可以配置 MDaemon 向您选择的用户或地址发送一封通知邮件。默认值是 1000 MB。

MDaemon 将自动禁用 TCP/IP 服务，如果磁盘可用空间低于 [xx] MB
在磁盘空间下降到某一个级别值时，如果您希望 MDaemon 禁用 TCP/IP 服务，启用此功能。默认值是 100 MB。

以检查如下磁盘 (例如：C、D、E)
如果您希望监控多个磁盘上的可用磁盘空间，请指定每个磁盘的磁盘字母。如果您将其留空，那么只会勾选包含 MDaemon\app\ 文件夹的磁盘。

如果出现这些数量的连续磁盘错误，则冻结进站队列 (0 = 无)
在处理进站队列时如果发生这一数量的磁盘错误，MDaemon 会停止处理该队列直至您解决这一情况。当出现队列关闭时，在邮件管理员邮件箱中会放入一封邮件。

磁盘清理和备份

删除存在时间大于这些天的坏队列文件 (0=从不)
如果您希望在旧文件的存在时间大于指定天数时，让 MDaemon 从坏邮件队列中删除这些旧文件，请使用此项。如果您不希望自动删除这些邮件，请在此项中使用 "0"。

每晚午夜备份配置文件
如果您希望每晚午夜，归档所有 MDaemon 配置文件到备份目录，点击此选择框。

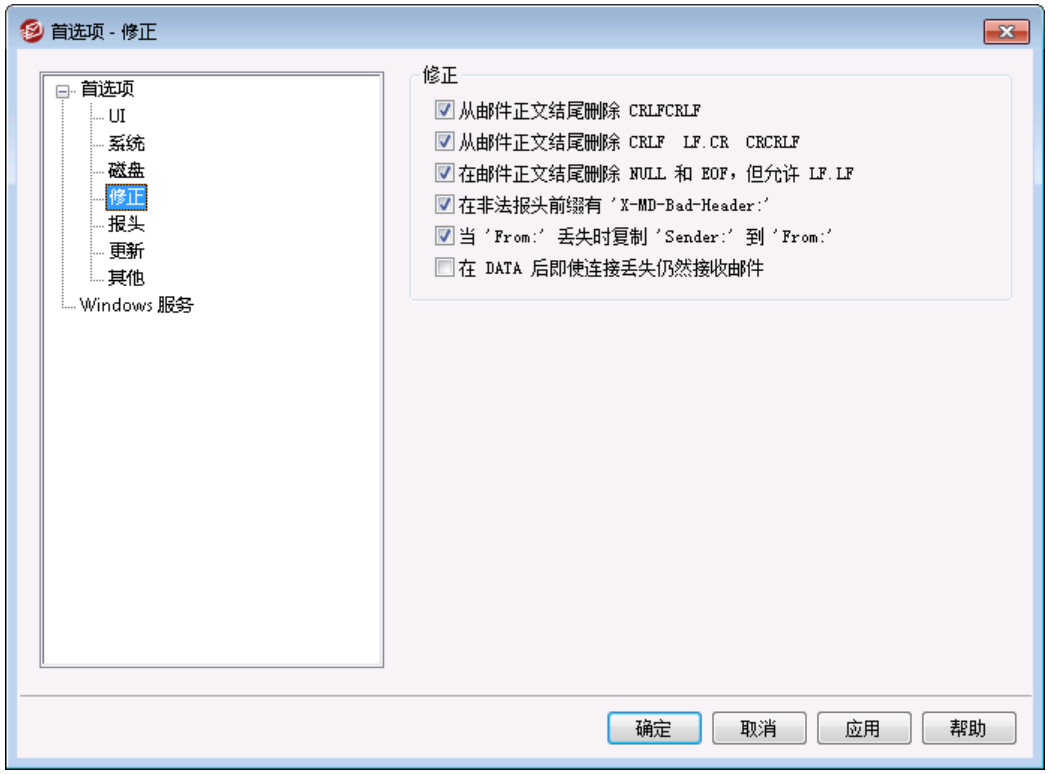
要备份的文件
使用此文本框精确地指定要备份的文件和文件扩展名。可以使用通配符，并且每一个文件或者扩展名必须使用 "|" 字符分隔。

删除存在时间大于这些天的备份 (0=从不)
如果您希望自动删除旧的备份文件，则使用此项。会将删除超过指定天数的旧文件这个操作作为每日夜间清理事件的一部分执行。默认设置是 "0"，表示不删除任何旧的备份文件。

将 MDaemon 文件夹访问限制为管理员、备份操作员和系统

点击此按钮将限制 \MDaemon\ 的根目录机器子目录访问以下 Windows 账户/群组：管理员、备份操作员和系统。

3.12.1.4 修复



从邮件正文结尾删除 CRLFCRLF
某些邮件客户端在显示邮件时会发生问题，结尾会出现连贯的回车与换行（比如 CRLFCRLF）。勾选该选框时，MDaemon 将会从邮件正文结尾剥除连贯的 CRLFCRLF 顺序。默认情况下启用此项。

从邮件正文结尾删除 CRLF LF.CR CRCRLF
默认情况下，MDaemon 会从邮件结尾删除该顺序，因为它会使某些邮件客户端发生问题。如果您不希望从邮件删除该顺序，请不要勾选该选择框。

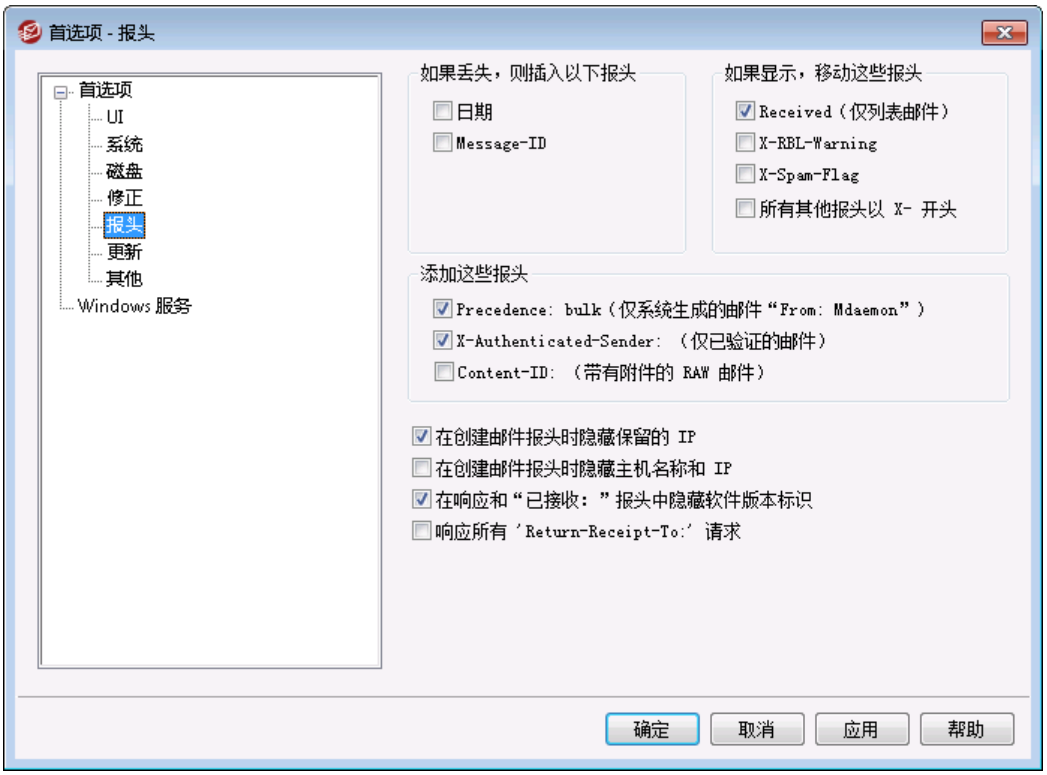
在邮件正文结尾删除 NULL 和 EOF，但允许 LF.LF
勾选该复选框时，MDaemon 会从邮件正文删除 Null 与 EOF 字符串，但它允许邮件以 LF.LF 与 CRLF.CRLF 顺序结尾。默认情况下启用此项。

在非法报头前缀有 "X-MD-Bad-Header:"
启用该选项时且 MDaemon 遇到一个坏的邮件报头，它就会以 "X-MD-Bad-Header:"为坏报头加上前缀。默认情况下启用此项。

复制 "Sender:"到 "From:"，当 'From:'缺失时
一些邮件客户端在您编辑一封邮件的时候，无法创建 FROM: 报头。而将 FROM: 报头的信息置于 Sender: 报头。）这将使一些邮件服务器以及您邮件的收件人发生问题。为了防范这些问题，MDaemon 在检查该复选框时将使用 Sender: 报头的内容创建缺失的 FROM: 报头。默认情况下启用此项。

如果在 DATA 后丢失连接仍然接收邮件
启用该选项后，在 SMTP 进程中即使 DATA 过程中或 DATA 完成后立即出现连接中止，MDaemon 仍会接收并投递邮件。在常规情况下不应使用，因为这样做会生成邮件副本。

3.12.1.5 报头



如果丢失，插入这些报头

日期
启用该选项时，当 MDaemon 遇到一封没有 "Date:"报头的邮件，它将创建一个并将其添加到邮件文件。它将是 MDaemon 首次收到邮件的日期，不是由发件人创建它的日期。有一些邮件客户端不能创建此报头，并且由于一些邮件服务器拒绝允许此类邮件，此功能将会使它们进行投递。

Message-ID
当 MDaemon 遇到一封没有 "Message-ID"报头的邮件时，它将创建一个并将其插入到邮件中。

如果显示，删除这些报头

Received（仅列表邮件）
如果您希望从邮件列表邮件中剔除所有现有的 "Received:"报头，请勾选该选项。

X-RBL-Warning
如果您希望剔除所有在邮件中发现的 "X-RBL-Warning:" 报头，请点击此选择框。默认情况下，禁用该选项。

X-Spam-Flag
如果您希望从邮件中剔除旧的 "X-Spam-Flag:" 报头，请启用该选项。

所有以 X- 开头的其他报头
MDaemon 和其他邮件服务器使用许多服务器指定的报头叫做 X-Type 报头以路由邮件并执行各种其他功能。启用该选项时，MDaemon 将从邮件剔除这些报头。**请注意：** 该选项不会删除 "X-RBL-Warning" 报头。如果您希望删除这些报头，请使用上方的 *"X-RBL-Warning"* 选项。

添加这些报头

Precedence: bulk（仅系统生成的邮件，发件人是 MDaemon）
勾选该选框时，所有由系统产生（即来自 MDaemon）的邮件（欢迎邮件、警告、"无法投递" 邮件等等）都会插入一个 "Precedence: bulk" 报头。

X-Authenticated-Sender:（仅已验证的邮件）
默认情况下，MDaemon 将添加 "X-Authenticated-Sender:" 报头到使用 AUTH 命令抵达被验证会话的邮件。如果您不希望添加该报头，请不要勾选该选择框。

Content-ID:（带有附件的 RAW 邮件）
如果您希望添加唯一的 MIME Content-ID 报头到 MDaemon 从包含附件的 RAW 文件创建的邮件，请勾选该选择框。

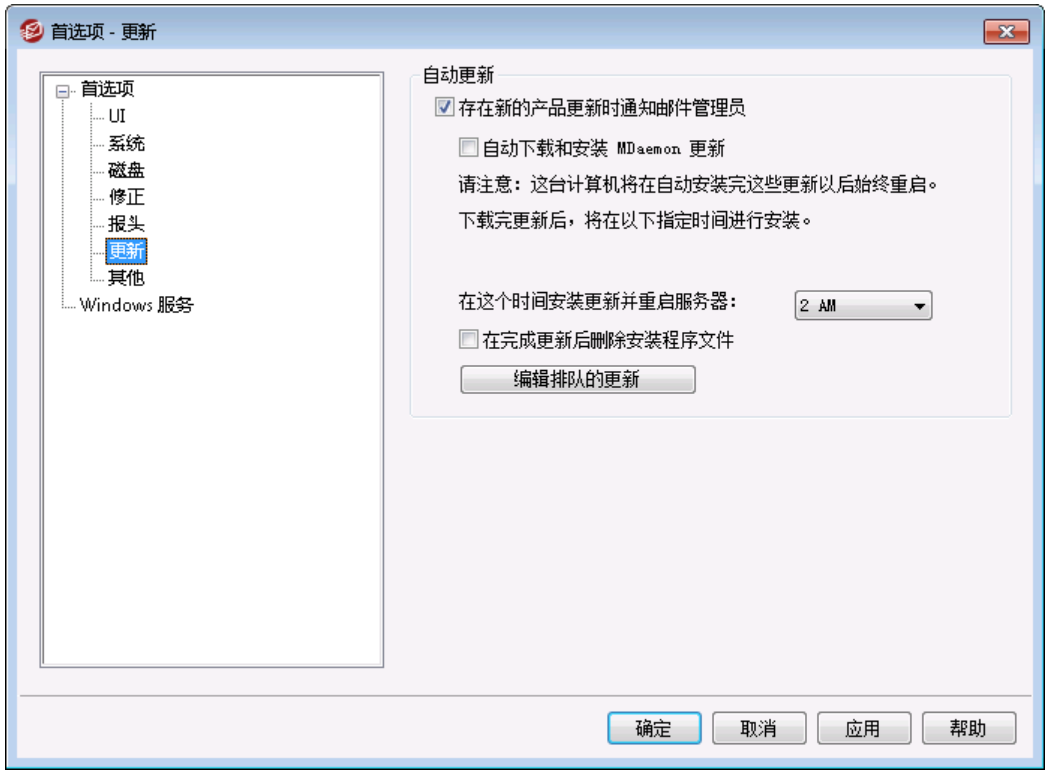
在创建邮件报头时隐藏保留的 IP"。
默认情况下启用此项来防止在 MDaemon 创建的某些邮件报头中出现保留的 IP 地址。保留的 IP 地址包括：127.0.0.*、192.168.*.*、10.*.*.* 和 172.16.0.0/12。如果您也希望在报头中隐藏您的域 IP（包括 LAN 域），您可以在 MDaemon 的 "app\MDaemon.ini" 文件中手动设置以下开关：[Special] HideMyIPs=Yes（默认值是 No）。

创建邮件标题时隐藏主机名和 IP
如果您希望从 "Received:" 中省略主机名和 IP 地址，请点击此选项。默认情况下，禁用该选项。

在响应和 "Received:" 报头中隐藏软件版本标识
如果您希望防止 MDaemon 在创建 "Received（已接收）" 报头或响应各种协议请求时说明其软件版本和其他标识信息，请使用此项。默认情况下，禁用该选项。

响应所有 "Return-Receipt-To:" 请求
如果您希望允许来自接收邮件的投递确认请求，并自动向发件人发送一封确认邮件，请点击此复选框。默认情况下，禁用该选项。

3.12.1.6 更新



自动更新

使用 "自动更新"功能，您可以配置 MDaemon，以便每当更新可用于 MDaemon 时通知邮件管理员，并且可以将其设置为自动下载并安装更新。每当自动安装更新时，服务器将始终重新启动。在检测到更新时下载文件，不过将在您指定的时间进行安装和重启。将在 MDaemon 系统日志中记录所有安装活动，并在更新后通知邮件管理员。

存在新的产品更新时通知邮件管理员
存在 MDaemon 可用更新时，此项使 MDaemon 通知邮件管理员。默认启用此项。

> 在将 MDaemon 设置成自动更新时，不会发送此邮件。而是通知邮件管理员已安装了更新，并告知有关更新的任何特殊注意事项。

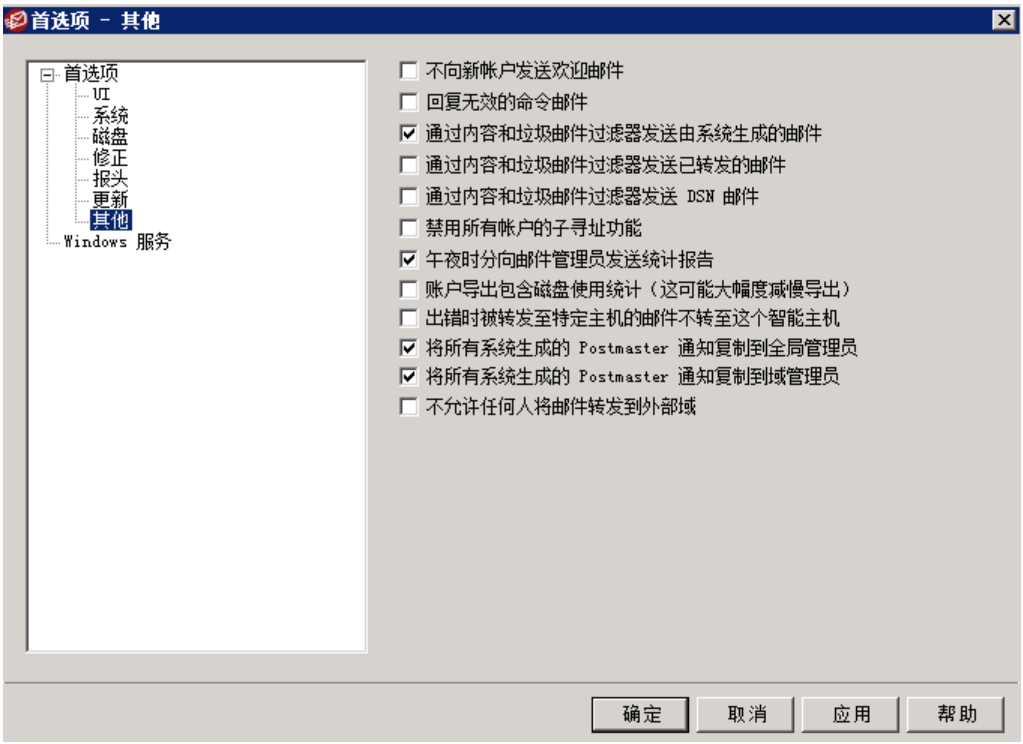
自动下载和安装 MDaemon 更新
如果您希望自动下载和安装 MDaemon 更新，请勾选此框。在检测到更新时将下载这些更新，并在下方指定的时间进行安装。默认情况下，禁用该选项。

在这个时间安装更新并重启服务器。
在检测到更新时将自动下载这些更新并将其保存在 \MDaemon\Updates 文件夹中，不过只在此处指定的时间进行安装。每次更新后将自动重启安装了 MDaemon 的服务器。默认情况下将此项设置成 2 AM。

更新完毕后删除安装程序文件
如果您希望在完成更新后删除保存的安装程序文件，请勾选此框。

编辑排队的更新
在检测和下载到更新时进行排队以便稍后安装。会将待更新列表保存在 QueuedUpdates.dat 文件中。点击这个按钮来审核列表或删除排队的更新。

3.12.1.7 其他选项



不向新账户发送欢迎邮件
默认情况下，在创建新账户时，MDaemon 会根据 NEWUSERHELP.DAT 文件生成欢迎邮件并将其分发给新用户。如果您希望阻止邮件生成，启用此控件。

向无效命令邮件发送响应
默认情况下，当有人向系统账户发送不含有效命令的邮件时，MDaemon 使用 "未找到有效命令"邮件不做响应。如果您希望向这些邮件发送响应，请启用此项。

系统生成的邮件已通过内容和垃圾邮件过滤器发送
默认情况下，会通过 "内容过滤器"和 "垃圾邮件过滤器"处理系统生成的邮件。如果您希望从内容过滤和垃圾邮件过滤中排除这些邮件，请清除该选择框。

DSN 邮件已通过内容和垃圾邮件过滤器发送
如果您希望通过“内容过滤器”或“垃圾邮件过滤器”处理转发的邮件，请勾选此框。默认情况下，禁用该选项。

DSN 邮件已通过内容和垃圾邮件过滤器发送
如果您希望通过内容和垃圾邮件过滤器发送 DSN 邮件[738]，请启用此项。默认情况下，禁用该选项。

禁用所有账户的子寻址功能
如果您希望全局禁用子寻址功能，请点击此选项。所有账户都不被允许子寻址，无论个别用户是如何设置的。要了解子寻址的更多详情，请参阅“账户编辑器”上的 IMAP 过滤器[617]屏幕。

午夜时分向邮件管理员发送统计报告
默认情况下，每晚半夜发送一份统计报告到邮件管理员。如果您不希望发送该报告，请清除此选择框。该选项与位于 MDaemon 主界面上的“统计[59]”选项卡相对应。

账户导出包括磁盘使用统计（这会大幅度减慢导出）
默认情况下，账户导出不包含磁盘文件计数和占用的空间信息。如果您希望在导出中包含这些信息，请启用此勾选框。不过这会大幅度减慢导出速度。

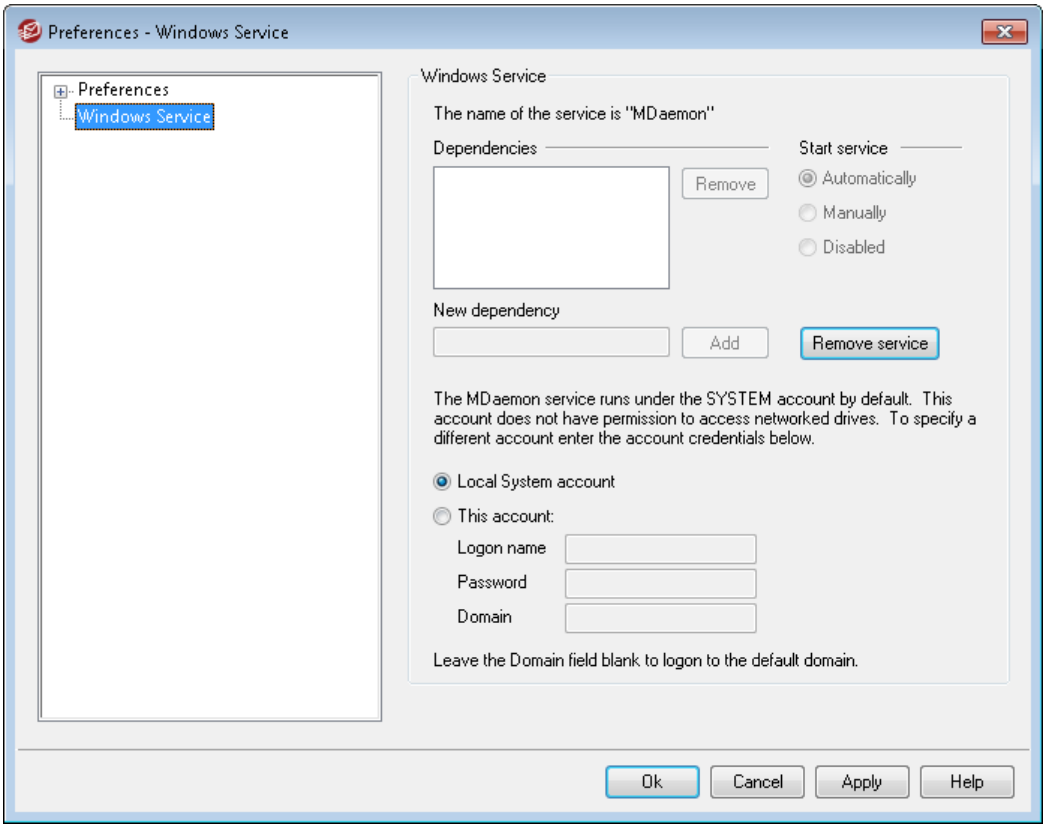
转发至特定主机的邮件不在遇到错误时前往智能主机
使用“账户编辑器”中“转发[610]”屏幕上的“高级转发设置”，可以将账户设置成将邮件转发至特定的智能主机，而不是使用 MDaemon 标准的投递流程。默认情况下，在 MDaemon 尝试转发这些邮件时遇到投递错误的情况下，会将该邮件置于坏邮件队列。如果您希望 MDaemon 使用常规的投递流程，将此邮件放入“重试队列[732]”做进一步投递尝试，请启用此项。

将所有系统生成的邮件管理员通知复制到全局管理员
默认情况下，发送给邮件管理员的系统生成的通知也将发送给全局管理员[636]。全局管理员会收到所有信息，包括队列摘要报告、统计信息报告、发行说明、（对于所有域而言）找到的“没有此类用户”、磁盘错误通知、账户冻结和禁用通知（与域管理员一样，他们可以取消冻结并重新启用）、有关许可证和测试版本即将到期的警告、“垃圾邮件摘要”报告等。如果您不希望全局管理员接收这些通知，请禁用此设置。

将所有系统生成的邮件管理员通知复制到域管理员
默认情况下，发送给邮件管理员的系统生成的通知也将发送给域管理员[636]。但是，域管理员被限制为仅接收属于其域的那些电子邮件。如果您不希望域管理员接收这些通知，请禁用此设置。

不允许任何人将邮件转发到外部域
如果您不允许账户将邮件转发到外域，请勾选此框。如果用户为其账户配置邮件转发，来将其发送到外域，则忽略远程转发地址。此设置仅适用于为账户使用邮件转发选项进行转发的邮件。此设置仅适用于为账户使用邮件转发选项[610]进行转发的邮件。

3.12.2 Windows 服务



Windows 服务

当 MDaemon 作为系统服务运行时，服务名称为 "MDaemon"。

相关性

使用该选项可指定在 MDaemon 服务启动**前**必须运行的服务。

启动服务

这是服务的初始状态：自动启动、必须手动启动或禁用。

安装/删除服务

点击该按钮可安装或删除 MDaemon 服务。

网络资源访问

当 MDaemon 作为 Windows 服务运行时，它默认在 SYSTEM 账户下运行。由于此账户不能访问网络设备，因此如果要将邮件存储在 LAN 内部的其他计算机上，MDaemon 将无法访问该邮件。更确切的说，除非您能提供某个账户的登录凭证，使得 MDaemon 服务能访问网络共享。如有必要，可创建 Windows 用户账户，专门用于使 MDaemon 在所需限制条件下运行，但该账户可访问 MDaemon 需要使用的网络共享资源。不仅如此，由 MDaemon 启动的所有应用程序将使用相同的凭证。

登录名

这是 Winodws 账户的登录名，MDaemon 服务应在此账户下运行。

密码
这是 Windows 账户的密码。

域
这是账户所在的 Windows 域。该字段留空可登录到默认域。

章节

4

4 安全菜单

MDaemon 配备有一套完善的安全功能和控件。点击 MDaemon 菜单栏上的安全按钮，可访问以下安全功能：

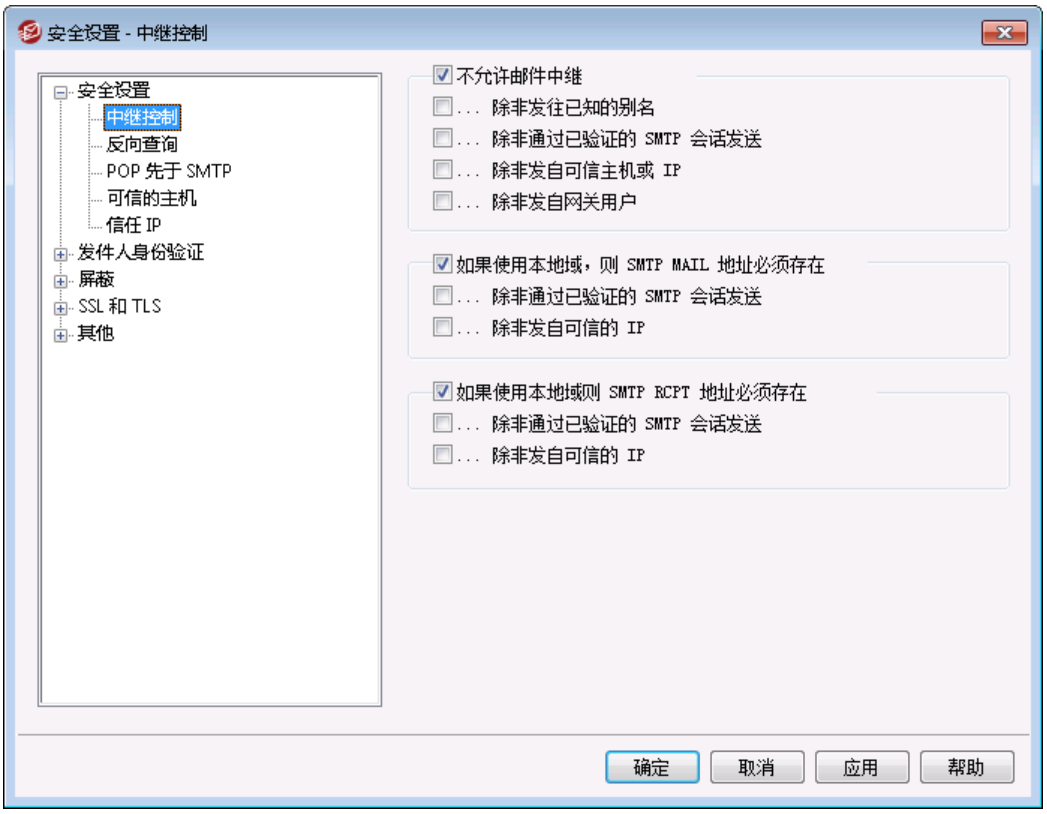
- **AntiVirus** 539 — MDaemon AntiVirus 通过为 MDaemon 用户提供最高级别的集成保护可帮助您阻止以电子邮件为载体的计算机病毒。它将捕获、隔离、修复和/或删除发现含有病毒的任何电子邮件。AntiVirus 还包含被称为 "爆发保护"的功能，可用来保护您免遭某些垃圾邮件、网络钓鱼和病毒爆发的侵害，这些攻击有时会躲过其他基于内容和特征的传统安全措施的监测。
- 内容过滤器 540——一个高度灵活且完全多进程的内容过滤系统使您能基于入站和出站邮件的内容定制服务器的行为。您可插入和删除邮件报头，添加邮件页脚，删除附件，将副本路由到其他用户，向某人发送即时消息，运行其它程序等等。
- 垃圾邮件过滤器 564 — 使用垃圾邮件过滤技术，以启发式方法来检查电子邮件，从而计算 "得分"。该分数用来确定邮件为垃圾邮件的可能性。基于该确定结果，服务器随后可执行某些操作，如拒收或标记邮件。另请参阅：垃圾邮件陷阱 592
- DNS 阻止列表 586 —允许您指定若干个 DNS 阻止列表服务，每次有人试图发送邮件到您的服务器时，都将对该邮件进行安全性检查。如果连接 IP 已被这些主机列入阻止列表，则拒收该邮件。
- 中继控制 428——用来控制当到达邮件服务器的邮件并非由本地地址所收发时，MDaemon 将采取的操作。
- IP 防护 436——如果在此列表中指定的域名试图连接到服务器，其 IP 地址必须与已指派给它的相匹配。
- 反向查询 430——MDaemon 可查询 DNS 服务器以检验在入站邮件中上报的域名和地址的有效性。该屏幕上的控件可用于拒绝可疑邮件或向其插入特殊报头。在 MDaemon 日志中也会报告反向查询数据。
- POP 先于 SMTP 433——该屏幕上的控件用来要求每个用户在被允许发送邮件到 MDaemon 之前必须首先访问其邮箱，这样就验证了用户是有效账户持有人并可使用该邮件系统。
- 可信主机 434——被视为 "中继控制"屏幕上所列中继规则的例外情况的域名和 IP 地址。
- SMTP 身份验证 438——用来设置多个选项，以指示当向 MDaemon 发送邮件的用户已经或尚未通过身份验证时，MDaemon 将如何操作。
- **SPF** 440 — 大多数域都发布 MX 记录来标识可接收邮件的计算机，但这并未标识允许发送邮件的位置。使用 "发件人策略框架"(SPF)，域还可发布 "反向 MX"记录以标识被授权发送邮件的位置。
- 域名密钥标识邮件 442 — 域名密钥标识邮件 (DKIM) 是一种可用来防止欺诈的邮件验证系统。它还可用来确保入站邮件的完整性，以保证邮件从离开发件人的邮件服务器直到抵达您的服务器中间未被篡改。这可通过使用加密的公钥/私钥配对系统来实现。出站邮件用私钥进行签名，而入站邮件通过使用发件人 DNS 服务器上发布的公钥测试其签名来进行验证。
- 证书 460—— "邮件证书"指的是一个实体担保或 "证明"另一个实体的良好邮件传输品行。 "证书"功能非常有用，因为它有助于确保邮件将不会错误地或不必要地经受不当的垃圾邮件过滤器的分析。它还有助于降低处理每封邮件所需的资源。

- 发件人阻止列表[466] — 不允许所列地址发送邮件到服务器。
- IP 屏蔽[468]——用来指定允许或拒绝连接到服务器的 IP 地址。
- 主机屏蔽[470]——用来指定允许或拒绝连接到服务器的主机 (域名)。
- 动态屏蔽[510] — 使用 "动态屏蔽",MDaemon 可以追踪入站连接的行为来识别可疑的活动并作出相应的响应。您可以阻止 IP 地址[513](或地址范围)进行连接,如果这些地址达到指定的验证失败次数。您也可以在账户太快达到验证失败次数时冻结账户[513]。
- SSL 和 TLS[479] — MDaemon 支持用于 SMTP、POP、IMAP 以及 Webmail网络服务器的安全套接字层 (SSL)协议。SSL 是保护服务器/客户端 Internet 通信安全的标准方案。
- 反向散射保护[498]—— "反向散射"指的是用户收到对其从未发送过的邮件的响应邮件。当垃圾邮件或病毒发送的邮件中包含伪造的 "返回路径"地址时就会发生反向散射。反向散射保护使用私钥散列方法生成并插入特殊的时间敏感代码到用户外发邮件的 "返回路径"地址中,以确保只向账户投递合法的投递状态通知和自动应答,从而有助于防止发生这种情况。
- 带宽节流[500]——带宽节流功能使您能控制 MDaemon 占用消耗的带宽。您可以控制会话或服务的进展速率,按域 (包括域和域网关)为 MDaemon 提供的每个主要服务设置不同的速率。
- 缓送[503]——一旦从邮件发件人处收到指定数量的 RCPT 命令,您可有意延迟连接。这是为了阻止垃圾邮件制造者试图向您发送未经请求的群发电子邮件。该技术背后的设想是如果垃圾邮件制造者向您发送每封邮件都需要花费相当长的时间,这将迫使他们以后不再重复同样的操作。
- 灰名单[505]——灰名单是一种抵御垃圾邮件的技术,它利用了 SMTP 服务器会重试投递任何收到暂时 (即 "稍后重试")错误代码的邮件这一特性。通过这项技术,当邮件来自未列入允许列表或先前未知的发件人时,其发件人、收件人和发件服务器的 IP 地址会被记入日志,然后在 SMTP 会话期间将由灰名单以暂时错误代码拒绝该邮件。几分钟以后,当合法服务器试图再次投递该邮件时,它们将被接受。因为垃圾邮件制造者通常不会进一步尝试投递,灰名单有助于显著减少用户收到的垃圾邮件数量。
- LAN IP 地址[508]——使用该屏幕列出 LAN (局域网)上的 IP 地址。为了带宽节流的目的,这些 IP 地址被视作本地通信地址,并可免除其他各种安全和垃圾邮件防范限制。
- 站点策略[509] — 用来创建站点策略,并在每个 SMTP 邮件会话开始时,将其传输到发送服务器。常用站点策略的一个范例是 "该服务器不支持中继"。

4.1 安全管理器

4.1.1 安全设置

4.1.1.1 中继控制



使用位于 "安全» 安全设置» 中继控制"页面的 "中继控制"可定义服务器如何响应邮件中继。当抵达邮件服务器的邮件既非来自也非发往本地地址，则要求此服务器代表另一台服务器中继（即投递）该邮件。如果您不想让服务器为未知用户中继邮件，则可使用此处所提供的设置进行控制。

> 不加选择地为其他服务器中继电子邮件可能会导致您的域被一个或多个 DNS-BL 服务 586 列入阻止列表。开放式中继极不可取，因为垃圾邮件制造者会利用开放式服务器来隐藏其踪迹。

邮件中继

不允许邮件中继
当启用该选项时，MDaemon 将拒绝接收和投递发件人和收件人皆非本地用户的邮件。

...除非发往已知别名
如果您想让 MDaemon 中继发往 "别名 699"的邮件而不去考虑 "中继"设置，请点击该复选框。

...除非通过已验证的 SMTP 会话发送
当启用该复选框时，MDaemon 始终会中继通过经身份验证的 SMTP 会话发送的邮件。

...除非发自可信主机或 IP
如果希望允许中继来自可靠主机或可靠 IP 地址的邮件，请启用该选项。

...除非发自网关用户
如果您希望 MDaemon 允许通过域网关中继邮件而不去考虑 "中继"设置，请启用该复选框。默认禁用该功能且不推荐使用。

账户验证

如果使用本地域，SMTP MAIL 地址必须存在
如果您希望当邮件声称来自本地域或网关时验证在 SMTP 过程中传递的 MAIL 值是否指向一个真实有效的账户，请点击该选项。

...除非通过已验证的 SMTP 会话发送
如果您希望当邮件通过经身份验证的 SMTP 邮件会话发送时，为该邮件免除 "*SMTP MAIL 地址必须存在...*"选项，请点击该选项。

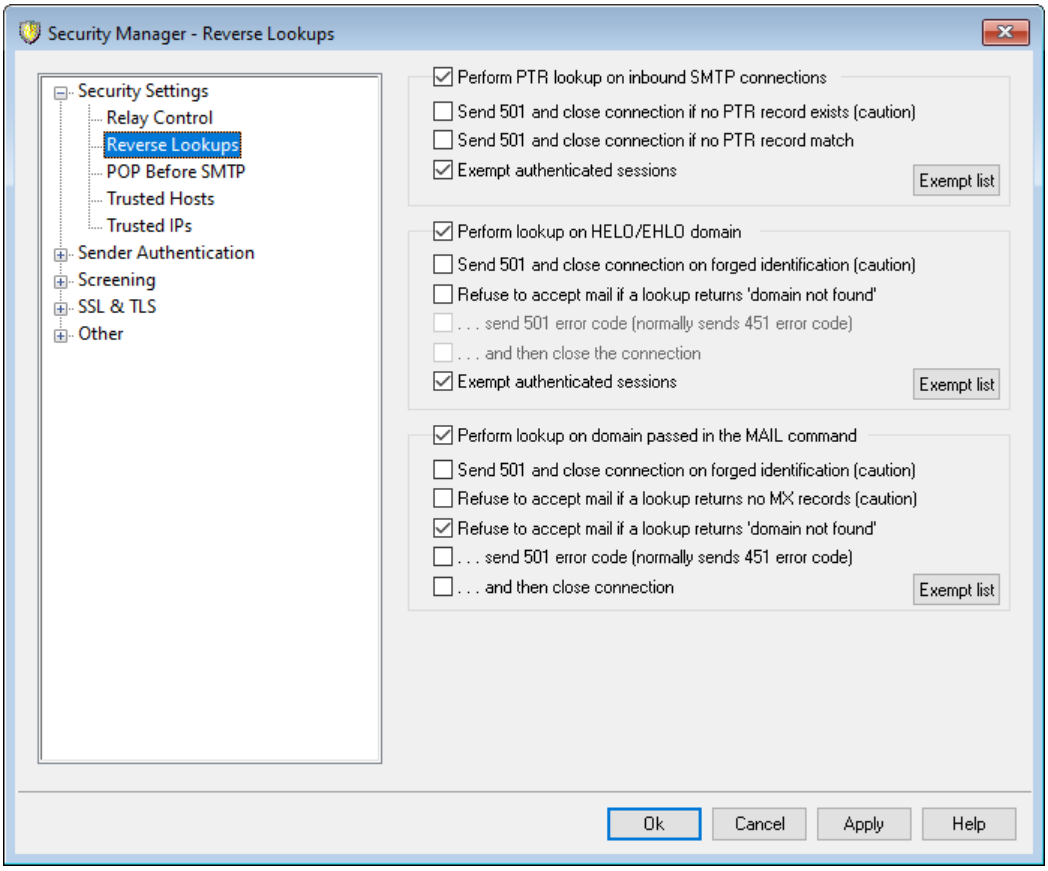
...除非发自可信主机或 IP
如果您希望为发自可信 IP 地址的邮件免除 "*SMTP MAIL 地址必须存在...*"选项，请点击该选项。

如果使用本地域，则 SMTP RCPT 地址必须存在
如果您希望当邮件声称来自本地域时验证在 SMTP 过程中传递的 RCPT 值是否指向一个真实有效的账户，请点击该选项。

...除非通过已验证的 SMTP 会话发送
如果希望当邮件通过经身份验证的 SMTP 邮件会话发送时，为该邮件免除 "*SMTP RCPT 地址必须存在...*"选项，请点击该选项。

...除非发自可信主机或 IP
如果您希望为发自可信 IP 地址的邮件免除 "*SMTP RCPT 地址必须存在...*"选项，请点击该选项。

4.1.1.2 反向查询



使用该屏幕上的选项，MDaemon 可配置为反向查询在 "HELO/EHLO"和 "MAIL"命令中通过的域。执行反向查询时，Mdaemon 将尝试获取指定域的所有 MX 和 A 记录 IP 地址。然后，将建立连接的服务器 IP 地址与该列表进行比较，力图确定发件人使用的是否是伪造的身份。

您还可反向查询入站 IP 地址的点式记录 (PTR)。使用该选项时，如果入站 IP 地址不匹配任何 PTR 记录，则可中止连接或向邮件中插入警告报头。

最后，业内达成共识，如果邮件来源使用不存在的域来标识自身，那么是否接受该邮件应是可选的。因此，提供一个选项使您能在反向查询过程从 DNS 服务器返回 "未找到域"消息时拒绝邮件。在这种情况下，Mdaemon 将返回 "451"错误代码，拒绝接收邮件，然后允许 SMTP 会话继续进行。然而，如果您希望返回 "501"错误代码，关闭套接字连接，或两样都做，则相应提供有其他选项。

可信 IP 地址和本地主机 (127.0.0.1)始终免于反向查询。

对入站 SMTP 连接执行 PTR 查询
如果希望 Mdaemon 对所有入站 SMTP 连接执行 PTR 查询，请启用该选项。

...如果不存在 PTR 记录，则发送 501 并关闭连接 (慎用)
如果选中该复选框，当该域不存在 PTR 记录时，MDaemon 将发送 "501"错误代码 (参数或变量中句法错误)并关闭连接。

…如果没有匹配的 PTR 记录，则发送 501 并关闭连接
如果选中该复选框，当 PTR 查询结果不匹配时，MDaemon 将发送 "501"错误代码 (参数或变量中句法错误)并关闭连接。

免除验证的会话
如果希望推迟对入站 SMTP 连接的 PTR 查询直至 SMTP MAIL 命令之后，以便查看该连接是否使用身份验证，请点击该选项。

豁免列表
点击此按钮来打开 "PTR 查询"豁免列表，在该列表上您可以指定将不受 PTR 反向查找的 IP 地址。

在 HELO/EHLO 域上执行查询
如果希望对在 "HELO/EHLO"会话阶段报告的域名执行查询，请点击该复选框。客户端 (发送机)使用 "HELO/EHLO"命令来向服务器标识自己。服务器使用客户端在该命令中上传的域名来填充 "已接收"报头中的 "发件人"部分。

...发送 501 并在伪造标识上关闭连接 (警告)
如果希望当查询结果显示为伪造的标识时，发送 501 错误代码然后关闭连接，请点击该复选框。

当反向查询的结果表明服务器正在使用一个伪造的标识时，该结果可能经常不正确。邮件服务器使用不匹配其 IP 地址的值来标识自己很常见。这是由 ISP 限制与约束以及其他合法理由造成的。所以请慎用该选项。使用该选项可能会导致您的服务器拒收一些合法邮件。

如果查询返回 "未找到域"
当查询结果是 "未找到域"时，启用该选项会拒收邮件并发送 "451"错误代码 (请求的操作中止：处理过程中出现本地错误)，然后会话可照常进行直至结束。

...发送 501 错误代码 (通常发送 451 错误代码)
如果希望为响应 "未找到域"查询结果发送 "501"错误代码 (参数或变量中句法错误)取代 "451"错误代码，请启用该复选框。

...然后关闭连接
如果您希望在反向查询的结果是 "未找到域"时立刻关闭连接而不是继续进行时，请点击该复选框。

免除验证的会话
如果您希望将查询推迟到 SMTP MAIL 命令之后，以便查看该连接是否使用身份验证，请点击该选项。

豁免列表
点击此按钮来打开 "HELO/EHLO 查询"豁免列表，您可以从中指定希望免于 HELO/EHLO 反向查询的站点的 IP 地址和域名/主机名。

执行查询 MAIL 命令中通过的值
启用该选项将导致对在邮件传输的 "MAIL"命令阶段传递的域名执行查询。 "MAIL"命令中通过的地址应该是邮件的反向路径，并且该地址通常就是发送邮件的邮箱。然而，有时它也会是报错邮件的投递地址。

...对伪造的标识发送 501 并关闭连接 (警告)
如果希望当查询结果显示为伪造的标识时，发送 501 错误代码然后关闭连接，请点击该复选框。

当反向查询的结果表明服务器正在使用一个伪造的标识时，该结果可能经常不正确。邮件服务器使用不匹配其 IP 地址的值来标识自己很常见。这是由 ISP 限制与约束以及其他合法理由造成的。所以请慎用该选项。使用该选项可能会导致您的服务器拒收一些合法邮件。

如果查询未返回 MX 记录则拒收邮件 (慎用)
如果您希望拒收来自没有 MX 记录域的邮件，请勾选此框。默认情况下禁用此选项，而且应该慎用此项，因为域无需 MX 记录来使其有效地存在或收发邮件。

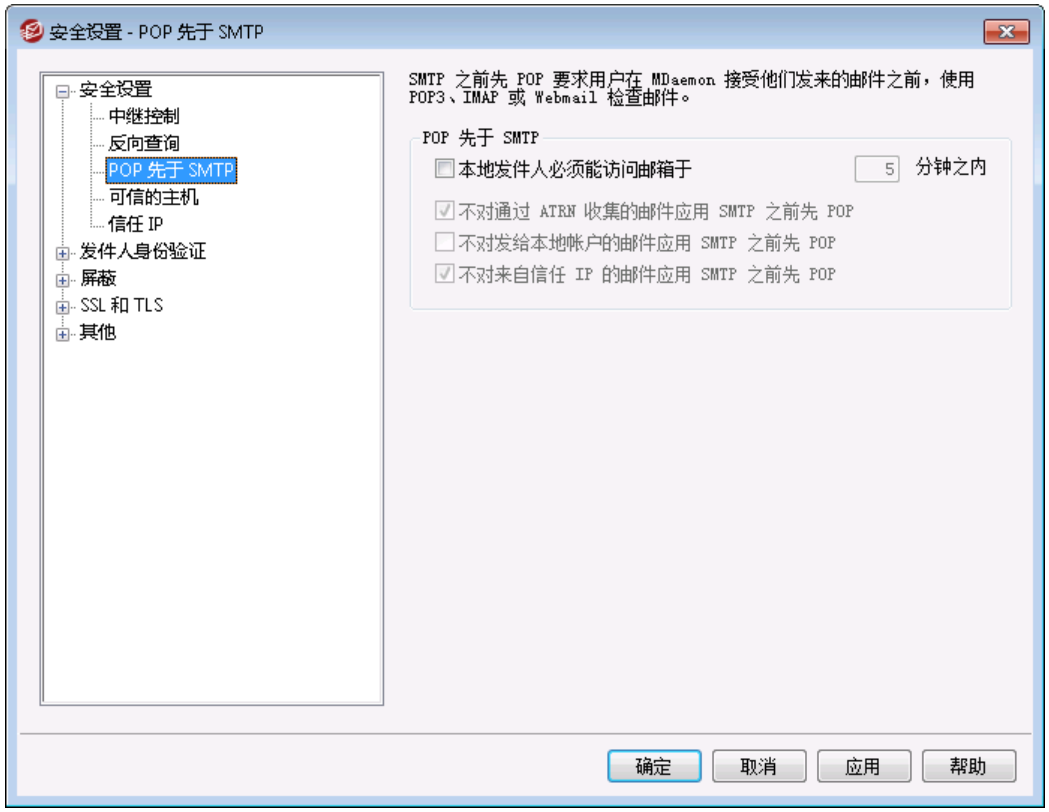
如果查询返回 "未找到域"，则拒收邮件
当查询结果是 "未找到域"时，启用该选项会拒收邮件并发送 "451"错误代码 (请求的操作中止：处理过程中出现本地错误)，然后会话可照常进行直至结束。

...发送 501 错误代码 (通常发送 451 错误代码)
如果希望为响应 "未找到域"查询结果发送 "501"错误代码 (参数或变量中句法错误)取代 "451"错误代码，请启用该复选框。

...然后关闭连接
如果您希望在反向查询的结果是 "未找到域"时立刻关闭连接而不是继续进行时，请点击该复选框。

豁免列表
点击此按钮来打开 "邮件查询"豁免列表。您可以从中指定希望免于邮件反向查询的站点的 IP 地址和域名/主机名。

4.1.1.3 POP 先于 SMTP



POP 先于 SMTP

本地发件人在最近的 [XX] 分钟内必须已访问过邮箱
启用该功能后，每当有邮件声称来自本地用户时，该用户账户必须已在指定分钟内登录并查看过其本地邮箱，之后才能获准发送邮件。

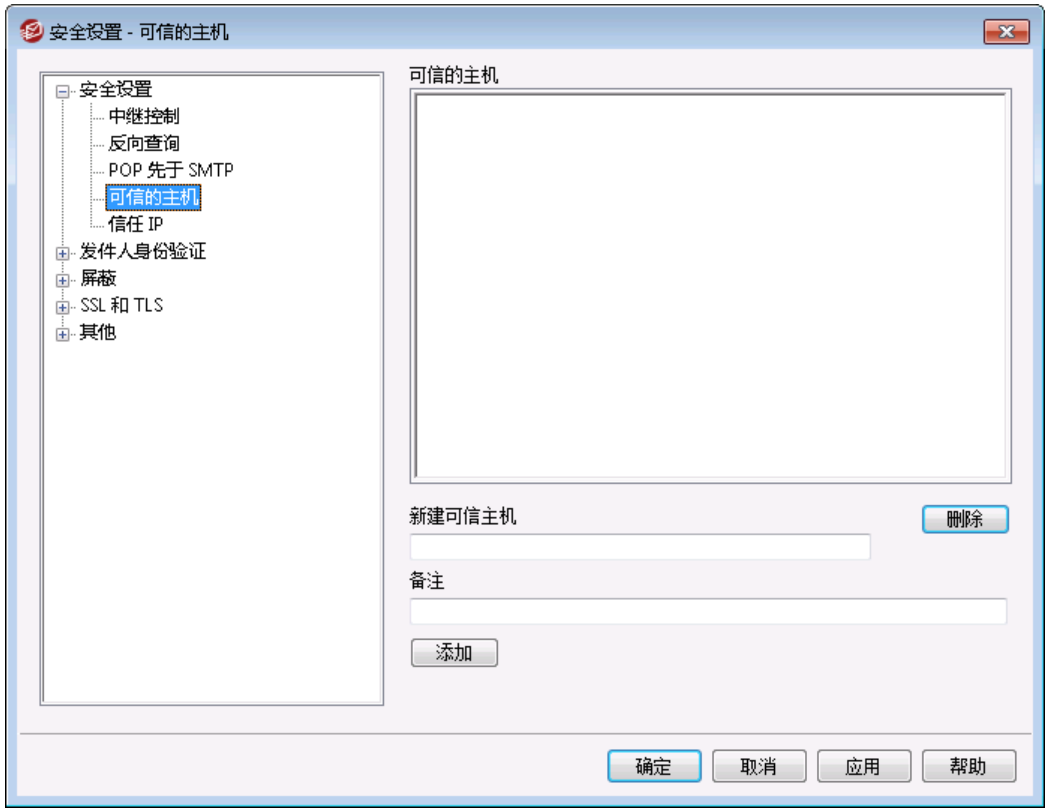
不对通过 ATRN 收集的邮件应用 "POP 先于 SMTP"
如果您希望为通过 ATRN 218 收集的邮件豁免 "POP 先于 SMTP"限制，请选中该复选框。

不对发给本地账户的邮件应用 SMTP 之前先 POP
如果希望从一个本地用户发送到另一个本地用户的邮件不受 "POP 先于 SMTP"要求的制约，请点击该复选框。通常情况下，MDaemon 一旦知道了发件人，将会强制执行该要求，但当启用此控件时，MDaemon 将等到邮件收件人显露后再确定该要求是否适用。

不对来自可信 IP 的邮件应用 "POP 先于 SMTP"
如果启用该复选框，来自可靠主机 434 屏幕上所列 IP 地址的邮件将不受 POP 先于 SMTP 限制。

通过 "SMTP 验证 438"屏幕上的选项可以为经身份验证的会话豁免 "POP 先于 SMTP"的限制。

4.1.1.4 可信主机



在整个 MDaemon 内的各种对话框和安全功能上，您将看到一些选项，允许您是否将 "可信主机"或 "可信域"作为例外或免于这些选项。这些选项会引用您在本屏幕上列出的主机。

可信主机
这是免除了某些指定安全选项的主机列表。

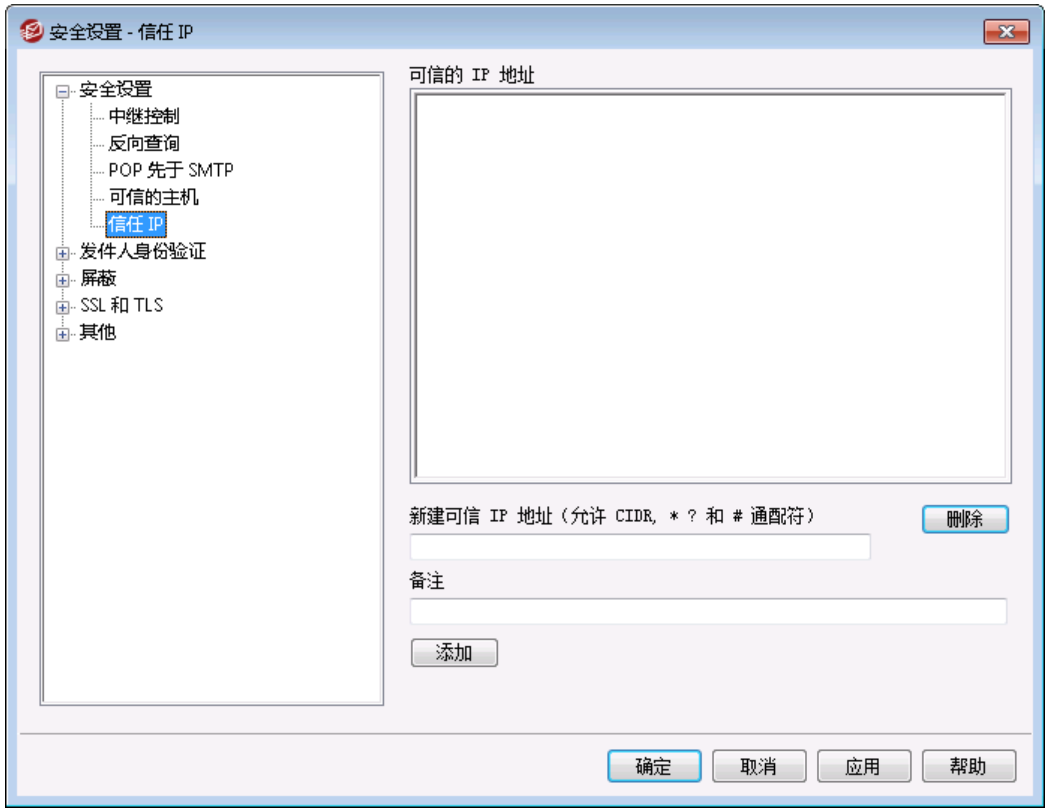
新建可信主机
输入要添加到 *"可信主机"*列表的新主机。

备注
使用此项来为条目输入任何备注文本。

添加
点击该按钮添加新域到 *"可信主机"*列表。

删除
点击该按钮从 *"可信主机"*列表中删除选定项。

4.1.1.5 可信 IP



在整个 MDaemon 内的各种对话框和安全功能上，您将看到一些选项，允许您是否将 "可信 IP"作为例外或免于这些选项。这些选项会引用您在本屏幕上列出的 IP 地址。

可信 IP 地址
这是免除了某些指定安全选项的 IP 地址列表。

新建可信 IP 地址
输入新的 IP 地址来将其添加到 *"可信 IP 地址"*列表。

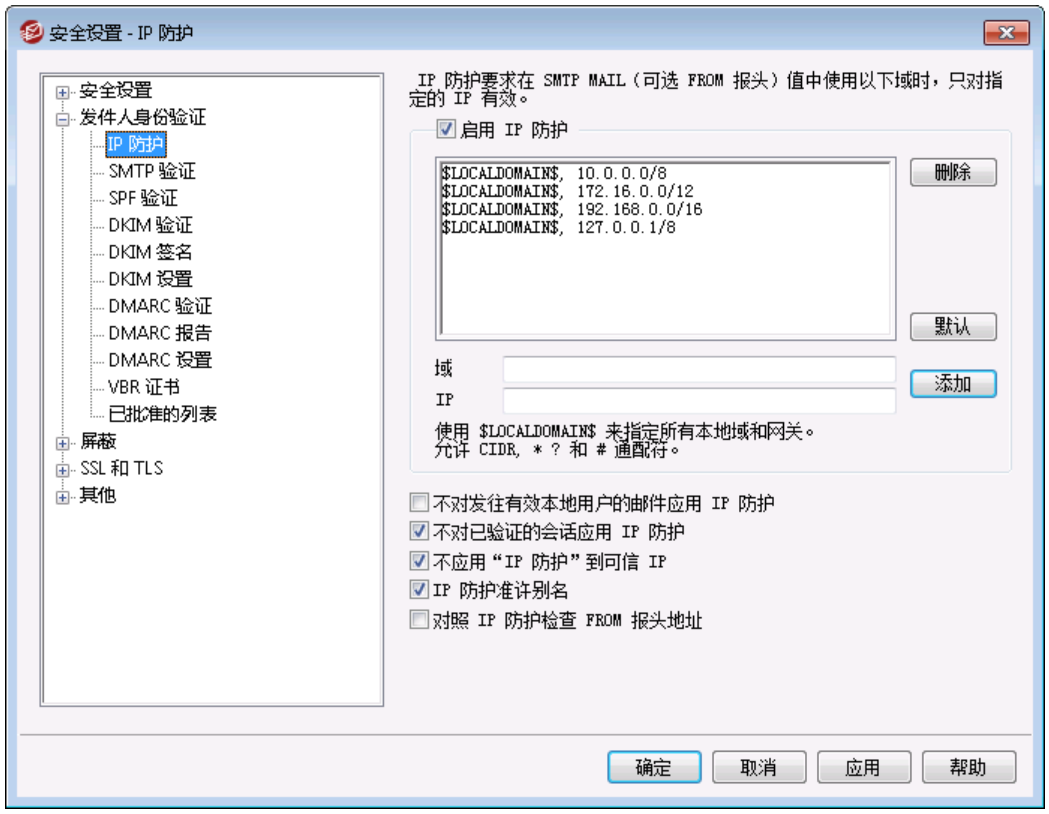
备注
使用此项来为条目输入任何备注文本。

添加
点击该按钮添加新的 IP 地址到 *"可信 IP 地址"*列表。

删除
点击该按钮从 *"可信 IP 地址"*列表中删除选定项。

4.1.2 发件人验证

4.1.2.1 IP 防护



IP 防护位于安全» 安全设置» 发件人验证菜单下，它包含在 SMTP 会话期间使用 MAIL From 命令时将要检查的域名和匹配 IP 地址的列表。自称来自某个所列域的 SMTP 会话仅当来自相关联的 IP 地址时才会被接受。例如，假设域名为 example.com，且本地局域网计算机使用从 192.168.0.0 到 192.168.0.255 范围内的 IP 地址。根据此信息，可设置 IP 防护，将域名 example.com 与 IP 地址范围 192.168.0.* (允许使用通配符)相关联。因此每当有计算机连接到您的 SMTP 服务器并声称 “MAIL FROM <someone@example.com>”时，连接计算机的 IP 地址必须在从 192.168.0.0 到 192.168.0.255 的规定范围内才会继续该 SMTP 会话。

启用 IP 防护
如要禁用 “IP 防护”，请清除此复选框。默认情况下启用 “IP 防护”。

域名
输入希望关联到特定 IP 地址范围的域名。您也可以使用 $LOCALDOMAIN$ 宏来涵盖所有本地域 (包括网关)。如果您使用此宏，在更改本地域或网关时，就不必将 “IP 防护”保持到最新。默认情况下，会将这些条目添加至 “IP 防护”，将已保留的所有 IP 地址段和 $LOCALDOMAIN$ 相关联。

IP 地址
输入希望与域名相关联的 IP 地址。必须以小数点十进制形式输入该地址。

添加
点击*添加*按钮可将域和 IP 地址范围添加到列表中。

删除
点击该按钮可从列表中删除选定项。

不对发往有效本地用户的邮件应用 IP 防护
如果希望只对那些目标为非本地用户或者无效本地用户的邮件作域/IP 匹配检查，请点击该选项。这将阻止那些伪装成本地用户的其他人通过您的服务器中继邮件，但是不检查发往本地用户的邮件将节省资源。如果同时启用该选项和下面的 *"IP 防护接受别名"*选项，则发往有效别名的邮件也会被接受。

不对已验证的会话应用 "IP 防护"
当该控件有效时，对已验证用户不应用 "IP 防护"限制。会接收来自已验证用户的邮件，无论他或她所连接的 IP 地址如何。此外，如果用户未经验证而且访问被拒时，会要求返回 SMTP 客户端的邮件 "进行验证"，由此来给予用户线索，使其能够通过配置邮件客户端在发送邮件前使用验证来修复该问题。默认情况下，启用该选项。

不对可信 IP 应用 IP 防护
启用此控件时，不会向来自可信 IP 地址[434]的连接应用 IP 防护功能。默认情况下启用此项。

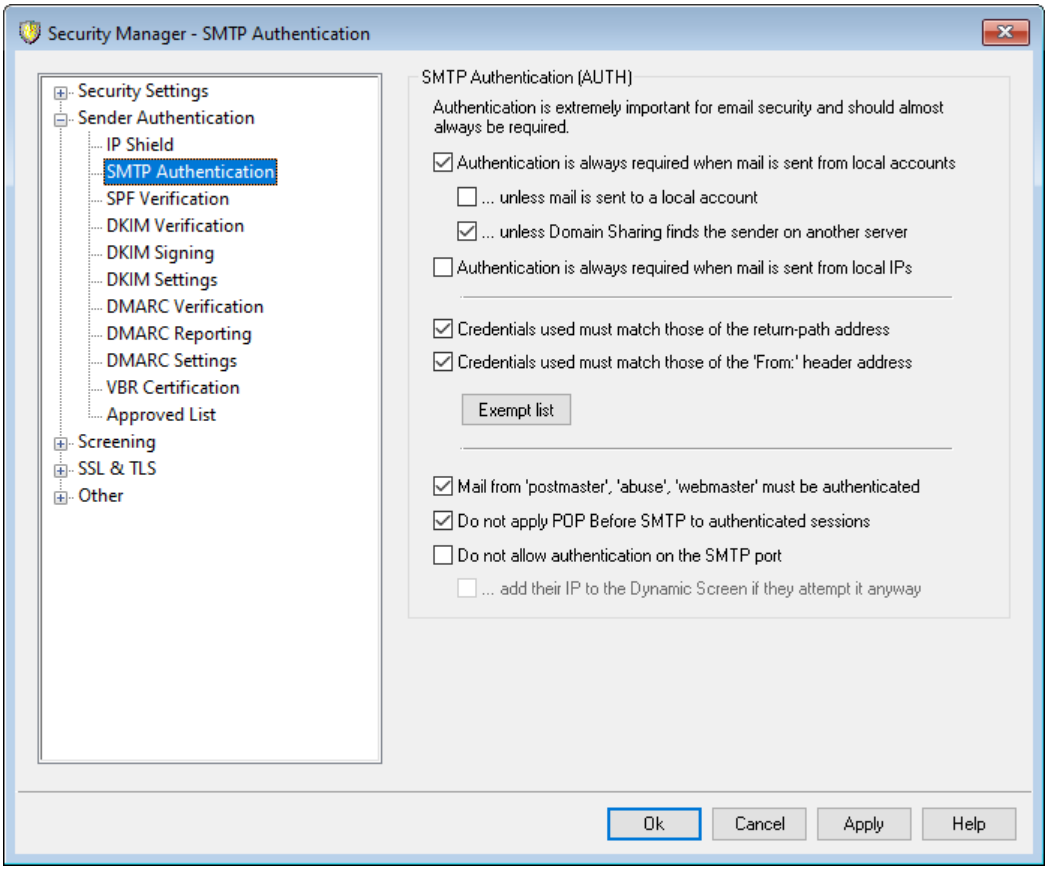
IP 防护接受别名
如果希望 IP 防护在检查域/IP 地址防护时接受地址别名，请启用该选项。"IP 防护"会将别名转换成其指向的实际账户，这样便能准许别名通过 "IP 防护"。如果未启用该选项，IP 防护将把每个别名视作与其所代表账户无关的独立地址。因此，如果一个别名的 IP 地址违反 IP 防护规则，该邮件将被拒绝。该选项同时反映在地址别名的设置屏幕[701]上——在此更改设置将会在那边反映出来。

如果希望为发往有效别名的入站邮件豁免 IP 防护，则点击该选项以及上述 *"不要应用 IP 防护到发往有效本地用户的邮件"*选项。

对照 IP 防护检查 FROM 报头。
如果您希望 "IP 防护"不仅比较取自 SMTP MAIL 值中的地址，还比较取自邮件 FROM 报头中的地址，请勾选此框。默认情况下，禁用该选项。

使用此项可能会对某些类型的邮件（例如那些来自邮件列表的邮件）造成问题。因此此项只有在您确实需要时才使用。

4.1.2.2 SMTP 验证



SMTP 验证 (AUTH)

当邮件来自本地账户时，始终要求身份验证
启用该选项时，如果入站邮件自称来自 MDaemon 的某个域，则该账户首先必须经过身份验证，否则 MDaemon 将拒绝接受并投递该邮件。默认情况下启用此项。

...除非邮件发往本地账户
如果当邮件来自本地发件人时要求进行身份验证，但当收件人也是本地用户时希望跳过身份验证限制，则可点击该选项。请注意：某些情况下，当您要求某些用户针对出站和入站邮件使用不同的邮件服务器时，可能需要用到该选项。

...除非"域共享"在另一台服务器上找到发件人
默认情况下，当域共享[93]在另一台服务器上找到发件人，该发件人将免除上方的*"始终要求验证..."*这个选项。如果您还希望这些发件人进行身份验证，请清除此复选框。

当邮件来自本地 IP 时，始终要求身份验证
如果您希望在从本地 IP 地址发送入站邮件时要求验证，请启用此项。如果未经验证将拒收邮件。可信 IP[435]将被免除，而且默认情况下为新安装启用此项。

使用的凭证必须与返回路径地址的凭证匹配
默认情况下，在 SMTP 验证期间使用的凭证必须匹配在邮件的返回路径中找到的地址。如果您不希望要求返回路径进行匹配，请禁用此项。为了支持网关邮件存储和转发，在全局网关设置 209 屏幕上相应的选项将在默认情况下*"从验证凭证匹配要求中免除网关邮件"*。

使用的凭证必须匹配 发件人:'报头地址
默认情况下，在 SMTP 验证期间使用的凭证必须匹配在邮件的 "发件人："报头中找到的地址。报头。）如果您不希望 "发件人:"报头进行匹配，请禁用此项。为了支持网关邮件存储和转发，在全局网关设置 209 屏幕上相应的选项将在默认情况下*"从验证凭证匹配要求中免除网关邮件"*。

豁免列表
使用 "匹配豁免列表的凭证"来使地址免于上方的*"使用的凭证必须匹配..."*这个选项。要免于*"..必须匹配这些返回路径地址"*选项，豁免地址必须匹配邮件的 **"返回路径"**中的地址。要免于*"..必须匹配这些发件人:'报头地址"*选项，豁免地址必须匹配邮件的 **"发件人:"**报头中的地址。

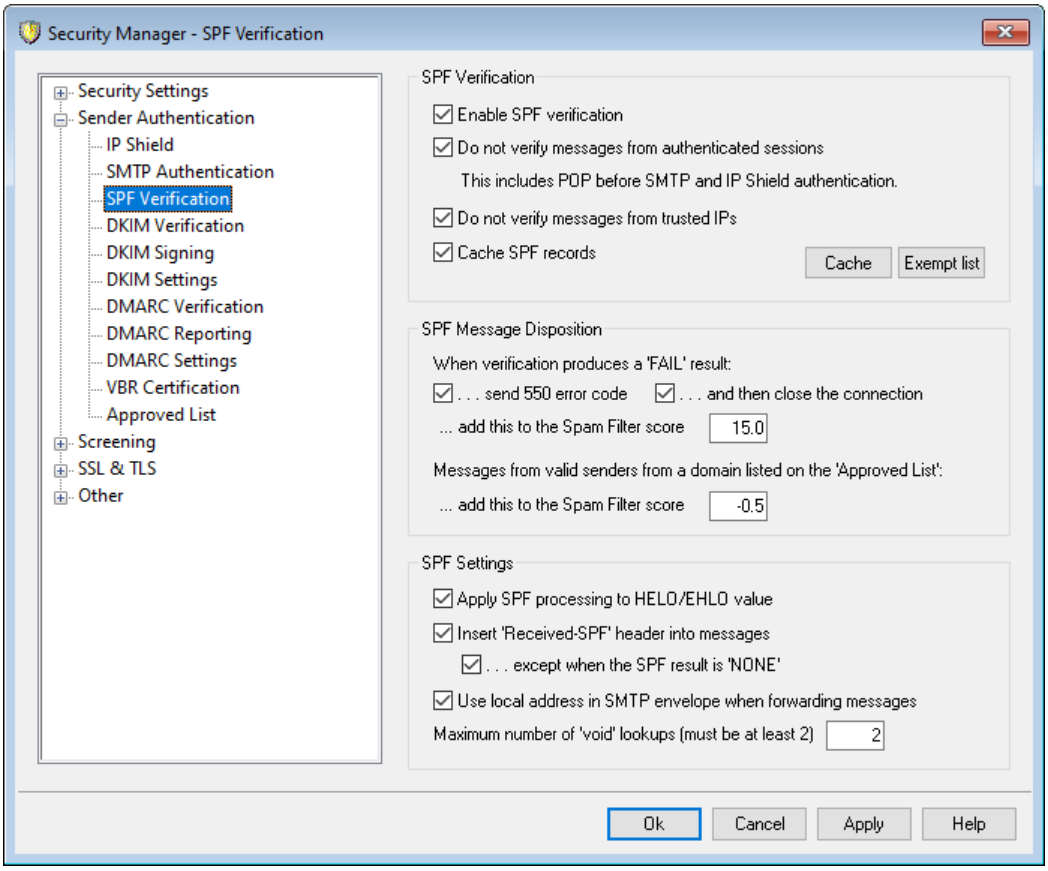
来自 "Postmaster"、"abuse"、"webmaster" 的邮件必须经过身份验证
点击该复选框，要求声称来自 "ostmaster@ ..."、"abuse@ ..."或 "ebmaster@ ..."别名或账户的邮件必须经过身份验证后◆◆能被 MDaemon 接受。垃圾邮件制造者和黑客知道这些地址可能存在，因而会试图利用这些地址通过您的服务器发送给您。该选项将阻止他们和其他未经授权的用户，使其无法达到目的。该选项同时出现在 "别名"的 "设置屏幕 701"上。在此改变设置将会在那里作出相同更改。

不对已验证的会话应用 SMTP 前先 POP
如果使用 POP 先于 SMTP 433 安全功能，点击该选项可使已验证用户不受此限制。已验证用户在发送邮件前无需检查其电子邮件。

不允许在 SMTP 端口验证
此选项禁用 SMTP 端口上的 AUTH 验证）支持。AUTH 不会在 EHLO 响应中提供，如果由 SMTP 客户端提供，则将被视为未知命令。此设置与下方的*"..添加其 IP 到动态屏蔽"*这个选项在所有合法账户都使用 MSA 或其他端口提交经过验证的邮件这种情况下的配置中很有用。在这种配置中，假定在 SMTP 端口上进行任何验证的尝试都必须来自攻击者。

> **...如果他们仍然尝试，则将其 IP 添加到动态屏蔽**
> 在使用上方的*"不允许在 SMTP 端口验证"*这个选项时，此项会将无论如何也要在 SMTP 端口尝试验证的任何客户端的任何 IP 地址添加到 "动态屏蔽"。连接也将立即终止。

4.1.2.3 SPF 验证



MDaemon 支持 "发件人策略框架 (SPF)"来帮助验证发件服务器并防范网络欺诈和钓鱼，这是两种常见的邮件造假类型，即发件人企图让邮件看起来象是他人发来的。

许多域都在域名系统 (DNS) 中发布 MX 记录来标识允许为该域接收邮件的服务器位置，但这并未标识出允许为该域*发送*邮件的服务器位置。使用 SPF，域还能发布发件人记录来标识有权发送邮件的服务器位置。通过对入站邮件执行 SPF 查询，MDaemon 可尝试确定发送服务器是否有权为所谓的发送域投递邮件，从而确定发件人地址是否可能是伪造的或 "冒牌的"。

使用屏幕上的这些选项来配置您服务器的 SPF 设置。

有关 SPF 的更多信息，请访问：

http://www.open-spf.org

SPF 验证

启用 SPF 验证
启用此项时，MDaemon 将对每封入站邮件所声称的发件人执行 DNS 查询来寻找 SPF 记录数据，由此来确保发件服务器受到许可来代表自身发送邮件。MDaemon 将要验证的主机名称是从 SMTP 处理期间所传递的 "MAIL"值中获取。默认情况下启用 SPF 验证。

不验证来自已验证会话的邮件
默认情况下，已验证的连接将免于 SPF 已验证的会话包括由 SMTP 验证[438]、POP 先于 SMTP[433] 或 IP 防护[436]验证的会话。如果您不希望已验证的会话免于 SPF，请禁用此项。

不验证来自可信 IP 的邮件
默认情况下，来自可信 IP 地址[435]的任何邮件将免于 SPF 验证。

缓存验证结果
默认情况下，MDaemon 将临时缓存在 DNS 查询期间获取的各个域的 SPF 策略记录。如果您不希望缓存 SPF 策略，请清除此勾选框。

缓存
此按钮打开 SPF 缓存，它列出当前已缓存的所有 SPF 记录。

豁免列表
点击此按钮来打开 SPF 豁免列表，您可以在其中指定希望免于 SPF 查找的 IP 地址、电子邮件地址和域。将电子邮件地址与 SMTP 信封而不是邮件的“发件人”报头进行比较。通过将“spf”一词放在域名之前，可将域豁免。MDaemon 将使用视其而定的“include:<domain>”标记，在每个 SPF 评估中包括该域的 SPF 记录。这样，您可以将备用的 MX 提供者视为所有发件人的有效 SPF 源。

SPF 邮件处理

当校验返回 FAIL 结果时：

...发送 550 错误代码
如果希望在 SPF 查询结果为“失败”时发送 550 错误代码，请点击该复选框。

...然后关闭连接
如果希望在发送 550 错误代码后立即关闭连接，请启用该选项。

...将此添加到垃圾邮件过滤器总值
当邮件未通过 SPF 验证时，指定要向该邮件的垃圾邮件总值中添加的分值。

来自“已批准列表”中所列域且来自有效发件人的邮件：

...将此添加到垃圾邮件过滤器总值
当“SPF”证实邮件的源域出现在“已批准列表[465]”中时，指定要向该邮件的“垃圾邮件总值”中添加的分值。

通常在这里指定的数字为负值，从而该已被核准的邮件的垃圾邮件分数才会降低。

SPF 设置

将 SPF 处理应用至 HELO/EHLO 值
该选项将 SPF 验证应用于在 SMTP 进程开始时在 HELO 或 EHLO 命令中传递的值。默认情况下，启用该选项。

插入 "Received-SPF"报头到邮件中
如果要把 "Received-SPF"报头插入每封邮件，请点击该选项。

...除非 SPF 结果为 "NONE"
如果不希望在 SPF 查询结果为 "none"时把 "Received-SPF"报头插入邮件，请启用该选项。

转发邮件时在 SMTP 信封中使用本地地址
E如果希望所有由 MDaemon 转发的邮件在 SMTP 信封中使用本地地址，请启用该选项。这有助于减少与转发相关的问题。通常，转发邮件使用原始发件人的邮件地址来发送，而不是实际执行转发操作的邮件地址。某些情况下，为了防止接收服务器错误地把转发邮件标识为 "冒用"地址，可能需要使用本地地址。默认情况下启用此项。

"无效"查询数量最大值 (必须至少为 2)
这是在 MDaemon 生成一个永久性错误前，在 SPF 查询中允许的无效查询结果数量的最大值。无效查询是导致 "域不存在"或 "不存在响应"的查询。该值必须至少为 "2"。

4.1.2.4 域名密钥标识邮件

DomainKeys Identified Mail (DKIM) 是加密邮件验证系统，它能用于防范网络诈骗 (伪造他人的邮件地址以假扮不同的邮件发件人)。不仅如此，因为大多数的垃圾邮件都包含欺骗性地址，因此尽管 DKIM 不是专门设计用于反垃圾邮件的工具，但它们有助于显著减少垃圾邮件。DKIM 还能用于确保入站邮件的完整性，或确保邮件从离开签名邮件服务器到送达您的服务器之间中途未被篡改。换言之，有了 DKIM 密码验证系统，接收服务器可以肯定到达的邮件是来自为其签名的服务器，且未以任何方式做过更改。

为了确保邮件的有效性和完整性，DKIM 使用公共和私人密钥对系统。经加密的公共秘钥被发布到发送服务器的 DNS 记录中，随后该服务器使用相应的经加密私人密钥为每个出站邮件签名。对于入站邮件，当接收服务器发现它已有签名时，将从发送服务器的 DNS 记录中检索公共秘钥，然后将其与该邮件的加密签名进行比较来确定该邮件的有效性。如果入站邮件无法通过验证，那么接收服务器就知道它包含了伪造的地址或曾被篡改。验证失败的邮件可以被拒收，或者被接受但同时调整其垃圾邮件分数。

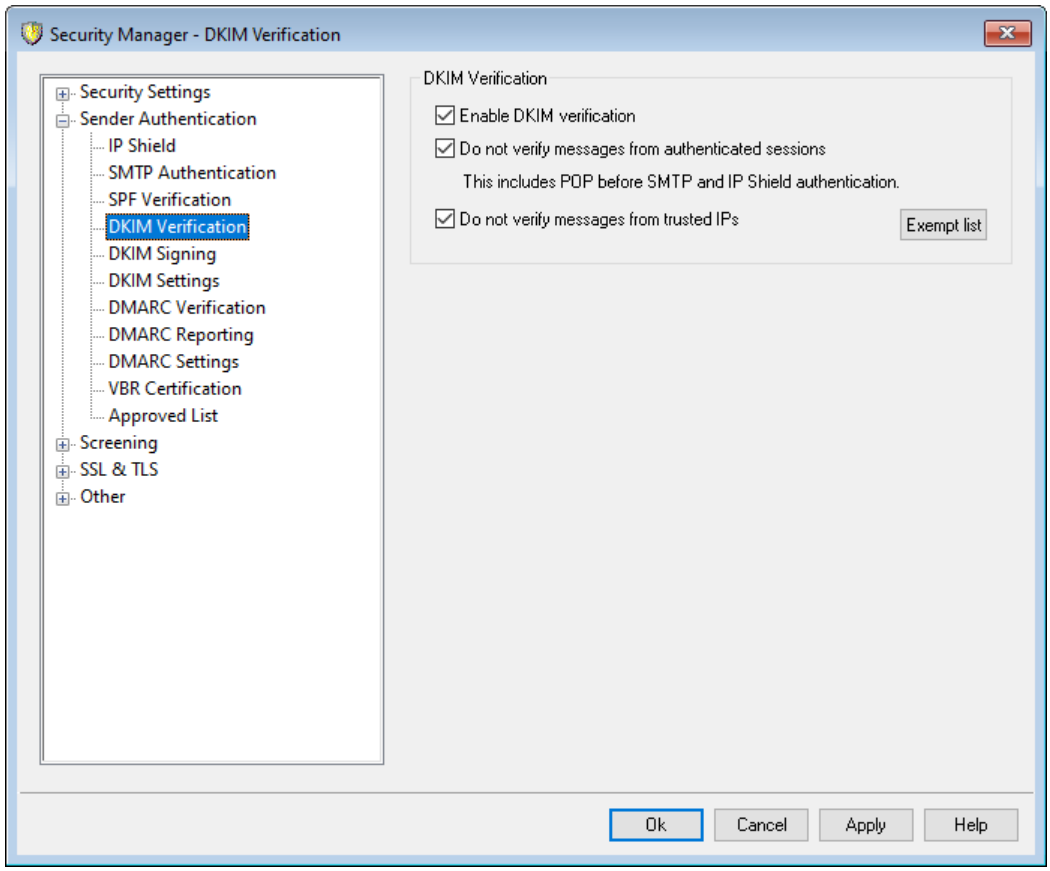
要将 MDaemon 配置为验证经加密签名的入站邮件，可使用在 "DKIM 验证 443"屏幕上提供的选项。要配置 MDaemon 为出站邮件签名，可使用在 "DKIM 签名 445"屏幕上提供的选项。两者都在 "安全设置"对话框中的 "发件人身份验证"部分下，位于：安全» 安全设置» 发件人身份验证。MDaemon 的主界面 58 包括一个 "DKIM"选项卡 (位于 "安全"选项卡下方)，可用于实时监控 DKIM 活动，不仅如此，使用下列位置的选项可记录 DKIM 活动日志：设置» 服务器设置» 日志» 设置。

还请参阅：

DKIM 验证 443
DKIM 签名 445
DKIM 设置 447

有关 DomainKeys Identified Mail的更多信息，请访问：http://www.dkim.org/。

4.1.2.4.1 DKIM 验证



使用该屏幕配置 MDaemon 来验证入站远程邮件中的 DomainKeys Identified Mail (DKIM) 签名。启用该功能且入站邮件已作加密签名时，MDaemon 将从签名中提取域，并从该域的 DNS 记录中检索公共密钥，然后使用该密钥测试邮件的 DKIM 签名以确定其有效性。

如果签名通过了验证测试，该邮件将继续常规投递过程中的下一步操作。此外，如果从签名中提取的域也出现在已批准列表 465中，对该邮件的垃圾邮过滤器分数将作有利调整。

有关于 DKIM 的更多信息，请参阅：http://www.dkim.org/

DKIM 验证

启用 DKIM 验证
点击这个选项来激活 DomainKey 邮件识别技术验证来自远程的邮件。

不验证来自已验证会话的邮件
如果希望在邮件会话通过身份验证时不对该邮件进行加密验证，请点击该选项。经身份验证的会话包括由 SMTP 身份验证 438、POP 先于 SMTP 433 或 IP 防护 436 验证的会话。

不验证来自可信 IP 的邮件
如果希望来自可信 IP 地址 434 的连接免于 DKIM 验证，请使用该选项。

豁免列表
点击该按钮可打开例外列表。源自该列表中指定的任何 IP 地址的邮件不会受到加密验证。

验证结果报头

每当使用 SMTP AUTH、SPF、DomainKeys Identified Mail 或 DMARC 对邮件进行身份验证时，MDaemon 将向该邮件插入身份验证结果报头，列出身份验证处理结果。如果 MDaemon 配置为接受哪怕未通过身份验证的邮件，那么身份验证结果报头将包含标识失败原因的代码。

因特网工程任务组（IETF）正在不断改进该报头以及本章节中所述的身份验证协议。更多相关信息，可访问以下 IETF 网站：http://www.ietf.org/。

邮件列表邮件中的 DKIM 报头

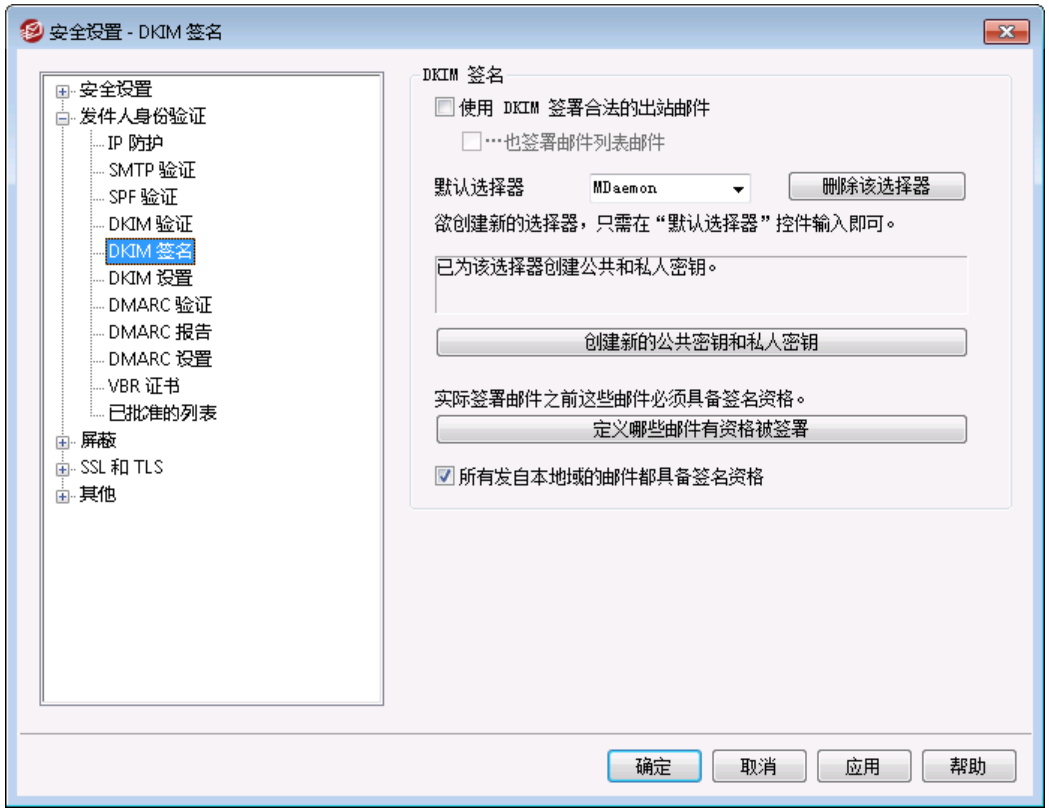
默认情况下，MDaemon 将从入站列表邮件中剔除 DKIM 签名，因为在列表处理过程中对邮件报头或内容所做的更改会破坏这些签名。如果想让 MDaemon 在列表邮件中保留签名，可通过在 MDaemon.ini 文件中手动设置以下选项来实现这一目的：

```
[DomainKeys]
StripSigsFromListMail=No （默认为“Yes”）
```

还请参阅：

域名密钥标识邮件 442
DKIM 签名 445
DKIM 设置 447

4.1.2.4.2 DKIM 签名



使用 "DKIM 签名"屏幕上的选项来配置 MDaemon 使用 DKIM 来签署合法的出站邮件，并定义使邮件合法的条件。还可使用该屏幕来指定选择器并生成适用于 DKIM 规范的相应公共/私人密钥。启动时自动为您创建默认选择器（"MDaemon"）和默认的公共及私人密钥。所有的密钥都是独一无二的——无论指定的是哪个选择器，站点和站点之间的密钥绝对不会相同。默认情况下，密钥的安全位深度为 2048 位。

DKIM 签名

使用 DKIM 签名合法出站邮件
如果想使用 DomainKeys Identified Mail 对某些出站邮件作加密签名，请点击该选项。为了让邮件获得签名，它必须符合 *"定义哪些邮件有资格获得签名"*按钮下指定的条件，并在经过身份验证的会话上由 MDaemon 接收后进行投递。还可使用 *"用 DKIM 选择器签名..."*这一内容过滤器操作为邮件签名。

...签名邮件列表邮件
如果想对所有出站邮件列表邮件作加密签名，请点击该复选框。因为 MDaemon 将对发往所有列表的所有邮件进行签名，因而无需使用 *"定义哪些邮件有资格获得签名"*选项来授权对它们进行加密签名。

签名列表邮件需要在"解析"列表后对每个列表邮件进行内容过滤处理。在处理大型且极其活跃的邮件列表时，这可能会影响服务器的性能。

默认选择器
从该下拉列表中选择某个选择器，其相应的公共/私人密钥对将用于为邮件签名。如果想用不同的选择器来创建新的密钥对，请在此输入所需选择器名称并点击下面的 *"创建新的公共密钥和私人密钥"*。如果您想使用其他选择器为某些邮件签名，请在 *"定义哪些邮件有资格获得签名"*选项下指定特定选择器，或使用 *"用 DKIM 选择器签名..."*操作来创建内容过滤器规则。

删除该选择器
如果您希望删除选择器，请点击此按钮。请遵照屏幕上出现的指示。

创建新的公共密钥和私人密钥
点击该按钮可为上述指定选择器生成一对公/私密钥。为选择器生成一对公/私密钥的同时将创建并自动打开 dns_readme.txt 文件。该文件包含了 DKIM 数据样本，您需要将其发布到域的的 DNS 记录中，它列出了您的 DKIM 策略以及指定选择器的公共密钥。该文件针对测试和非测试状态，以及是否为所有邮件签名还是仅仅为源自您的域的邮件签名列出了数据样本。如果您当前正在测试 DKIM 或该选择器，那么根据您的测试内容，需要使用测试条目中包含的针对策略或选择器的信息。否则将使用非测试条目。

所有密钥的存储格式都为 PEM，且所有选择器和密钥都按以下方式存储在 \MDaemon\Pem 文件夹中：

```
\MDaemon\Pem\<Selector>\rsa.public - 该选择器的公共密钥
\MDaemon\Pem\<Selector>\rsa.private - 该选择器的私人密钥
```

这些文件夹内包含的文件并未作加密或隐藏，但是它们包含的 RSA 私人加密密钥未经许可决不能被他人读取。因此应使用 OS 工具来采取必要措施确保这些文件夹和子文件夹的安全。

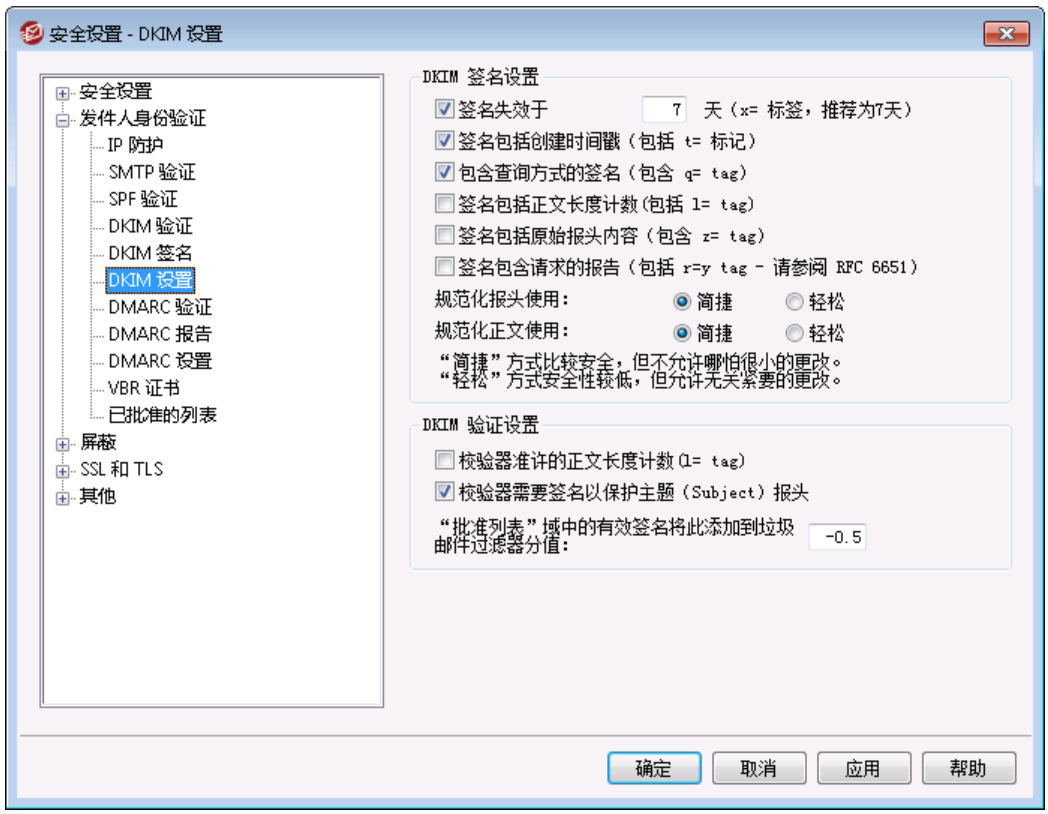
定义哪些邮件有资格获得签名
如果您已选择签名合法的出站邮件，点击该按钮可编辑 "DKSign.dat"文件，它包含了 MDaemon 用于确定是否要为某个邮件签名的域及地址列表。对所列的每个地址，必须指定有资格获得签名的邮件应发往还是源自该地址，或者您可指定其他报头，如 "Reply-To"或 "Sender"。你还可选择为每个条目指定一个选择器，用于对匹配该条目的邮件进行签名。最后，您可以指定在签名报头内 "d="标签中使用的可选签名域。举个例子，当您有多个子域为邮件签名时，该标记会非常有用。在这种情况下，您可使用 "d="标记告诉接收服务器在单个域的 DNS 记录中查找 DKIM 密钥，这就使您能在一个记录中管理所有密钥，而不必为每个子域管理单独的记录。在域和地址中允许使用通配符。

来自本地域的所有邮件都有资格获得签名
如果希望所有来自本地域的邮件都有资格获得签名，请使用该选项 如果使用该选项，您不必添加任何本地域到资格列表 (即 DKSign.dat 文件)中，除非想要指定特定选择器或 "d="标记用于为特定域的邮件签名。默认情况下启用此项。

还请参阅：

域名密钥标识邮件 442
DKIM 设置 447
DKIM 验证 443

4.1.2.4.3 DKIM 设置



DKIM 签名设置

签名在 [XX] 天后到期（"x=" 标签，推荐7天）
如果要限制 DKIM 签名的有效天数，请激活该选项并指定所需天数。若邮件的签名已到期，那么该邮件将总无法通过验证。该选项对应的是签名的 "x=" 标签。默认启用该选项，并设为 7 天。

签名包括创建时间戳（包括 t= 标签）
启用该选项时，签名中将包括创建时间戳（"t=" 标签）。默认启用此项。

签名包括查询方式(包括 q= tag)
默认启用该选项。它使得签名中包括查询方式标签（例如 "q=dns"）。

签名包括正文长度计数(包括 l= 标签)
如果要在 DKIM 签名中包括正文长度计数标签，请启用该选项。

签名包括原始报头内容（包括 z= 标签）
若您希望在 DKIM 签名中包含 "z="标签，请点击此选项。这个标记将包含邮件原始报头的副本。这可能使签名变得极大。

签名包含请求的报告（包含 r=y 标签）
如果您希望在签名邮件中包含 r=y 这个标签，请启用此项。此标签向准许这个标签的收件服务器作出如下指示：在遇到生成来自您的域却无法通过 DKIM 验证的邮件时，从该服务器接收 AFRF 故障报告。要接收这些报告，您必须配置您域的 DNS 中的 DKIM 报告 TXT 记录。请参阅 RFC-6651：*针对故障报告的域名秘钥标识邮件（DKIM）的扩展*来了解操作语法和指令。由于此项需要更改 DNS，默认情况下已禁用此项。

规范化

规范化是一个将邮件的报头和正文转化为规范化的标准，并在创建 DKIM 签名之前将其"常规化"的过程。这样做是必要的，因为在常规处理的过程中，一切邮件服务器和中继系统会对邮件做出各种无关紧要的改变，如若在准备签名每封邮件时不使用规范化的标准，那么可能会造成签名被破坏。目前有两种用于 DKIM 签名和验证的规范化方法：简单和轻松。简单是最严谨的方法，不允许对邮件做出改变，或只允许细微改变。轻松则要求相对交送，允许一些无关紧要的改变。

规范化报头使用：简单，轻松
这是在签名邮件时用于邮件报头的规范化方法。"简单"表示在任何情况下都不允许对报头字段进行更改。轻松则允许将报头名称转换为小写（不是改变报头的值），将一个或多个连续空格转换为一个空格，以及其他一些无害改变。默认设置为"简单"。

规范化正文使用：简单，轻松
这是在签名邮件时用于邮件正文的规范化方法。简单可忽略邮件正文末尾的空行— 不再允许其他任何对于邮件正文的更改。轻松则允许邮件末尾的空白行，忽略行末尾的空格，将一行中的所有连续空格减少为一个空格字符，以及其他一些小的更改。默认设置为"简单"。

DKIM 验证设置

验证程序接受正文长度计数（l= 标签）
启用该选项后，MDaemon 将接受在入站邮件的 DKIM 签名中找到的正文长度计数标记。如果实际正文长度计数大于此标签中所含值，MDaemon 将仅验证该标签中指定的数量——对邮件的其余部分不将验证。这就表明邮件中有附加内容，因而不验证的部分可认为是可疑的。若真实的正文长度小于该标签中所包含的值，该签名将不会通过验证（例如：它将收到一个"失败"结果）。这表明邮件的某些部分已被删除，从而导致正文长度计数小于此标签中所指定的数值。

验证程序需要签名来保护"主题"报头
如果想要求入站邮件的 DKIM 签名来保护"主题"报头，请启用此选项。

将"已批准列表"域中的有效签名将此添加到"垃圾邮件过滤器"分值：
当从签名中提取的域出现在已批准列表 465 中时，在此指定的分值将被添加由 DKIM 签名并"通过"验证的任何邮件的垃圾邮件过滤器总值中。如果邮件的签名经过验证，但是域不在已批准列表中，则不会调整垃圾邮件过滤器总值——经验证的签名不会影响该分数。不过，常规的垃圾邮件过滤器处理和评分仍将应用于该邮件。

通常在此指定的值应为负数，因而当邮件包含有效的加密签名且从签名中提取的域位于已批准列表[465]中时，将减少该邮件的垃圾邮件总值。MDaemon 中该选项的默认值是 -0.5。

还请参阅：

域名密钥标识邮件[442]
DKIM 验证[443]
DKIM 签名[445]

4.1.2.5 DMARC

基于域的邮件验证、报告和一致性 (DMARC) 这个规范旨在减少邮件滥用 (例如通过伪造邮件的 "From:" 报头。) DMARC 帮助域拥有者使用 "域名系统" (DNS) 来向收件服务器告知其 DMARC 策略，例如他们希望这些服务器如何处理自称来自他们域但无法验证实际来源的邮件。收件服务器在处理入站邮件时通过 DNS 查询检索到的这个策略，可以向服务器表明应该隔离或拒收不符合这个策略的邮件，或根本不采取任何操作 (例如继续照常处理邮件)。除了这个策略以外，该域的 DMARC DNS 记录也可以包含服务器请求来向某人发送 DMARC 报告、概述自称来自此域的入站邮件的总数、它们是否通过验证、以及任何失败的详细信息。DMARC 的报告功能在确定您的邮件验证流程是否有效，以及伪造邮件使用您域名的频率时极其有用。

在 "安全设置" 对话框的 "发件人验证" 部分中，提供以下三个部分供您配置 MDaemon 的 DMARC 验证和报告功能：DMARC 验证、DMARC 报告和 DMARC 设置。

DMARC 验证[454]

作为 DMARC 验证流程的一部分，MDaemon 对在每封入站邮件的 "From:" 报头中找到的域执行 DMARC DNS 查询。这用来确定该域是否使用 DMARC，如果使用了 DMARC 则检索其 "DMARC DNS 记录[450]"，其中包含了它的策略和其他 DMARC 相关信息。此外，DMARC 使用 SPF[440] 和 DKIM[443] 来验证每封邮件，并要求它至少通过一项测试来通过 DMARC 验证。如果该邮件通过验证，则按照 MDaemon 其余投递和过滤流程来照常处理这封邮件。如果未通过验证，则取决于该域的 DMARC 策略以及您对于 MDaemon 如何处理这些邮件的配置来确定该邮件的命运。

如果一封邮件未通过 DMARC 验证，而且 DMARC 域拥有一个 "p=none" 策略，则不会采取任何惩罚性操作并照常处理这封邮件。相反，当 DMARC 域拥有一个存在限制的策略，例如 "p=quarantine" 或 "p=reject"，MDaemon 可以有选择性地将该邮件自动过滤到接收用户垃圾邮件 (例如：垃圾邮件) 的文件夹。您也可以选择在该域使用 "p=reject" 策略时，让 MDaemon 完全拒收未通过验证的邮件。对于使用限制性策略且未通过验证的邮件，MDaemon 将取决于策略插入 "X-MDDMARC-Fail-policy: quarantine" 或 "X-MDDMARC-Fail-policy: reject" 报头。这帮助您使用 "内容过滤器"，基于这些报头来执行一些操作，例如将该邮件发送至特定的文件夹进行审核。

建议默认情况下为大多数 MDaemon 配置启用 DMARC 验证。

DMARC 报告 456

在 MDaemon 查询 DNS 是否存在 DMARC 记录时，该记录可能包含一些标签，指示域的拥有者是希望接收与声称来自此域邮件相关的 DMARC 综合报告还是故障报告。"DMARC 报告"屏幕上的一些选项供您用来指定是否希望发送请求的报告类型，并指定这些报告应该包含的元数据。将在每晚午夜 (UTC)发送综合报告，将按邮件来发送故障报告，因为每个发生的事件将触发这个报告。报告以打包压缩 (ZIP)的 XML 文件附件形式发送，而且在线提供各种分析工具，帮助收件人更简便地进行查看。

默认情况下 MDaemon 不发送综合或故障报告。如果您希望发送这些报告，请在 "DMARC 报告"屏幕上启用相应的选项。

DMARC 设置 459

DMARC 设置屏幕包含各种选项，例如在 DKIM 报告中包含特定信息、记录 DMARC DNS 记录、以及更新 MDaemon 用于 DMARC 的 "公共后缀"文件。

DMARC 验证和邮件列表

因为 DMARC 的目的在于确保在邮件 "From:"报头中找到的域不被伪造，必须允许发件服务器代表该域来发送邮件。这会给邮件列表带来一个问题，因为列表通常代表来自外部域的列表成员来分发邮件，并使 "From:"报头保持不变。这就意味着在收件服务器尝试对这些邮件使用 DMARC 验证时，邮件会被不关联 "From:"报头域的服务器发送。如果 DMARC 域正好使用了存在限制的 DMARC 策略，这会导致邮件被隔离甚至被收件服务器拒收。在某些情况下，这会导致从列表的成员中删除收件人。为了避免这个问题，在 MDaemon 发现列表邮件来自使用了受限 DMARC 策略的域时，MDaemon 将使用邮件列表的地址来替换 "From:"报头。此外，您也开始配置 MDaemon 在列表邮件来自存在受限策略的域时，拒收这些邮件。后者使所在域使用了受限策略的用户能够向列表发送邮件。用来替换 "From:"报头的选项位于邮件列表编辑器的 "报头 233"屏幕。用来拒收邮件的选项位于 "设置 231"屏幕。

为您的 MDaemon 域使用 DMARC

如果您希望为您自己的域使用 DMARC，这就意味着您希望支持 DMARC 的收件服务器使用 DMARC 来验证声称由您发送的邮件，您首先必须确保您已为该域创建了格式正确的 SPF 和 DKIM DNS 记录；而且您必须使这些选项正确工作来使用 DMARC。如果您正在使用 DKIM，您也要配置 MDaemon 的 "DKIM 签名 445"选项来签署该域的邮件。此外，您必须为该域创建一个 DMARC DNS 记录。通过查询 DNS 是否存在这个拥有特殊格式的 TXT 记录，收件服务器可以确定您的 DMARC 策略和各种可选的参数，例如：您使用的验证模式、您是否希望接收综合报告、应接收报告的邮件地址等。

一旦您正确配置了 DMARC 并开始接收 DMARC XML 报告，您可以使用大量在线工具来阅读这些报告并诊断任何潜在的问题。方便起见，在 \MDaemon\App\ 文件夹中还为您提供一个 DMARC Reporter 工具。请参阅 DMARCReporterReadMe.txt 来获得使用说明。

定义 DMARC TXT 资源记录

以下是 DMARC 记录常用组件的基本概述。要获得更多详细信息或有关高级配置的更多信息，请参阅：www.dmarc.org.

拥有者字段
DMARC 资源记录的 "拥有者"(也叫做 "姓名"或 "左侧")字段必须始终为 **_dmarc**，如果您希望指定该记录应用到的域或子域，也可以采用 **_dmarc.domain.name** 这种形式。

示例：

域 **example.com** 的 DMARC 记录

```
_dmarc IN TXT "v=DMARC1;p=none"
```
该记录将应用于发自 user@example.com 或子域为 example.com 的电子邮件，例如 user@support.example.com、user@mail.support.example.com 等。

```
_dmarc.support.example.com IN TXT "v=DMARC1;p=none"
```
该记录仅应用于发自 user@support.example.com 的电子邮件，不应用于发自 user@example.com 的电子邮件。

```
_dmarc.support IN TXT "v=DMARC1;p=none"
```
该记录将应用于发自：user@support.example.com、user@a.support.example.com、user@a.b.support.example.com 等的电子邮件。

DMARC 记录标签和值

必需标签

标签	值	便笺
v=	**DMARC1**	这是 "版本"标签，必须作为该记录的 DMARC 特定文本部分的第一个标签。即使其他 DMARC 标签值不区分字母大小写，**v=** 标签的值必须是大写字母：**DMARC1**。 示例： `_dmarc IN TXT "v=DMARC1;p=none"`
p=	**none** **quarantine** **reject**	这是 "策略"标签，必须作为 DMARC 记录中的第二个标签，紧接 **v=** 这个标签。 **p=none** 表示收件服务器基于 DMARC 查询结果不采取任何操作。不得基于未通过 DMARC 检查这个失败隔离或拒收邮件。不过可以出于其他理由隔离或拒收这些邮件，例如未通过垃圾邮件过滤测试或与 DMARC 无关的其他安全检查。对于 **p=none** 的使用有时被称为 "监控"或 "监控模式"，因为您可以配合 **rua=** 这个标签一起使用来从收件域接收有关您邮件的综合报告，不过不会对未通过 DMARC 检查的这些邮件执行任何惩罚性操作。您可以一直使用这个策略，直到您彻底测试了您的 DMARC 实施，并确保您已准备好使用更具有限制性的 **p=quarantine** 策略。 **p=quarantine** 这个策略用于以下场景：在邮件的 **"From:"** 报头声称由您所发送但未通过 DMARC 检查时，您希望其他邮件服务器将该邮件视为可疑邮件。取决于服务器的本地策略，这

		可以表示对邮件进行额外审核、将其放入收件人的垃圾邮件文件夹、将其路由到不同的服务器或采取其他操作。 **p=reject** 表示您希望收件服务器拒收未通过 DMARC 验证的任何邮件。不过一些服务器仍然接收这些邮件，不过将其隔离或进行额外审核。这是限制性最高的策略，通常不使用该策略，除非您对自己的邮件策略、以及您允许账户使用的邮件或服务类型把握十足。例如，如果您允许您的用户加入第三方邮件列表，使用邮件转发服务，并使用网站上的 "共享"功能，使用 **p=reject** 将可能导致一些合法邮件被拒收。而且该设置也会使某些用户被一些邮件列表删除或阻止。 示例： `_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:dmarc-report@example.net"`

额外标签
以下列出的所有标签都是可选标签。如果未在记录中使用任何这些标签，则假定其默认值。

标签	值	便笺
sp=	**none** **quarantine** **reject** — 默认值： 如果未使用 **sp=**，则对域和子域应用 **p=** 这个标签。	此标签用来指定应用 DMAR 记录的域的子域将使用的策略。例如，如果应用于 example.com 的记录中使用了这个标签，那么会将 **p=** 这个标签中指定的策略应用于来自 example.com 的邮件，将 **sp=** 这个标签中指定的策略应用于来自 example.com 子域的邮件，例如 mailexample.com。如果在记录中忽略了这个标签，则将 **p=** 这个标签应用于该域及其子域。 示例： `_dmarc IN TXT "v=DMARC1;p=quarantine;sp=reject"`
rua=	由逗号分隔的将接收 DMARC 综合报告的邮件地址列表 必须使用以下格式输入作为 URI 的 地址：**mailto:user@example.com** —	此标签表示您希望从接收了一封 "**From:**"声称来自您所在域邮件的收件服务器接收 DMARC 综合报告。使用以下格式指定作为 URI 的一个或多个邮件地址：**mailto:user@example.com**，使用逗号分隔多个 URI。 示例： `_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:user01@example.com,mailto:user02@example.com"`

	默认值：
	none
	如果未使用这个标签，则不发送综合报告。
		通常这些地址将位于此记录覆盖的域。如果您希望将报告发送至其他域的地址，则该域的 DNS 区域文件必须也包含一个专用的 DMARC 记录，指示它将接收该域的 DMARC 报告。
		example.com 的记录示例：
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:non-local-user@example.net"`
		example.net 的记录：
		`example.com._report._dmarc TXT "v=DMARC1"`

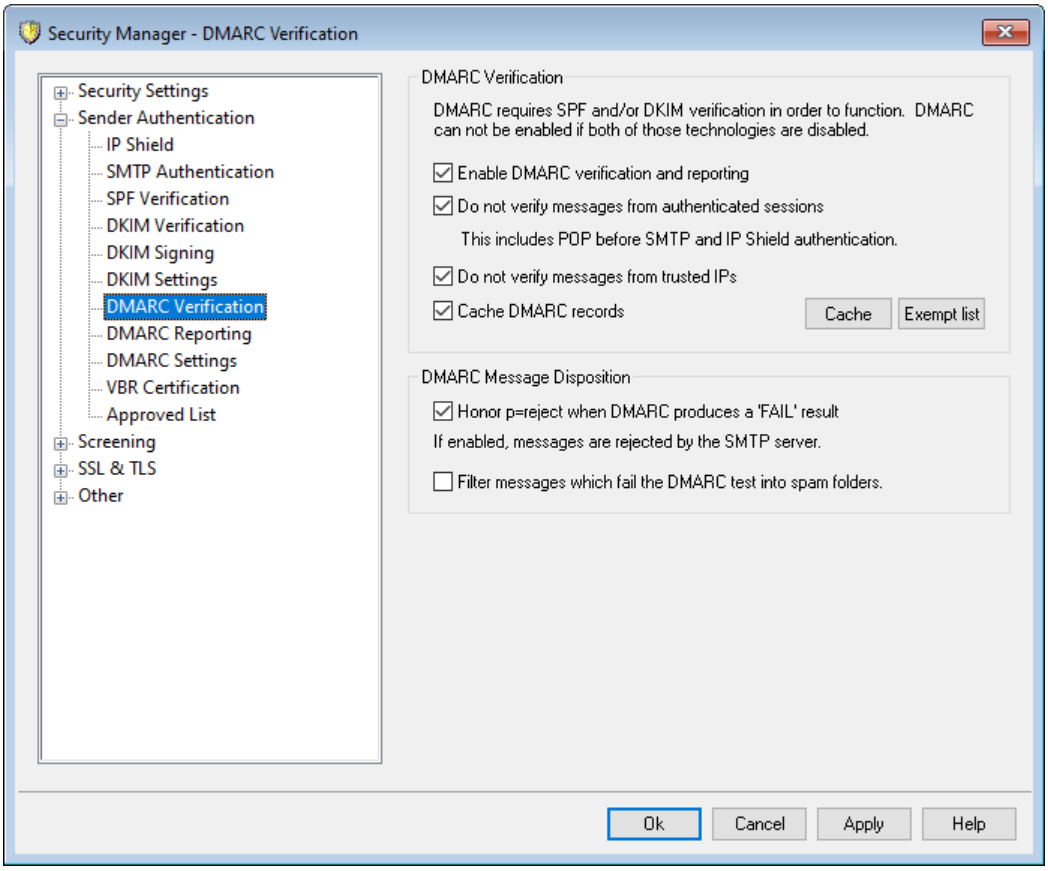
ruf=	由逗号分隔的将接收 DMARC 故障报告的邮件地址列表 必须使用以下格式输入作为 URI 的 地址：**mailto:user@example.com**
	—
	默认值：
	none
	如果未使用这个标签，则不发送故障报告。
		此标签表示您希望从接收了一封 **From:**”声称来自您所在域邮件的服务器接收 DMARC 故障报告，前提是满足了在 **fo=** 这个标签中指定的条件。在默认情况下，如果未指定 **fo=** 这个标签，在邮件未通过所有 DMARC 验证检查时将发送故障报告 例如未通过 SPF 和 DKIM 验证）。使用以下格式指定作为 URI 的一个或多个邮件地址：**mailto:user@example.com**，使用逗号分隔多个 URI。
		示例：
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:dmarc-failures@example.com"`
		通常这些地址将位于此记录覆盖的域。如果您希望将报告发送至其他域的地址，则该域的 DNS 区域文件必须也包含一个专用的 DMARC 记录，指示它将接收该域的 DMARC 报告。
		example.com 的记录示例：
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:non-local-user@example.net"`
		example.net 的记录：
		`example.com._report._dmarc TXT "v=DMARC1"`

要了解有关 DMARC 规范的更多扩展信息，请参阅：www.dmarc.org。

还请参阅：

DMARC 验证 454
DMARC 报告 456
DMARC 设置 459
邮件列表 » 设置 231
邮件列表 » 报头 233

4.1.2.5.1 DMARC 验证



DMARC 验证

启用 DMARC 验证和报告
启用此项时，MDaemon 将对在入站邮件的 "From:" 报头中找到的域执行 DMARC DNS 查询，并按照您在 "DMARC 报告 456" 屏幕上所设置的发送综合和故障报告。DMARC 使用 SPF 440 和 DKIM 443 来验证邮件，因此必须至少启用其中一个功能才能使用 DMARC。默认情况下启用 DMARC 验证和报告，而且应用于大多数 MDaemon 配置。

> 禁用 DMARC 支持会导致您的用户收到呈增长趋势的垃圾邮件、网络钓鱼邮件或其他伪造的邮件。还会引起您的一些邮件列表邮件被其他服务器拒收，甚至从您的列表中删除一些列表成员。您不得禁用 DMARC，除非您确认您必须那么做。

不验证来自已验证会话的邮件
默认情况下，MDaemon 不对通过已验证会话收到的邮件执行 DMARC 查询。已验证的会话包括由 SMTP 验证 438、POP 先于 SMTP 433 或 IP 防护 436 验证的会话。

不验证来自可信 IP 的邮件
默认情况下，MDaemon 不对来自可信 IP 地址 435 的邮件执行 DMARC 查询。

缓存 DMARC 记录

默认情况下，MDaemon 将在 DNS 查询期间缓存找到的 DMARC 记录数据。通过临时缓存这些信息，在未来处理来自相同域的邮件时，您可以提高效率。

缓存

此按钮打开 DMARC 缓存，它列出当前已缓存的所有 DMARC 记录。

豁免列表

点击此按钮来打开 DMARC 豁免列表。来自该列表中指定的任何 IP 地址的邮件不会受到 DMARC 验证。

DMARC 验证还准许 VBR 证书 462 和已批准列表 465，可以基于来自可信源的已验证 DKIM 标识符和 SPF 路径被豁免。例如，如果抵达的一封邮件无法通过 DMARC 检查，不过拥有一个有效的 DKIM 签名，而且该签名来自位于“批准列表”的域，那么此邮件不受惩罚性 DMARC 策略的限制（例如将此邮件视为其策略是“p=none”）。如果 SPF 路径验证匹配“批准列表”上的一个域，将发生相同的情况。

DMARC 邮件处理

在 DMARC 生成“FAIL”结果时准许 p=reject

默认情况下，启用这个选项，意味着 MDaemon 将准许 p=reject DMARC 策略，前提是邮件的“发件人：”域已在其 DMARC 记录中发布了一个策略，而该邮件未通过 DMARC 验证。将在 SMTP 会话期间拒收未通过 DMARC 验证的邮件。

默认情况下禁用此项，而且当邮件无法通过 DMARC 验证时，MDaemon 会将“X-MDDMARC-Fail-policy: reject”报头插入该邮件而不是拒收这封邮件。在这种情况下，您可以使用“内容过滤器”，基于这些存在的报头来执行一些操作，例如将该邮件发送至特定的文件夹进行审核。此外，您可以使用下方的“*将未通过 DMARC 测试的邮件过滤到垃圾邮件文件夹*”这个选项来将该邮件放入收件人的垃圾邮件文件夹。

即使您禁用此项，也会出于一些与 DMARC 无关的原因拒收这种邮件，例如该邮件拥有超过许可阈值的“垃圾邮件过滤器总值 565”。

将未通过 DMARC 测试的邮件过滤到垃圾邮件文件夹

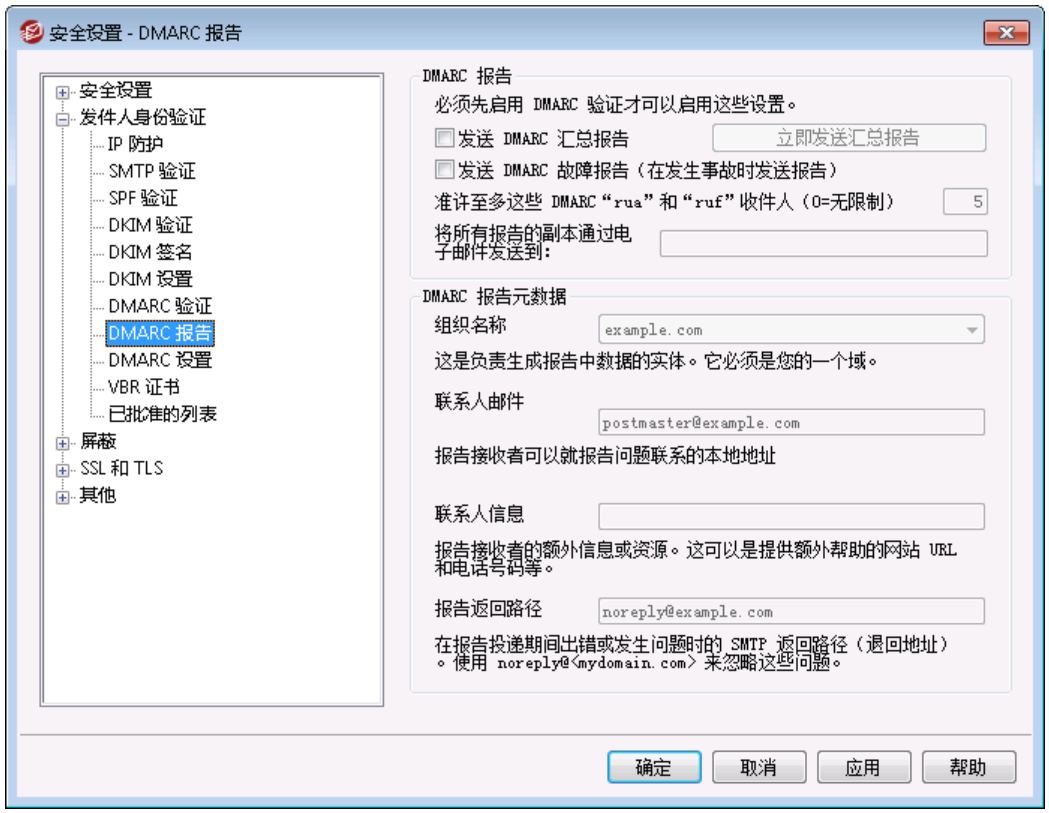
如果您希望在收到未通过 DMARC 验证的邮件时，将该邮件自动过滤到收件人账户的垃圾邮件（例如 junk e-mail）文件夹，请启用此项。如果该用户没有这个文件夹，MDaemon 将在需要时创建此文件夹。

启用此项时，仅在“From:”域发布了存在限制的 DMARC 策略（例如 p=quarantine or p=reject）时应用这个选项。当域发布了 p=none 策略，这表示该域仅监控 DMARC，不采取任何惩罚性措施。

还请参阅：

DMARC 449
DMARC 报告 456
DMARC 设置 459
邮件列表 » 设置 231
邮件列表 » 报头 233
批准列表 465

4.1.2.5.2 DMARC 报告



在 MDaemon 查询 DNS 是否存在 DMARC 记录时，该记录可能包含各种标签，指示域的拥有者是希望接收与声称来自此域邮件相关的 DMARC 综合报告还是故障报告。"DMARC 报告"屏幕上的一些选项供您用来指定是否希望发送请求的报告类型，并指定这些报告应该包含的元数据。只有启用了*"启用 DMARC 验证和报告"*这个选项（位于 DMARC 验证 454"屏幕），该屏幕的选项才可用。此外，DMARC 规范要求使用报告收件人提供的 STARTTLS 481。因此您应该尽可能启用 STARTTLS。

DMARC 报告

发送 DMARC 综合报告
如果您希望向要求 DMARC 综合报告的域发送该报告，请启用此项。如果对入站邮件的 "From:" 执行 DMARC DNS 查询时发现其 DMARC 记录包含 "rua="这个标签（例如

rua=mailto:dmarc-reports@example.com)，这就表示该域的拥有者希望接收 DMARC 综合报告。因此 MDaemon 将存储有关此域和声称来自此域的入站邮件的 DMARC 相关信息 它会记录接收综合报告的邮件地址、每封邮件使用的验证方式 (SPF、DKIM 或两者)、该邮件是否通过验证、发件服务器、其 IP 地址和应用的 DMARC 策略等。然后在每晚午夜 (UTC)，MDaemon 将使用存储的数据来生成各个域的报告，并将其发送至指定的地址。一旦发送了这些报告，已存储的 DMARC 数据将被清除，MDaemon 也将再次重新开始整个流程。

MDaemon 不支持对综合报告使用 DMARC 报告的间隔标签 (例如 "i=")。MDaemon 从上次生成和发送 DMARC 报告后，在每晚午夜 (UTC)将综合报告发送至为其编译了 DMARC 数据的任何域。

立即发送综合报告
如果您希望从当前已存储的 DMARC 数据生成并发送批量的综合报告，而不是等候 MDaemon 在执行下一个午夜批量事件时进行这个任务，请点击此项。这将立即发送报告并清除已存储的 DMARC 数据，就和每晚午夜执行的操作一样。然后 MDaemon 将开始再次存储 DMARC 数据，直到执行下一个午夜 UTC 事件或您再次点击此按钮为止。

因为 MDaemon 必须在午夜 UTC 自动运行来发送综合报告并清除已存储的 DMARC 数据，如果您在那时关闭了 MDaemon，则不会生成任何报告，也不会清除 DMARC 数据。每当 MDaemon 再次运行时便会继续收集 DMARC 数据，不过直到下一个午夜 UTC 事件或您点击了 *"立即发送综合报告"*这个按钮时才会生成报告并清除数据。

发送 DMARC 故障报告 (仅在发生事件时发送该报告)
如果您希望向要求 DMARC 故障报告的域发送该报告，请启用此项。如果对入站邮件的 "From:"执行 DMARC DNS 查询时发现其 DMARC 记录包含 "ruf="这个标签 (例如 ruf=mailto:dmarc-failure@example.com)，这就表示该域的拥有者希望接收 DMARC 故障报告。这些报告不像综合报告那样是实时创建的，故障报告只在发生事件时才被触发，而且包含有关各个事件和故障错误的详细信息。域管理员可以使用这些报告来进行取证分析，并通过修改其邮件系统的配置来修复问题或识别其他问题，例如持续网络钓鱼攻击。

将触发故障报告的故障类型取决于该域的 DMARC 记录中 "fo="标签的值。默认情况下，仅在未通过所有基本的 DMARC 检查 (例如未通过 SPF 和 DKIM)时才生成故障报告，不过域可以使用各种 "fo="标签值来表示它们希望仅在未通过 SPF、DKIM 或其他验证组合时就接收故障报告。因此，取决于在 DMARC 记录的 "ruf="标签中的收件人数量、"fo="标签的值、以及在邮件处理期间遇到的独立验证失败的数量，可以从一封邮件生成多个故障报告。如果您希望限制接收 MDaemon 将发送的指定报告的收件人数量，请使用下方的 *"准许至多这些 DMARC 'rua'和 'ruf'收件人"*这个选项。

至于报告格式，MDaemon 只准许 "f=afrf"这个标签 (使用滥用报告格式的验证故障报告)，这是 DMARC 的默认值。所有报告都以这个格式发送，即使域的 DMARC 记录含有 "f=iodef 这个标签。

为了支持 DMARC 故障报告，MDaemon 完全支持：RFC 5965：邮件反馈报告的可扩展格式、RFC 6591：使用滥用报告格式的验证故障报告、RFC 6652：使用滥用报告格式的发件人策略框架（SPF）验证故障报告、RFC 6651：针对故障报告的域名秘钥标识邮件（DKIM）的扩展 和 RFC 6692：滥用报告格式（ARF）报告中的源端口.

当 DMARC 的 "fo="标签要求报告 SPF 相关故障时，MDaemon 将按照 RFC 6522 来发送 SPF 故障报告。因此，在该域的 SPF 记录中必须存在那个规范的扩展。SPF 故障报告不独立于 DMARC 处理或在缺少 RFC 6522 扩展的情况下进行发送。

当 DMARC 的 "fo="标签要求报告 DKIM 相关故障，MDaemon 将按照 RFC 6651 发送 DKIM 故障报告。因此，在 DKIM 签名报头字段中必须存在该规范的扩展，而且这个域必须在 DNS 中发布有效的 DKIM 报告 TXT 记录。DKIM 故障报告不独立于 DMARC 处理或在缺少 RFC 6651 扩展的情况下进行发送。

准许至多这些 DMARC "rua"和 "ruf"收件人（0 = 无限制）
如果您希望限制将接收 MDaemon 所发送的指定 DMARC 综合报告或 DMARC 故障报告的收件人数量，请在此处指定最大值。如果 DMARC 记录的 "rua="或 "ruf="标签包含的地址数量大于您所指定的限制，那么 MDaemon 会将指定报告按顺序发送至列出的地址，直到达到地址最大值为止。默认情况下不设置限制。

将所有报告的副本通过电子邮件发送到：
在此处输入一个或多个由逗号分隔的电子邮件地址，来将所有 DMARC 汇总报告和 DMARC 失败报告的副本发送到这些地址（仅 fo=0 或 fo=1）。

DMARC 报告元数据

使用这些选项来指定您公司或组织的元数据，会将这些数据包含于您所发送的 DMARC 报告中。

组织名称
这是负责生成 DMARC 报告的实体。它必须是您的 MDaemon 域之一。从下拉列表中选择域。

联系人邮件
使用此项来指定报告收件人在报告问题时可以联系的本地邮件地址。使用逗号来分隔多个地址。

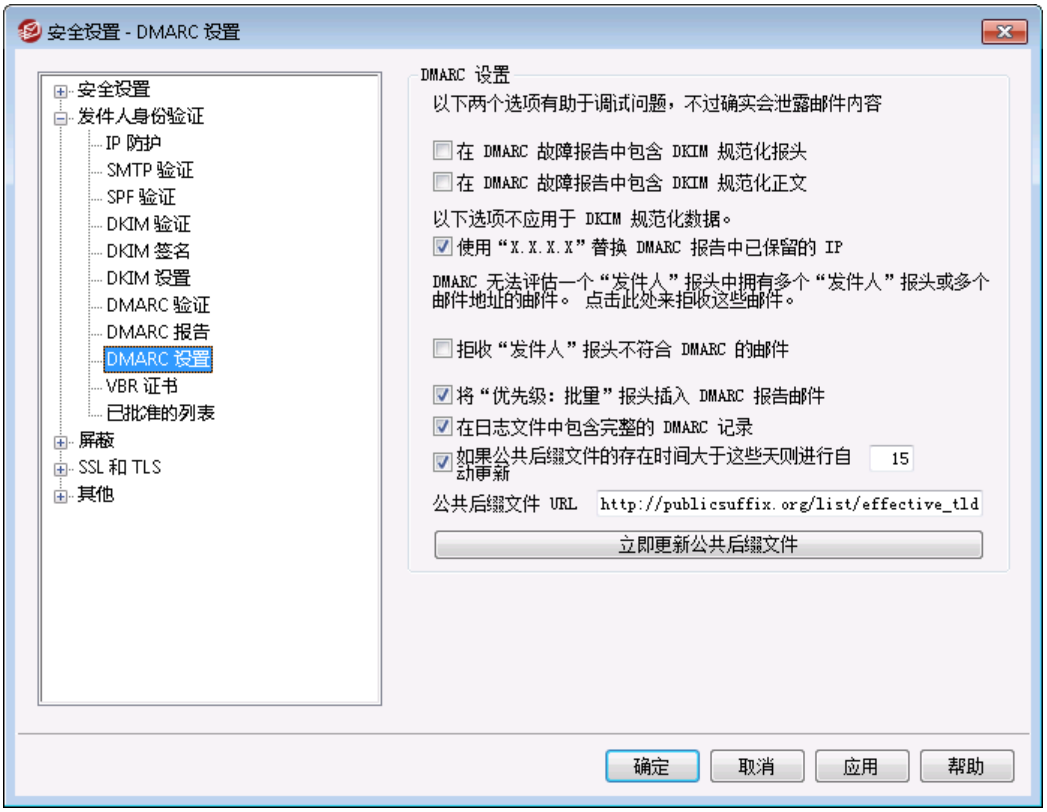
联系信息
使用此项为报告收件人包含任何额外的联系信息，例如网站和电话号码等。

报告返回路径
这是用于 MDaemon 所发送的报告邮件的 SMTP 返回路径（退回地址），以防投递出现问题。使用 "noreply@<mydomain.com>"来忽略这些问题。

还请参阅：

DMARC 449
DMARC 验证 454
DMARC 设置 459

4.1.2.5.3 DMARC 设置



DMARC 设置

在 DMARC 故障报告中包含 DKIM 规范化报头
如果您希望将 DKIM 规范化报头 447 包含于 DMARC 故障报告 456 中，则启用此项。默认情况下，禁用该选项。

在 DMARC 故障报告中包含 DKIM 规范化正文
如果您希望将 DKIM 规范化正文 447 包含于 DMARC 故障报告 456 中，则启用此项。默认情况下，禁用该选项。

在 DMARC 报告中使用 “X.X.X.X”替换保留的 IP
默认情况下，MDaemon 在 DMARC 报告中使用 “X.X.X.X”来替换您保留的 IP 地址。如果您希望使您保留的 IP 在 DMARC 报告中可见，请禁用此项。此项不应用于 DKIM 规范化数据。

如果“发件人”与 DMARC 不兼容则拒收邮件
如果您希望在邮件的“发件人”报头结构与 DMARC 要求不兼容的情况下拒收这封邮件，请启用此项。这些是拥有多个“发件人”报头的邮件，或在一个“发件人”报头中拥有多个邮件地址的邮件。当前从 DMARC 处理中免除这些邮件。默认情况下禁用此设置，因为在一个“发件人”报头中拥有多个地址将在技术上引起协议违规，不过启用此设置有助于最大化 DMARC 保护。在启用 DMARC 验证 454 时仅应用这个设置。

插入“Precedence:bulk”报头到 DMARC 报告邮件
默认情况下 MDaemon 会将群发邮件报头插入 DMARC 报告邮件。如果您不希望插入该报头，请清除该复选框。

在日志文件中包含完整的 DMARC 记录
默认情况下 MDaemon 记录在 DMARC DNS 查询期间获得的完整 DMARC DNS 记录。如果您不希望在日志文件中包含完整的 DMARC 记录，请禁用此项。

如果存在时间长于这些天则自动更新公共前缀文件
DMARC 需要公共后缀文件来确定查询 DMARC DNS 记录的正确域。默认情况下，每当 MDaemon 存储的公共后缀文件的存在时间大于 15 天，它将自动更新这些文件。如果您希望更新公共后缀文件的时间值大于或小于此值，请更改此项的值。如果您不希望进行自动更新，请禁用此项。

公共后缀文件 URL
这是 MDaemon 用来为 DMARC 下载公共后缀文件的 URL。默认情况下 MDaemon 使用位于以下位置的文件：http://publicsuffix.org/list/effective_tld_names.dat。

立即更新公共后缀文件
点击此按钮来从上方指定的“*公共后缀文件 URL*”手动更新公共后缀文件。

还请参阅：

DMARC 449
DMARC 验证 454
DMARC 报告 456
DKIM 设置 447

4.1.2.6 邮件证书

邮件证书指的是一个实体担保或“证明”另一个实体的良好邮件传输品行。因此，当发证实体被收件邮件服务器信任，则由该实体担保的域所发邮件可以较少怀疑地查看。因此接收服务器在一定程度上获得保证，发送域会遵守一套良好的邮件实践且不发送垃圾邮件或其他有问题的信息。证书非常有用，因为它有助于确保邮件将不会错误地或不必要地遭受无担保的垃圾邮件过滤器分析。邮件证书还有助于降低处理每封邮件所需的资源。

MDaemon通过在全球范围内第一个将名为“Vouch-By-Reference”(VBR)的 Internet 邮件新协议用于商业目的，进而支持邮件证书。MDaemon Technologies 通过加入 Domain Assurance Council(DAC)，致力于协助创建并扩展这一协议。通过 VBR 提供的机制，证书服务提供商(CSP)或“认证方”为特定域的良好邮件实践提供担保。

证明入站邮件

将 MDaemon 的邮件证书功能配置为检查入站邮件非常方便。只需点击 *"启用入站邮件认证"*选项，位于认证对话框上（安全 » 安全设置 » 发件人身份验证 » 认证），并输入一个或多个您信任的认证提供商以担保入站邮件（如 vbr.emailcertification.org）即可。您还可以选择为已认证邮件豁免垃圾邮件过滤处理，或为其垃圾邮件过滤器总值设置有利的调整值。

证明出站邮件

配置 MDaemon 将证书数据插入出站邮件之前，首先需要安排一个或多个 CSP 来证明您的邮件。MDaemon Technologies 为 MDaemon 客户提供证书服务。要了解详细信息，请访问：www.mdaemon.com。

要在注册 CSP 后将 MDaemon 服务器配置为对出站邮件使用邮件证书：

1. 打开 "VBR 证书"对话框：点击 安全 » 安全设置 » 发件人身份验证 » VBR 证书。
2. 点击 *"在出站邮件中插入证书数据"*。
3. 点击 *"为邮件证书配置域"*。这会打开 "证书设置"对话框。
4. 输入 *域名*，其出站邮件将包含证书数据。
5. 使用 *邮件类型* 下拉列表选择 CSP 同意为该域认证的邮件类型，如果所需类型未列出，可输入新类型。
6. 输入一个或多个愿意认证该域出站邮件的 CSP。如果有多个 CSP 则使用空格将其隔开。
7. 点击 *"确定"*。
8. 配置服务器在该域的出站邮件中使用 DKIM 442 签名，或确保邮件发自经 SPF 440 认可的服务器。这对保证您发出的邮件非常必要。除非接收服务器能首先确定邮件是可靠的，否则无法认证该邮件。

VBR 不需要 CSP 签名或传输已认证的邮件。CSP 并非要签名或验证指定的邮件，而是担保域的良好邮件实践。

技术支持是整个 MDaemon Technologies 客户体验的重要部分。

http://www.mdaemon.com/email-certification/

VBR 规范 - RFC 5518：

http://tools.ietf.org/html/rfc5518

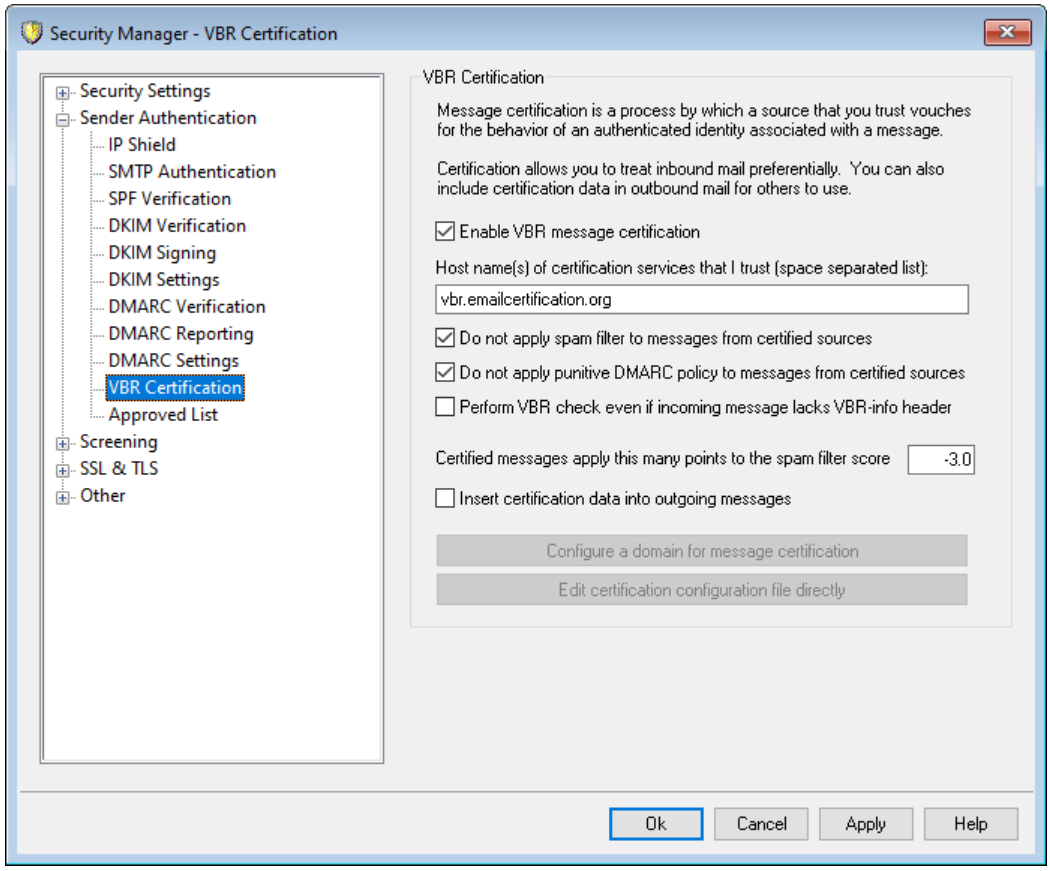
有关 DKIM 的更多信息，请访问：

http://www.dkim.org/

还请参阅：

VBR 证书 462

4.1.2.6.1 VBR 证书



VBR 证书对话框位于："安全» 安全设置» 发件人身份验证» VBR 证书"

VBR 证书

启用 VBR 邮件证书
点击该复选框启用入站邮件的证书。当 MDaemon 收到需要证书的入站邮件时，将查询可信的证书服务供应商 (CSP)以确认该邮件是否确为 "已认证"邮件。如果是这样，则根据以下选项的设置，邮件将免于进行垃圾邮件过滤或对其垃圾邮件过滤器 564分值进行调整。

我信任的证书服务主机名 (通过空格隔开的列表)：
使用该文本框输入您信任的证书服务主机名。如果您信任多个服务，则相互之间用空格分隔。

不对来自已验证源的邮件应用垃圾邮件过滤器
如果您希望让来自已验证源的邮件免于“垃圾邮件过滤器”，则选择该选项。

不对来自已验证源的邮件应用惩罚性 DMARC 策略。
如果发件域发布了存在限制的“DMARC 策略 454”(例如 p=quarantine or p=reject)而且邮件未通过 DMARC 检查，该选项确保来自已验证源的认证邮件不受惩罚。默认情况下启用此项。

即使入站邮件缺少“VBR-info”报头也执行 VBR 检查
如果您希望即使入站邮件缺少“VBR-info”报头时也执行 VBR 检查，则启用此项。通常这个报头十分必要，不过 VBR 仍能在缺少此报头的情况下工作。在缺少上述报头时，MDaemon 将使用“全部”邮件类型查询您的可信 CSP。默认情况下，禁用该选项。

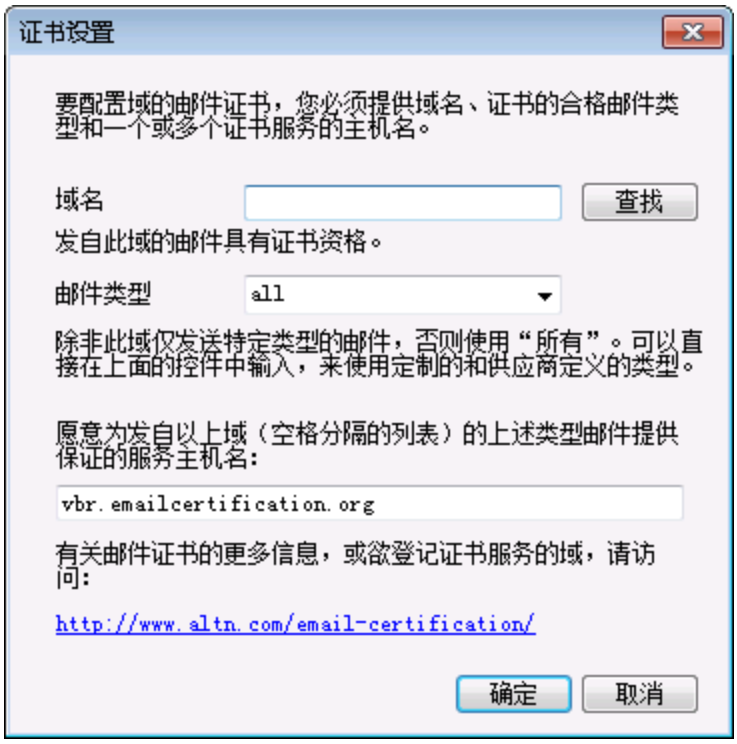
已认证的邮件向垃圾邮件过滤总值中应用此分数
如果不希望使已认证邮件免于进行垃圾邮件过滤处理，则可使用该选项为邮件指定垃圾邮件过滤器总值的调整分数。通常应该为负数，便于已证明的邮件得到有利的调整。默认设置为“-3.0”。

在出站邮件中插入证书信息
点击该复选框向出站邮件中插入证书数据。然后，点击*为邮件证书配置域*按钮打开证书设置对话框指定要认证的特定域及其关联的 CSP。

为邮件证书配置域
启用上述*在出站邮件中插入证书数据*选项后，点击该按钮可打开证书设置对话框。在此对话框中将指定对其出站邮件要进行认证的域，要认证的邮件类型以及与该域关联的 CSP。

直接编辑证书配置文件
启用上述*在出站邮件中插入证书数据*选项后，点击该按钮可打开 Vouch-by-Reference (VBR) 配置文件。任何通过“证书设置”对话框配置为使用 VBR 的域以及相关的 VBR 数据都将列在此文件中。您可以使用此文件编辑这些条目或手动创建新条目。

证书设置



启用证书对话框上的 *"在出站邮件中插入证书数据"*选项后，点击 *"为邮件证书配置域"*按钮可打开证书设置对话框。此对话框用于指定要认证的出站邮件的域，要认证的邮件类型以及与域相关联的 CSP。

证书设置

域名
使用该选项输入要认证的出站邮件的域。

查找
如果以前为特定域配置过邮件证书设置，输入 *"域名"*然后点击该按钮会在证书设置对话框选项中罗列出该域的设置。

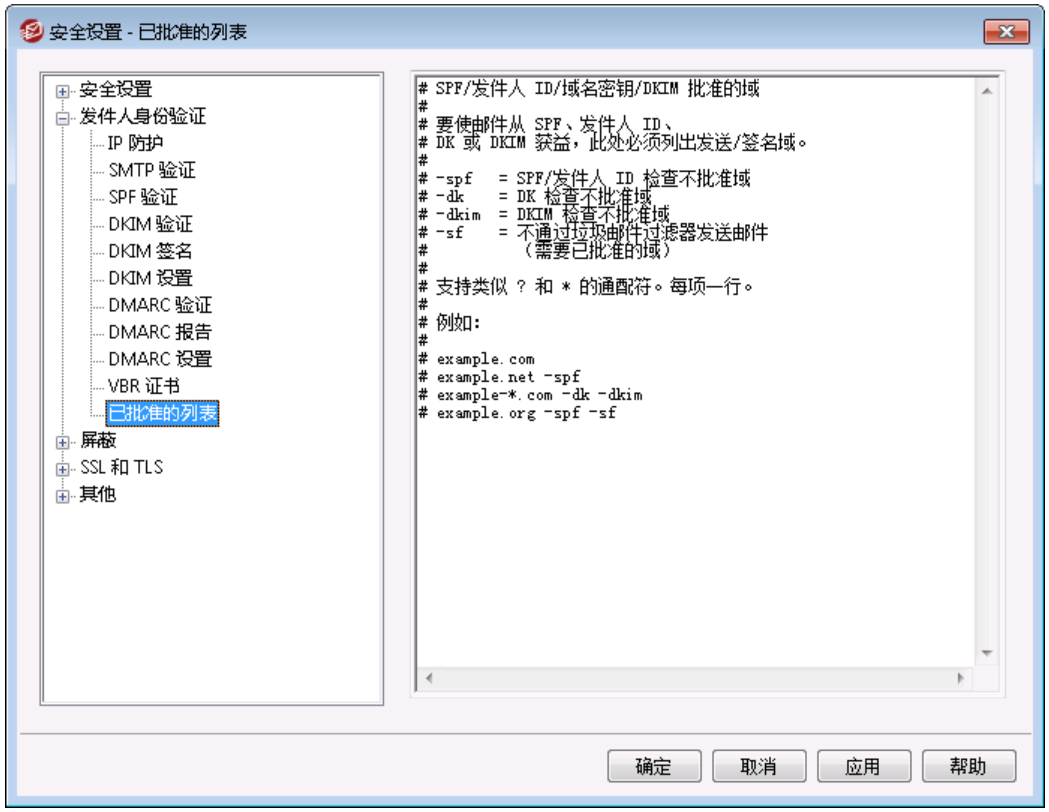
邮件类型
使用此下拉列表选择相关联的 CSP 已同意为该域认证的邮件类型。如果类型未列出，则可手动输入。

服务域名…
输入 CSP 的主机名，此 CSP 已同意认证该域的出站邮件 (例如 vbr.emailcertification.org)。如果输入多个 CSP，则互相之间用空格隔开。

还请参阅：

邮件证书 460

4.1.2.7 批准列表



由于某些垃圾邮件制造者和群发邮件发件人已开始使用 SPF 或有效的 DKIM 邮件签名，因此经过签名和验证的邮件尽管能确保是来自有效源，但无法保证它并非垃圾邮件。因此，邮件的垃圾邮件总值不会因为 SPF 或 DKIM 验证结果而降低，除非取自签名的域在已批准列表中。这实质上是一个允许列表，用于指定在验证入站邮件时，允许降低其邮件的垃圾邮件总值的域。

当由这些域签名的邮件通过 SPF 或 DKIM 验证时，将根据 SPF 440 以及 DKIM 验证 443 屏幕上的设置，降低其垃圾邮件总值。不过，如果要防止这些验证方法降低总值，可以附加以下列出的任何旗标。还有一种参数可用于防止已验证邮件经由 "垃圾邮件过滤器"的处理。

-spf 不降低由该域发送的经 SPF 验证邮件的垃圾邮件总值。

-dkim 不要降低来自该域的经 DKIM 验证邮件的垃圾邮件总值。

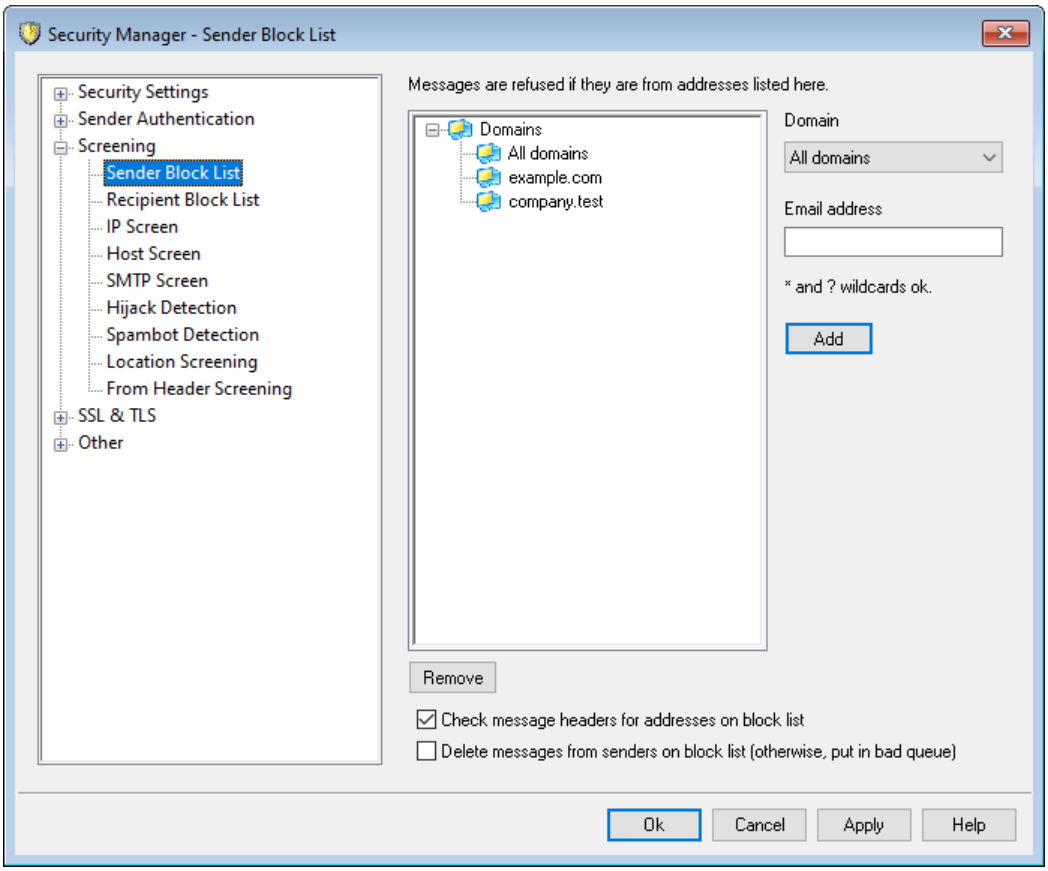
-sf 不要通过垃圾邮件过滤器处理来自该域的已验证邮件。

DMARC 和已批准列表

DMARC 验证 454 也使用 "批准列表"，可以基于来自可信源的已验证 DKIM 标识符和 SPF 路径被豁免。例如，如果抵达的一封邮件无法通过 DMARC 检查，不过拥有一个有效的 DKIM 签名，而且该签名来自位于 "批准列表"的域，那么此邮件不受惩罚性 DMARC 策略的限制（例如将此邮件视为其策略是 "p=none"）。如果 SPF 路径验证匹配 "批准列表"上的一个域，将发生相同的情况。

4.1.3 屏蔽

4.1.3.1 发件人阻止列表



发件人阻止列表位于：安全 » 安全设置 » 屏蔽。该名单中包括了禁止发送邮件到服务器的地址。如果邮件来自该名单中的地址，则在 SMTP 会话期间会拒绝该邮件。这对控制问题用户是非常有用的。可按域或在全局范围内（应用于所有 MDaemon 域）将地址列入阻止列表。

如果邮件来自此处列出的地址，则拒收这些邮件
此窗口显示当前列入阻止列表的所有地址，按域排列。

域
选择与列入阻止列表的地址相关联的域。换句话说，希望阻止哪个域接收来自指定地址的邮件？从列表中选择“所有域”可在全局范围内将地址列入阻止列表。

电子邮件地址
输入希望列入阻止列表的地址。支持通配符，因此“*@example.net”将阻止来自“example.net”域上任何用户的所有邮件，而“user1@*”将阻止来自地址以“user1@”开头的所有邮件（无论该邮件来自哪个域）。

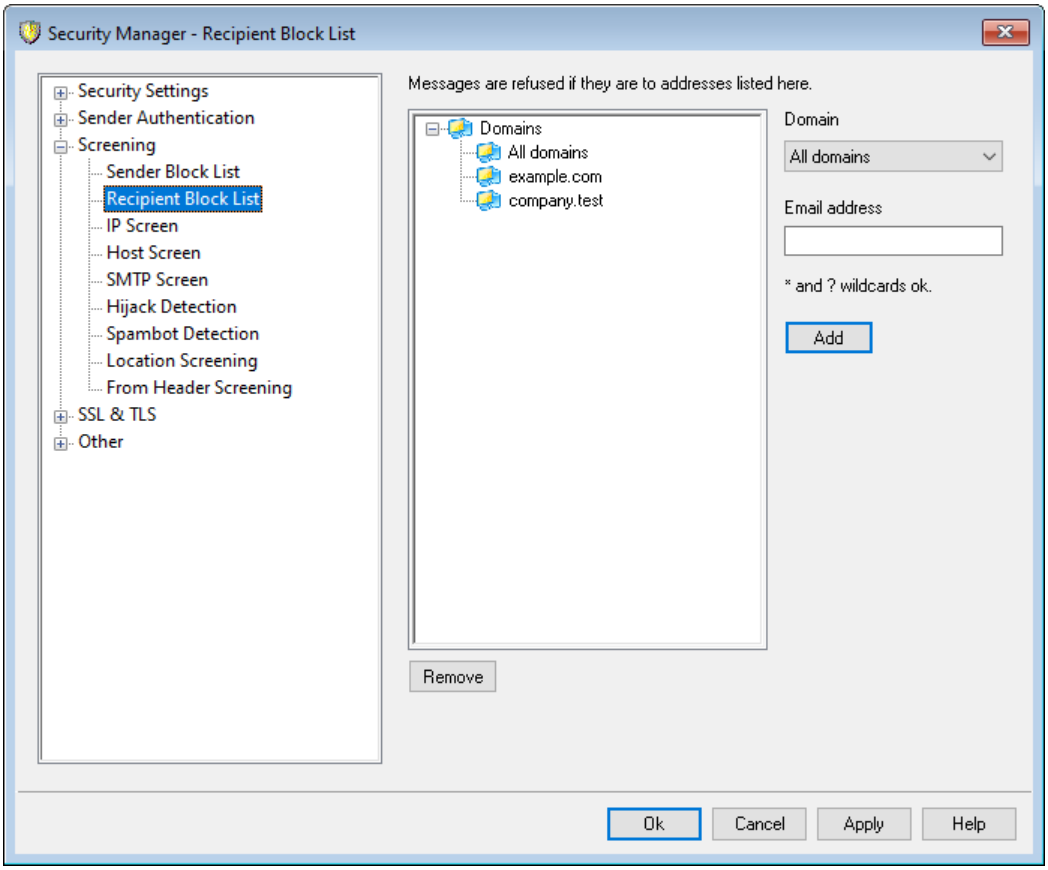
添加
点击该按钮将指定地址添加到阻止列表中。

删除
点击该按钮删除黑名单中的选定项。

检查邮件报头是否存在阻止列表上的地址
默认情况下，MDaemon 会将阻止列表应用至在 SMTP 会话期间取自邮件 From/Sender（发件人）报头的值。这避免了 MTA 线程在稍后捕获邮件并将其移至坏队列中。

删除由阻止列表上的发件人发送的邮件
如果您希望 MDaemon 删除发自被列入阻止列表的入站邮件，请启用此项。除了常规邮件以外，此项还适用于通过 MultiPOP 和 DomainPOP 抵达的邮件。禁用此项时，不会删除这些邮件，而是将其放入“坏邮件队列”中。默认情况下，禁用该选项。

4.1.3.2 收件人阻止列表



收件人阻止列表位于：安全 » 安全设置 » 屏蔽。该名单中含有不允许通过您的服务器接收邮件的电子邮件地址。如果邮件来自该名单中的地址，则拒绝该邮件。可按域或在全局范围内（应用于所有 MDaemon 域）将地址列入阻止列表。“收件人阻止列表”SMTP 操作仅包封 RCPT 数据（非邮件报头）。

如果邮件发往此处列出的地址，则拒收这些邮件
此窗口显示当前列入阻止列表的所有地址，按域排列。

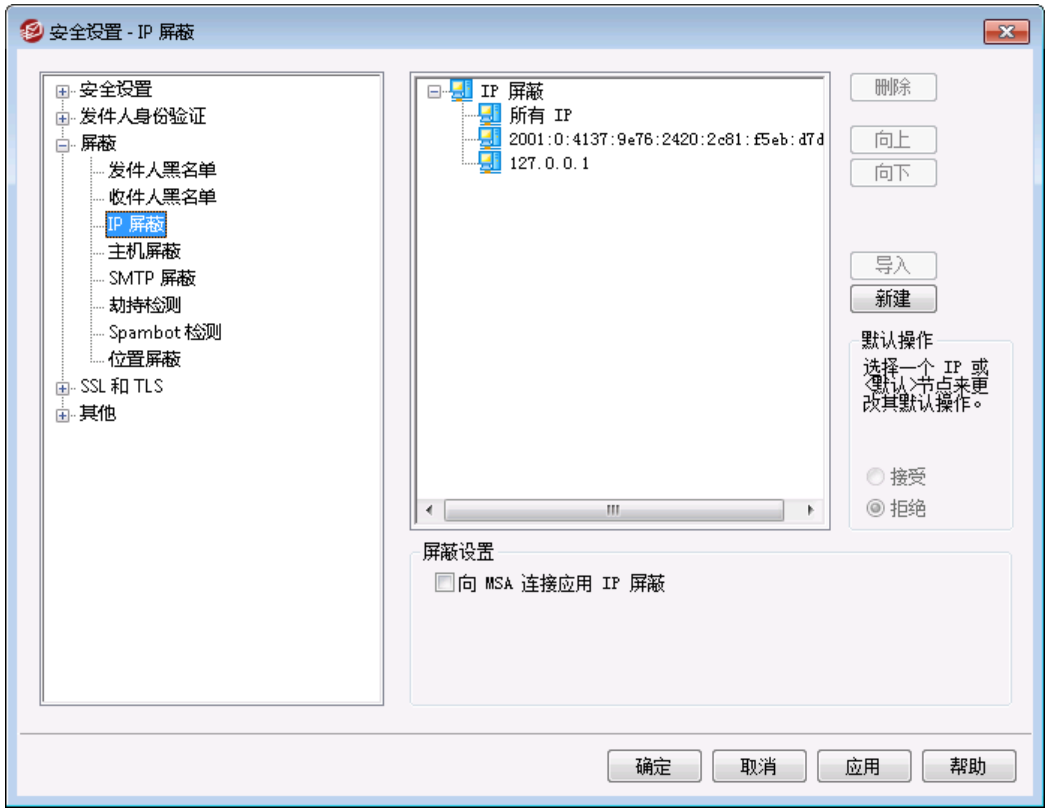
域
选择与列入阻止列表的地址相关联的域。换句话说，希望阻止哪个域接收来自指定地址的邮件？ 从列表中选择 "所有域"可在全局范围内将地址列入阻止列表。

电子邮件地址
输入希望列入阻止列表的地址。支持通配符，因此 "*@example.net"将阻止指向 "example.net"域上任何用户的所有邮件，而 "user1@*"将阻止指向地址以 "user1@ "开头的所有邮件（无论该邮件发往哪个域）。

添加
点击该按钮将指定地址添加到阻止列表中。

删除
点击该按钮删除黑名单中的选定项。

4.1.3.3 IP 屏蔽



IP 屏蔽位于：安全>>安全设置>>屏蔽。它用来定义允许或不允许连接到您本地 IP 地址的远程 IP 地址。置于 IP 屏蔽中的远程 IP 地址可以与所有本地 IP 地址或个别 IP 地址相关联。允许使用 DIDR 记数法和 *、#、? 通配符。

例如：

..*.*	匹配任何 IP 地址
..*.*	匹配任何 IP 地址
192.*.*.*	匹配任何以 192 开头的 IP 地址

192.168.*.239	匹配从 192.168.0.239 到 192.168.255.239 范围内的 IP 地址
192.168.0.1??	匹配从 192.168.0.100 到 192.168.0.199 范围内的 IP 地址

新建IP屏蔽条目

要新建 "IP 屏蔽"条目，请点击 **新建**"。这将打开 "新建 IP 屏蔽"项目对话框供您创建新条目。

本地 IP
在下拉列表中选择此项目将应用到的 "所有 IP"或特定 IP。

远程 IP (支持 CIDR、*? 和 # 通配符)
输入要添加到列表中与上面指定的 "本地 IP"相关联的远程 IP 地址。

接受连接
选择该选项意味着允许指定的远程 IP 地址连接到相关联的本地 IP 地址。

拒收连接
选择该选项意味着不允许指定的远程 IP 地址连接到相关联的本地 IP 地址。连接将被拒绝或放弃。

添加
以上选项中的信息输入完毕，点击该按钮可将此条目添加到列表中。

导入

如果您希望导入 APF 或 .htaccess 文件中的 IP 地址数据，请选择一个 IP 地址并点击此按钮。现在 MDaemon 对这些文件的支持包括：

- 支持 "拒绝发件人"和 "允许发件人"
- 只导入 IP 值 (非域名)
- 允许 CIDR 表示法，不过不允许部分 IP 地址。
- 每行可以包含任何数量的由空格分隔或逗号分隔的 IP 地址。例如 "deny from 1.1.1.1 2.2.2.2/16"和 "3.3.3.3, 4.4.4.4, 5.5.5.5"等。
- 将忽视由 # 开头的行。

删除

要删除条目，请在列表中选择这个条目并点击 **删除**"。

默认操作

要为来自未定义的远程 IP 地址的连接指定默认操作，请从列表中选择一个 IP 地址并点击 **接受**"或 **拒收**"。一旦指定了默认操作，您可以通过在 IP 地址下方选择 "<default>"节点，并选择新的默认设置来进行更改。

接受
选择该选项时，将接收 "IP 屏蔽"上未特别定义的任何 IP 地址发起的连接。

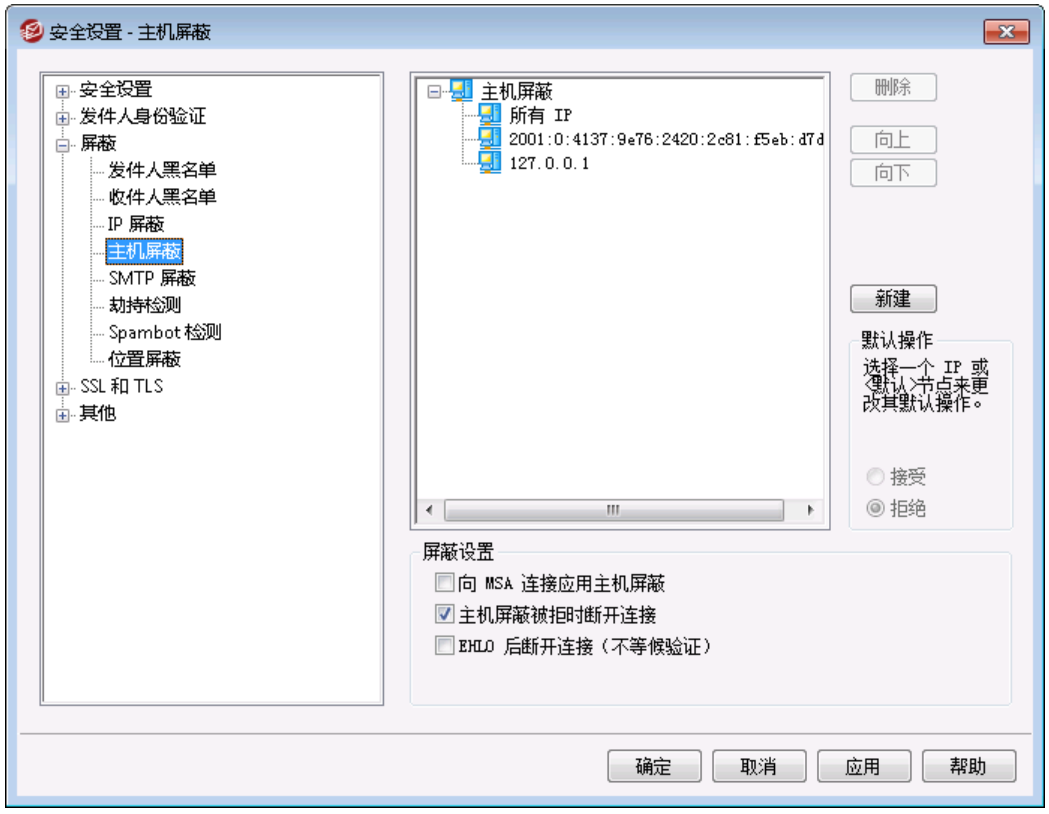
拒绝
选择该选项时，将放弃或拒绝“IP 屏蔽”上未特别定义的任何 IP 地址发起的连接。

> “IP 屏蔽”决不会阻止可信 IP[434]或本地 IP。

屏蔽设置

向 MSA 连接应用 IP 屏蔽
使用此项来向与服务器的 MSA 端口[87]建立的连接应用“IP 屏蔽”。通常这不是必要的。默认情况下启用此设置。

4.1.3.4 主机屏蔽



主机屏蔽位于：安全 » 安全设置 » 屏蔽。主机屏蔽用于定义允许哪些主机与本地 IP 地址建立连接。您可指定一列主机并将服务器配置为只允许来自这些主机的连接，或拒绝来自所列主机的连接。主机屏蔽将在 SMTP 会话期间确定的 EHLO 和 PTR 值与在此指定的值进行比较。

新建主机屏蔽条目

要新建“主机屏蔽”条目，请点击**新建**”。这将打开“新建主机屏蔽”项目对话框供您创建新条目。

本地 IP
使用该下拉列表可选择本地 IP 地址，在其上应用此主机屏蔽条目。如果要应用到所有本地 IP 地址，请选择 "所有 IP 地址"。

远程主机 (允许 * 和 # 通配符)
输入要添加到列表中与上面指定的本地 IP 相关联的远程主机。

接受连接
选择该选项意味着允许指定的远程主机连接到相关联的本地 IP 地址。

拒收连接
选择该选项意味着不允许指定的远程主机连接到相关联的本地 IP 地址。连接将被拒绝或放弃。

删除
要删除条目，请在列表中选择这个条目并点击 **删除**"。

默认操作
要为来自未定义的远程主机的连接指定默认操作，请从列表中选择一个 IP 地址并点击 **接受**"或 **拒收**"。一旦指定了默认操作，您可以通过在 IP 地址下方选择 "<default>"节点，并选择新的默认设置来进行更改。

接受
选择该选项时，将接收主机屏蔽上未特别定义的任何主机发起的连接。

拒绝
选择该选项时，将拒绝主机屏蔽上未特别定义的任何主机发起的连接。

主机屏蔽决不会阻止可信 434 或本地主机。

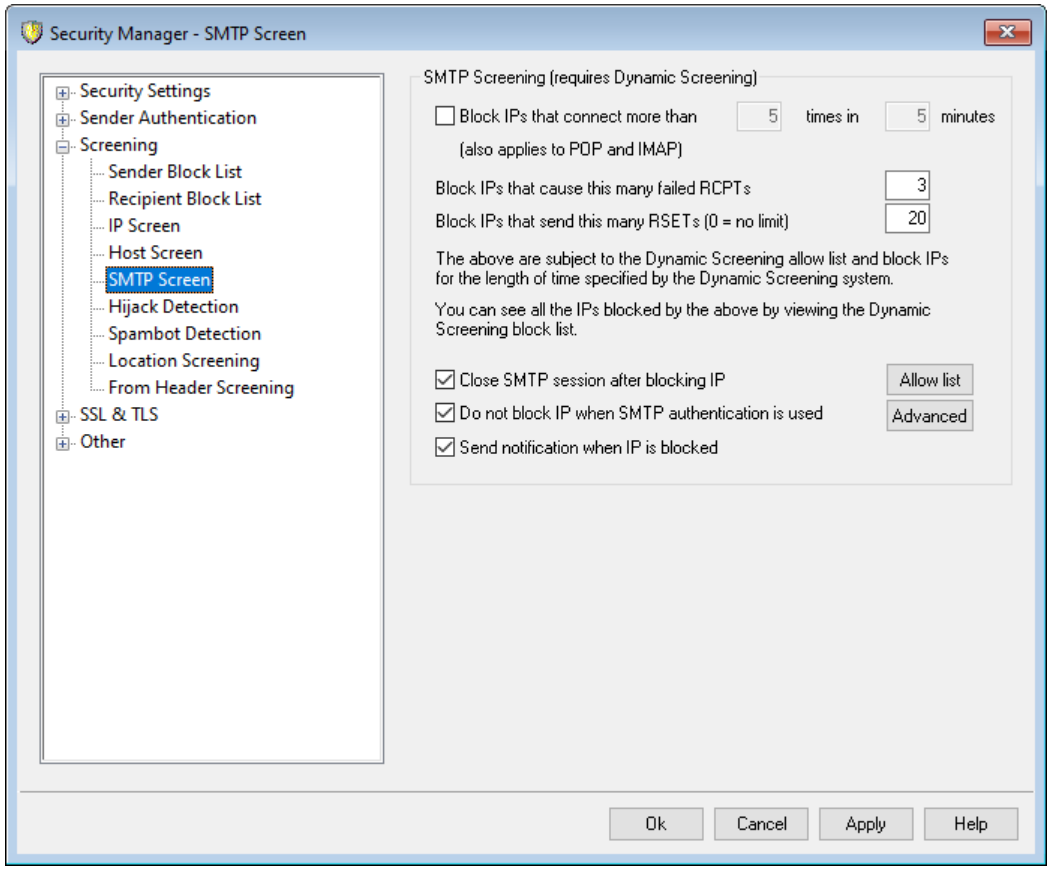
屏蔽设置

向 MSA 连接应用主机屏蔽
使用此项来向与服务器的 MSA 端口 87 建立的连接应用 "主机屏蔽"。默认情况下启用此设置。

在主机屏蔽拒绝时断开连接
在启用此项时，将在 "主机屏蔽"拒绝时立即断开连接。

在 EHLO 后断开连接 (不等候验证)
如果您希望在 EHLO/HELO 后立即断开连接，请启用此项。通常您将等候验证。默认情况下启用此项。

4.1.3.5 SMTP 屏蔽



使用 "SMTP屏幕"，您可以在指定的分钟数内阻止多次连接到 MDaemon 的 IP 地址。您也可以阻止那些引起太多失败 RCPT 的 IP 地址，以及那些发送太多 RSET 命令的 IP 地址。"SMTP 屏蔽"需要 "动态屏蔽"功能，并使用 动态阻止列表[524]和动态允许列表[522]。

阻止在 [X] 分钟内连接超过 [X] 次的 IP 地址
点击该复选框可以暂时阻止在限定时间内与服务器连接次数过多的 IP 地址。指定在该时段的分钟数以及在此期间允许的连接次数。可以在 "验证失败跟踪[513]"屏幕上指定阻止这些地址长达多少时间。此项也应用于 POP 和 IMAP 连接。

阻止造成这么多次 RCPT 尝试失败的 IP
如果在邮件会话期间 IP 地址导致这么多次 "收件人未知"错误，将自动阻止该地址达在以下的 "验证失败跟踪[513]"屏幕中指定的时间。频繁的 "收件人未知"错误往往暗示发件人是垃圾邮件制造者，因为垃圾邮件制造者通常会试图将邮件发送给过时的或不正确的地址。

阻止发送这么多 RSET 的 IP (0=不限)
如果您希望在一个邮件会话期间，阻止任何发出指定数量 RSET 命令的 IP 地址，请使用此选项。如果您不希望限制设置则使用 "0"。在 "服务器设置"下的 "服务器[74]"屏幕上有一个类似选项，可以用来设置所允许的 RSET 命令数量的硬限制。可以在 "验证失败跟踪[513]"屏幕上指定阻止这些地址长达多少时间。

阻止 IP 后关闭 SMTP 会话
启用该选项将造成 MDaemon 在阻止 IP 地址后关闭 SMTP 会话。默认启用此项。

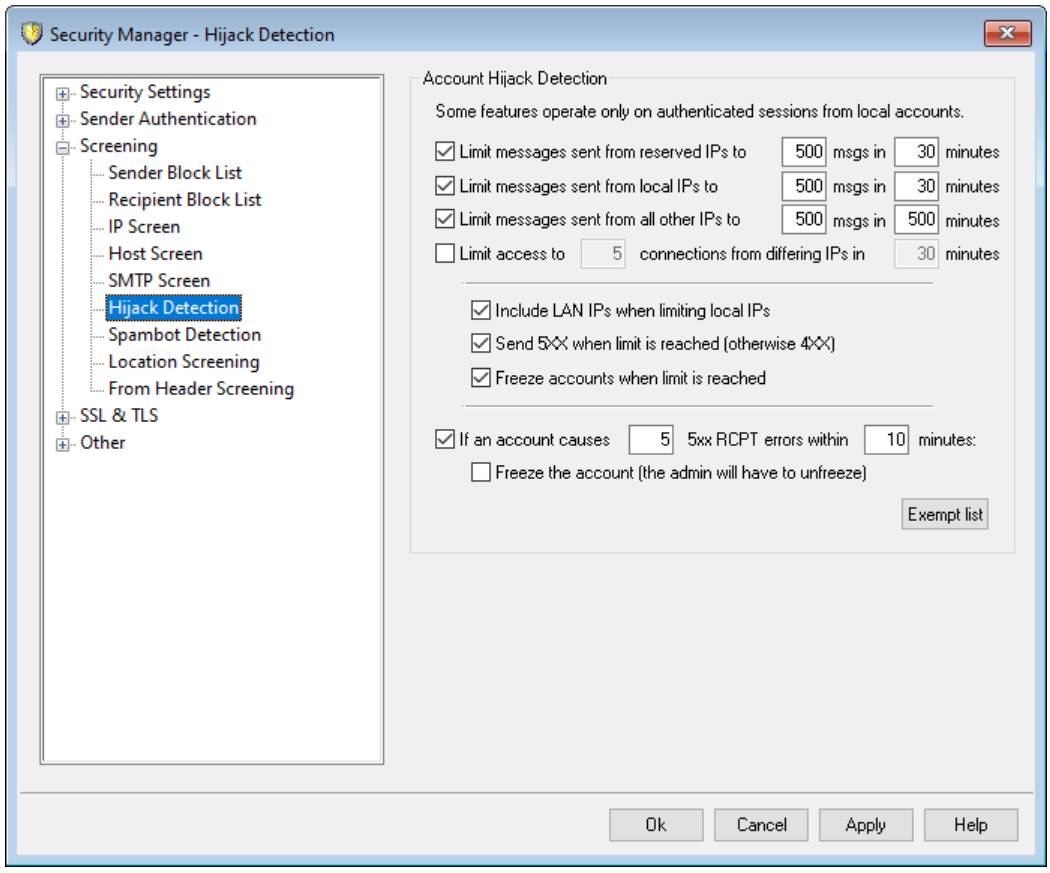
使用 SMTP 验证时不阻止 IP
如果要从动态屏蔽中排除发送前对邮件会话进行身份验证的发件人，则点击该复选框。默认启用此项。

在 IP 被阻止时发送通知
默认情况下，当"动态屏蔽"系统自动阻止 IP 地址时，"动态屏蔽"的"*IP 地址阻止报告*[517]"选项将用于通知您相关操作。如果由于 SMTP 屏蔽功能阻止 IP 地址时不希望收到通知，请清除此复选框。

允许列表
点击此按钮来打开 动态允许列表[522]过期时，此项会将报告发送至指定的地址。在此列出的 IP 地址免于 SMTP 屏蔽。

高级
此按钮打开动态屏蔽[510]对话框。

4.1.3.6 劫持检测



账户劫持检测

可以使用这个屏幕的选项来检测可能被劫持的 MDaemon 账户，并自动阻止该账户通过您的服务器发送邮件。例如，如果垃圾邮件发件人不知如何获得了一个账户的电子邮件地址和密码，然后该功能可以阻止垃圾邮件发件人使用此账户通过您的系统发送大量垃圾邮件。您可以指定在给定的分钟数内，以及基于与其建立连接的 IP 地址，可由一个账户发送的最大邮件数量。您也可以选择禁用达到这个限制的账户。还提供一个 *豁免列表*，可用于使一些特定的地址免于该限制。默认情况下启用 "账户劫持检测"。

"账户劫持检测"仅适用于已验证会话中的本地账户，并自动免除邮件管理员账户。

限制发自已保留 IP 的邮件为 [xx]封邮件于 [xx]分钟内
如果您希望阻止连接了已保留 IP 的 MDaemon 账户在指定的分钟数内发送超过指定数量的邮件，请使用此项。绝大多数情况下，由 RFC 定义已保留的 IP 地址（例如 127.0.0.*、192.168.*.*、10.*.*.*、172.16.0.0/12、::1、FD00::/8、FEC0::/10 和 FE80::/64）。

限制发自本地 IP 的邮件为 [xx]封邮件于 [xx]分钟内
如果您希望阻止连接了任何本地 IP 的 MDaemon 账户在指定的分钟数内发送超过指定数量的邮件，请使用此项。本地 IP 是为您的任何 MDaemon 域进行配置的所有 IP 地址。

限制发自所有其他 IP 的邮件为 [xx]封邮件于 [xx]分钟内
如果您希望阻止连接了任何其他 IP 的 MDaemon 账户在指定的分钟数内发送超过指定数量的邮件，请使用此项。

限制访问来自不同 IP 的 [xx]连接，在 [xx]分钟内
使用此项来限制指定分钟数内允许来自不同 IP 地址的连接数量。例如：在常规情况下，如果仅在几分钟内就有 10 个不同的 IP 地址访问了您的账户，您的账户就可能被劫持。默认情况下禁用此项。

在限制本地 IP 时包含 LAN IP
默认情况下包含 LAN IP[508]（在使用上方的 *"限制从本地 IP 发送的邮件..."*时）。如果在限制本地 IP 时您不希望包含 LAN IP，请取消勾选此框。

在达到限制时发送 5XX（否则 4XX）
默认情况下在达到限制时 MDaemon 会向被劫持的账户发送 5XX 响应代码。如果您希望发送 4XX 代码请禁用此项。

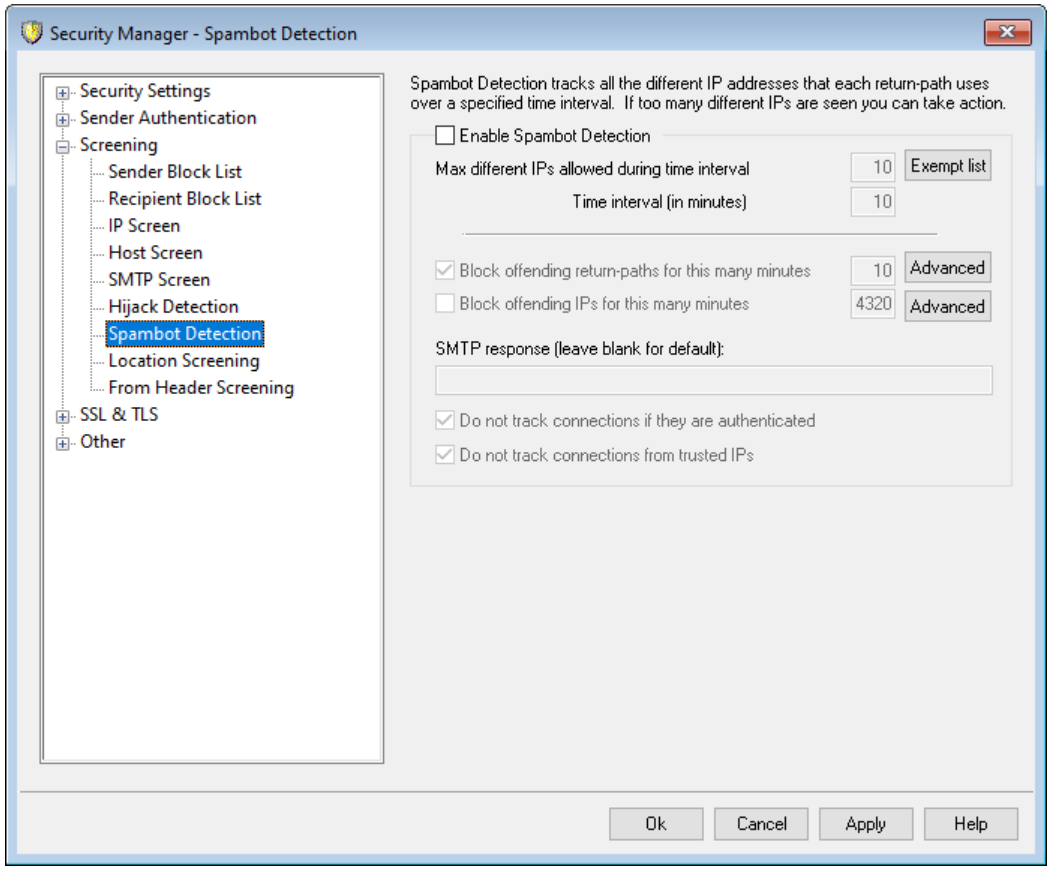
在达到限制时冻结账户
如果您希望冻结尝试发送超过指定数量邮件的账户，请勾选此框。发生上述情况时，服务器将发送 552 错误，断开连接，并立即冻结该账户。被冻结的账户不再能发送邮件或检查其邮件，不过 MDaemon 将仍然为此账户接收入站邮件。而且在冻结账户时，会向邮件管理员发送一封有关此账户的电子邮件。如果邮件管理员希望重新启用此账户，他只需回复这封邮件即可。

如果账户在 [xx] 分钟内引起 [xx] 5xx RCPT 错误
此选项监控账户在固定时间内尝试将邮件发送给无效收件人的次数。垃圾邮件的一个普遍特征是，由于垃圾邮件发送者试图将其发送到旧的电子邮件地址，或猜测新的电子邮件地址，因此通常将这些邮件发送给大量无效的收件人。因此，如果 MDaemon 账户在短时间内开始向大量无效收件人发送邮件，则表明该账户已被劫持，并被用于发送垃圾邮件。结合下方的 *"冻结此账户..."*这个选项一起使用这个选项，有助于在造成太多损失之前停止被劫持的账户。请注意：对于此项而言，在尝试发送账户的邮件时，为了响应 RCPT 命令，将无效的收件人定义为 5xx 错误代码。

冻结此账户（管理员将不得不解冻）
在达到上方的 *"如果账户引起 [xx] 5xx RCPT 错误..."*这个阈值时，如果您希望冻结账户，请使用此项。发生这种情况时，将通过电子邮件通知管理员，以便他可以调查问题并取消冻结账户。

豁免列表
使用 *"豁免列表"*来指定您希望免于 "账户劫持检测"的任何地址。允许通配符。例如 "newsletters@example.com"将免除 example.com 的 "newsletters"MDaemon 账户，而 "*@newsletters.example.com"将免除属于 newsletters.example.com 域的所有 MDaemon 账户。邮件管理员账户将被自动免于 "账户劫持检测"。

4.1.3.7 Spambot 检测



"Spam bot 检测"跟踪各个 "SMTP MAIL"(返回-路径) 使用了一段指定时间的 IP 地址。如果短时间内数量异常的 IP 地址使用了相同的返回-路径，这就表明 Spam bot 网络在作祟。在检测到 spam bot 时，将立即断开当前连接，并能按照您指定的时间长度有选择性地阻止返回路径值。您还能选择阻止所有已知的 spam bot IP 地址长达一段指定的时间。

启用 Spam bot检测
点击此框来启用 Spam bot 检测。默认情况下，禁用该选项。

时间间隔期间允许的不同 IP 的最大值
这是在指定的时间间隔内，指定的返回路径可以连接的不同 IP 的地址数量。

时间间隔 (单位是分钟)
在尝试检测 spam bot 网络时指定要使用的时间间隔 (单位是分钟)。

豁免列表
点击此按钮来打开 "Spam bot 检测"豁免列表。您可以在此处指定免于 spam bot 检测的 IP 地址、发件人和收件人。

阻止引起冲突的返回路径长达这些分钟
如果您希望阻止检测到的 spam bot 返回路径，请使用此项。MDaemon 在指定的分钟数内，不会接受其返回路径被阻止的邮件。默认情况下启用此项。

高级
点击该按钮可打开 "Spam bot 发件人文件"。它显示当前被阻止的的返回路径，以及在这些路径被移出阻止列表前所剩的分钟数。

阻止引起冲突的 IP 长达这些分钟
如果您希望阻止检测到的 spam bot IP 地址，请使用此项。MDaemon 在指定的分钟数内，不会接受其 IP 地址被阻止的邮件。默认情况下，禁用该选项。

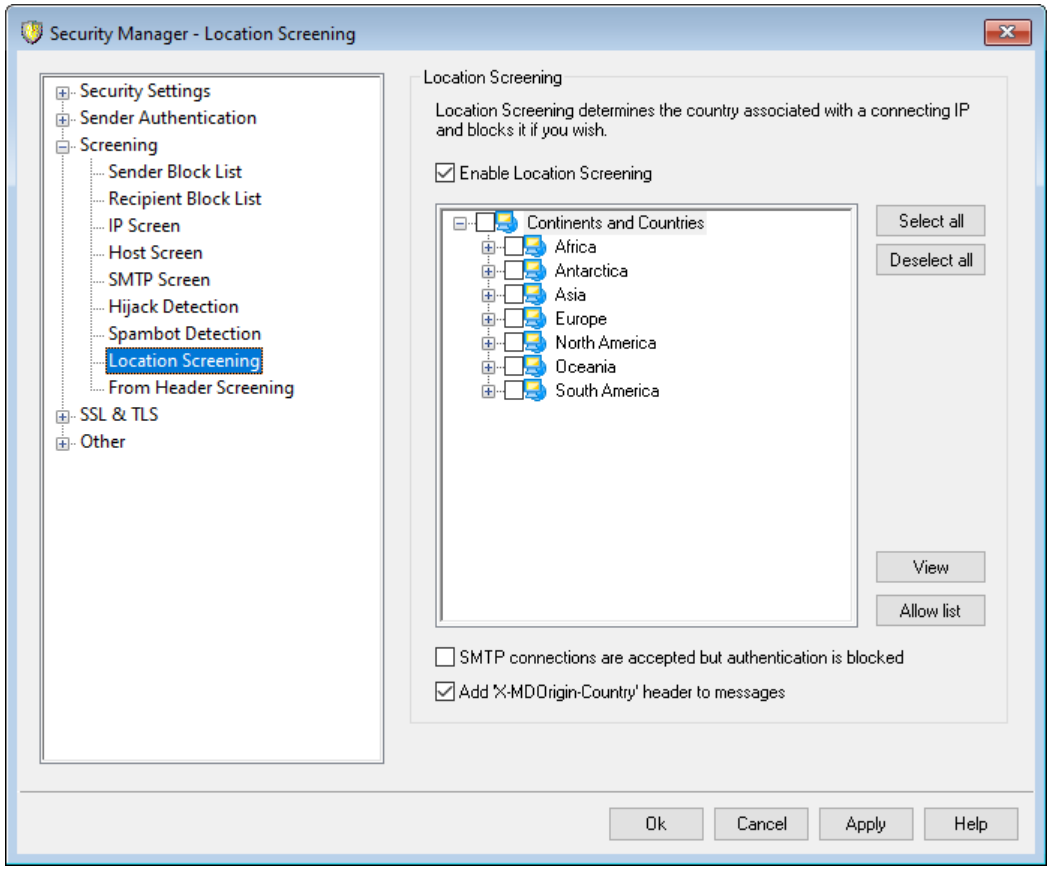
高级
点击该按钮可打开 "Spam bot IP 文件"。它显示当前被阻止的的 IP 地址，以及在这些路径被移出阻止列表前所剩的分钟数。

SMTP 响应 (默认为空)
如果您希望为尝试从被阻止的返回路径或 IP 地址发送邮件的 spam bot 定制相应的 SMTP 响应，请使用此项。MDaemon 将返回 SMTP 响应，"551 5.5.1 <您定制的文本>"，而不是默认响应。留空则使用 MDaemon 的默认响应。

如果会话经过验证则不跟踪连接
默认情况下，MDaemon 不为 "Spam bot 检测"跟踪经过验证的 438 会话。如果您不希望排除经过验证的连接，请清空该选择框。

不跟踪来自可信 IP 的连接
默认情况下 "Spam bot 检测"不跟踪来自可信 IP 435 的地址。如果您不希望排除可信 IP，请清理该选择框。

4.1.3.8 位置屏蔽



位置屏蔽

位置屏蔽"一种基于地理位置的阻止系统，允许您阻止尝试从全球未经授权的区域建立的入站 SMTP、POP、IMAP、Webmail、ActiveSync、AutoDiscovery、XML API、Remote Administration、CalDAV/CardDAV、XMPP 和 Minger 连接。MDaemon 确定与连接 IP 地址关联的国家，然后阻止该连接（如果来自受限位置），并向屏蔽日志添加一行信息。对于 SMTP，"位置屏蔽"可以选择性地阻止使用 AUTH 的连接。例如，如果您在特定国家/地区没有用户，但仍然希望能够接收来自此处的邮件，则该功能非常有用。这样您只会阻止那些试图登录到您服务器的尝试。

\MDaemon\Geo\ 文件夹包含作为主要国家 IP 数据库的数据库文件。这些文件由 MaxMind (www.maxmind.com) 提供并能按照您的需求从其站点下载更新。

启用位置屏蔽

默认情况下，"位置屏蔽"处于打开状态，但不阻止任何地区或国家/地区；MDaemon 仅记录连接的国家或地区。要阻止一个位置，请点击此框以及您想要屏蔽的任何区域或国家旁边的框，然后点击"确定"或"应用"。启用"位置屏蔽"时，无论是否阻止了任何位置，MDaemon 都会将"X-MDOrigin-Country"报头插入邮件，来进行内容过滤或用于其他目的。该报头包含双字母的 ISO 3166 国家和洲代码。

选择/取消全选

使用这些按钮来选择或取消选择列表中的所有位置。

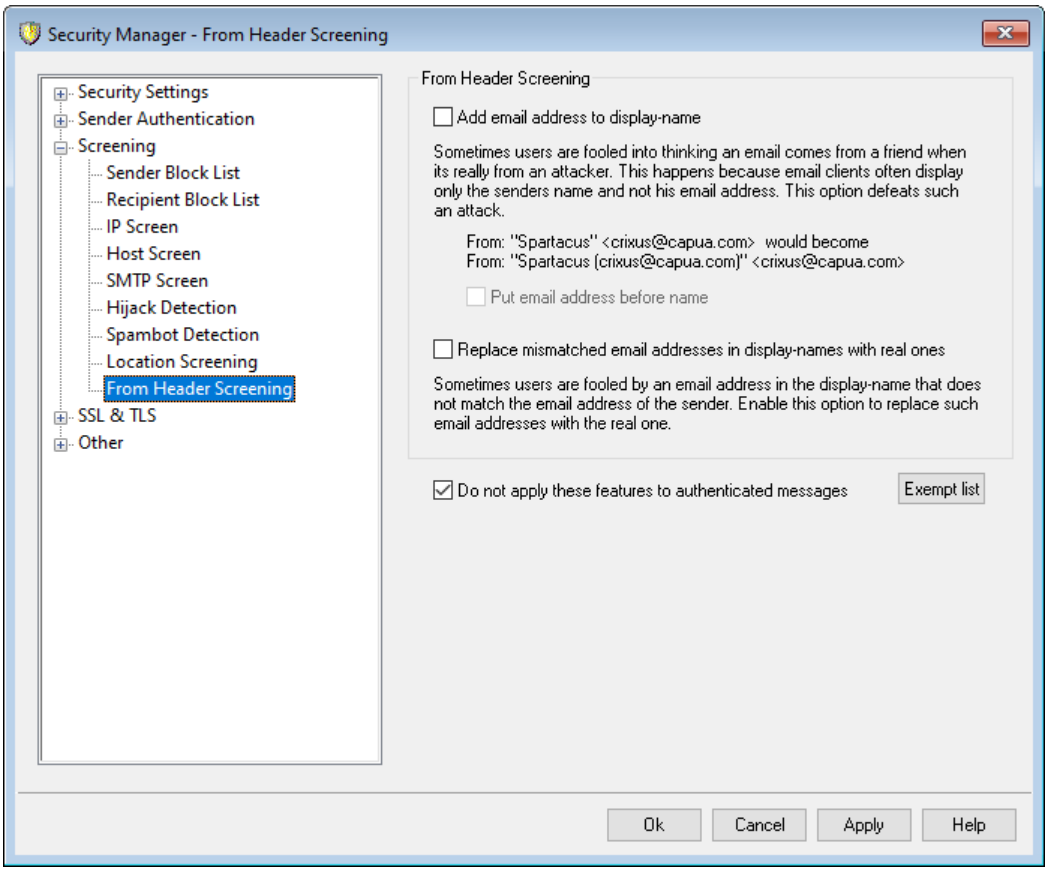
查看
点击此按钮来查看当前由 "位置屏蔽"功能阻止的所有位置的文本文件列表。如果您勾选/取消勾选位置列表中的任何框，*"查看"*按钮还是不可用，直到您点击了 "应用"为止。

允许列表
该按钮打开动态屏蔽允许列表 522, 它也用于 "位置屏蔽"。如果您希望将 IP 地址从 "位置屏蔽"免除，请点击此按钮并指定 IP 地址以及您希望条目过期的时间。

接受 SMTP 连接，但阻止验证
对于 SMTP 连接，如果您只希望阻止使用验证的连接尝试，请选中此框。

将 "X-MDOrigin-Country"报头添加到邮件
默认情况下，在启用 "位置屏蔽"时"，MDaemon 会将 "X-MDOrigin-Country"报头插入邮件，来进行内容过滤或用于其他目的。该报头包含双字母的 ISO 3166 国家和洲代码，而不是全名。如果您不希望插入该报头，请清除该复选框。

4.1.3.9 发件人报头屏蔽



发件人报头屏蔽
这个安全功能修改入站邮件的 "发件人："报头，来使报头的仅姓名部分包含姓名和邮件地址。这是为了抵御垃圾邮件和攻击中通常使用的策略，即伪装成邮件来自其他人。在显示

邮件列表时，邮件客户端通常仅显示发件人的姓名，而不是姓名和邮件地址。要查看邮件地址，收件人必须先打开邮件或采取一些其他操作，例如右键点击条目或将鼠标悬停在姓名上等。出于这个原因，攻击者通常在可见的 "发件人"报头放置合法的人名或公司名称来构建邮件，并隐藏不合法的电子邮件地址。例如，一封邮件的实际 "发件人："报头可以是 "Honest Bank and Trust"<lightfingers.klepto@example.com>，但是您的客户端可能只将"Honest Bank and Trust"作为发件人显示。此功能会更改报头的可见部分来显示这两个部分。在上例中，现在会将发件人显示成 "Honest Bank and Trust (lightfingers.klepto@example.com)" <lightfingers.klepto@example.com>"，清楚为您指示这是伪造的欺诈邮件。

添加邮件地址到显示名
如果您希望将入站邮件的 "发件人："报头的客户端可见部分修改成 包含发件人的姓名和邮件地址，请启用此项。会将新报头的结构从 "发件人姓名"<mailbox@example.com> 更改成"Sender's Name (mailbox@example.com)"<mailbox@example.com>。默认情况下禁用此项，而且仅适用于指向本地用户的邮件。由于一些用户可能不希望修改 "发件人："报头，即使这有助于识别欺诈邮件，请慎用此项。

将邮件地址置于姓名前
在使用 上方的 *"将邮件地址置于姓名前"*这个选项时，如果您希望在修改后的 "发件人："报头中交换姓名和电子邮件地址，请启用此项。使用上方示例，"Sender's Name" <mailbox@example.com> 现在将修改成："mailbox@example.com (发件人的姓名)"<mailbox@example.com>。

将显示名称中不匹配的电子邮件地址替换为真实的电子邮件地址
垃圾邮件中使用的另一种策略是在 "发件人："报头的显示名称部分中添加了看似合法的姓名和电子邮件地址。即使它不是实际的发件电子邮件地址。如果您希望使用实际发件人地址替换此类邮件中的可见电子邮件地址，请使用此选项。

不向已验证的邮件应用这些功能
如果您不希望将 "发件人屏蔽"选项应用于已通过 MDaemon 验证的入站邮件，请选中此框。

豁免列表
使用此选项可将地址添加到 "发件人报头屏蔽豁免"白名单。发送到列出地址的邮件将不修改其 "发件人："报头。

4.1.4 SSL 和 TLS

MDaemon 支持 Secure Sockets Layer (SSL)/Transport Layer Security (TLS) 协议用于 SMTP、POP 和 IMAP[481]，以及 MDaemon Remote Administration[487] 和 Webmail's[483] web 服务器。由网景通讯公司开发的 SSL 协议是保护服务器/客户端网络通信安全的标准方案。它为 TCP/IP 连接提供服务器身份验证、数据加密，以及可选的客户端身份验证。此外，由于 SSL 内置于所有当前主流浏览器中，因此只需在服务器上安装有效的数字证书，即可在连接 MDRA 或 Webmail时激活连接浏览器的 SSL 功能。

如果通过邮件客户端而不是使用 Webmail来连接标准邮件端口，MDaemon 支持 SMTP 和 IMAP 在 TLS 上的 STARTTLS 扩展，以及 POP3 的 STLS 扩展。但是，你必须首先将你的客户端配制成为使用SSL，以及它必须支持那些扩展 -不是所有的邮件客户端都支持它们。使用 无 STARTTLS 列表[491]和 STARTTLS 列表[492]页面来指定不能、必须或分别使用 STARTTLS 的特定主机和地址。

SSL & TLS 对话框还包含一个页面，用于启用 DNSSEC[495] (DNS 安全扩展)，SMTP 扩展[493] 页面用于启用 RequireTLS、MTA-STA 和 TLS 报告，而 Let's Encrypt[496] 页面用于使用 Let's Encrypt 证书颁发机构 (CA)。

用于启用和配置 SSL 的选项位于 "安全设置"对话框的 SSL & TLS 部分下：安全» 安全管理器» SSL & TLS。SMTP、POP3 和 IMAP 的 SSL 端口设置在 "端口[87]"屏幕上，位于：设置» 服务器设置 » DNS & IPs。用于 Webmail[483] 和 Remote Administration[487] 的 HTTPS 端口位于各自的屏幕上。

创建和使用 SSL 证书的更多信息，请参阅：

创建和使用 SSL 证书[764]

—

TLS/SSL 协议 位于 RFC-4346: The Transport Layer Security (TLS) Protocol Version 1.1

针对 SMTP 的 STARTTLS 扩展位于 RFC-3207: SMTP Service Extension for Secure SMTP over Transport Layer Security

结合使用 TLS 和 IMAP 与 POP3 协议位于 RFC-2595: Using TLS with IMAP, POP3 and ACAP

DNSSEC (DNS 安全扩展) 在以下链接定义：RFC -4033: DNS Security Introduction and Requirements and RFC-4035: Protocol Modifications for the DNS Security Extensions as

有关 RequireTLS 的完整说明，请参阅：RFC 8689: SMTP Require TLS Option.

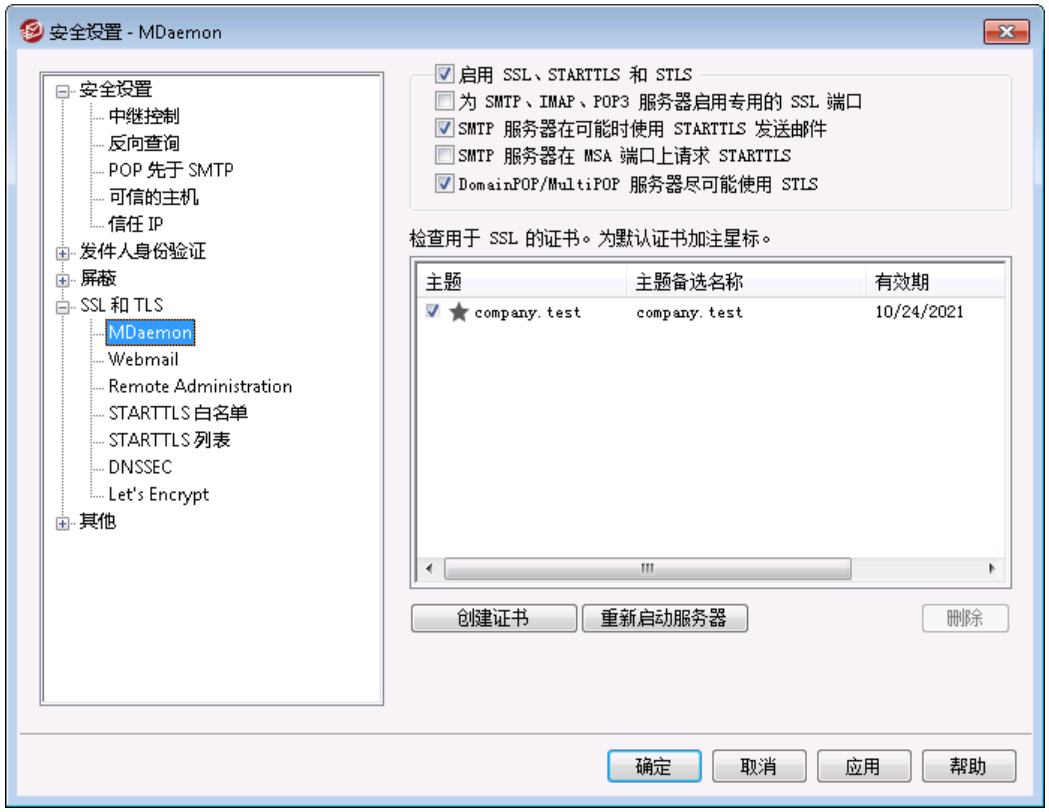
MTA-STS 支持在以下地址说明，RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

TLS 报告在以下链接说明，RFC 8460: SMTP TLS Reporting.

还请参阅：

SSL 和 TLS » MDaemon[481]
SSL & TLS » Webmail[483]
SSL & TLS » Remote Administration[487]

4.1.4.1 MDaemon



启用 SSL、STARTTLS 和 STLS
点击此复选框激活对 SSL/TLS 协议，STARTTLS 以及 STLS 扩展的支持。之后，从以下列表选择您希望使用的证书。

为 SMTP、IMAP、POP3 服务器启用专用的 SSL 端口
如果您希望在 "默认域与服务器"下方端口[87]上指定的专用 SSL 端口可用，请启用此选项。这不会影响客户端在默认邮件端口上使用 STARTTLS 和 STLS——它只不过提供一个对 SSL 的附加级别支持。

SMTP 服务器尽可能使用 STARTTLS 发送邮件
若您希望 MDaemon 为它发送的每一封 SMTP 邮件都使用 STARTTLS 扩展名，请点击此选项。若与 MDaemon 相连的服务器不支持 STARTTLS，那么邮件将以常规方式投递而不使用 SSL。如果您希望阻止某些域使用 STARTTLS，请使用无 STARTTLS 列表[491]。

SMTP 服务器需要在 MSA 端口上请求 STARTTLS
如果您希望向与 MSA 端口[87]建立连接的服务器请求 STARTTLS 连接，请启用此项。

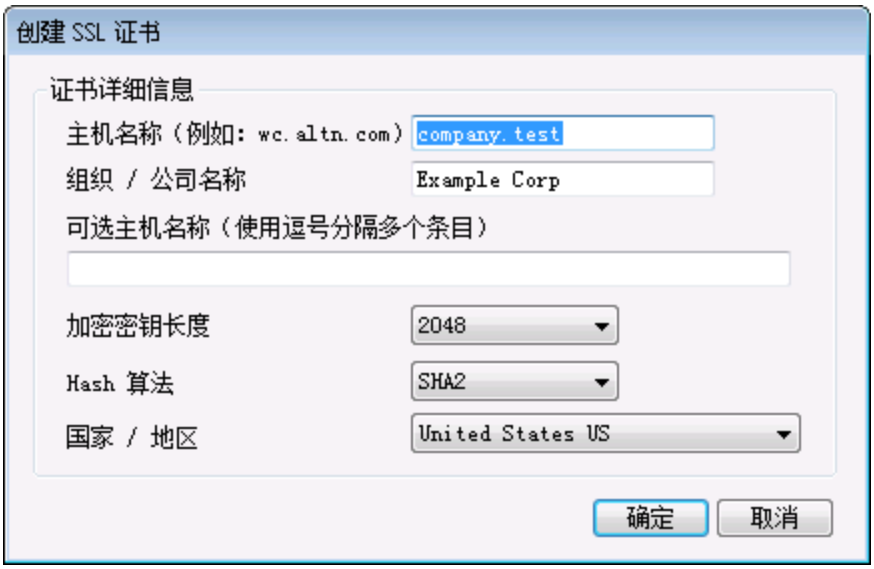
DomainPOP/MultiPOP 服务器尽可能使用 STLS
如果您希望 DomainPOP 与 MultiPOP 服务器在必要时使用 STLS 扩展，请勾选此框。

选择用于 SSL 的证书
此选框显示您的 SSL 证书。选中您希望激活的任何证书旁边的框。点击要设置为默认证书旁边的星号。MDaemon 支持 TLS 协议的服务器名称指示 (SNI)扩展，它允许为您的每

个服务器主机名使用不同的证书。MDaemon 将查看活动证书，并在 "主题备选名称"字段中选择具有所请求主机名的证书 (您可以在创建证书时指定备选名称)。如果客户端未请求主机名，或者未找到匹配的证书，则使用默认证书。双击证书以在 Windows "证书"对话框中将其打开以供审阅 (仅在应用程序界面中可用，而不在基于浏览器的远程管理中可用)。

删除
在此列表中选择一个证书，然后点击此按钮将其删除。会打开一个确认框并询问您是否确定删除该证书。

创建证书
点击此按钮来打开 "创建 SSL 证书"对话框。



证书详细信息

主机名
当创建一个证书时，输入您的用户将会连接的主机名称 (例如，"mail.example.com")。

企业/公司名
在此输入 "拥有"此证书的机构或公司。

替换主机名 (用逗号分隔多个项目)
如果您的用户可能连接到备选主机名，您也希望此证书应用到那些名称，那么请输入那些域名，通过逗号分隔。允许通配符，所以 "*.example.com"可以应用于所有 example.com 的子域 (例如 "wc.example.com"、"mail.example.com"等等)。

MDaemon 支持 TLS 协议的服务器名称指示 (SNI)扩展，它允许为您的每个服务器主机名使用不同的证书。MDaemon 将查看活动证书，并在其 "使用者备用名称"字段中选择具有所请求主机名的证书。如果客户端未请求主机名，或者未找到匹配的证书，则使用默认证书。

密钥长度
为此证书选择所需位长度的加密密钥。加密密钥的位数越长，已传输的数据也将越安全。不过请注意，并非所有的应用程序都支持大于 512 的密钥长度。

Hash 算法
选择您希望使用的 hash 算法：SHA1 或 SHA2。默认设置是 SHA2。

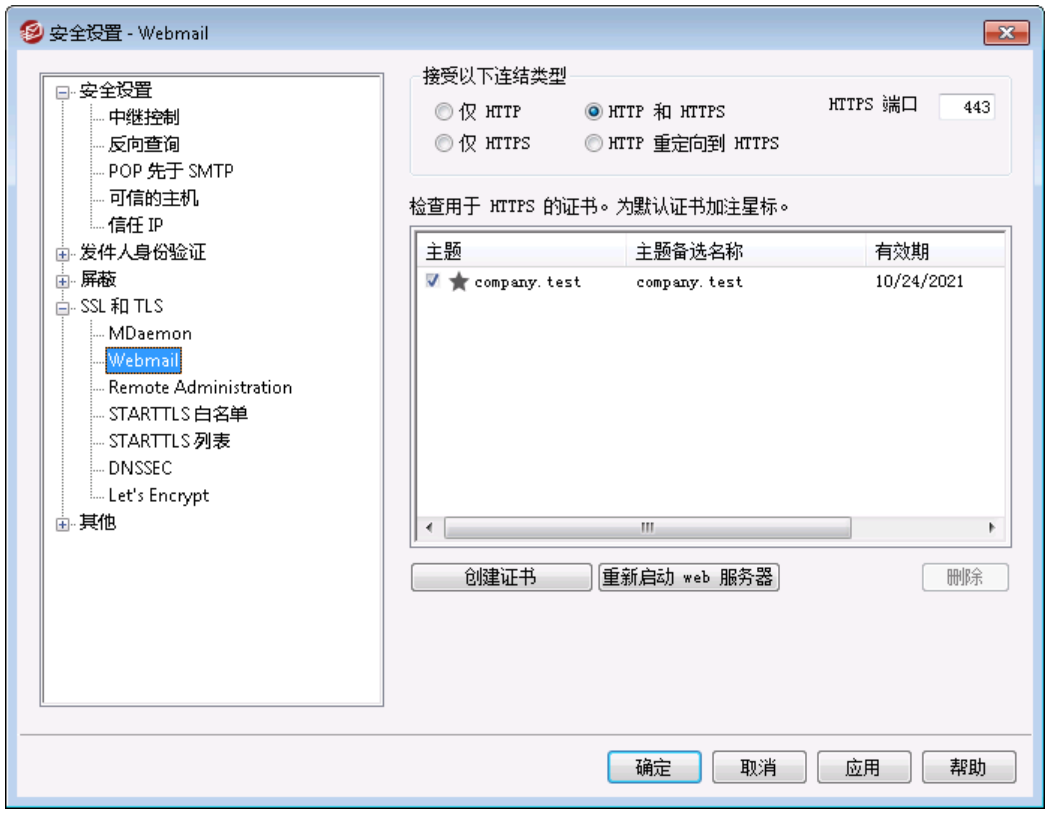
国家/地区
选择您的服务器所在国家或地区。

重新启动服务器
点击以重启 SMTP/IMAP/POP 服务器。在更改证书时，这些服务器必须重启。

还请参阅：

SSL 和 TLS 479
创建和使用 SSL 证书 764

4.1.4.2 Webmail



MDaemon 内置的 Web 服务器支持安全套接字层 (SSL)协议。SSL 是保护服务器/客户端

web 通信安全的标准方案。它提供了服务器验证、数据加密和用于 TCP/IP 连接的可选客户端验证。此外，由于在所有主要的浏览器中都内置了 HTTPS 支持（比如通过 SSL 的 HTTP），只要在您的服务器上安装一个有效的数字认证将会激活连接客户端的 SSL 能力。

启用和配置 Webmail来使用 HTTPS 的选项位于“设置» Web & IM 服务» Webmail（web 配置）下的SSL & HTTPS 屏幕”。但是为了您使用起来更加方便，这些选项还被镜像于“安全» 安全管理器» SSL & TLS » Webmail”之下。

要了解 SSL 协议与证书的更多详情，请参阅：“SSL 和证书 479”

在使用 MDaemon 内置的 web 服务器时，该屏幕仅应用于 Webmail。如果您配置 Webmail使用其它的网络服务器，如 IIS，则不会使用这些选项——SSL/HTTPS 支持必需使用其它网络服务器的工具来配置。

接受以下连接类型

仅 HTTP
如果您不允许任何 HTTPS 连接到 Webmail，请选择此项。仅接受 HTTP 连接。

HTTP 和 HTTPS
如果您希望在 Webmail中启用 SSL 支持，但不希望强迫您的 Webmail用户使用 HTTPS，请选择此选项。Webmail对在以下指定的 HTTPS 端口上的连接进行监听，但是它仍将会回应 Webmail端口上正常的 http 连接，该端口在 Webmail（web 邮件）的 Web 服务器 270屏幕上指定。

仅 HTTPS
如果想在连接 Webmail时要求使用 HTTPS，请选择此选项。当此选项启用时，Webmail将会只响应 HTTPS 连接——它不会响应 HTTP 请求。

HTTP 重定向到 HTTPS
如果您希望重定向所有的 HTTP 连接到在 HTTPS 端口上的 HTTPS，请选择此选项。

HTTPS 端口
这是 Webmail将为 SSL 连接监听的 TCP 端口。默认 SSL 端口是 443。如果使用默认 SSL 端口，则在通过 HTTPS 进行连接时，您将不必在 Webmail的 URL 中包含端口号（比如“https://example.com”等于“https://example.com:443”）。

这不同于在 Webmail（web 配置）的 Web 服务器 270屏幕上指定的 Webmail端口。如果你仍允许 HTTP 连接到 Webmail，则那些连接必须使用其他端口连接才能成功。HTTPS 连接必须使用 HTTPS 端口。

选择用于 HTTPS/SSL 的证书

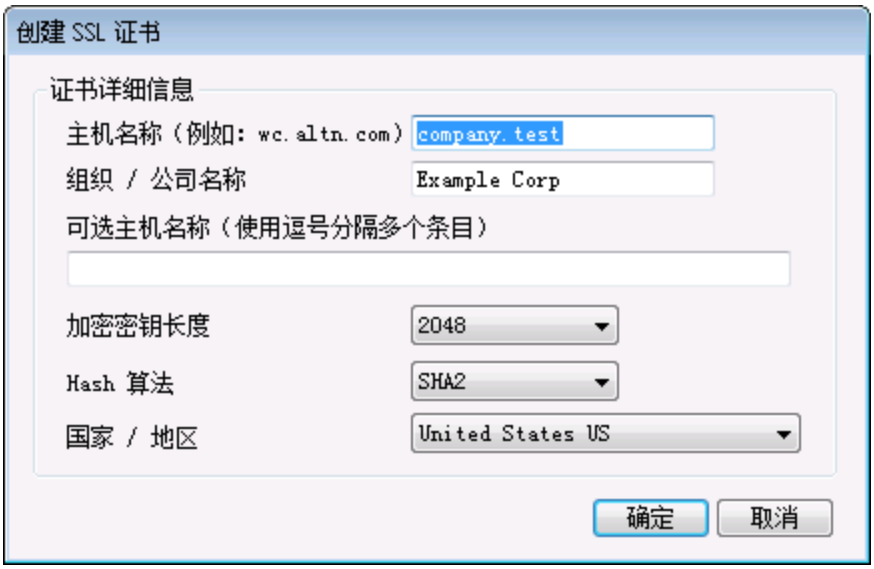
该框显示您的 SSL 证书。选中您希望激活的任何证书旁边的框。点击要设置为默认证书旁边的星号。MDaemon 支持 TLS 协议的服务器名称指示（SNI）扩展，它允许为您的每个服务器主机名使用不同的证书。MDaemon 将查看活动证书，并在“主题备选名称”字段中选择具

有所请求主机名的证书（您可以在创建证书时指定备选名称）。如果客户端未请求主机名，或者未找到匹配的证书，则使用默认证书。双击证书以在 Windows "证书"对话框中将其打开以供审阅（仅在应用程序界面中可用，而不在基于浏览器的远程管理中可用）。

删除
在此列表中选择一个证书，然后点击此按钮将其删除。会打开一个确认框并询问您是否确定删除该证书。

创建证书

点击此按钮来打开"创建 SSL 证书"对话框。



证书详细信息

主机名
在创建证书时，输入您用户将会连接的主机名称（例如"wc.example.com"）。

企业/公司名
在此输入"拥有"此证书的机构或公司。

替换主机名（用逗号分隔多个项目）
如果您的用户可能连接到备选主机名，您也希望此证书应用到那些名称，那么请输入那些域名，通过逗号分隔。允许通配符，所以"*.example.com"可以应用于所有 example.com 的子域（例如"wc.example.com"、"mail.example.com"等等）。

MDaemon 支持 TLS 协议的服务器名称指示（SNI）扩展，它允许为您的每个服务器主机名使用不同的证书。MDaemon 将查看活动证书，并在其"使用者备用名称"字段中选择具有所请求主机名的证书。如果客户端未请求主机名，或者未找到匹配的证书，则使用默认证书。

密钥长度
为此证书选择所需位长度的加密密钥。加密密钥的位数越长，已传输的数据也将越安全。不过请注意，并非所有的应用程序都支持大于 512 的密钥长度。

国家/地区
选择您的服务器所在国家或地区。

Hash 算法
选择您希望使用的 hash 算法：SHA1 或 SHA2。默认设置是 SHA2。

重启 web 服务器
点击此按钮来重启 web 服务器。使用新证书前，必须重启 web 服务器。

使用 Let's Encrypt 来管理您的证书

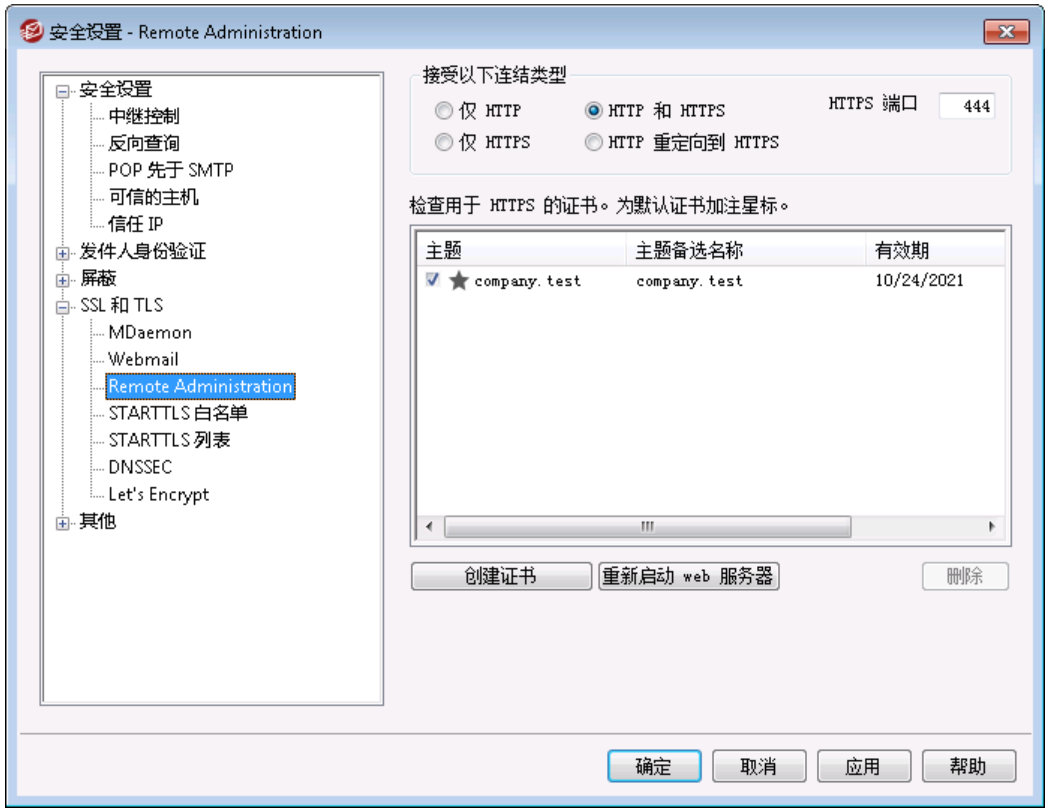
Let's Encrypt 是一个证书颁发机构 (CA)，通过专门设计的自动化流程来为"传输安全层 (TLS)"加密提供免费的证书，该流程使您可以免于现在复杂的手动创建、验证、签名、安装、以及续订证书这些用来保护网站安全的环节。

要支持使用 Let's Encrypt 的自动化流程来管理证书，提供 Let's Encrypt 496 屏幕来帮助您轻松简便地配置和运行 PowerShell 脚本，位于"MDaemon\LetsEncrypt"文件夹。运行该脚本将使一切为 LetsEncrypt 准备就绪，包括将一些必要的文件放置在 WebmailHTTP 的目录中来完成 http-01 挑战。它将 SMTP 主机名 151 (属于默认域 149)用作证书域，包含您已指定的任何*备选主机名称*，检索证书，将其导入 Windows，并配置 MDaemon 如何使用针对 MDaemon、Webmail 和 Remote Administration 的证书。此外，该脚本将在名为 LetsEncrypt.log 的"MDaemon\Logs\"目录中创建一个日志文件 LetsEncrypt.log。每次运行脚本时,都会删除并重新创建该日志文件，并且包含脚本的开始日期和时间。此外，如果您指定了*通知的管理员邮件*，将在出错时发送通知邮件。请参阅 Let's Encrypt 496 主题了解更多信息。

还请参阅：

SSL 和证书 479
创建和使用 SSL 证书 764

4.1.4.3 Remote Administration



MDaemon 的内置 Web 服务器支持安全套接字层 (SSL)协议。SSL 是保护服务器/客户端 web 通信安全的标准方案。它提供了服务器验证、数据加密和用于 TCP/IP 连接的可选客户端验证。此外，由于在所有主要的浏览器中都内置了 HTTPS 支持 (比如通过 SSL 的 HTTP)，只要在您的服务器上安装一个有效的数字认证将会激活连接客户端的 SSL 能力。

启用和配置 Remote Administration 来使用 HTTPS 的选项位于“设置» Web & IM 服务» Remote Administration”下的“SSL & HTTPS”屏幕。不过为方便起见，这些选项也镜像到“安全» 安全设置» SSL & TLS » Remote Administration”。

要了解 SSL 协议与证书的更多详情，请参阅：“SSL 和证书 479”

在使用 MDaemon 的内置 web 服务器时，该屏幕仅应用于 Remote Administration。如果您配置 Remote Administration 使用其它的网络服务器，如 IIS，则不会使用这些选项——SSL/HTTPS 支持必需使用其它网络服务器的工具来配置。

接受以下连接类型

仅 HTTP
如果您不允许任何 HTTPS 连接到 Remote Administration，请选择此项。仅接受 HTTP 连接。

HTTP 和 HTTPS
如果您希望在 Remote Administration 中启用 SSL 支持，但不希望强制您的 Remote Administration 用户使用 HTTPS，请选择此选项。Remote Administration 将监听在下方指定的 HTTPS 端口上的连接，但是它仍会响应 Remote Administration TCP 端口上正常的 http 连接，该端口在 "Web 服务器"[294]屏幕上指定。

仅 HTTPS
如果您希望连接到 Remote Administration 时要求 HTTPS，选择此选项。当此选项启用时，Remote Administration 只会响应 HTTPS 连接——不会响应 HTTP 请求。

HTTP 重定向到 HTTPS
如果您希望重定向所有的 HTTP 连接到在 HTTPS 端口上的 HTTPS，请选择此选项。

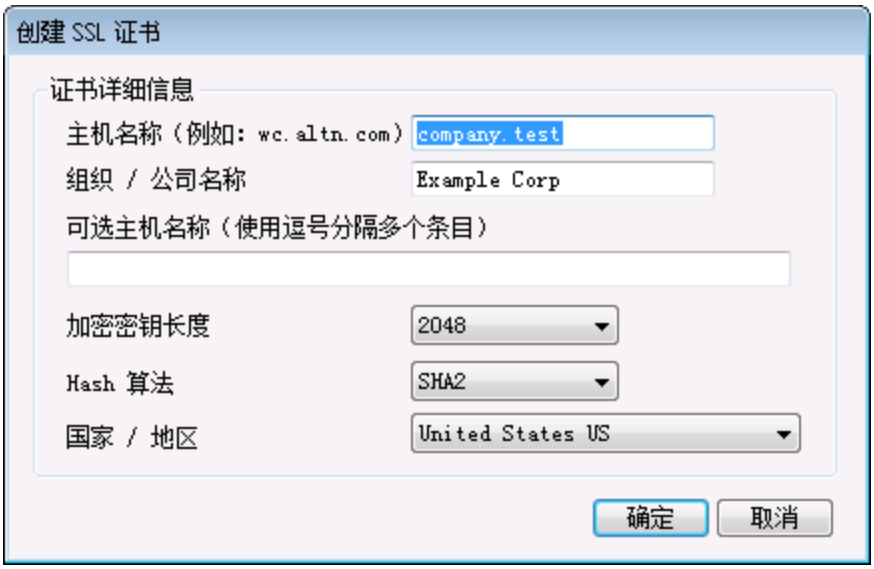
HTTPS 端口
这是 Remote Administration 将为 SSL 连接监听的 TCP 端口。默认的 SSL 端口是 444. 如果使用默认的 SSL 端口，在通过 HTTPS 连接时，您不必在 Remote Administration 的 URL 中包含端口号（例如 "https://example.com" 等于 "https://example.com:444"）。

这不同于在 "Web 服务器"[294]屏幕上指定的 Remote Administration 端口。如果您仍然允许 HTTP 连接到 Remote Administration，则那些连接必须使用其他端口才能连接成功。HTTPS 连接必须使用 HTTPS 端口。

选择用于 HTTPS/SSL 的证书
此选框显示您的 SSL 证书。选中您希望激活的任何证书旁边的框。点击要设置为默认证书旁边的星号。MDaemon 支持 TLS 协议的服务器名称指示 (SNI) 扩展，它允许为您的每个服务器主机名使用不同的证书。MDaemon 将查看活动证书，并在 "主题备选名称" 字段中选择具有所请求主机名的证书（您可以在创建证书时指定备选名称）。如果客户端未请求主机名，或者未找到匹配的证书，则使用默认证书。双击证书以在 Windows "证书" 对话框中将其打开以供审阅（仅在应用程序界面中可用，而不在基于浏览器的远程管理中可用）。

删除
在此列表中选择一个证书，然后点击此按钮将其删除。会打开一个确认框并询问您是否确定删除该证书。

创建证书
点击此按钮来打开 "创建 SSL 证书" 对话框。



证书详细信息

主机名
在创建证书时，输入您用户将会连接的主机名称（例如“wc.example.com”）。

企业/公司名
在此输入“拥有”此证书的机构或公司。

替换主机名（用逗号分隔多个项目）
如果您的用户可能连接到备选主机名，您也希望此证书应用到那些名称，那么请输入那些域名，通过逗号分隔。允许通配符，所以“*.example.com”可以应用于所有 example.com 的子域（例如“wc.example.com”、“mail.example.com”等等）。

> MDaemon 支持 TLS 协议的服务器名称指示（SNI）扩展，它允许为您的每个服务器主机名使用不同的证书。MDaemon 将查看活动证书，并在其“使用者备用名称”字段中选择具有所请求主机名的证书。如果客户端未请求主机名，或者未找到匹配的证书，则使用默认证书。

密钥长度
为此证书选择所需位长度的加密密钥。加密密钥的位数越长，已传输的数据也将越安全。不过请注意，并非所有的应用程序都支持大于 512 的密钥长度。

国家/地区
选择您的服务器所在国家或地区。

Hash 算法
选择您希望使用的 hash 算法：SHA1 或 SHA2。默认设置是 SHA2。

重启 web 服务器

点击此按钮来重启 web 服务器。使用新证书前，必须重启 web 服务器。

使用 Let's Encrypt 来管理您的证书

Let's Encrypt 是一个证书颁发机构 (CA)，通过专门设计的自动化流程来为 "传输安全层 (TLS)"加密提供免费的证书，该流程使您可以免于现在复杂的手动创建、验证、签名、安装、以及续订证书这些用来保护网站安全的环节。

要支持使用 Let's Encrypt 的自动化流程来管理证书，提供 Let's Encrypt 496 屏幕来帮助您轻松简便地配置和运行 PowerShell 脚本，位于 "MDaemon\LetsEncrypt"文件夹。运行该脚本将使一切为 LetsEncrypt 准备就绪，包括将一些必要的文件放置在 WebmailHTTP 的目录中来完成 http-01 挑战。它将 SMTP 主机名 151 (属于默认域 149)用作证书域，包含您已指定的任何*备选主机名称*，检索证书，将其导入 Windows，并配置 MDaemon 如何使用针对 MDaemon、Webmail 和 Remote Administration 的证书。此外，该脚本将在名为 LetsEncrypt.log 的 "MDaemon\Logs\"目录中创建一个日志文件 LetsEncrypt.log。每次运行脚本时,都会删除并重新创建该日志文件，并且包含脚本的开始日期和时间。此外，如果您指定了*通知的管理员邮件*，将在出错时发送通知邮件。请参阅 Let's Encrypt 496 主题了解更多信息。

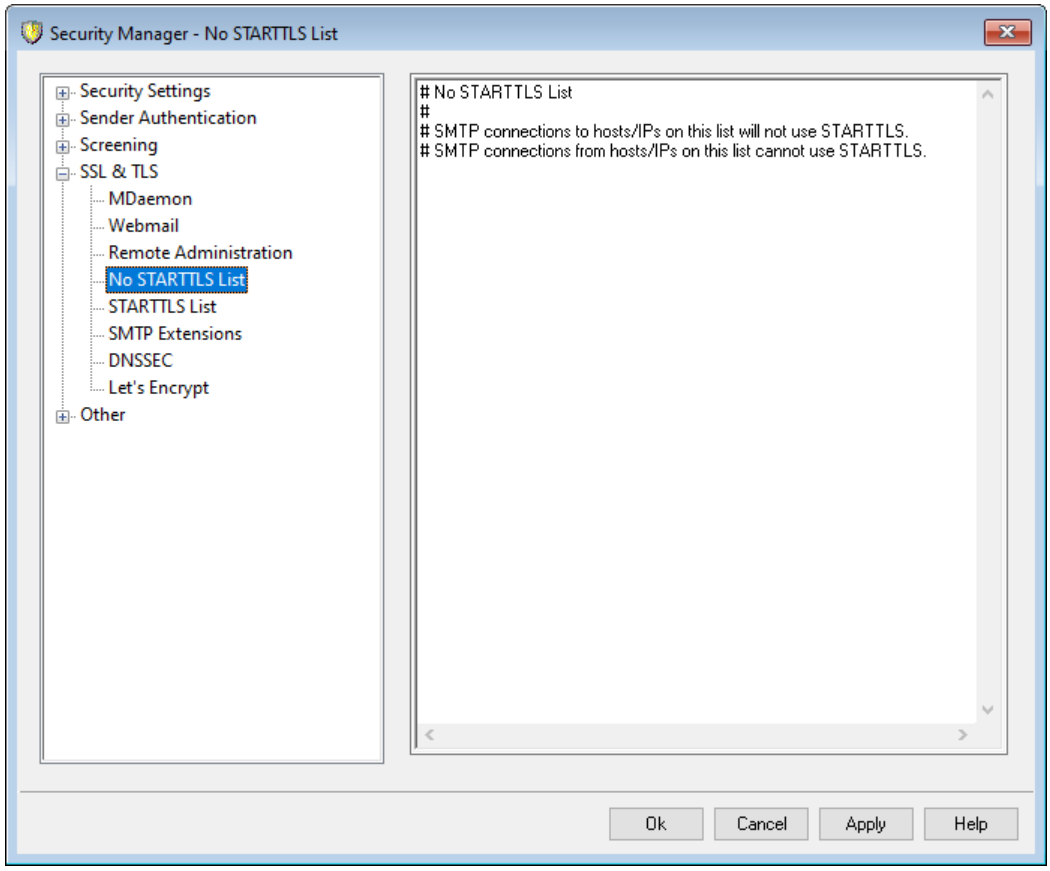
更多 SSL 协议与证书的更多信息，请参阅：

在 IIS 下运行 Remote Administration 300
SSL 与证书 479
创建和使用 SSL 证书 764

要了解有关 Remote Administration 的更多信息，请参阅：

远程配置 293
Remote Administration » Web 服务器 294
Web 访问默认值 672
账户编辑器 » Web 603

4.1.4.4 无 STARTTLS 列表



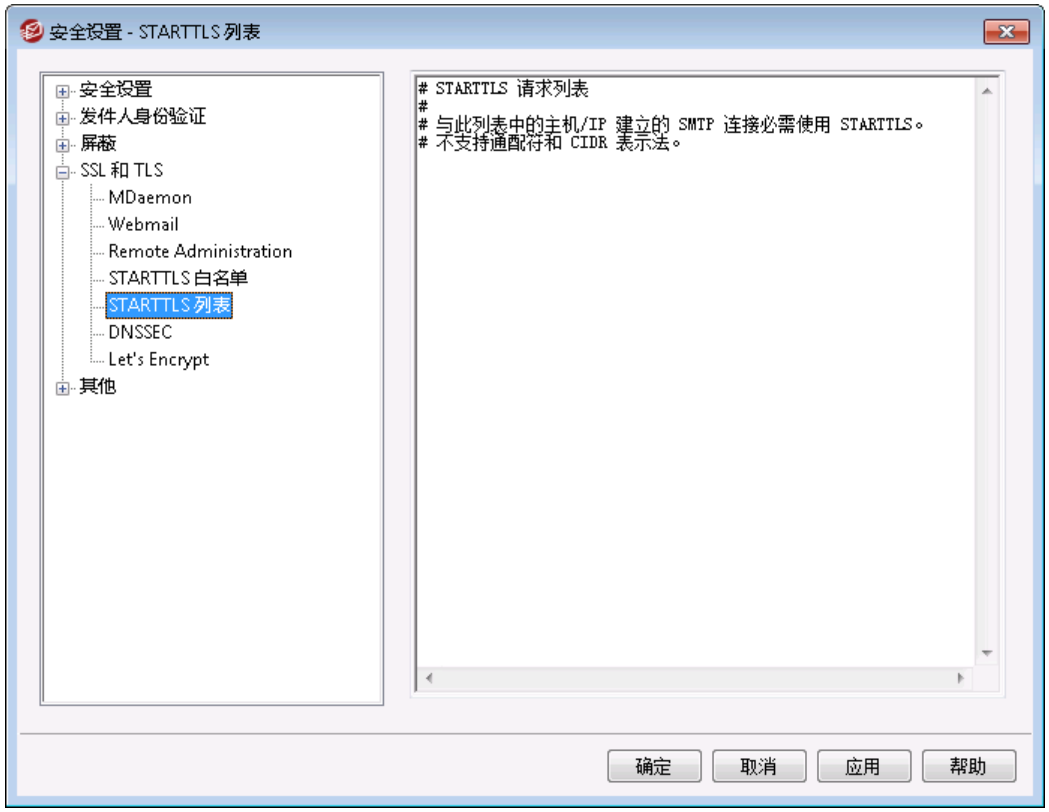
使用此列表，在通过特定主机或 IP 地址收发邮件时阻止 STARTTLS 的使用。

无 STARTTLS 列表优先于 STARTTLS 请求列表[492]和 *SMTP 服务器需要在 MSA 端口上请求 STARTTLS*[481]这个选项。

在 RFC -3207 中探讨了 SMTP 的 STARTTLS 扩展，要查看请参阅：

http://www.rfc-editor.org/rfc/rfc3207.txt

4.1.4.5 STARTTLS 列表

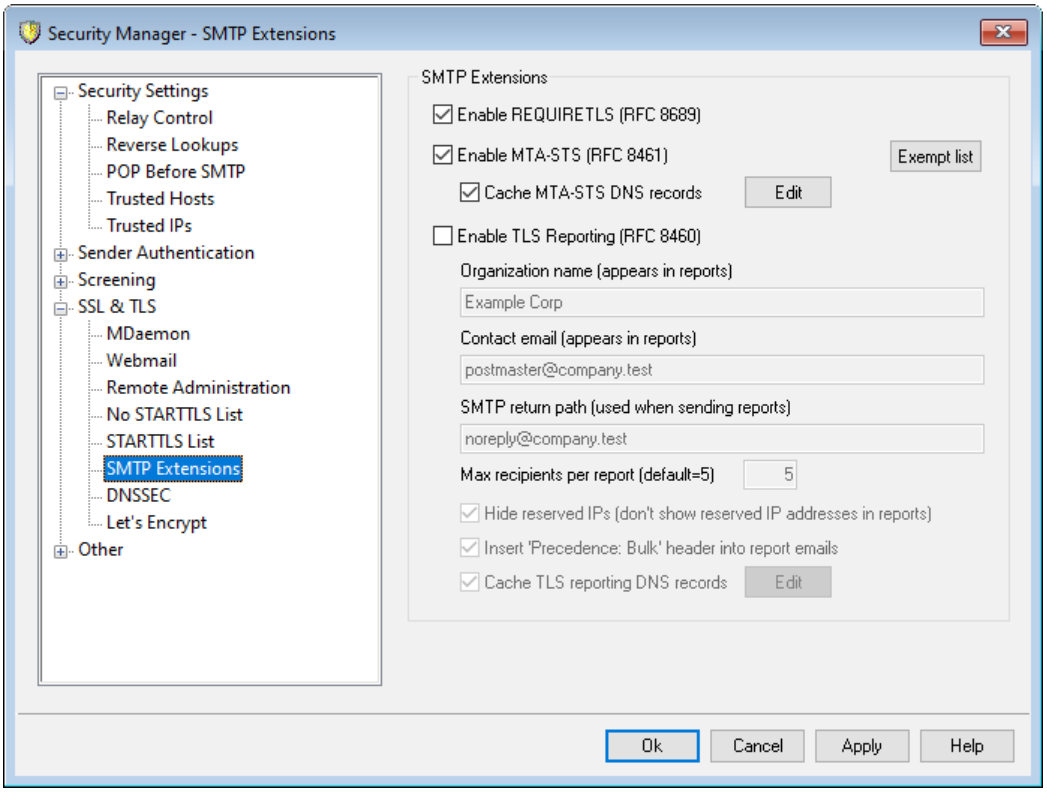


使用此屏幕可指定主机、IP 地址和邮件发件人地址，这些地址需要使用 STARTTLS 扩展才能向您的服务器发送或接收邮件。

在 RFC -3207 中探讨了 SMTP 的 STARTTLS 扩展，要查看请参阅：

http://www.rfc-editor.org/rfc/rfc3207.txt

4.1.4.6 SMTP 扩展



SMTP 扩展

启用 REQUIRETLS (RFC 8689)
RequireTLS 允许您标记*必须*使用 TLS 发送的邮件。如果无法使用 TLS 或者 TLS 证书交换的参数不可接受），则退回邮件，而不是不安全地投递邮件。有关 RequireTLS 的完整说明，请参阅：RFC 8689: SMTP Require TLS Option.

默认情况下，启用 RequireTLS，但是将受 RequireTLS 进程约束的唯一邮件是被使用新的内容过滤器操作 542，“*为 REQUIRETLS 标记邮件...*”的“内容过滤器”规则特别标记的邮件，或发送至 `<local-part>+requiretls@domain.tld`（例如 `arvel+requiretls@mdaemon.com`）的邮件。将所有其他邮件视为已禁用该服务。此外，必须满足几个要求才能使用 RequireTLS 发送邮件。如果它们中的任何一个失败，该邮件将弹回，而不是以明文形式发送。这些要求是：

- 必须启用 RequireTLS。
- 必须通过“内容过滤器”操作或“`<localpart>+requiretls@...`”地址将该邮件标记为需要 RequireTLS 处理。
- 针对收件 MX 主机的 DNS 查询必须使用 DNSSEC 495（见下），或者 MX 必须由 MTA-STS 验证。
- 指向收件主机的连接必须使用 SSL (STARTTLS)。
- 收件主机的 SSL 证书必须与 MX 主机名匹配，并链接到受信任的 CA。
- 收件邮件服务器必须支持 REQUIRETLS，并在 EHLO 响应中声明。

RequireTLS 需要 MX 记录主机的 DNSSEC 查找，否则 MX 必须由 MTA-STS 验证。您可以通过指定查询根据什么条件请求 DNSSEC 服务区来配置 DNSSEC 495。MDaemon 的 IP 缓存 91 拥有一个选项，用来接受 DNSSEC 声明，在 MX 主机文件 85 顶部还有与 DNSSEC 相关的指令。最后，DNSSEC 需要适当配置的 DNS 服务器，这超出了此帮助文件的范围。

启用 MTA-STS (RFC 8461)

默认情况下启用 MTA-STS 支持，详细说明请参阅 RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

SMTP MTA 严格传输安全 (MTA-STS)是一种机制，使邮件服务供应商 (SP)能够声明其接收传输层安全 (TLS)和保护 SMTP 连接的能力，并指定发件 SMTP 服务器是否应拒绝投递给不为 TLS 提供受信任的服务器证书的 MX 主机。要为您自己的域设置 MTA-STS，您需要一个 MTA-STS 策略文件，该文件可以通过 HTTPS 从 URL https://mta-sts.domain.tld/.well-known/mta-sts.txt 下载，其中 "domain.tld"是您的域名。策略文本文件应包含以下格式的几行信息：

```
version: STSv1
mode: testing
mx: mail.domain.tld
max_age: 86400
```

模式可以是 "none"、"testing"或 "enforce"。每个 MX 主机名应有一个 "mx"行。通配符可用于子域，例如 "*.domain.tld"。存在时间最大值以秒为单位。常规值是 86400 (1 天) 和 604800 (1 周)。

还需要 _mta-sts.domain.tld 上的 DNS TXT 记录，其中 "domain.tld"是您的域名。它必须具有以下格式的值：

```
v=STSv1; id=20200206T010101;
```

每次更改策略文件时，都必须更改 "id"的值。通常为这个 id 使用时间戳。

豁免列表
使用此列表可使特定域免于 MTA-STS。

缓存 MTA-STS DNS 记录
默认情况下，MDaemon 缓存 MTA-STS DNS 记录。请点击 **"编辑"**来查看或编辑当前的缓存文件。

启用 TLS 报告 (RFC 8460)

默认情况下禁用 TLS 报告功能，更多详细信息请参阅RFC 8460: SMTP TLS Reporting.

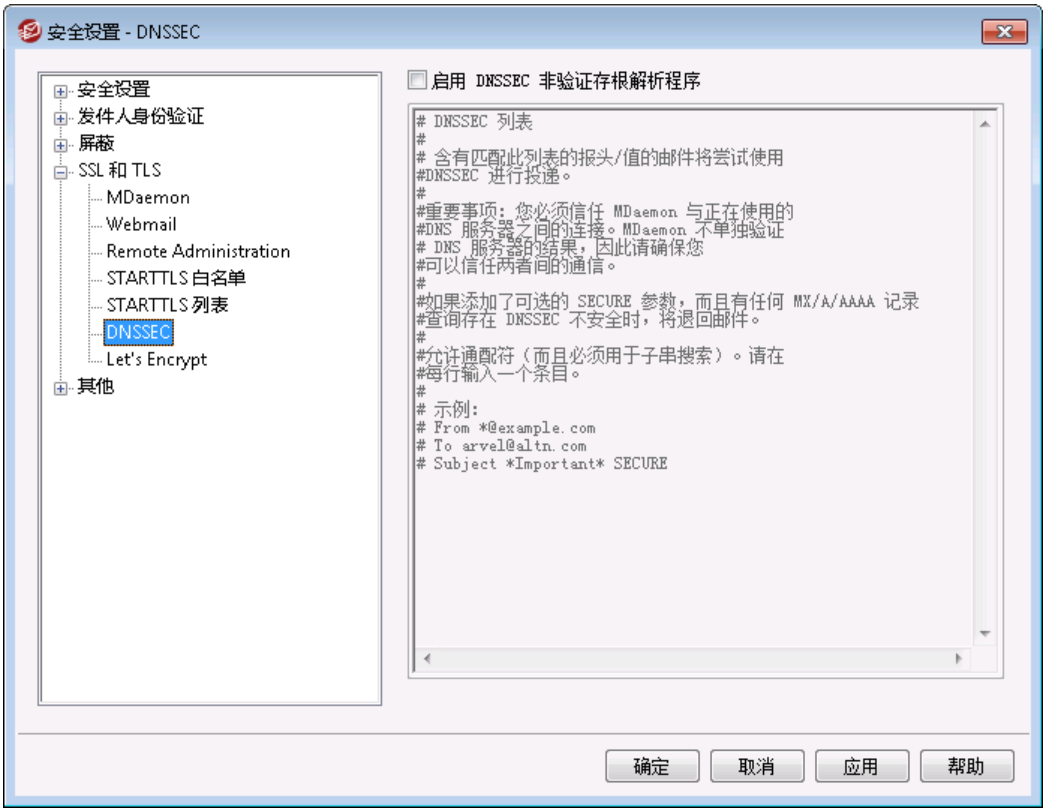
TLS 报告功能允许使用 MTA-STS 的域收到有关检索 MTA-STS 策略或使用 STARTTLS 协商安全通道的任何失败的通知。启用后，MDaemon 会每天向已在当天向其发送 (或尝试发送)邮件的每个启用 STS 的域发送报告。提供了多个选项来配置报告将包含的信息。

要为您的域设置 TLS 报告，请启用 DKIM 签名 445，并在 _smtp._tls.domain.tld 创建一个 DNS TXT 记录，其中 "domain.tld"是您的域名，具有以下格式的值：

```
v=TLSRPTv1; rua=mailto:mailbox@domain.tld
```

其中 mailbox@domain.tld 是您要向其发送域报告的电子邮件地址。

4.1.4.7 DNSSEC



DNSSEC (DNS安全扩展)选项允许 MDaemon 充当非验证安全感知存根解析程序的作用，这在4033 和 4035作为 "发送 DNS 查询、接收 DNS 响应、并能与与认知安全的递归命名服务器建立合适的安全通道的实体，该服务器代表认知安全的存根解析程序提供这些服务"。这意味着，在 MDaemon 的 DNS 查询过程中，您可以向 DNS 服务器请求 DNSSEC 服务，在查询中设置 AD (真实数据）位并在并在回应中进行检查。这可以在 DNS 过程中为某些邮件提供额外的安全级别，但不是全部邮件，因为 DNSSEC 尚不受所有 DNS 服务器或所有顶级域名的支持。

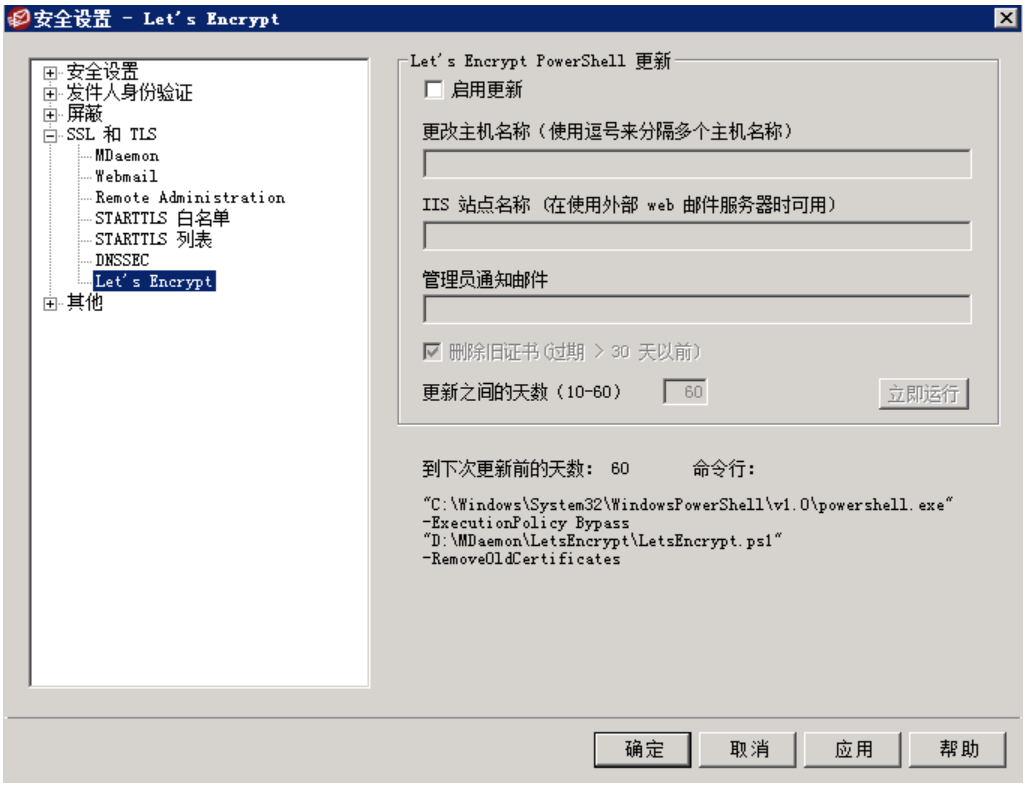
启用时，DNSSEC 服务仅适用于符合您选择标准的邮件；它可以根据您的选择广泛或狭义地请求或要求。只需指定您在 DNSSEC 屏幕上选择的任何 "报头值"组合即可，每当执行 DNS 查询时，MDaemon 都将为符合该标准的任何邮件请求 DNSSEC 服务。当 DNS 结果未

包含验证数据时，则不会产生负面后果；MDaemon 只是回退到常规的 DNS 行为。如果您希望为某些邮件 *请求* DNSSEC，则将 "安全"添加到报头/值组合（例如 "To *@example.net SECURE"）。对于这些邮件，当 DNS 结果无法包含验证的数据，会将该邮件退回发件人。**请注意：**因为 DNSSEC 查找需要更多时间和资源，而且并非所有服务器都支持 DNSSEC，因此默认情况下，MDaemon 未配置成将 DNSSEC 应用于每封邮件传递。不过如果您希望为每封邮件请求 DNSSEC，您可以在条件中包含 "To *"来实现这点。

如果使用 DNSSEC 服务，邮件会话日志将在顶部包含一行，并且日志中的安全数据旁边将显示 "DNSSEC"。

由于 MDaemon 是一个非验证存根解析器，它将向您的 DNS 服务器请求验证数据，但无法独立验证从服务器获得的数据是否安全。出于这个原因，为了安全地使用 DNSSEC 选项，您必须确保您信任与您的 DNS 服务器建立的连接。例如，它运行在本地主机上或安全局域网或工作区内。

4.1.4.8 Let's Encrypt



使用 Let's Encrypt 来管理您的证书

要支持 SSL/TLS and HTTPS 479 for MDaemon 481、Webmail 483 & Remote Administration 487，您需要 SSL/TLS 证书。证书是由证书颁发机构（CA）颁发的小型文件，用于向客户端或浏览器验证与预期服务器建立的连接，并启用SSL / TLS / HTTPS 来保护与该服务器的连

接。Let's Encrypt 是一个证书颁发机构，通过专门设计的自动化流程来为“传输安全层（TLS）”加密提供免费的证书，该流程使您可以免于现在复杂的手动创建、验证、签名、安装和续订用于保护网站安全的证书。

要支持使用 Let's Encrypt 的自动化流程来管理证书，此屏幕来帮助您轻松简便地配置和运行 PowerShell 脚本，位于“MDaemon\LetsEncrypt”文件夹。运行该脚本将使一切为 LetsEncrypt 准备就绪，包括将一些必要的文件放置在 WebmailHTTP 的目录中来完成 http-01 挑战。它将 SMTP 主机名 151（属于默认域 149）用作证书域，包含您已指定的任何*备选主机名称*，检索证书，将其导入 Windows，并配置 MDaemon 如何使用针对 MDaemon、Webmail 和 Remote Administration 的证书。此外，该脚本将在名为 LetsEncrypt.log 的“MDaemon\Logs\”目录中创建一个日志文件 LetsEncrypt.log。每次运行脚本时，都会删除并重新创建该日志文件，并且包含脚本的开始日期和时间。此外，如果您指定了*通知的管理员邮件*，将在出错时发送通知邮件。

> 该脚本需要 PowerShell 3.0，这就意味着它不适用于 Windows 2003。此外，Webmail 270 必须监听 80 端口，而且如果您有一个不指向 MDaemon 服务器的默认域，还有一个针对该域的 SMTP 主机名称 151（例如 FQDN）设置，则该脚本不起任何作用。

Let's Encrypt PowerShell 更新

启用更新
如果您希望通过 Let's Encrypt 脚本自动创建和更新 SSL/TLS 证书，请点击此框。将根据下方的*“更新间的天数”*设置，证书将每隔 10~60 天更新一次。

备选主机名（用逗号分隔多个项目）
如果您希望在证书中设置备用主机名，请在此处指定这些主机名，并用逗号分隔。您无需在此列表中包含默认域的 SMTP 主机名。例如，如果您的默认域是“example.com”，使用“mail.example.com”作为 SMTP 主机名称，而且您希望使用“imap.example.com”作为备选主机名，那么您只需包含“imap.example.com”作为备选主机名。如果您不想使用任何必选主机名，则将该选项留空。**请注意：**如果您包含备选主机名，则必须完成 Let's Encrypt 的 HTTP 质询，以验证您的服务器对该主机名的控制权。如果未完成全部质询，将无法继续处理。

IIS 站点名称（在使用外部 webmail 服务器时可用）
如果您通过 IIS 运行 Webmail，请在此输入 IIS 的站点名称。您必须安装 Microsoft 的 Web Scripting 工具，以便在 IIS 中自动设置该证书。

用于通知的管理员邮件
如果您希望在 Let's Encrypt 更新期间发生错误时收到通知，请在此处指定管理员电子邮件地址。

删除旧证书（过期时间 > 30 天）
默认情况下，MDaemon 将删除过期时间大于 30 天的任何旧证书。如果您不希望自动删除这些证书，请不要勾选该复选框。

更新间的天数（10-60）
使用此选项可以指定从 10~60 天内更新证书的频率。默认设置是 60 天。

立即运行
点击这个按钮来立即运行脚本。

4.1.5 其他

4.1.5.1 反向散射保护 - 概述

反向散射

“反向散射”表示用户接收到他们从未发出过的邮件的响应邮件。当病毒发送的垃圾邮件或邮件中包含伪造的“返回路径”地址时会发生反向散射。因此，当其中一封邮件被收件人服务器拒收时，或如果收件人使用自动应答程序或“外出”/假期邮件与其帐户关联，响应邮件随之将指向伪造的地址。这会导致海量的伪造投递状态通知 (DSN) 或自动应答邮件撑爆用户的邮件箱。另外，垃圾邮件发送者和病毒编写者会经常利用该现象，有时使用它对邮件服务器启动拒绝服务 (Denial of Service, DoS) 攻击，造成从世界各地的邮件服务器接收大量无效的邮件。

MDaemon 的解决方案

为了防止反向散射，MDaemon 包含了所谓的反向散射保护 (BP) 功能。BP 使用私钥散列法生成并插入特殊的时间敏感代码到用户外发邮件的“返回路径”地址中，从而可以帮助确保帐户仅收到合法的投递状态通知和自动应答邮件。这样，当其中一封邮件因遭遇投递问题而被退回时，或收到带有“mailer-daemon@...”或者 NULL 反向路径的自动答复时，MDaemon 将查看该特殊代码，以确定这的确是对由您的账户所发送邮件的自动答复。如果地址中未包含该特殊代码，或代码日期超过 7 天，则该邮件将被 MDaemon 记入日志并有权拒收。

反向散射保护 499 在 MDaemon 的安全菜单下，位于：安全 » 安全设置 » 其他 » 反向散射保护。

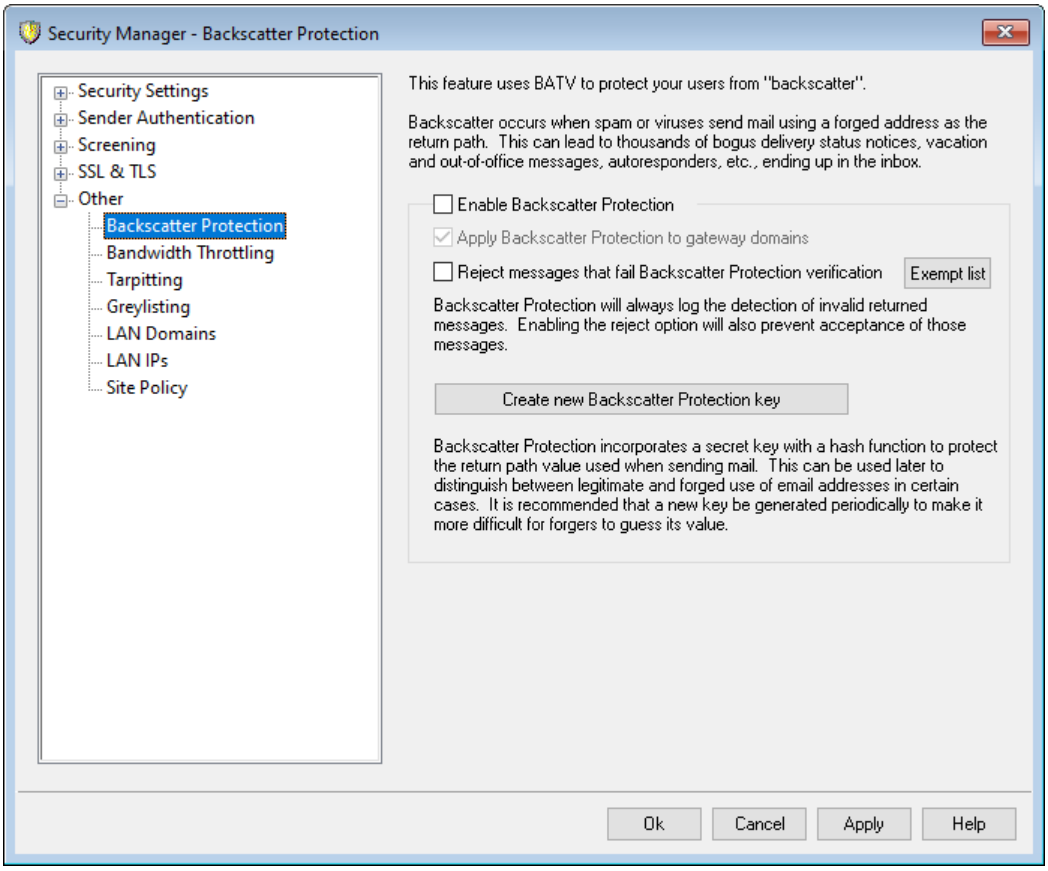
反向散射保护应用了退回地址标记验证 (Bounce Address Tag Validation, BATV)。有关 BATV 的更多信息，请访问：

http://www.mipassoc.org/batv/

还请参阅：

反向散射保护 499

4.1.5.1.1 反向散射保护



反向散射保护

启用反向散射保护
如果要在每封外发邮件的"返回路径"地址中插入特殊的"反向散射保护代码"代码，可以选中该复选框。MDaemon 将使用 rsa.private 文件（位于 MDaemon 的 PEM_batv\ 文件夹）中的私钥生成特殊代码，该代码的有效期为 7 天。任何入站 DSN 或其他自动应答邮件（带有 "mailer-daemon@..."或 NULL 反向路径）必须拥有未过期的有效 BP 代码，否则将无法通过反向散射保护验证。

如果禁用该选项，MDaemon 将不会在出站邮件中插入特殊的"反向散射保护"代码。不过，它仍将继续检查入站的 DSN 及自动应答邮件以确保不会错误地拒收任何带有正确代码的接收邮件。

应用"反向散射保护"到网关域
启用反向散射保护时，点击该选项可以同时将 BP 应用到 MDaemon 为之充当网关或备份服务器的域（参见域网关 206）。

拒收验证反向散射保护失败的邮件
如果要拒收 BP 验证失败的 DSN 或其他自动应答邮件，可以点击此选择框。带有 "mailer-daemon@..."或 NULL 反向路径的邮件如果不包含特殊代码或超过代码的七天有效期，将无法通过 BP 验证。由于反向散射保护具有坚实的可靠性，所以不存在误

报或“灰色区域”——邮件要么有效，要么无效。因此，配置 MDaemon 拒收无效的邮件非常安全，只要确保所有账户的外发邮件中都包含特殊的 BP 代码即可。即使您选择不拒收验证失败的邮件，但在所有情况中，BP 验证的结果都会被记录到 SMTP-in 日志文件中。除非选中上述的“*..应用反向散射保护到网关域*”选项，否则将不会拒收网关的入站邮件。

启用反向散射保护后，将其设置为拒收无效自动应答邮件前应等待一周左右时间。因为在此期间，您仍可能接收激活 BP 前发送的邮件的 DSN 或自动应答。如果在此期间将 BP 配置为拒绝无效邮件，则会错误地拒收这些合法的应答邮件。大约一周后开始拒收无效的邮件比较安全。当创建新的 BP 密钥并立即删除旧密钥（而不是允许旧密钥继续使用 7 天）时，相同的警告同样适用。（请参阅以下“*创建新的反向散射保护密钥*”选项）。

豁免列表
点击此按钮来打开“反向散射保护”豁免列表。使用该名单可指定任何不受反向散射保护的 IP 地址或域。

创建新的“反向散射保护”密钥
点击该按钮可生成新的反向散射保护密钥。MDaemon 使用此密钥创建并验证插入到邮件中的特殊 BP 代码。该密钥位于 MDaemon 的 PEM_batv\ 文件夹中的 rsa.private 文件内。生成新密钥时，将打开对话框提醒您原来的密钥在未来 7 天中继续有效，除非您希望将其立即删除。大多数情况下应点击“否”，选择允许该密钥再使用 7 天。如果选择立即删除密钥，可能导致某些入站邮件无法通过 BP 验证，因为它们所响应的原始邮件包含的特殊代码是由原来的密钥生成的。

如果将邮件数据流分布在多个服务器上，则需要在其他所有服务器或邮件传输代理（MTA）上共享密钥。

还请参阅：

反向散射保护 - 概述 498

4.1.5.2 带宽节流 - 概述

“带宽节流”功能使您能管理 MDaemon 所使用的带宽。您可以控制会话或服务器的比例——以每个域为基础，您可为每个 MDaemon的主要服务器设置不同的比例，包括域和域网关。您也可以在一个下拉框中通过选择“本地通信量”来设置针对本地连接的限制。这将允许您创建特殊的带宽设置，从而在连接到或被本地 IP 地址或域名连接时启动。

“带宽节流”可以按会话或按服务进行应用。当在使用每个会话模式时，每个会话将分别根据设置的比例节流。因此同时产生的同一服务器类型的多个会话可能会超出一个服务的配置值。如果在每个服务器的基础上设置带宽限制，MDaemon将监控同一服务器类型的所有会话的结合使用并对每一个会话分配同样的带宽。多个会话将共同平均使用设置的最大带宽。这将允许你为整个服务设置一个限制。

当扩展“带宽节流”到“域网关”时，与处理普通域时有点不同。这是由于“域网关”没有与其相关联的特定 IP 地址。MDaemon 必须通过使用通过 RCPT 指令的值，来决定一个本地的 SMTP会话是否是在门的本地范围内。如果是，本地 SMTP 会话的带宽限制将适用。由于 SMTP 的限制，即使（指向多个收件人）邮件的一个收件人被指定一个“域网关”，那么整个会话将被节流。

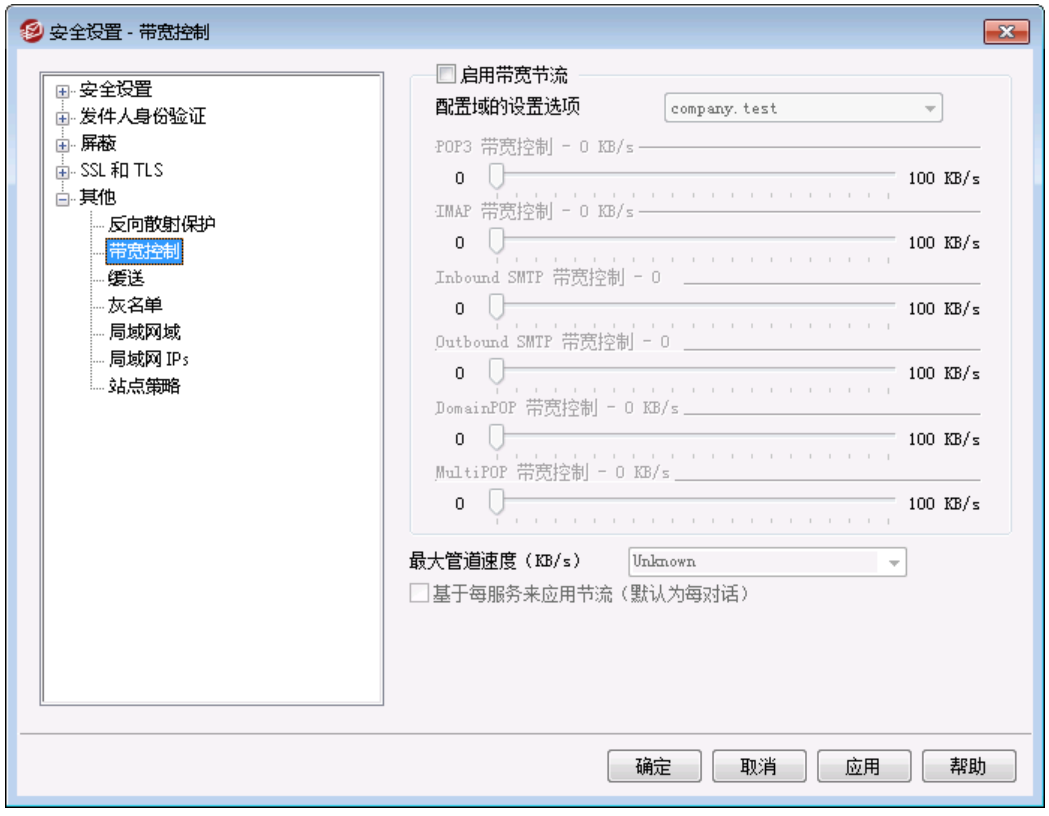
“带宽节流”系统将以千字节每秒（KB/S）进行校准。“0”值表示此会话（或服务）进度没有速度限制，因此它将使用可利用的最大带宽。例如，“10”将强制 MDaemon 刻意对传输速度进行节流，使其保持或稍大于 10KB/S 的速度。

会话开始时的突发活动可能会超出限定的范围。节流将在会话过程中开始起作用并达到稳定。

还请参阅：

带宽节流 501
局域网 IP 508

4.1.5.2.1 带宽限制



启用带宽节流
如果您希望激活带宽节流功能，请勾选此框。

配置域的设置
从下拉列表框中选择域，然后对选择的域调整不同服务器设置的带宽限制选项。将任何特定控件设置为 "0"表示对于此服务器类型没有带宽限制。在下拉列表框中，底部列出的是*本地流量*。对此选项设置带宽限制将决定对本地流量的限制（例如：会话和服务器出现在您的本地局域网上，而不是在外部局域网上）。局域网 IP 屏幕可用来列出可视为本地的 IP 地址。

服务

[服务类型]带宽控制—XX KB/秒
从下拉列表框中选择域后，调整这些控件来为选定域设置带宽限制。"0"设置表示对此特定服务器类型不应用带宽限制。将滑动条设置为 "0"以外的任何数字会将指定服务的最大带宽限制为此数字的千字节每秒。

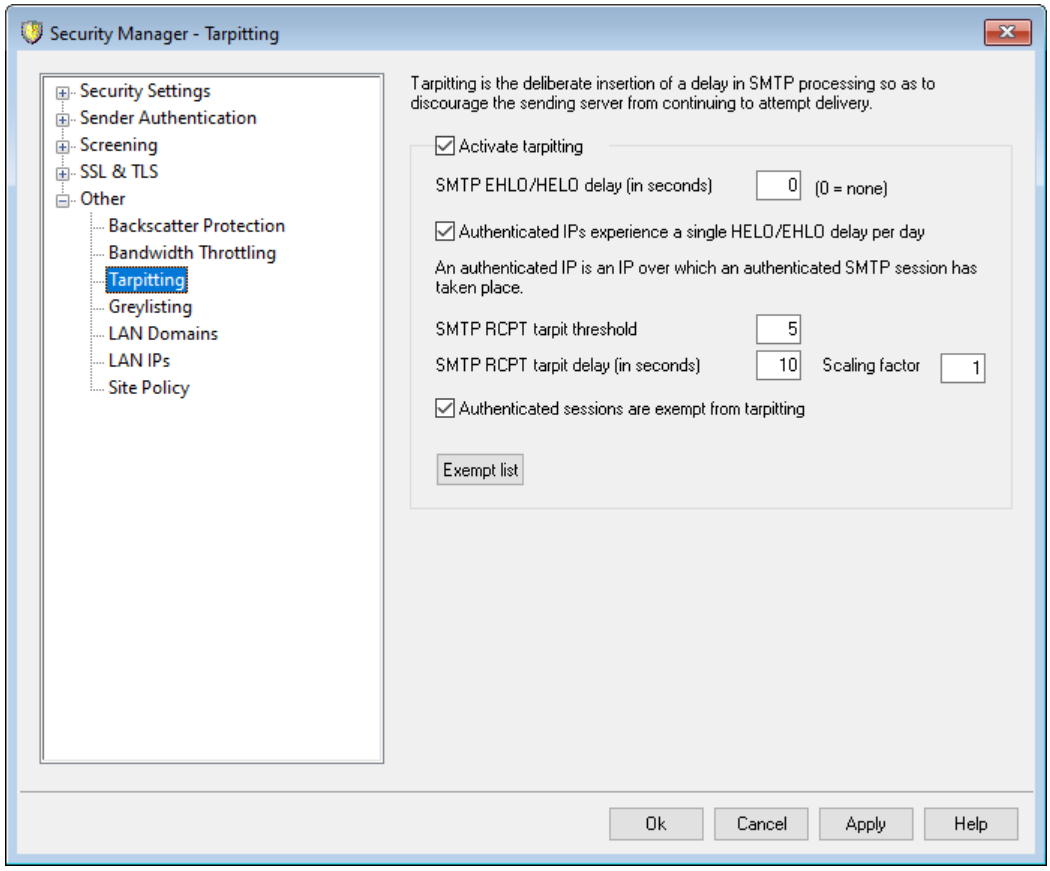
最大管道速度（KB/秒）
从下拉列表框中选择您连接的最大速度，以千字节每秒（KB/秒）为单位。

基于每服务来应用节流（默认为每会话）
如果您想对每个服务器，而不是默认的每个会话节流带宽，请选择此项。当对每个服务器节流时，该服务所指定的带宽数量将平均分配给所有此服务类型的活动会话。因此，无论多少用户连接，同时连接的多个 IMAP 用户使用的带宽总量将不会超出设置的量。如果对每个*会话*节流，单个 IMAP 会话不会超出设置量，而多个并发会话的总量可能会超出限制。

还请参阅：

带宽节流 - 概述

4.1.5.3 缓送



"缓送"在"安全"菜单下，位于："安全» 安全设置» 其他» 缓送"。

缓送使得一旦从邮件发件人处收到指定数量的 RCPT 命令后可有意延迟连接。这将阻止垃圾邮件制造者企图利用您的服务器发送未经请求的群发邮件（"垃圾邮件"）。您可指定缓送开始前允许的 RCPT 命令数以及在连接期间每当从该主机收到后续命令时延迟连接的秒数。该技术背后的设想是如果垃圾邮件制造者发送每封邮件都需要花费相当长的时间，这将阻止他们以后不再企图利用您的服务器做同样的操作。

激活缓送
点击该复选框可激活 Mdaemon 的缓送功能。

SMTP EHLO/HELO 延时（以秒计算）
使用该选项可延迟服务器对于 EHLO/HELO SMTP 命令的响应。延迟响应哪怕 10 秒钟也可能会节省大量处理时间，因为它减少了收到的垃圾邮件数量。垃圾邮件制造者常常依赖于邮件的快速投递，因而不会长时间等待对 EHLO/HELO 命令的响应。使用哪怕很小的延时，有时会使垃圾邮件制造工具放弃等待响应而继续群发操作。MSA 端口（在端口 87 屏幕上指定）上的连接始终免于该延迟。该选项的默认设置是"0"，表示不会延迟 EHLO/HELO 响应。

经身份验证的 IP 地址每天经历单次 EHLO/HELO 延迟
如果希望限制来自给定 IP 地址的已验证连接每天只经历一次 EHLO/HELO 延迟，请点击该复选框。来自该 IP 地址的第一封邮件将被延迟，但相同地址发来的后续邮件不会。

SMTP RCPT 缓送阈值
指定在邮件会话期间，Mdaemon 开始缓送处理前，允许给定主机发送的 SMTP RCPT 命令数。例如，如果该阈值设为 10 且发送主机试图将邮件发送到 20 个地址 (即 20 条 RCPT 命令)，那么 MDaemon 将照常处理前 10 条命令，而在之后的每条命令后暂停下方 "*SMTP RCPT 缓送延时*"控件中指定的秒数。

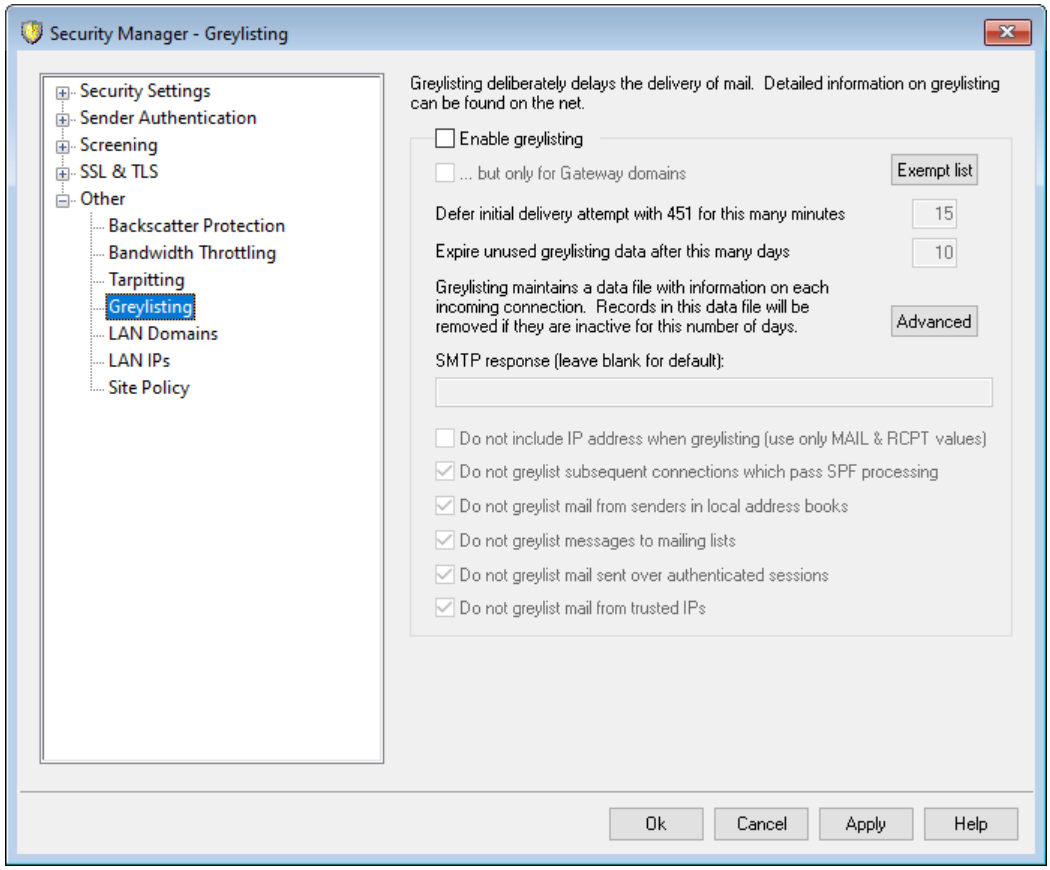
超过限额的 SMTP RCPT 之间的延时 (以秒计算)
一旦主机达到 *SMTP RCPT 缓送阈值*，MDaemon 将在邮件会话期间从该主机收到的每条后续 RCPT 命令后暂停这些秒数。

缩放系数
基本缓送延时随时间按此倍数增加。当达到缓送阈值且将缓送延时应用于会话时，每一延时将与该值相乘以确定会话中的下一延时长度。例如，如果缓送延时设为 10 而缩放系数设为 1.5，那么第一个延时将为 10 秒钟，第二个延时为 15 秒钟，第三个延时 22.5 秒钟，然后是 33.75，依此类推 (即 10 x 1.5 = 15，15 x 1.5 = 22.5 等等)。. 默认缩放系数为 1，意味着延时不会增加。

已验证的会话免于缓送
如果希望对其邮件会话进行了身份验证的发件人免于缓送，请点击该复选框。

豁免列表
点击此按钮来打开 动态允许列表 522，这也用于 "缓送"。在此可指定免于缓送的 IP 地址。

4.1.5.4 灰名单



灰名单在安全对话框之下，位于：安全» 安全设置» 其他» 灰名单。灰名单是一种抵御垃圾邮件的技术，它利用了 SMTP 服务器会重试投递任何收到暂时（即"稍后重试"）错误代码的邮件这一特性。通过这项技术，当邮件来自未列入允许列表或先前未知的发件人时，其发件人、收件人和发件服务器的 IP 地址会被记入日志，然后在 SMTP 会话期间将由灰名单以暂时错误代码拒绝该邮件。不仅如此，在指定时段内（如 15 分钟），任何重新投递的企图都将暂时被拒绝。因为垃圾邮件制造者在邮件被拒绝后通常不会进一步尝试投递，灰名单有助于显著减少用户收到的垃圾邮件数量。即使垃圾邮件制造者以后试图重新投递，但到那时垃圾邮件制造者很可能已被识破并将被其它反垃圾邮件选项（如 DNS 阻止列表 586）成功拦截。然而，值得注意的是，这项技术也会同时延缓某些正常邮件的接收。但是，在灰名单时间段过期后仍会投递合法邮件。还有需要注意的一点是，您无法知道发送服务器在作进一步投递尝试之前将等待多久。以暂时错误代码故意拒收邮件可能导致其延迟时间从几分钟到一整天不等。

灰名单存在几个常见问题和负作用，灰名单屏幕包含多个选项来应对这些问题。

首先，有一些发件域是由多个邮件服务器汇集而成的，用来发送出站邮件。由于每一次投递尝试可以使用一个不同的邮件服务器，每一次尝试可视作是与灰名单引擎的一次新连接。这可以大大缩短邮件通过灰名单的时间，因为每一个尝试都会列入灰名单，就好像它们都是分离的邮件而不是重试先前的邮件。通过使用一个 SPF 查找选项，可以为那些发布其 SPF 数据的发件域解决该问题。此外，有一个选项可完全忽略发件邮件服务器的 IP 。使用该选项降低了灰名单的效能，但能彻底解决服务器集合问题。

其次，由于必须追踪每个入站连接，灰名单通常需要一个大型数据库。MDaemon 通过将灰名单功能放置在 SMTP 处理序列接近末尾处，从而将追踪连接的需求降到最低。这使得

MDaemon 的所有其它选项可在邮件到达灰名单阶段前先拒绝该邮件。因此大大减小了灰名单数据文件的大小，而且由于它驻留在内存中，因而对性能的实际影响很小。

最后，有多个选项可尽量降低灰名单对正常邮件的影响。首先，发送到邮件列表的邮件可以被排除在外。其次，灰名单有自己的豁免列表，可以在其中指定免于列入灰名单的 IP 地址、发件人和收件人。最后，"灰名单"包含一个选项，可使用每个账户的地址簿来作为豁免列表。这样，从用户地址簿中的某联系人发给该用户的邮件可排除在灰名单之外。

有关灰名单的更多介绍信息，请访问 Even Harris 的网站：

http://projects.puremagic.com/greylisting/

灰名单

启用灰名单
点击该选项可启用 MDaemon 内的灰名单功能。

...但仅用于网关域
如果只想对发往网关域的邮件应用灰名单，请点击该复选框。

豁免列表
该按钮打开了灰名单豁免列表，从中你可以指定哪些发件人、收件人和 IP 地址将免于列入灰名单。

延迟起初用 451 的投递尝试达这些分钟
指定初始投递尝试后将投递尝试列入灰名单的分钟数。在此期间，将以另一个暂时错误代码拒绝相同服务器/发件人/收件人组合（即"灰名单三元组"）的任何后续投递尝试。灰名单时限过后，除非灰名单数据库记录已过期，否则灰名单延迟不再应用于该三元组。

终止不用的灰名单数据库记录在这些天之后
给定灰名单三元组的初始灰名单时限过后，灰名单不再延迟匹配该三元组的邮件。然而，如果在该选项中指定的天数内未收到匹配该三元组的邮件，其灰名单数据库记录将会过期。该三元组的后续尝试将导致创建新的灰名单记录，并将不得不再次经历初始灰名单时期。

高级
点击该按钮可打开灰名单数据库，用于浏览或编辑灰名单三元组。

SMTP 响应（默认为空）
如果您在此区域提供自定义文本字符串，那么 MDaemon 将返回 SMTP 响应，使用"451 <您的自定义文本>"取代默认的"451 已启用灰名单，请于 X 分钟后重试。"这十分有用，例如，如果您希望为灰名单说明提供一个包含 URL 的字符串。

列入灰名单时不要包括 IP 地址（只使用 MAIL 和 RCPT 值）
若您不希望将发件服务器的 IP 地址用作灰名单的其中一个参数，请点击此选择框。这解决了服务器集合可能导致的潜在问题，但降低了灰名单的效率。

不将通过 SPF 处理的后续连接列入灰名单
使用该选项时，如果入站邮件匹配三元组的发件人和收件人但不匹配发送服务器，而 SPF 处理确定该发送服务器是此三元组中所列项的有效替代，那么该邮件将被视作匹配此三元组的后续投递而不是需要新的灰名单记录的新建连接。

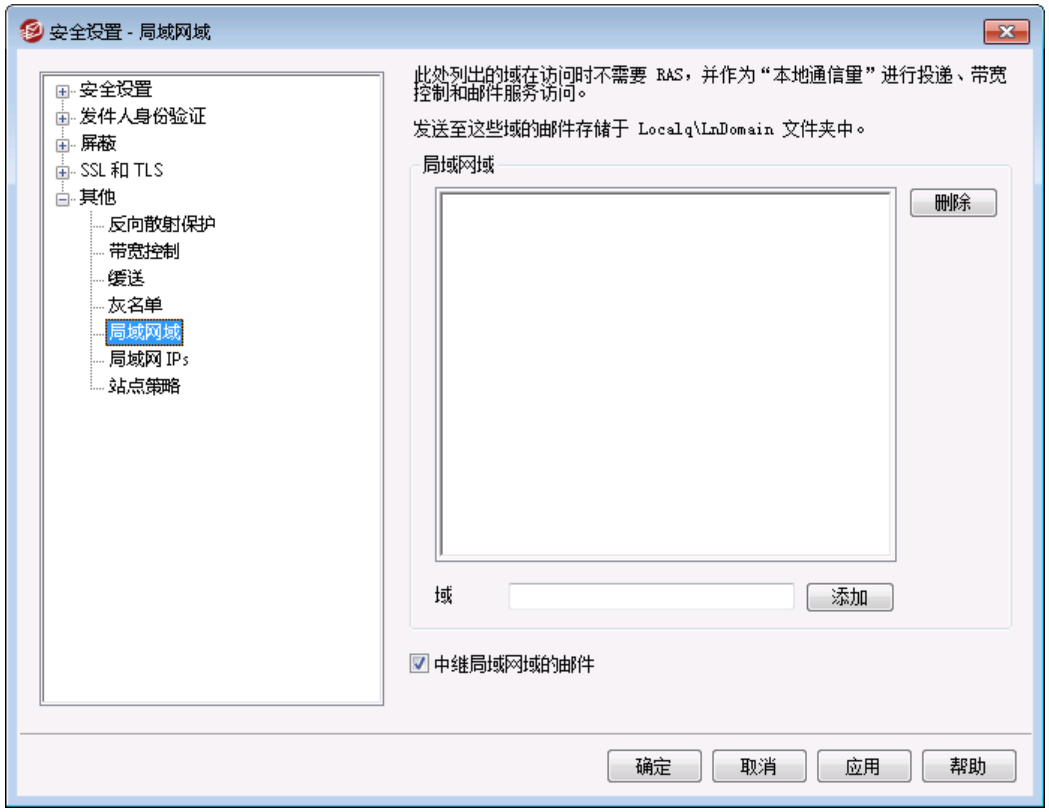
不将发件人位于本地地址簿的邮件列入灰名单
如果希望从灰名单中排除发件人列于收件人地址簿的邮件，请点击该选项。

不将发往邮件列表的邮件列入灰名单
如果想让发往邮件列表的邮件免于被列入灰名单，请点击该复选框。

不将通过已验证会话发送的邮件列入灰名单
如果想让所有通过已验证会话抵达的邮件免于被列入灰名单，请使用该选项。

不将来自可靠 IP 地址的邮件列入灰名单
如果想让所有来自可靠 IP 地址的邮件免于被列入灰名单，请使用该选项。

4.1.5.5 局域网域



局域网域

MDaemon 认为此处所列域是本地局域网 (LocalArea Network)的一部分。因此，在投递邮件时无需拨号或互联网连接。

域
输入域名，然后点击*添加*将其添加到列表中。

添加
在*"域"*选项中指定了一个域后，点击此按钮将其添加到列表。

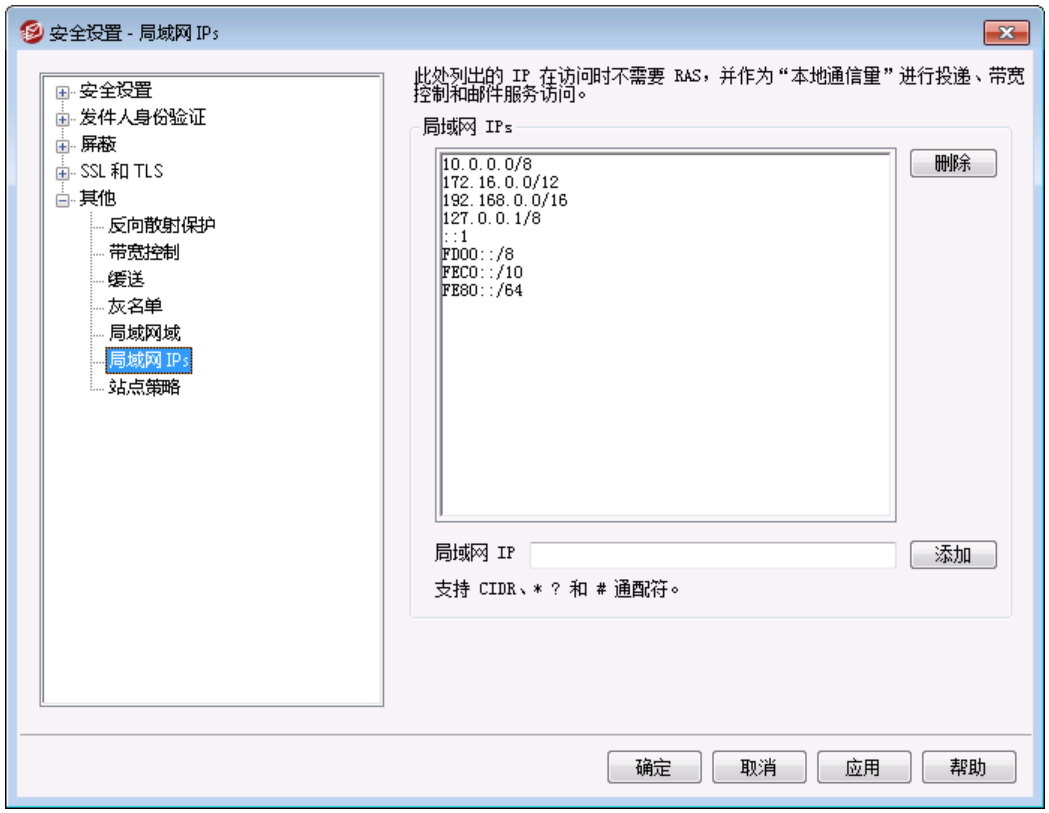
删除
在列表中选择一个域，然后点击该按钮将其删除。

中继本地域的邮件
如果选中该复选框，MDaemon 将中继这些域的邮件。这提供了一些方式来控制这些域间发送的通行量。

还请参阅：

局域网 IP 508

4.1.5.6 局域网 IP



局域网 IP

类似于局域网域 507，该屏幕用于列出位于局域网内的 IP 地址。因此，访问这些 IP 地址不需要 RAS 或互联网连接，而且它们被视作本地通信以利于带宽节流。此外，因为它们是本地地址，因而可能会豁免多种其它安全和垃圾邮件防范限制。

删除
从列表中选择一个 IP 地址，然后点击此按钮将其删除。

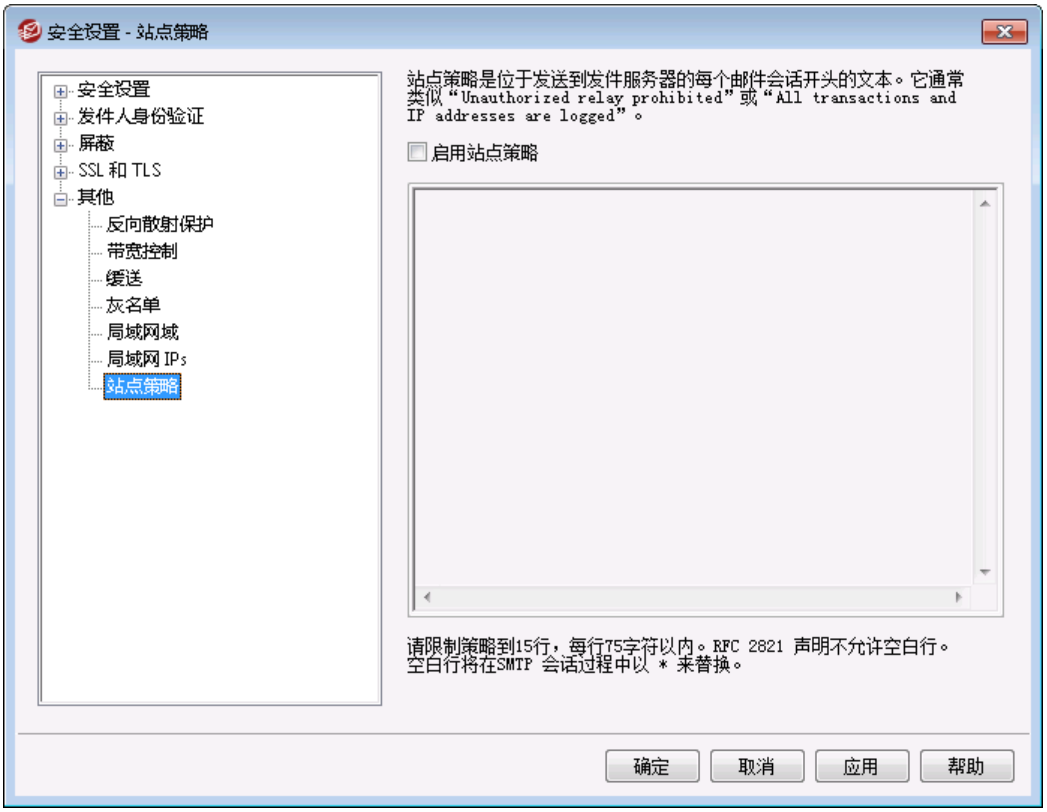
局域网 IP 地址
输入要添加到局域网 IP 列表中的 IP 地址，然后点击*添加*。支持通配符，如 127.0.*.*。

添加
在*"局域网 IP"*控件中输入 IP 地址后，点击该按钮将其添加到列表中。

还请参阅：

局域网域 507

4.1.5.7 站点策略



陈述 SMTP 站点策略
使用该对话框可陈述服务器的站点策略。策略文本存储在 policy.dat 文件中，位于 MDaemon 的 \app\ 子文件夹内，并在每个 SMTP 邮件会话开头传输到发送服务器。常用站点政策的示例是 "该服务器拒绝中转"或 "未经授权不得使用"。每行前无需添加 "220"或 "220-"。无论有没有这些前缀码，MDaemon 将对每行作相应处理。

在 SMTP 传输期间有关邮件中继的站点使用策略声明类似于：

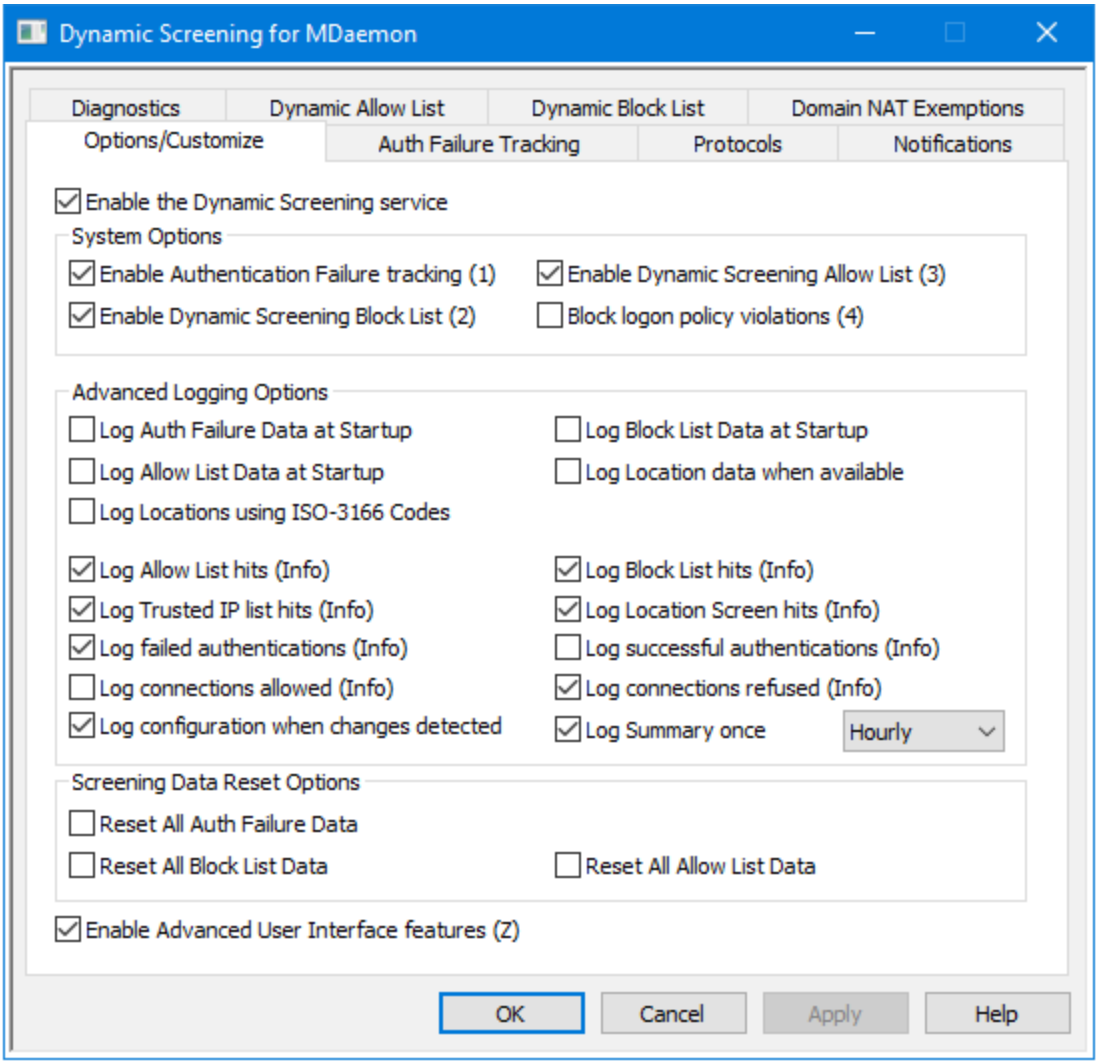
```
220-MDaemon Technologies ESMTP MDaemon
220-本站点不会中转未经授权的邮件。
220-如果您不是我们的服务器的授权用户
220-那么您不得通过本站点中转邮件。
220
```

```
HELO example.com...
```

POLICY.DAT 文件只能由可打印的 ASCII 文本组成且每行不得超过 512 个字符，然而强烈建议您每行不要使用超过 75 个字符。此文件的最大容量为 5000 字节。MDaemon 不会显示大于 5000 字节的文件。

4.2 动态屏蔽

4.2.1 选项/定制



使用动态屏蔽，MDaemon 可以追踪入站连接的行为来识别可疑的活动并作出相应的响应。您可以阻止 IP 地址 513 (或地址范围)进行连接，如果这些地址达到指定的验证失败次数。您也可以在账户太快达到验证失败次数时冻结账户 513。此外，IP 地址的阻止和账户的冻结都不是永久性质的。连接的 IP 地址将被阻止达到指定的分钟数，小时数或天数，冻结的账户可以在指定的时间段后自动 "解冻"，或由管理员手动解冻。

启用动态屏蔽服务
选中此框来启用 "动态屏蔽"服务。您还可以在 MDaemon 主用户界面内导航窗格中的 "服务器"部分下启用/禁用该服务。

系统选项

启用验证失败跟踪
启用此项时，"动态屏蔽"服务将为在协议[516]选项卡上指定的协议跟踪验证失败，并执行验证失败跟踪[513]选项卡上的选项确定的操作。默认情况下启用此项。

启用动态屏蔽阻止列表
此项启用 "动态屏蔽"服务用来阻止 IP 地址和 IP 范围的功能。您可以从动态阻止列表[524]选项卡管理阻止列表。默认情况下，阻止列表选项处于启用状态。

启用动态屏蔽允许列表
此项启用 "动态屏蔽"服务的 动态允许列表[522]功能，您可以使用它来豁免 IP 地址和范围，以将它们从 "动态屏蔽"中排除。默认情况下启用允许列表。

阻止登录策略违规
默认情况下，MDaemon 要求账户在登录时，使用其完整的电子邮件地址，而不仅是其地址的邮箱部分 (例如他们必须使用 "user1@example.com"而不仅是 "user1")。这由 *"服务器需要完整的邮件地址进行验证"*这个选项控制，它位于系统[414]页面。在启用该项时，如果您希望阻止不使用完整的邮件地址尝试登录的任何 IP 地址，您也可以启用 *"阻止登录策略违规"*这个选项。默认情况下，禁用该选项。

高级日志选项

在开机时记录验证失败数据
此项帮助用户在开机时将当前由 "动态屏蔽"保存的所有验证失败数据[513]写入日志文件。默认情况下，禁用该选项。

开机时记录阻止列表数据
此项帮助用户在开机时将当前由 "动态屏蔽"保存的所有动态阻止列表[524]数据写入日志文件。默认情况下，禁用该选项。

开机时记录允许列表数据
此项帮助用户在开机时将当前由 "动态屏蔽"保存的所有动态允许列表[522]数据写入日志文件。默认情况下，禁用该选项。

在可用时记录位置数据
如果您希望记录每个连接的位置数据 (如果可用)，请选中此框。

使用 ISO-3166 代码来记录位置
如果您希望在记录位置时使用 ISO-3166 双字母的国家/地区代码，而不是使用名称，请选中此框。

记录所有允许列表匹配项
每次入站连接来自动态允许列表[522]上的地址时，此项会将条目添加到 "动态屏蔽"日志中。

记录所有阻止列表匹配项
每次入站连接来自动态阻止列表[524]上的地址时，此项会将条目添加到 "动态屏蔽"日志中。

记录所有可信 IP 列表点击
每次入站连接来自可信 IP[435]地址时，此项会将条目添加到 "动态屏蔽"日志中。

记录所有位置屏蔽点击
每次入站连接由于位置屏蔽[477]被拒绝时，此项会将条目添加到 "动态屏蔽"日志中。

记录所有失败验证
每次入站连接验证失败时，此项会将条目添加到 "动态屏蔽"日志中。

记录所有成功验证
如果您希望记录每个成功的入站验证尝试，请启用此选项。默认情况下，禁用该选项。

记录所有允许的连接
如果您希望为每个通过动态屏蔽的连接创建日志条目并允许继续处理，请启用此选项。默认情况下，禁用该选项。

记录所有被拒的连接
每次 "动态屏蔽"拒绝入站连接时，此项都会向日志添加条目。

在检测到变更时记录配置
当从外部来源检测到变更时（例如手动编辑 INI文件），此项会将条目添加到所有动态屏蔽配置的日志中。以信息级别记录常规变更

[每天 |每小时 |每分钟]记录摘要一次
每天、每小时或每分钟向动态屏蔽日志添加动态屏蔽统计信息的摘要。默认情况下每小时记录摘要一次。

屏蔽数据重置选项

重置所有验证失败数据
如果您希望清除所有动态屏蔽验证数据，请点击此复选框。然后您必须点击 "应用"或 "确定"来使重置生效。

重置所有阻止列表数据
如果您希望清除所有 "动态屏蔽阻止列表"数据，请点击此复选框。然后您必须点击 "应用"或 "确定"来使重置生效。

重置所有允许列表数据
如果您希望清除所有 "动态屏蔽允许列表"数据，请点击此复选框。然后您必须点击 "应用"或 "确定"来使重置生效。

启用高级用户界面功能

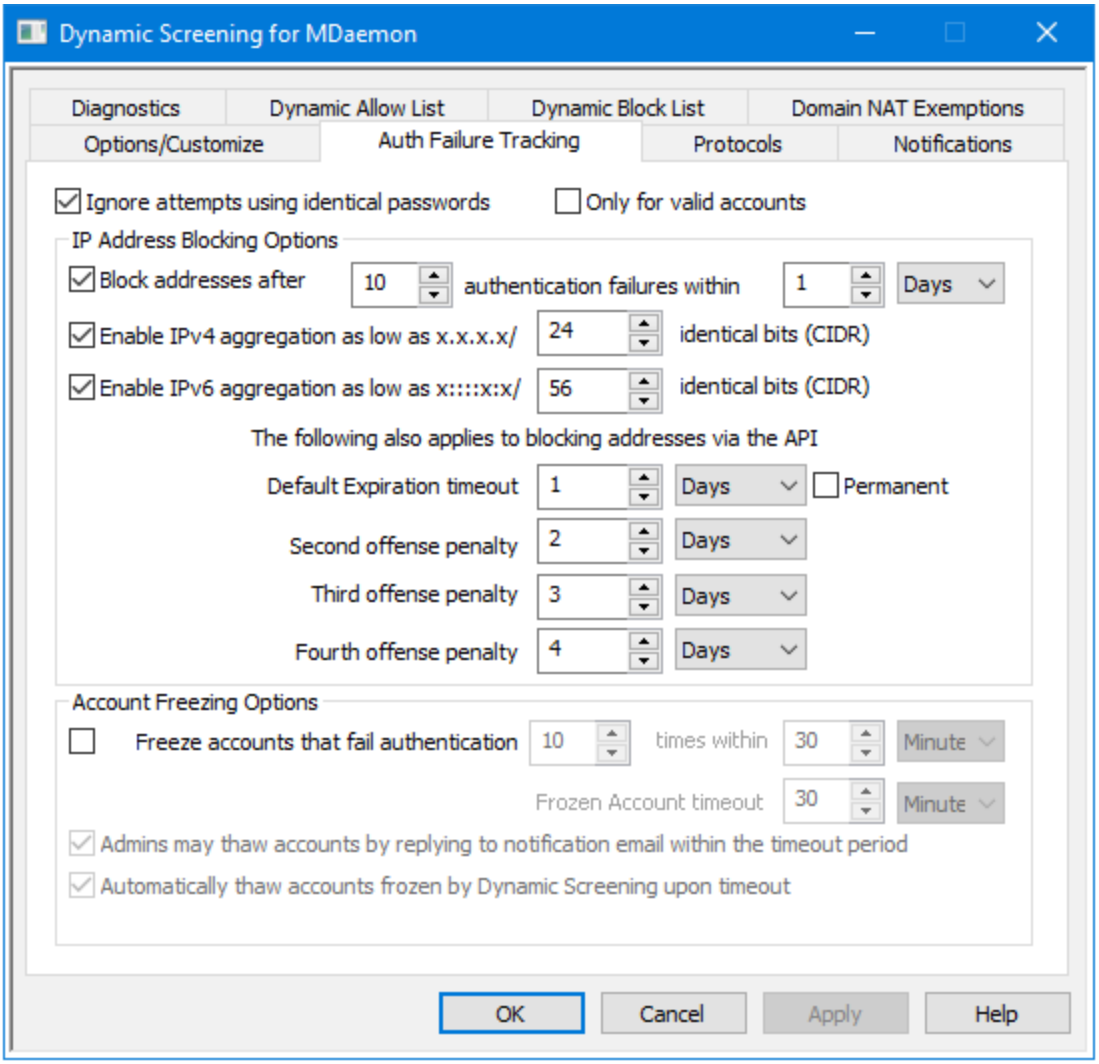
选中此框，然后关闭/重新打开 MDaemon 的配置界面来添加几个高级的动态屏蔽功能。已将 "动态 NAT 豁免[526]"屏幕添加到 "动态屏蔽"对话框，您可以从中指定特定的 IP 地址/域组合，以便在使用这个 IP 地址的有效用户无法通过密码验证时，将上述组合从 "动

态屏蔽”阻止中免除。在工具栏的“动态屏蔽”部分中还添加了几个“动态屏蔽”快捷方式，并且在主界面的“服务器”部分下的“动态屏蔽”快捷菜单中添加了一个选项，允许您暂停而不是禁用“动态屏蔽”服务，从而防止客户端在管理其设置时访问服务。

还请参阅：

验证失败跟踪 513
动态允许列表 522
动态阻止列表 524
域 NAT 豁免 526
协议 516
位置屏蔽 477
SMTP 屏蔽 472

4.2.2 验证失败跟踪



忽略使用相同密码的验证尝试

该选项适用于 "IP 地址阻止选项"和下方的 "账户冻结选项"。默认情况下，当验证尝试失败时，在使用相同密码的情况下，后续验证尝试将被忽略。在阻止 IP 地址或冻结账户之前，它们不会被计入允许的失败次数。例如，当用户的电子邮件密码已更改或过期，并且其客户端自动尝试使用旧密码进行登录时，通常会出现多次尝试使用相同的不正确密码的情况。

仅适用于有效账户
如果您只希望在尝试登录有效账户时，忽略重复的密码身份验证尝试，请激活此选项。这就意味着，例如，如果用户在一个客户端中更新了密码，但另一个客户端仍使用旧密码运行，则仍将忽略该旧客户端的登录尝试，因为它将具有正确的登录名。尝试使用类似的密码和随机登录名称的机器人不会有同样的好处，并且一旦超过验证失败阈值就会被阻止。

IP 地址阻止选项

在 [xx]次验证失败后阻止地址，时间范围是 [xx][分钟 |小时 |天]内
如果您希望暂时阻止在有限的时间内，向您的服务器进行验证时失败次数过多的 IP 地址，请点击此复选框。指定分钟、小时或天数以及在此期间允许的失败次数。

启用 IPv4 聚类低至 x.x.x.x/[xx]相同位 (CIDR)
当身份验证失败来自彼此靠近的 IP 地址，而不是单个地址时，此项将阻止一系列 IPv4 地址。

启用 IPv6 聚类低至 x:::x:x/[xx]相同位 (CIDR)
当身份验证失败来自彼此靠近的 IP 地址，而不是单个地址时，此项将阻止一系列 IPv6 地址。

多重违规惩罚

这是 "动态屏蔽"系统在指定次数的验证尝试失败时，IP 地址或 IP 地址范围将被阻止的时间。默认情况下，IP 地址被阻止的时间将随着后续违规而增加。也就是说，默认情况下，如果一个 IP 地址违反了验证失败的限制，它将被阻止的时间将长达一天。如果这个 相同的 IP 地址再次违反限制，会将 *"第二次违规惩罚"*添加到 *"默认过期超时"*中，然后会将 *"第三次违规惩罚"*添加到默认超时，以此类推。惩罚的时间长度会依次叠加，直到*第四次违规惩罚*为止。

默认过期超时
这是一个 IP 地址或 IP 地址范围违反上述验证失败限制时，阻止其连接到 MDaemon 的时间。默认值为 1 天。

第二次违规惩罚
这是在 "动态屏蔽"第二次阻止一个 IP 地址或 IP 范围时被添加到*默认过期超时*的时长。

第三次违规惩罚
这是在 "动态屏蔽"第三次阻止一个 IP 地址或 IP 范围时被添加到*默认过期超时*的时长。

第四次违规惩罚
这是在 "动态屏蔽"第四次阻止一个 IP 地址或 IP 范围时被添加到*默认过期超时*的时长。

永久
如果您希望永久阻止违反身份验证失败限制的 IP 地址，而不是使用上方指定的违规惩罚临时阻止他们，请点击此框。

账户冻结选项

冻结验证失败 [xx]次的账户，时间范围是 [xx][分钟 |小时 |天]内
如果您希望当账户在指定的时间内未通过指定次数的验证尝试时将账户状态[598]切换成 "冻结"，请勾选此框。MDaemon 仍然接受冻结账户的入站邮件，但是没有人可以登录该账户发送或收集邮件，直到其 "解冻"（即账户状态被切换回启用）为止。默认情况下启用此项。

冻结账户超时
如果您启用了下面的选项 *"超时后自动解冻由动态屏蔽冻结的账户"*，这是账户被冻结的时间。

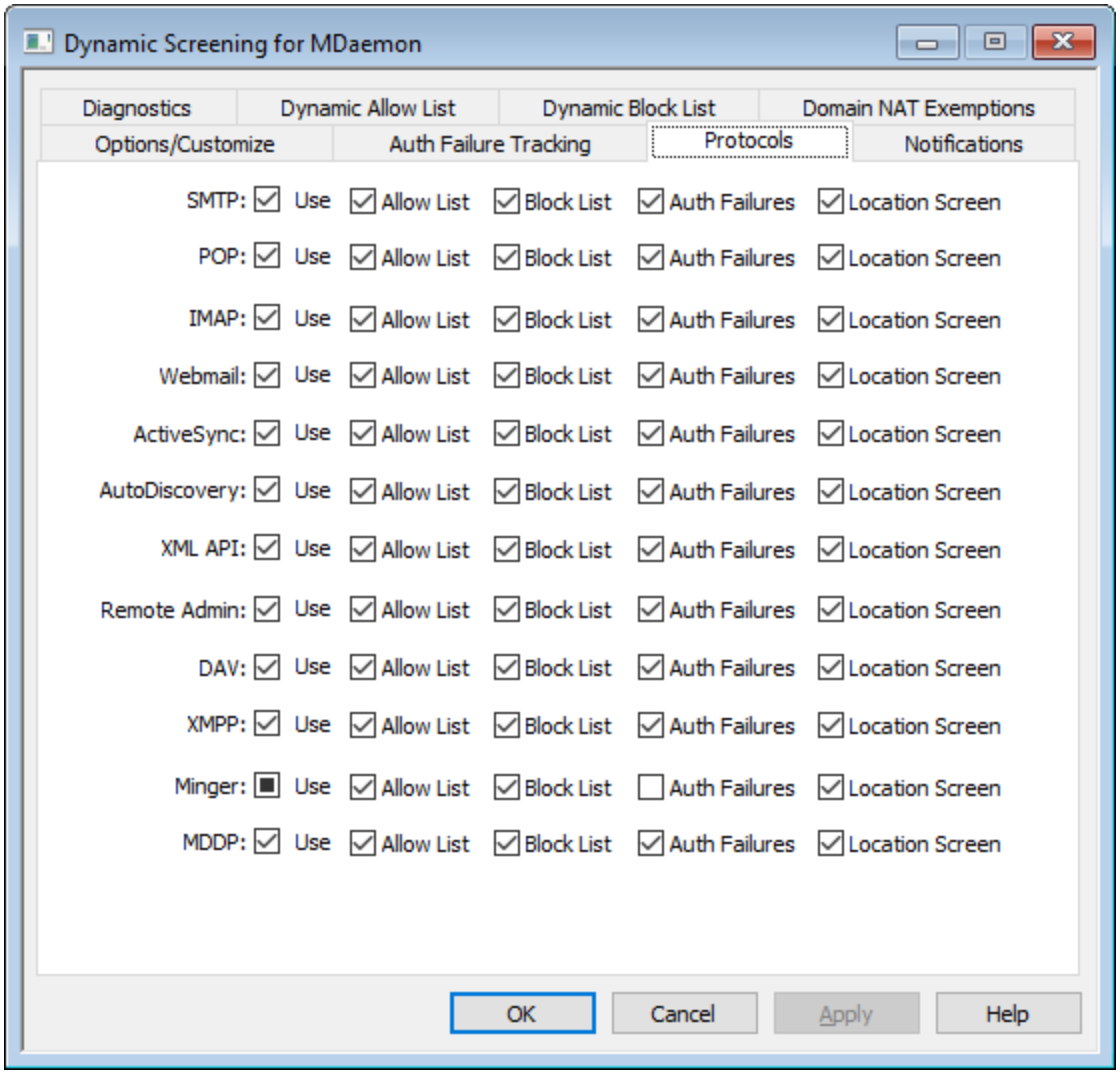
管理员可以在超时期限内通过回复通知邮件来解冻账户。
当账户被 "动态屏蔽"冻结时，默认情况下管理员会收到一封关于它的通知邮件。如果启用此项，管理员可以通过简单地回复电子邮件来 "解冻"账户（即将其状态切换回 "启用"）。默认情况下启用此项，并且需要启用通知[517]选项卡上的 "冻结账户报告"选项。

在超时后自动解冻由 "动态屏蔽"冻结的账户
如果您希望在 *"冻结账户超时"*时间过去后自动解冻被冻结的账户，请勾选此框。默认情况下，禁用该选项。

还请参阅：

选项/定制[510]
动态允许列表[522]
动态阻止列表[524]
通知[517]

4.2.3 协议

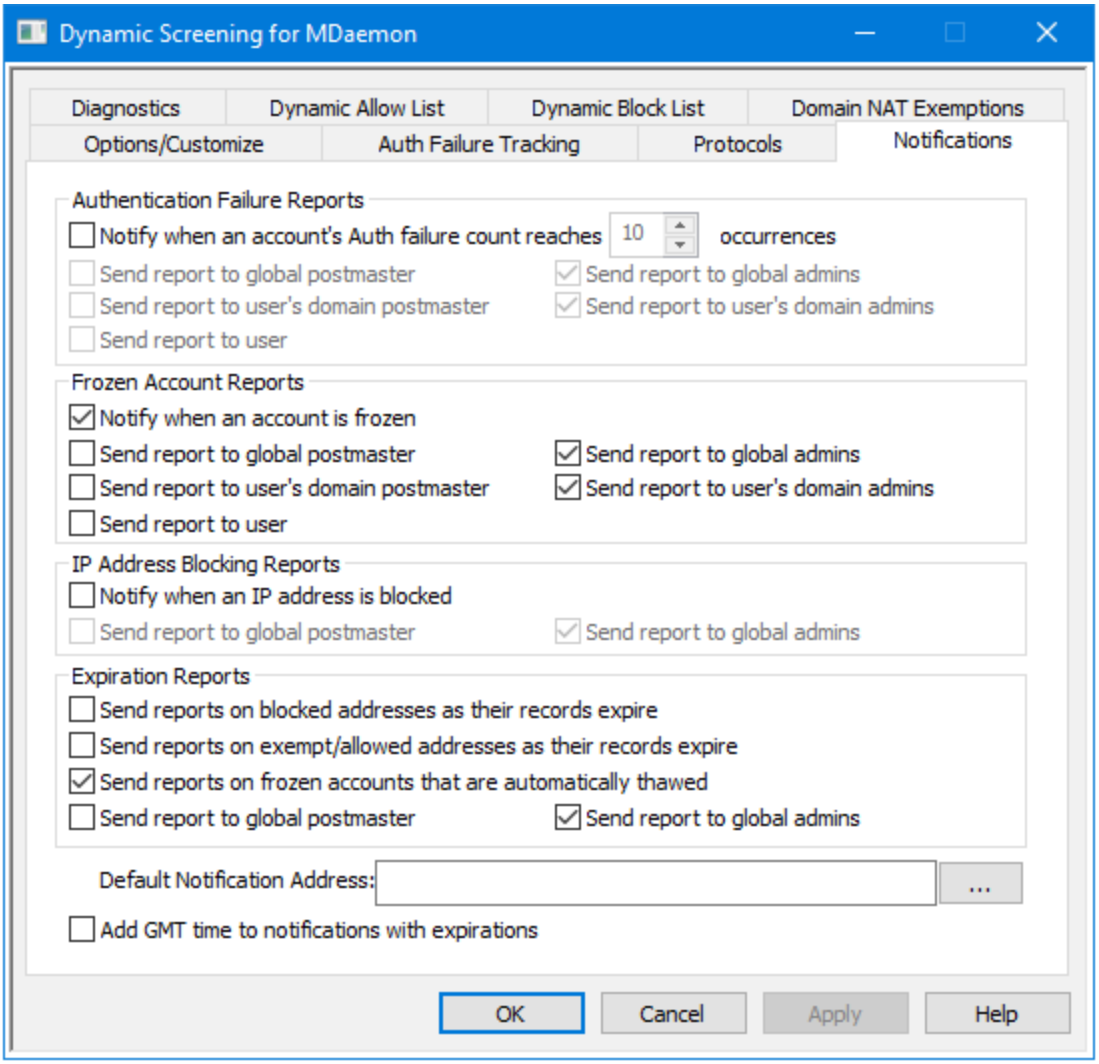


默认情况下，动态屏蔽服务应用于以下协议：SMTP、POP、IMAP、Webmail、ActiveSync、AutoDiscovery[62]、Management API 和 MDaemon Remote Administration。WebDAV 和 CalDAV、XMPP 和 Minger。使用 "协议"选项卡上的选项来确定哪些协议将对照 动态允许列表[522]和 动态阻止列表[524]检查其入站会话，哪些协议将使其验证失败被跟踪[513]，以及哪些将应用位置屏蔽[477]。默认情况下，除 了Minger验证失败以外，启用此对话框中的所有选项。

还请参阅：

验证失败跟踪[513]
动态允许列表[522]
动态阻止列表[524]

4.2.4 通知



验证失败报告

在账户的验证失败次数达到 [xx] 次数时发送通知
当一个账户达到指定次数的验证失败时，此选项会使 MDaemon 向邮件管理员或其他选定的收件人发送通知邮件。如果没有选定的地址可以解析，MDaemon 会将邮件发送至下方指定的 *"默认通知地址"*。如果没有指定地址，则不会发送邮件。该选项默认启用并被设置为 10 次

将报告发送至邮件管理员
如果您希望将报告发送至全局邮件管理员 699，请勾选此框。默认启用此项。

将报告发送至全局管理员
如果您希望将报告发送至全局管理员 636，请勾选此框。

将报告发送至用户的域邮件管理员
如果您希望在账户达到指定的失败验证尝试次数后，将报告发送至域邮件管理员[699]，请勾选此框。

将报告发送至用户的域管理员
如果您希望在账户达到指定的失败验证尝试次数后，将报告发送至域管理员[636]，请勾选此框。

向用户发送报告
如果您希望向账户无法进行身份验证的用户发送失败报告，请选中此框。

冻结账户报告

在账户被冻结时发送通知
当一个账户因为验证失败太多[513]被冻结时，此选项会使 MDaemon 向邮件管理员或其他选定的收件人发送通知邮件。如果没有选定的地址可以解析，MDaemon 会将邮件发送至下方指定的 "默认通知地址"。如果没有指定地址，则不会发送邮件。默认情况下，启用该选项。

将报告发送至邮件管理员
如果您希望将报告发送至全局邮件管理员[699]，请勾选此框。默认启用此项。

将报告发送至全局管理员
如果您希望将报告发送至全局管理员[636]，请勾选此框。

将报告发送至用户的域邮件管理员
如果您希望在账户被冻结后，将报告发送至域邮件管理员[699]，请勾选此框。

将报告发送至用户的域管理员
如果您希望在账户被冻结后，将报告发送至域管理员[636]，请勾选此框。

向用户发送报告
如果您希望将报告发送到已冻结的账户，请选中此框。

IP 地址阻止报告

在 IP 地址被阻止时接收通知
此项使 MDaemon 在 "动态屏蔽"系统阻止账户时，发送通知邮件给邮件管理员或其他选定的收件人。如果没有选定的地址可以解析，MDaemon 会将邮件发送至下方指定的 "默认通知地址"。如果没有指定地址，则不会发送邮件。默认情况下，启用该选项。

将报告发送至邮件管理员
如果您希望将报告发送至全局邮件管理员[699]，请勾选此框。默认启用此项。

将报告发送至全局管理员
如果您希望将报告发送至全局管理员[636]，请勾选此框。

过期报告

在受阻地址的记录过期时发送报告
每当被阻止的 IP 地址从 动态阻止列表 524 过期时，此项会将报告发送至指定的地址。默认情况下，启用该选项。

在豁免/允许地址的记录过期时发送报告
每当被允许的地址从 动态允许列表 522 过期时，此项会将报告发送至指定的地址。默认情况下，启用该选项。

发送有关冻结账户被自动解冻的报告
每当被冻结的账户自动解冻 513 (在*冻结账户超时*的时间过后)，此项会将报告发送至指定的地址。默认情况下，启用该选项。

将报告发送至邮件管理员
如果您希望将报告发送至全局邮件管理员 699，请勾选此框。默认启用此项。

将报告发送至全局管理员
如果您希望将报告发送至全局管理员 636，请勾选此框。

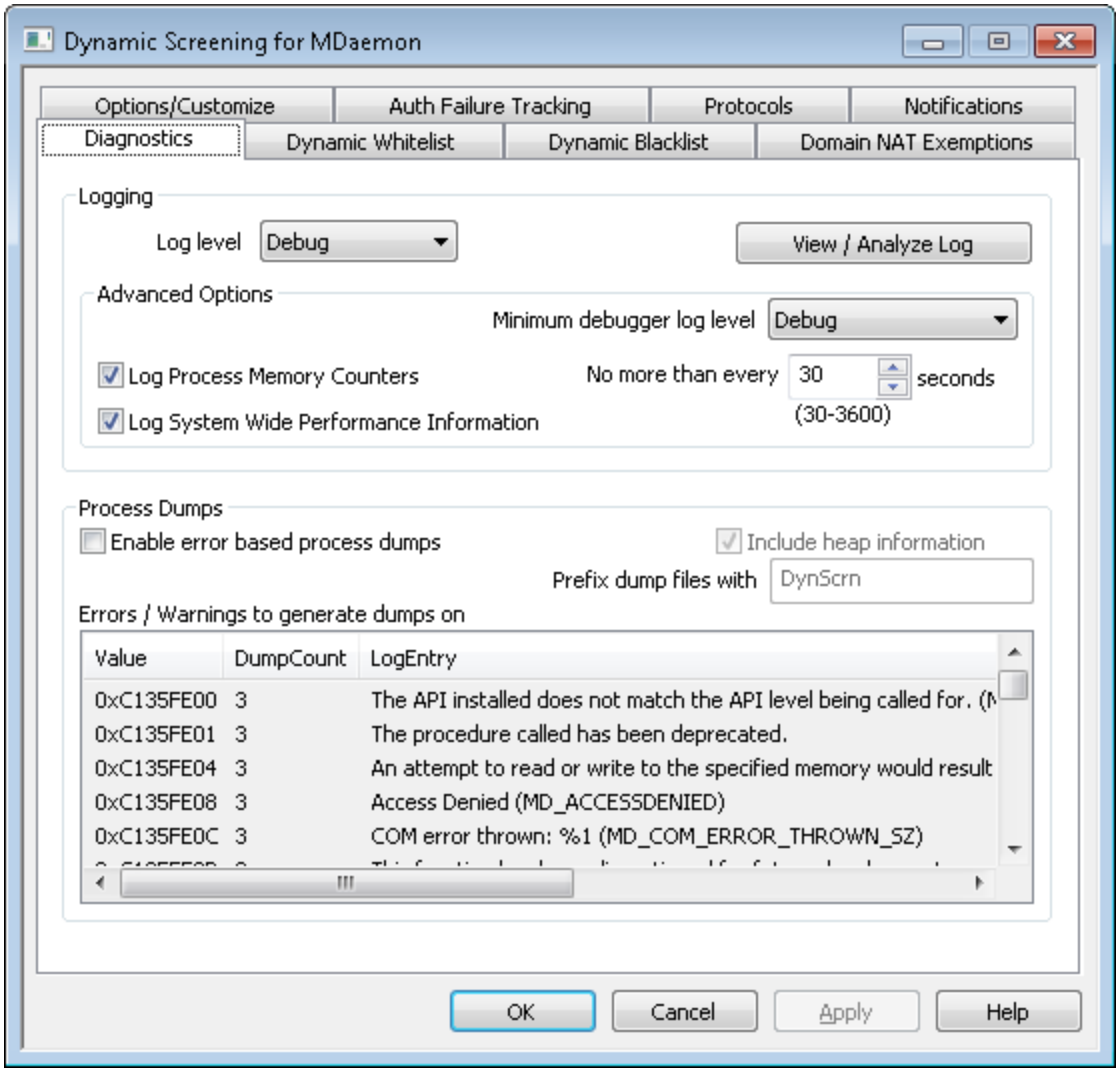
默认通知地址
没有指定其他地址或者没有指定地址可以解析时，这是通知报告将被发送到的地址。如果没有指定地址可以解析，而且未指定*默认通知地址*时，则不发送报告。

将 GMT 时间添加到含有过期的通知中
默认情况下，发送包含过期时间的通知报告时，列出的时间是本地服务器时间。如果您还希望包含 GMT 时间，请启用此选项。当您的电子邮件管理员位于其他时区时，这非常有用。

还请参阅：

选项/定制 510
验证失败跟踪 513

4.2.5 故障诊断



该屏幕包含高级选项，在大多数情况下，除非您尝试诊断 "动态屏蔽"问题或寻求技术支持，否则不需要使用这些选项。

日志

日志级别
支持 6 种日志级别，将按记录的数据量由高到低进行说明：

调试 这是最丰富的日志级别。记录所有可用条目，通常仅在诊断问题或管理员需要详细信息时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

查看/分析日志文件
点击此按钮来打开 MDaemon 高级系统日志查看器。默认情况下，将日志保存在："..\MDaemon\Logs\"

高级选项

最小化调试器日志级别
这是发送至调试器的日志最小级别。可用的日志级别与上述相同。

记录进程内存计数器
选中此框可将特定于进程的内存、句柄和线程信息记录到日志文件中。这对于发现潜在的故障和资源分配问题很有用。仅当数据自上次记录以来发生变更时，才会发出日志条目。

记录系统范围的性能信息
如果您希望将系统范围的性能信息记录到日志文件中，请选中此框。这对于发现潜在的故障和资源分配问题很有用。仅当数据自上次记录以来发生变更时，才会发出日志条目。

不大于每隔 [xx]秒
使用此选项可以设置对于进程和性能信息的记录频率的限制。

进程转储

启用基于进程转储的错误
如果您希望在发生您于下方指定的特定警告或错误时生成进程转储，请启用此项。

在转储中包含堆信息
默认情况下，在进程转储中包含堆信息。如果您不希望包含这个信息，请清除该复选框。

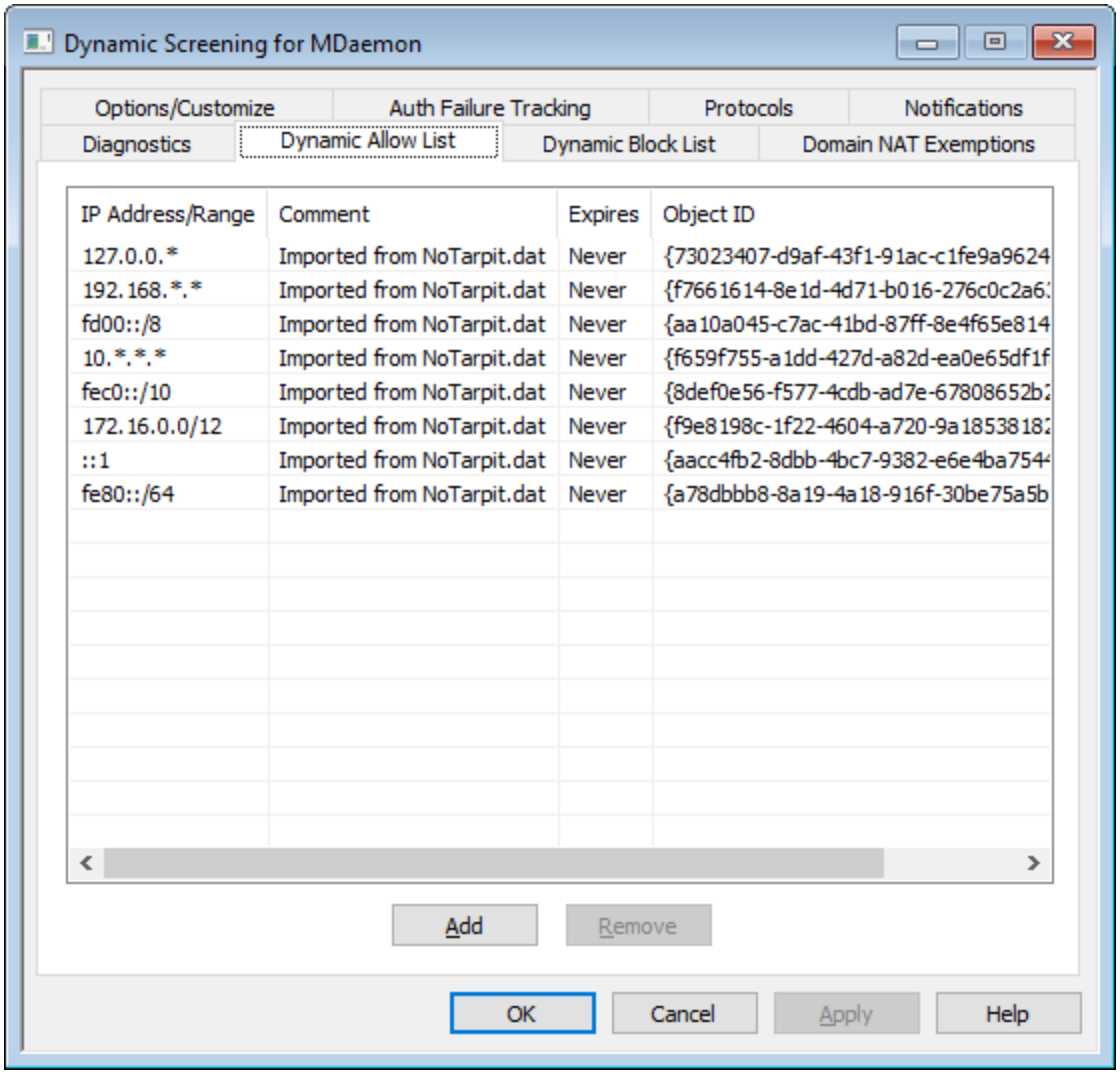
为转储文件使用前缀
进程转储文件名将使用这个文本开头。

出错/警告时生成转储
右键单击此区域并使用 *"添加/编辑/删除条目..."*选项来管理将触发进程转储的错误或警告列表。对于每个条目，您可以指定取消激活前进程转储数量。

还请参阅：

动态屏蔽 » 选项/自定义 510

4.2.6 动态允许列表



动态允许列表包含尝试连接到 MDaemon 时免于被“动态屏蔽”服务阻止的 IP 地址或地址范围列表。可以通过点击“添加”按钮将这些地址添加到“动态允许列表”中。每个条目都包含 IP 地址或范围，条目将过期的日期和时间（如果不会过期则为“从不”），您希望对条目做出的任何备注以及对象 ID。“动态允许列表”还适用于 SMTP 屏蔽 472、位置屏蔽 477 和缓送 503。

将 IP 地址或范围添加到“动态允许列表”

要将条目添加到列表：

1. 点击“添加”。这将打开“添加 IP 列表条目”对话框。

2. 输入 IP 地址或 IP 地址范围。
3. 选择您希望条目过期的日期和时间，或点击 "从不"。
4. 输入条目的备注（可选）。
5. 点击 "确定"。

删除列表中的条目

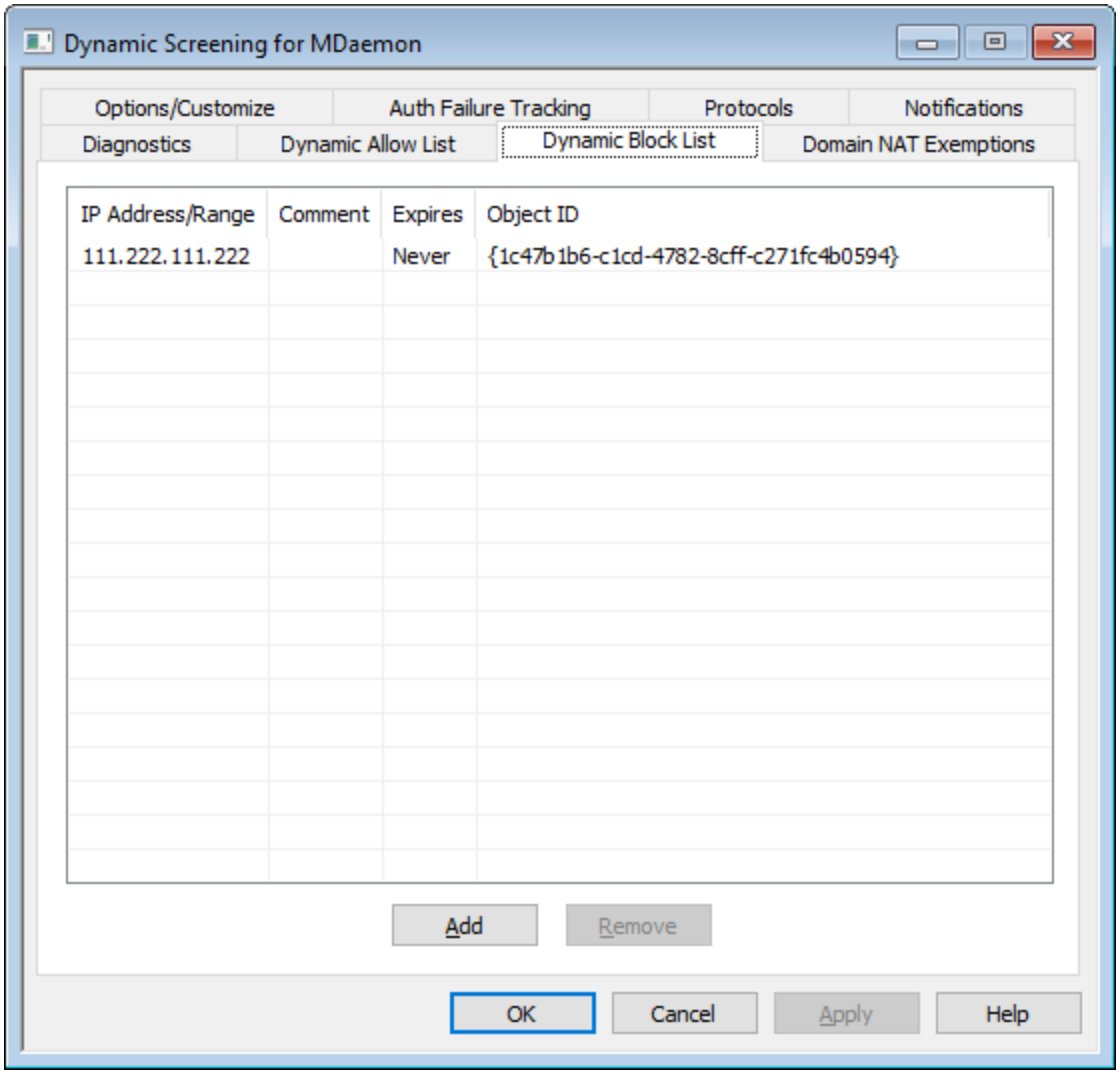
要从列表删除一个或多个条目：

1. 选择您希望从列表删除的一个或多个条目（Ctrl+click 来选择多个条目）。
2. 点击 "删除"。

还请参阅：

选项/定制 510
验证失败跟踪 513
动态阻止列表 524
协议 516

4.2.7 动态阻止列表



"动态阻止列表"包含尝试连接到 MDaemon 时被"动态屏蔽"服务阻止的 IP 地址或地址范围列表。可以由验证失败跟踪[513]和 SMTP 屏蔽[472]选项自动添加这些地址，也可以通过点击"添加"按钮手动添加。每个条目都包含 IP 地址或范围，条目将过期的日期和时间（如果不会过期则为"从不"），您希望对条目做出的任何备注以及对象 ID。

1. 点击"添加"。这将打开"添加 IP 列表条目"对话框。

2. 输入 IP 地址或 IP 地址范围。
3. 选择您希望条目过期的日期和时间，或点击 "从不"。
4. 输入条目的备注（可选）。
5. 点击 "确定"。

删除列表中的条目

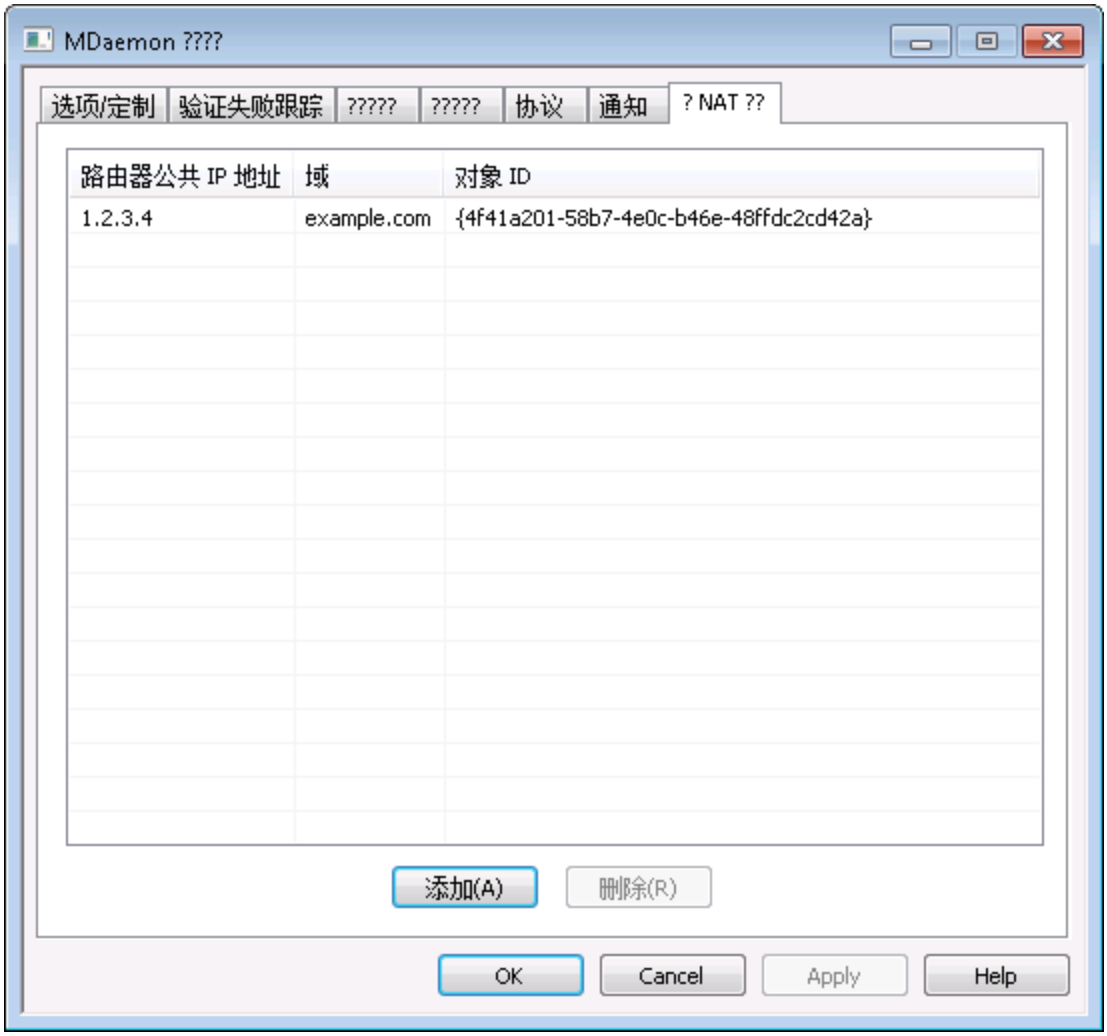
要从列表删除一个或多个条目：

1. 选择您希望从列表删除的一个或多个条目（Ctrl+click 来选择多个条目）。
2. 点击 "删除"。

还请参阅：

选项/定制 510
验证失败跟踪 513
动态允许列表 522
协议 516

4.2.8 域 NAT 豁免



当您激活 *"启用高级用户界面功能"*选项（位于 "动态屏蔽"的 "选项/定制[510]"屏幕）时，将提供此屏幕。

使用此功能可容纳驻留在同一外部局域网（LAN）上的一组 MDaemon 用户，该用户使用网络地址转换（NAT），为所有用户提供一个共享的公共 IP 地址。通过添加其 LAN 的公共 IP 地址和账户所属的 MDaemon 域，当一个或多个用户由于密码错误而导致身份验证失败时，可以防止动态屏蔽阻止 IP 地址。如果没有此功能，具有配置错误的邮件客户端的有效用户可能会导致 LAN 的 IP 地址被阻止，从而阻止所有用户访问其邮件。例如，当用户的密码发生变化，但用户忘记使用新密码更新邮件客户端时，可能会发生这种情况。

此处列出的 IP 地址仍可能由于其他原因而被阻止，例如尝试登录无效账户的机器人，尝试登录到与该 IP 地址关联的不同 MDaemon 域的配置错误的客户端等等。如果您希望从 "动态屏蔽"中完全排除 IP 地址，请使用动态允许列表[522]。

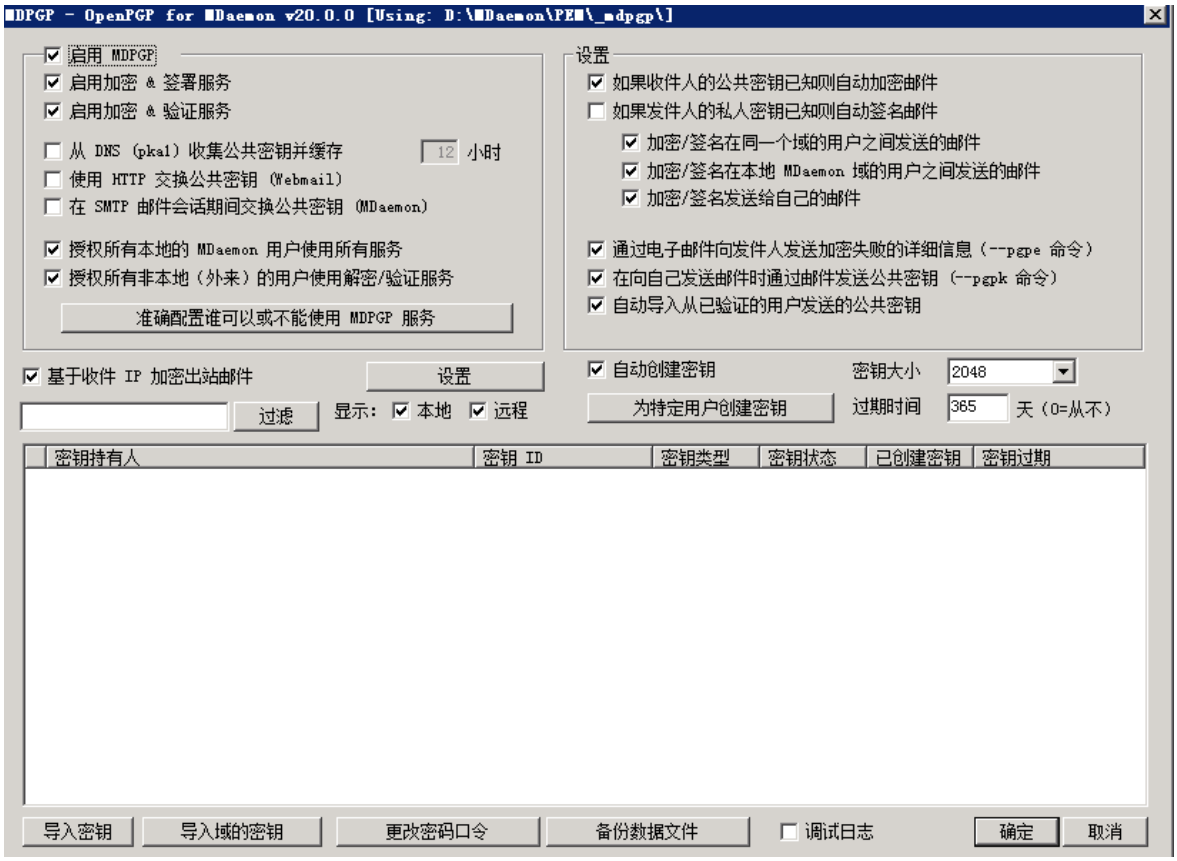
添加域 NAT 豁免

点击 **添加**，输入外部 LAN 的 *"路由公共 IP 地址"*，并选择从该 IP 进行登录的 MDaemon *域*。然后点击 **确定**"。

还请参阅：

选项/定制 510

4.3 MDPGP



OpenPGP 是用来交换加密数据的业内标准协议，提供各种面向邮件客户端的 OpenPGP 插件，帮助用户收发加密邮件。MDPGP 是 MDaemon 的集成式 OpenPGP 组件，可以为您的用户提供加密、解密和基本的密钥管理服务，而且无需他们使用邮件客户端插件。

MDPGP 使用公共-密钥/私人-密钥系统来加密和解密电子邮件。要实现这点，在您希望使用 MDPGP 来向某人发送安全的私人邮件时，MDPGP 将使用您以前从那人 (例如他的 "公共密钥")获取并导入 MDPGP 的 "密钥"来加密邮件。反之亦然，如果他希望向您发送私人邮件，他必须使用从您那儿获取的公共密钥来加密这封邮件。向发件人提供您的公共密钥十分必要，因为没有这个密钥的话，他不能向您发送 OpenPGP 加密的邮件。必须使用您唯一的公共密钥来加密邮件，因为您唯一的私人密钥是 MDPGP 用来在邮件抵达时解密的。

为了让 MDPGP 管理邮件签名、邮件加密和解密，它维护两个密钥存储 (例如密钥环)——分别用于公共密钥和私人密钥。MDPGP 可以自动生成用户需要的密钥，您也可以为特定用户

手动创建它们。您还可以导入在其他位置创建的密钥。此外 MDaemon 可以查询附加至来自本地用户已验证邮件的公共密钥，并自动导入这些密钥。这样用户便能请求来自某人的公共密钥，然后通过电子邮件将密钥发送给自己，MDPGP 将对此进行检测并将其导入公共密钥环。MDPGP 从不存储相同密钥的多个副本，不过一个地址会有多个不同的密钥。最后，每当一封邮件抵达在密钥环中存在密钥的地址，MDPGP 将根据您的设置按需签名、加密或解密这封邮件。如果一个地址有多个密钥，MDPGP 将使用您指定成首选的密钥来加密这封邮件。如果未指定首选的密钥，MDPGP 将使用第一个密钥。在解密一封邮件时，MDaemon 将尝试每一个密钥。

您可以配置 MDPGP 的签名和加密服务自动或手动运行。在设置成自动运行时，MDPGP 将在可能时自动签名和加密邮件。在设置成手动运行时，MDPGP 将仅在发件用户将特殊命令插入邮件的 "主题"时签名或加密邮件。无论是何种情况 只在账户被授权使用这些服务时签名或加密 (或解密)这些邮件。

OpenPGP 规范概述位于 RFCs 4880 和 3156.

启用 MDPGP

启用 MDPGP

默认情况下启用 MDPGP，不过只有在您创建了密钥，或将密钥导入密钥环，或使用了下方的选项来设置 MDPGP *自动创建密钥*时，MDPGP 才会签名、加密或解密任何邮件。

启用加密和签名服务

在启用 MDPGP 时，默认当所需密钥位于密钥环时可以签名和加密邮件。如果您不希望允许 MDPGP 签名或加密邮件，请禁用此项。

可以在不加密的情况下签名邮件，不过将始终签名由 MDPGP 加密的任何邮件。

启用解密和验证服务

默认情况下，如果已知收件人的私人密钥，将解密入站的加密邮件。此外 MDPGP 也将验证未加密邮件中的内嵌签名。注意：必须授权收件人和发件人使用解密和验证服务 ，可以通过下方的 *"授权所有人..."*选项或 *"配置谁..."*选项来实现这点 (默认情况下授权每个人)。如果您不希望验证内嵌的签名或允许 MDPGP 解密任何邮件，例如您希望您的所有用户通过邮件客户端插件处理其自己的解密，请禁用此项。禁用时，将照常处理任何加密的入站邮件，并将其放入收件人的邮箱。

收集 DNS (pka1)中的公共密钥并缓存 [xx]小时

如果您希望 MDPGP 通过使用 PKA1 的 DNS 来查询邮件收件人公共密钥，请启用此项。这非常有用，因为它自动处理获取一些收件人的公共密钥 ，防止您或您的用户为了发送加密邮件而不得不手动获取和导入这些密钥。在进行 PKA1 查询时，将立即收集和验证找到的任何密钥 URI，并将其添加到密钥环。将在名为 `fetchedkeys.txt` 的文件中跟踪使用上述方式成功收集和导入密钥环的密钥，而且在达到此项中指定的小时数后，或按照引用它们的 PKA1 记录的 TTL 值 (这些值更大)来自动过期这些密钥。因此在此处指定的值是密钥将被缓存的时长最小值。默认值是 12 小时，允许的最小值是 1 小时。

如果您希望将自己的公共密钥发布到 DNS，您必须创建专用的 TXT 记录。例如，用户 frank@example.com 使用以下密钥-id：0A2B3C4D5E6F7G8H，在用于域 "example.com"的 DNS 中，您将创建一个 TXT 记录 "frank._pka.example.com"(替换邮件地址中的 @ 的是 "._pka."字符串)。TXT 记录的数据格式如下："v=pka1; fpr=<key's full fingerprint>; uri=<Webmail-URL>/WorldClient.dll?view=mdpgp&k=0A2B3C4D5E6F7G8H"，其中 <key's full fingerprint> 是密钥的完整指纹 (40 字符长度，表示完整的 20 字节指纹值)。您可以通过在 MDPGP GUI 中双击这个密钥来查看其完整的指纹值。

使用 HTTP 处理公共密钥 (Webmail)
如果您希望将 Webmail 用作基本的公共密钥服务器，请启用此项；Webmail 将准许您用户的公共密钥的请求。创建请求的 URL 格式如下所示："http://<Webmail-URL>/WorldClient.dll?View=MDPGP&k=<Key-ID>"。其中 <Webmail-URL> 是转至您 Webmail 服务器的路径 (例如 "http://wc.example.com")，<Key-ID> 是您所需密钥的长度为 16 个字符的密钥 id (例如 "0A1B3C4D5E6F7G8H")。密钥 id 由密钥指纹的最后 8 个字节构成 - 总共 16 个字符。

在 SMTP 邮件会话期间处理公共密钥 (MDaemon)
如果您希望启用公钥自动传输作为 SMTP 邮件投递过程的一部分，请选中此框。为此，MDaemon 的 SMTP 服务器将准许名为 RKEY 的 SMTP 命令。将电子邮件发送到支持 RKEY 的服务器时，MDaemon 将提供发送者当前首选的公钥发送给其他主机。该主机将响应，表明它已经拥有该密钥 ("250 2.7.0密钥已知")或者需要该密钥，在这种情况下密钥立即以 ASCII 形式传输 ("354 Enter"键，以 CRLF.CRLF"结尾)就像电子邮件。不会传输过期或撤销的密钥。如果 MDaemon 有多个发件人的密钥，它始终会发送当前标记为首选的密钥。如果没有首选密钥，则发送找到的第一个密钥。如果无有效密钥则不进行任何操作。只提供属于本地用户的公共密钥。

公共密钥传输是作为投递用户邮件的 SMTP 邮件会话的一部分发生的。为了接受以这种方式传输的公共密钥，它必须和由密钥持有者属于的域进行 DKIM 签名 445 的邮件一起发送，其中将 i= 设置成密钥持有者的地址，而且必须准确匹配 唯一的发件人报头地址。"密钥持有者"取自密钥本身。此外，该邮件必须从发件人的 SPF 地址 440 中的主机抵达。最后，通过向 MDPGP 规则文件添加一个适当的条目 (说明在这个规则文件中)，必须为 RKEY 授权密钥持有者 (或其整个域，通过使用通配符)，指示该域可以被信任用于密钥交换。上述检查都将为您自动完成，不过您必须启用 DKIM 442 和 SPF 验证 440，否则无法有效完成这些步骤。

MDPGP 日志显示导入或删除的所有密钥的结果和详细信息，SMTP 会话日志也跟踪此活动。该进程跟踪现有密钥的删除和新的首选密钥的选定，并在这些事件发生变化时更新其发送邮件的所有服务器。

授权所有本地 MDaemon 用户使用所有服务
默认情况下，授权所有本地 MDaemon 用户账户使用您已启用的任何 MDPGP 服务：签名、加密、解密和验证。如果您希望允许特定的用户使用其中一种服务或更多服务，您可以使用下方的 *"精确配置谁能及不能使用 MDPGP 服务"*这个选项来排除他们。如果您仅希望授权特定的本地用户，请禁用此项。在那种情况下，请使用下方的 *"精确配置谁能及不能使用 MDPGP 服务"*这个选项来为您选择的人授予访问权限。

授权所有非本地 (外来)用户使用解密/验证服务
默认情况下，如果 MDPGP 知道本地收件人的私人密钥，可以解密从非本地发件人发往本地收件人的任何入站加密邮件。类似的，MDPGP 将验证来自非本地用户的入站邮件中的内嵌签名。如果存在您不希望对其邮件进行解密或验证的非本地发件人，您可以使用下方的*"精确配置谁能及不能使用 MDPGP 服务"*这个选项来为发件人限制这些服务。如果在发件人是非本地地址时，您不希望解密邮件或验证内嵌签名，请禁用此项。在那种情况下，您仍然可以使用下方的*"精确配置谁能及不能使用 MDPGP 服务"*这个选项来指定限制例外。

精确配置谁能及不能使用 MDPGP 服务
点击此按钮来打开 "rules.txt"文件，用于为 MDPGP 配置用户权限。使用此文件，您可以指定允许谁来签名邮件、加密邮件和解密邮件。您还可以专门限制用户使用这些选项。例如您可以使用 "+*@example.com"规则来允许所有 example.com 用户解密邮件，不过可以通过专门添加 "-frank@example.com"来禁止 frank@example.com 这么做。请参阅 rules.txt 文件顶部的文本来获得示例和指示说明。

Rules.txt备注和语法

- 只有来自 MDaemon 服务器用户经过验证的 SMTP 邮件有资格进行加密服务。不过您可以指定希望限制加密服务的非本地地址，这就意味着 MDPGP 就算知道其公共密钥也**不会**加密邮件。
- 如果 rules.txt 和*"授权所有本地 MDaemon 用户使用所有服务"*全局选项发生冲突，将使用 rules.txt 设置。
- 如果 rules.txt 和*"授权所有非本地 (外来)用户使用解密/验证服务"*全局选项发生冲突，将使用 rules.txt 设置。
- 忽略行上 # 后的文本。
- 在同一行使用空格分隔多个邮件地址。
- 允许在电子邮件中使用通配符 (* 和 ?)。
- 即使**始终**签名 MDPGP 加密邮件，向用户授予加密权限也不会向这名用户授予签名未加密邮件的权限。要签名未加密的邮件，必须授予这名账户签名权限。
- 每个电子邮件地址必须使用以下标签作为前缀：

+ (加号) - 地址可以使用 MDPGP 加密服务。

- (减号) - 地址**不能**使用 MDPGP 加密服务。

! (感叹号) - 地址可以使用 MDPGP 解密服务。

~ (浪号) - 地址**不能**使用 MDPGP 解密服务。

^ (插入号) - 地址可以使用 MDPGP 签名服务。

= (等号) - 地址**不能**使用 MDPGP 签名服务。

$ (美元)- 地址可以使用 MDPGP 验证服务。

& (和号) - 地址**不能**使用 MDPGP 验证服务。

示例：

+*@* — 所有域的所有用户可以加密。

!*@* — 所有域的所有用户可以解密。

^*@* — 所有域的所有用户可以签名。

^*@example.com — example.com 的所有用户可以签名。

+frank@example.com ~frank@example.com — 用户可以加密但是不能解密。

+GROUP:EncryptingUsers — MDaemon EncryptingUsers 群组的成员可以加密

^GROUP:Signers — MDaemon Signers 群组的成员可以签名

加密/签名模式

自动模式

使用 "设置"选项来配置 MDPGP 自动为所有被许可的账户签名和加密邮件。在账户发送已验证的邮件，而且 MDPGP 知道所需密钥时，将按照下方设置签名或加密邮件。

在下方 "手动模式"中所述的专用 "主题"代码的优先级始终高于 "自动模式"选项。因此如果禁用了其中一个选项，被许可签名或加密邮件的账户仍能使用代码手动签名或加密邮件。

设置

如果已知收件人的公共密钥则自动加密邮件
默认情况下，如果允许账户加密邮件，而且已知收件人的公共密钥，MDPGP 将自动为其加密。如果您不希望自动为其加密请禁用此项；可以使用在下方 "手动模式"中概述的专用代码手动加密邮件。

如果已知发件人的私人密钥则自动签名邮件
如果您希望在已知发件人账户的私人密钥的情况下，而且允许该账户签署邮件时，希望 MDPGP 自动签署邮件，请点击此项。即使禁用了此项，仍然可以使用下方 "手动模式"这一部分中概述的特殊代码来手动签署邮件。

加密/签名同一个域中用户间的邮件
将 MDPGP 设置成自动加密或签名邮件时，即使邮件发自同一个域中的用户之间，只要已知所需密钥，此项仍能使 MDPGP 这么做。默认情况下启用此项。

加密/签名本地 MDaemon 域中用户间的邮件
将 MDPGP 设置成自动加密或签名邮件时，即使邮件发自本地 MDaemon 域中的用户之间，只要已知所需密钥，此项仍能使 MDPGP 这么做。例如，如果您的 MDaemon 域包含 "example.com"和 "example.net"，将自动加密或签名发自这些域的用户之间的邮件。默认情况下，启用该选项。

加密/签名发给自己的邮件
在将 MDPGP 设置成自动加密或签名邮件时，即使账户正在将邮件发给自己(例如从 frank@example.com 发送至 frank@example.com)，此项也能使 MDPGP 这么做。如果账户有权使用加密和解密，那么将能有效使 MDPGP 接受邮件，对其加密，然后立即对其解密，并将该邮件放入同一名用户的邮箱。不过如果没有为账户配置解密，便会使邮件被加密，并将其以加密状态放入同一名用户的邮箱。默认情况下启用此项。

手动模式

如果您禁用了上述的 *"自动签名邮件..."*和 *"自动加密邮件..."*选项，您正在以 "手动模式"使用 MDPGP。MDPGP 不会签名或加密任何邮件，除非邮件经过验证，而且在其 "主题"报头中存在以下代码之一：

--pgps 可能时签名这封邮件。可以将代码放在 "主题"的开头或结尾。

--pgpe 可能时加密这封邮件。可以将代码放在 "主题"的开头或结尾。

--pgpx 邮件**必须**进行加密。如果它不能进行加密（例如未知收件人的密钥），那么就不投递这封邮件，会将该邮件退回发件人。可以将代码放在 "主题"的开头或结尾。

--pgpk 向我发送公共密钥。用户将此代码放在 "主题"的开头并将该邮件发送给自己。然后 MDPGP 会通过电子邮件向用户发送他的公共密钥。

--pgpk<Email> 向我发送这个地址的公共密钥。用户将此代码放在 "主题"的开头并将该邮件发送给自己。然后 MDPGP 会通过电子邮件向用户发送这个地址的公共密钥。

示例：

主题：--pgpk<frank@example.com>

密钥管理

使用在 MDPGP 对话框下半部分的选项来管理公共和私人密钥。每个密钥都有一个条目，您可以右键点击任何条目来导出密钥，对其进行删除，启用/禁用操作，将其设置成 "首选密钥"（请参阅上方的 *"在 SMTP 邮件会话期间处理公共密钥"*），或将其设置成域的密钥（见下方）。在您点击 "**导出密钥**"时，会将其保存到\MDaemon\Pem_mdpgp\exports\ 文件夹，而且您可以有选择性地通过电子邮件将公共密钥发送到一个邮件地址。提供 "显示本地/远程"和 "过滤器"选项来帮助您定位特定的地址或群组。

使用域密钥

（可选）您可以使用单个密钥对发往特定域的所有邮件进行加密，而不考虑发件人。例如，如果您的域之一和托管在其他地方的域希望对它们之间发送的所有电子邮件进行加密，但是他们不希望为域中的每个用户账户设置和管理单独的加密密钥，则此功能很有用。有多种方式来实现这个目的：

- 如果您已经拥有另一个域的公共密钥，并且希望使用该密钥对指向该域的所有出站邮件进行加密，请右键单击该密钥，然后点击 "**设置成域的密钥**"。然后输入域名并点击 "**确定**"。这将创建一个 "内容过滤器"规则，以导致所有指向该域的邮件 "收件人："使用指定的密钥进行加密。
- 如果已经向您提供了域的公共密钥，但尚未在列表中，请点击 "**导入域的密钥**"，输入域名并点击 "确定"，然后导航至该域的 public.asc 文件并点击 "**打开**"。这还将创建 "内容过滤器"规则，用来加密指向该域的这些邮件。
- 根据需要自定义 "内容过滤器"规则，以准确修改在发送到域之前已加密的邮件。

- 要为您的一个域创建一个新密钥，并分配给另一个域来加密发送给您的邮件，请按照说明进行操作，这些说明位于下方的*"为特定用户创建密钥"*这个选项之下，请从列表中选择"_Domain Key (domain.tld)_ <anybody@domain.tld>"。

不使用密钥来加密您也具有相应私人密钥的出站邮件。如果这样做，MDPGP 将加密邮件，然后立即看到解密密钥是已知的，并立即解密该相同的邮件。

通过电子邮件向发件人发送加密失败的详细信息（-pgpe 命令）
在用户使用 --pgpe 命令来发送加密邮件并遇到加密失败的情况时（例如失败原因是未找到加密密钥），此项会通过电子邮件将失败通知发送给发件人。默认情况下禁用此项，这意味着不发送失败通知邮件。

当邮件发给自己时通过邮件发送公共密钥 (--pgpk command)
当用户向自己发送邮件时，使用"--pgpk<email address>"作为主题（例如 --pgpk<frank@example.com>）。如果存在用于<电子邮件地址>的公共密钥，则会通过电子邮件发送回请求者。

自动导入发自己验证用户的公共密钥
默认情况下，在已验证的用户发送的邮件中附加了 ASCII 格式的公共密钥时，MDPGP 会将这个密钥导入密钥环。这是一种供用户将联系人的公共密钥导入 MDPGP 的简单方式，通过将公共密钥作为邮件附件发送给自己来实现。如果您不希望自动导入公共密钥，请禁用此项。

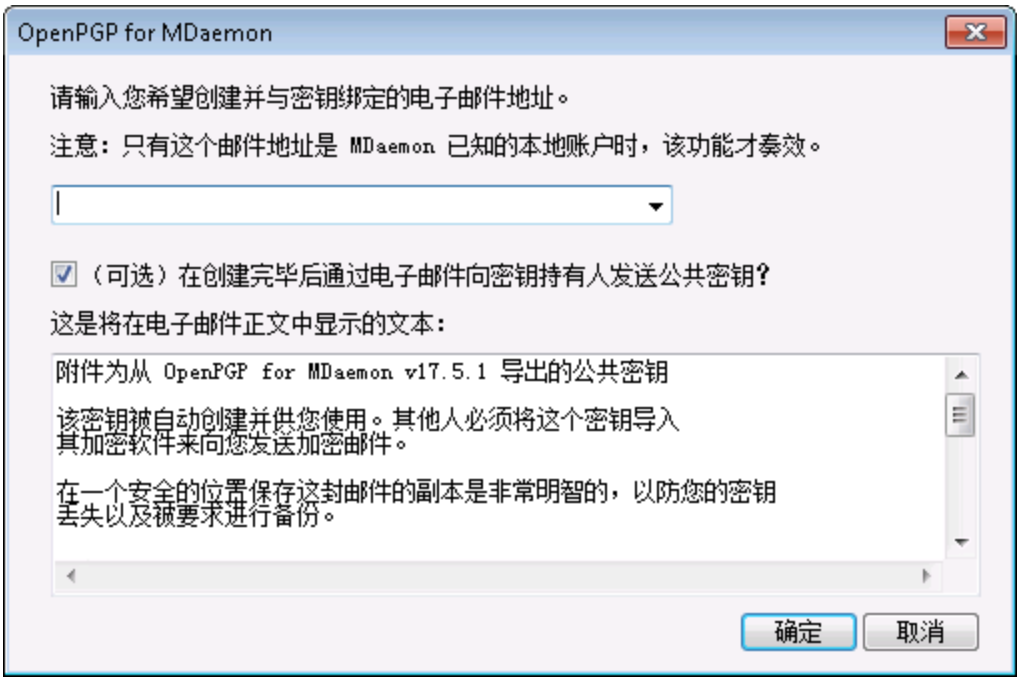
自动创建密钥
如果您希望 MDPGP 自动为每个 MDaemon 用户创建公共/私人密钥对，请启用此项。MDPGP 不是一次全部生成，而是随时间进行创建，在下一次为该用户处理一封邮件时创建各个用户的密钥对。默认情况下禁用此项来节约资源，并避免为从不使用 MDPGP 的账户生成密钥。

密钥大小
使用此项来为 MDPGP 生成的密钥指定其大小。您可以将密钥大小设置成 1024、2048 或 4096。默认设置是 2048 位密钥。

在 [xx] 天后过期（0=从不）
使用此项来指定由 MDPGP 生成的密钥自创建之日起，在过期前有几天有效时间。如果您不希望密钥过期，则将此项设置成"0"。默认设置是 0。

为特定用户创建密钥
要为账户手动生成密钥对：

1. 点击**"为特定用户创建密钥"**。
2. 从下拉列表选择账户。如果您希望创建一个密钥以应用于域的所有账户，请选择列表中的"_Domain Key (domain.tld)_ <anybody@domain.tld>"选项。
3. **可选：**如果您希望将密钥作为邮件附件发送给用户，请勾选**"通过电子邮件将密钥发送给密钥拥有者..."**。
4. 点击**"确定"**。



基于收件 IP 加密出站邮件
如果您希望使用特定的加密密钥来加密指向特定 IP 地址的所有邮件，请启用此项并点击 **"设置"**来打开 "MDaemon 邮件传输加密"文件，您可以在其中列出 IP 地址和关联的密钥 ID。将邮件投递到所列 IP 的任何出站 SMTP 会话都将在投递之前，使用关联的密钥对邮件进行加密。如果邮件已被其他密钥加密，则将跳过此步骤。

导入密钥
如果您希望将密钥文件手动导入 MDPGP，请点击这个按钮，找到密钥文件并点击 **"打开"**。在导入私人密钥文件时，您无需导入相应的公共密钥，因为它已被包含在私人密钥中。如果您正在导入受密码口令保护的私人密钥，MDPGP 将提示您输入这个密钥口令。如果没有密钥口令，您便不能导入这个私人密钥。导入了私人密钥后，MDaemon 会将密钥的密码口令更改成 MDPGP 当前正在使用的密码口令。

导入域的密钥
如果提供了公共加密密钥来加密发送到某个域的所有邮件，请点击此按钮，输入域名，然后点击 **"确定"**，导航到域的 public.asc 文件并点击 **"打开"**。这会将域的公共密钥添加到列表中，并创建 "内容过滤器"规则来对该域的所有出站邮件进行加密，而不考虑发件人。

更改密码口令
私人密钥始终受密码口令保护 在您尝试导入一个私人密钥时，您必须输入其密码口令。在导出私人密钥时，导出的密钥仍然受到密码口令的保护，而且没有密码口令的话便无法使用或导入到其他位置。MDPGP 默认的密码口令是 **MDaemon**。出于安全原因，您应该在使用 MDPGP 后更改这个密码口令，因为直到您这么做之后，创建或成功导入 MDPGP 的各个密钥才会将其密码口令设置（或更改成）**MDaemon**。您可以通过点击 MDPGP 屏幕上的 **"更改密码口令"**来随时更改密码口令。在您更改密码口令时，会将密钥环上的各个私人密钥更新成新的密码口令。

备份数据文件
点击这个按钮来备份您当前的 Keyring.private 和 Keyring.public 密钥环文件。默认情况下，会将备份文件复制到："\MDaemon\Pem_mdpgp\backups"，并在文件名后附加日期和 .bak 扩展名。

- 不加密转发的邮件。
- 不加密自动应答邮件。
- 不支持密钥服务器和密钥撤销，就如上方的 *"收集 DNS (pka1) 中的公共密钥并缓存 [xx] 小时"*和 *"通过 HTTP 发送公共密钥 (Webmail)"*这两个选项所述。
- "内容过滤器"的加密操作不对已加密的邮件执行操作，而且其加密和解密操作受到所有 MDPGP 配置要求的限制。
- 默认情况下这个显示 MDaemon 账户的下拉列表显示前 500 个账户。您可以设置 MaxUsersShown=0 (位于plugins.dat)来查看所有账户。这可能花费更长时间来加载较大的用户列表。
- MDPGPUtil.exe 这款工具可以通过命令行选项来加密和解密。在无参数的情况下从命令行外壳运行 MDPGPUtil来获得帮助。

4.4 爆发保护

爆发保护是 MDaemon AntiVirus 558 功能的可选部分。初次启用 MDaemon AntiVirus 将开始 30 天试用。如果您希望购买此功能，请联系您的授权 MDaemon 经销商或访问：www.mdaemon.com。

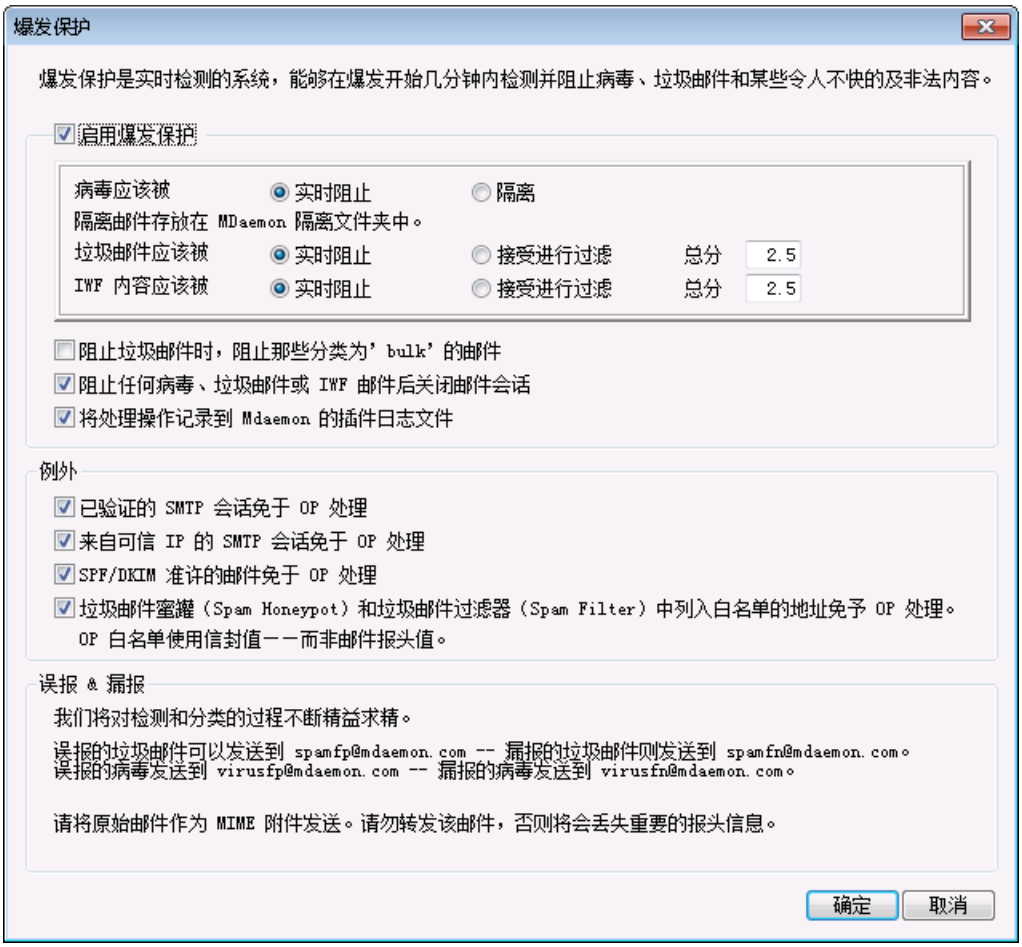
爆发保护 (OP) 可以从 MDaemon 的"安全"菜单（"安全»爆发保护..."或"Ctrl+Shift+1"）访问。它是一种革命性的实时反垃圾邮件、反病毒和反网络钓鱼的技术，能够在爆发发生后的数分钟内前瞻性地自动保护 MDaemon 邮件架构。

"爆发保护"是完全的内容不可知保护，这意味着它不依赖于严格的邮件内容词法分析。因此不需要任何启发式规则、内容过滤或签名更新。此外，这表示它不会被附加的种子文件、"聪明"的拼写更改、社会工程策略、语言障碍或不同的编码技术所欺骗。取而代之的，OP 基于 的循环模式检测和零时技术创建而成。它依据对于邮件结构和通过 SMTP 邮件分发特征的数学分析——分析与邮件传输相关联的"模式"，并从全世界收集的具有类似模式的数千万邮件中抽样与之进行比较，抽样和比较都是实时进行的。**请注意：**OP 从不传输邮件的实际内容，也不从提取的模式中推导邮件内容。

由于邮件是在全球范围内进行实时分析，因此在新爆发发生的数分钟——往往是数秒钟内即可提供保护。对于病毒来说，这种级别上的保护非常重要，因为病毒爆发后，传统的防病毒开发者通常需要数小时才能验证并提交病毒签名更新，这样将更新用于产品使用所需的时间则更长。在此期间，不带爆发保护的服务器容易遭受这种特定爆发的攻击。同样，对

于垃圾邮件，在其没有被传统的基于启发式和内容的系统识别出来之前，爆发保护将经常花大量时间和精力分析这些垃圾邮件并创建安全的过滤规则。

不过值得注意的是，"爆发保护"功能并不能取代传统的反病毒、反垃圾邮件和反网络钓鱼技术。而爆发保护实际上是为 MDaemon 中现有的基于启发式、签名和内容的工具顶层提供了另一层专门的保护。爆发保护专门用于处理大范围的爆发，而不是处理那些通过传统工具可以更为轻松捕获的旧的、特殊的或特定目标的邮件。



爆发保护

启用爆发保护

选中该复选框为服务器启用"爆发保护"。将对接收的邮件进行分析，看其是否为进行中的病毒、垃圾邮件或网络钓鱼爆发的一种。对话框上的其余选项用于确定对属于爆发成分的邮件作何处理，并指定免于 OP 处理的发件人。

病毒应被...

实时拦截

如果希望在 SMTP 处理过程中拦截确定为属于病毒爆发成分的邮件，请选择该选项。这些邮件不会被隔离或投递给预期的收件人——服务器将拒绝这些邮件。

隔离
如果要接受 OP 确认为属于病毒爆发成分的邮件，请选择该选项。尽管服务器不会拒绝这些邮件，但该邮件将被隔离而非投递给其目标收件人。被隔离的邮件放在隔离文件夹中。

垃圾邮件应被...

实时拦截
如果希望在 SMTP 处理过程中拦截 OP 确认为属于垃圾邮件爆发成分的邮件，请选择该选项。这些邮件将不会被标记为垃圾邮件并投递给其目标收件人——服务器将拒绝这些邮件。该选项不会拦截 OP 所归类的 "群发"邮件，除非激活以下*拦截垃圾邮件时，亦拦截所归类的 "群发"垃圾邮件*选项。OP 分类的 "群发"邮件可能只是某些十分庞大的邮件列表的一部分，或其他类似的广泛发布的内容，因此是否将这些类型的邮件视为垃圾邮件由您自行决定。所以这些类型的邮件通常不应被 OP 拦截或打上不利分数。

接受供过滤
如果希望接受 OP 确认为属于垃圾邮件爆发成分的邮件，请选择该选项，以便它们接着经受垃圾邮件过滤和内容过滤器处理。OP 不会拦截这些邮件，但将根据以下 "*分数*"选项调整其垃圾邮件过滤器总值。

> 当使用 "*接受供过滤*"选项时，OP 不会直接导致已确认的垃圾邮件被拦截，但在 SMTP 处理过程中 MDaemon 仍可能会拦截邮件，条件是垃圾邮件过滤器已配置为使用*SMTP 拒绝邮件，其分数不小于 [xx]*选项，位于 "垃圾邮件过滤器 565"屏幕上。
>
> 例如，如果下面的评分选项导致邮件的垃圾邮件过滤器总值达到 15.0，同时垃圾邮件过滤器的 "*SMTP 拒收...*"选项已配置为拒绝总值不小于 15.0 的邮件，那么该邮件仍将当成垃圾邮件而被拒绝。

分值
当使用上述 "*接受供过滤*"选项时，如果 OP 确认邮件属于垃圾邮件爆发成分，该分值将被添加到邮件的垃圾邮件过滤器总值中。

IWF 内容

以下选项适用于由 "因特网观察基金会（IWF）标识为访问儿童淫秽图像站点（即儿童色情站点）的内容。它允许 OP 使用 IWF 提供的集成 URI 列表来检测并标记访问该内容的邮件。IWF 开设独立的网络 "热线"，用于举报潜在的非法在线内容，包括世界任何地区的儿童淫秽内容。他们与警方、政府、更广的在线产业和社会合作，与不法在线内容作斗争。基金会的 URL 列表每天使用承载儿童淫秽图像的新站点进行更新。

很多机构使用内部遵从的规则管理其雇员收发的邮件内容，尤其是色情或非法资料。此外，很多国家已经颁布法令宣布收发这类内容为非法行为。该功能可协助您确保遵守规则。

有关 IWF 的更多信息，请参阅：

http://www.iwf.org.uk/

IWF 内容应被...

实时拦截
如果希望在 SMTP 过程中拒绝包含 IWF 禁止内容的入站邮件，其选择该选项。

接受供过滤
如果希望当邮件包含 IWF 禁止内容时，提高该邮件的垃圾邮件过滤器总值而不是拒绝它，请选择该选项。垃圾邮件过滤器总值将会提高在下面的 *"分值"*选项中指定的数值。

分值
当选择上述 *"接受供过滤"*选项时，如果邮件包含 IWF 禁止的内容，该邮件的 "垃圾邮件过滤器"总值中将添加该数值。

拦截垃圾邮件时，亦拦截归类为 "群发"的垃圾邮件
有时 OP 会标识某些邮件，它们可能被视作垃圾邮件，但并非发自已知的垃圾邮件制造者或僵尸网络——有时合法的群发邮件和新闻简报就是这样。OP 将这些类型的邮件归类为 *"垃圾邮件 (群发)"*而不是 *"垃圾邮件 (已确认)"*。如果想让 OP 的垃圾邮件拦截功能也应用于 *"垃圾邮件 (群发)"*邮件，请点击该复选框。如果禁用该选项，只有被归类为 *"垃圾邮件 (已确认)"*的邮件才受 OP 的上述垃圾邮件拦截功能的影响。对于希望接收群发邮件但鉴于种种原因无法将源或收件人豁免的站点来说，接受这类垃圾邮件以便将来处理非常必要。

记录处理活动到 MDaemon的插件日志文件
如果要将所有的 OP 处理活动记录到 MDaemon 的插件日志文件中，则启用该复选框。

例外

已验证的 STMP 会话免于进行 OP 处理
启用该选项后，已验证的 SMTP 会话将免于进行 OP 处理。这意味着该会话期间发送的邮件将免于进行爆发保护检查。

来自可信 IP 的 SMTP 会话免于进行 OP 处理
如果希望可信 IP 地址免于进行爆发保护则启用该选项——来自可信 IP 地址服务器的邮件将免于进行 OP 检查。

SPF/DKIM 认可的邮件免于进行 OP 处理
如果希望当邮件的发送域出现在 "已认可列表 465"上，并且该邮件通过了 SPF 或 DKIM 验证时，豁免该邮件的 OP 处理，请点击该复选框。

垃圾邮件蜜罐和垃圾邮件过滤器允许的地址免于爆发保护处理
如果您希望从 "爆发保护"免除 "垃圾邮件蜜罐 592"和垃圾邮件过滤器允许列表，请点击此选项。允许列表适用于收件人，或 SMTP 会话期间给定的 RCPT 值。 "允许列表 (发件人)"适用于发件人或 SMTP 会话中给定的 MAIL 值。这些操作并非基于邮件报头值。

误报和漏报

误报，即将合法邮件错误归类为爆发成分的情况，几乎不会发生。然而，万一发生，对于垃圾邮件/网络钓鱼误报您可以将邮件发送到 spamfp@mdaemon.com，对于病毒误报可以发送邮件到 virusfp@mdaemon.com，以便帮助我们精益求精地改进检测和分类的过程。

漏报，即将垃圾邮件或攻击归类为非爆发成分的情况，比误报的发生更为频繁。但是，OP 不是设计用于捕捉所有垃圾邮件、病毒攻击等类似的东西，这毫无意义——它只是专门用于指向爆发的保护层。旧邮件，特别是定向的邮件等，不是当前正在进行的爆发，因此可以通过 OP 检查。这种邮件随后应该由 AntiVirus 和 MDaemon 处理流程中的后续功能进行捕获。然而，如果发生漏报，对于垃圾邮件/网络钓鱼漏报您可以将邮件发送到 spamfn@mdaemon.com，对于病毒漏报可以发送邮件到 virusfn@mdaemon.com，以便帮助我们精益求精地改进检测和分类的过程。

向我们发送归类不当的邮件时，原始邮件应作为 MIME 邮件附件发送，而不要转发。否则将丢失对于分类处理至关重要的报头和其他信息。

4.5 内容过滤器与反病毒

内容过滤器

"内容过滤器 540"("安全性» 内容过滤器")拥有大量用途，例如：在他们到达他们的最终目标前阻止垃圾邮件，截取包含病毒的邮件，复制邮件到一个或者多个额外用户，在文件底部附加一个记录或者拒绝，添加并删除邮件头，去除邮件附件，删除邮件等。由于管理员创建个人内容过滤器规则，并且由于它们的多样性，他们可以在很多情况中使用，并在大多数部分进行限制。花上少许功夫和试验，该功能是非常有用的。

MDaemon AntiVirus (MDAV)

在使用 MDaemon 可选的 AntiVirus 功能时，您可以访问 "内容过滤器"对话框上的两个额外屏幕：病毒扫描 558和 AV 更新程序 562。这些屏幕被用来直接控制 AntiVirus 的功能，以及在检测到病毒时，指定 MDaemon 将会采取什么操作。MDAV 配备了两个病毒扫描引擎：Cyren Anti-Virus 和 ClamAV。您可以使用任何一个或这两个引擎来扫描邮件，以获得额外的安全层。MDAV 还包含爆发保护 535"功能，它不同于其他基于启发式或签名的传统保护工具，可以用来捕获正在进行的爆发，例如垃圾邮件、网络钓鱼和病毒进攻，而这些爆发通常会被传统的工具所忽略。

初次启用 MDaemon AntiVirus 558将开始 30 天试用。如果您希望购买此功能，请联系您的授权 MDaemon 经销商或访问：www.mdaemon.com。

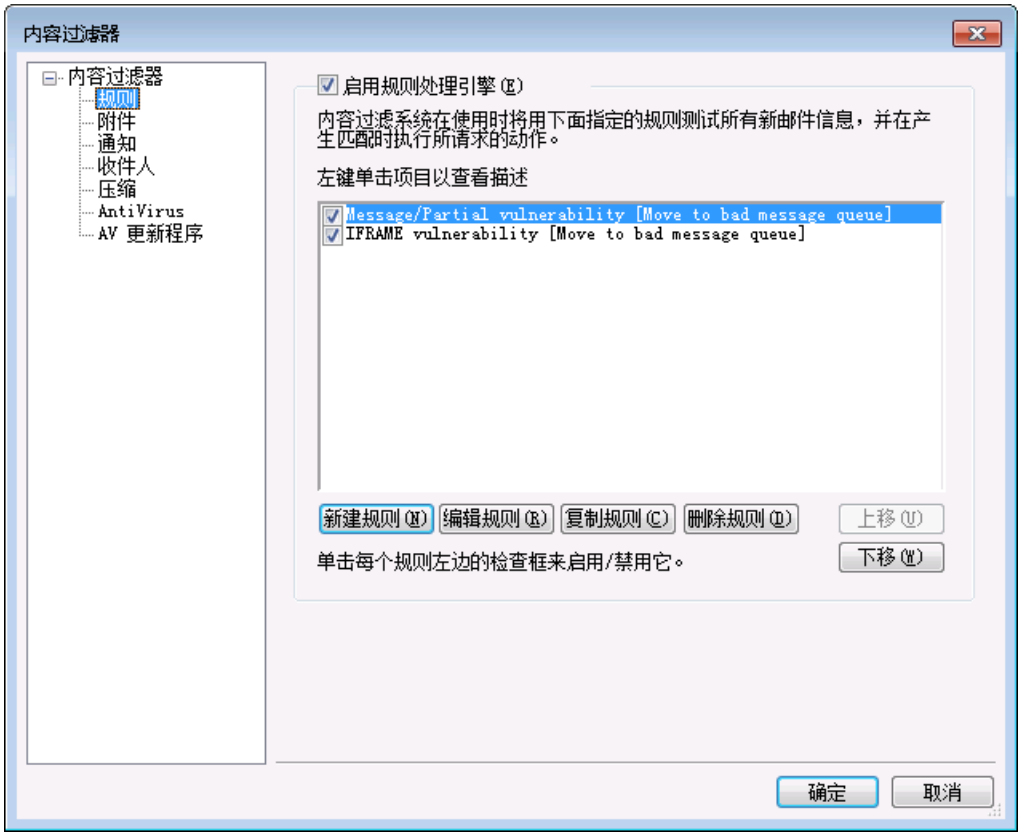
还请参阅：

内容过滤编辑器 540
创建新的内容过滤器规则 542
修改现有的内容过滤器规则 546
在您的过滤器规则中使用正则表达式 546

病毒扫描 558
反病毒更新程序 562
爆发保护 535

4.5.1 内容过滤编辑器

4.5.1.1 规则



所有通过 MDaemon 处理的邮件将在邮件队列临时点上。当内容过滤器启用时，在任意邮件被允许离开对列前，它将首先通过内容过滤器规则被处理。此步骤的结果将决定如何操作此邮件。

文件名以字母 "P"开始的邮件将会被内容过滤过程所忽略。每一个其他的邮件将会通过内容过滤器系统进行处理。一旦处理，MDaemon 将首先更改文件名的第一个字母为 "P"。在此种方法中，一个邮件只会通过内容过滤器系统处理一次。

内容过滤规则

启用规则处理引擎
点击此检查框启用内容过滤器。所有通过 MDaemon 处理的邮件在递送前，将会被内容过滤规则进行过滤。

现有的内容过滤规则
此框中列出您所有的内容过滤器规则，每条规则旁边都有一个选择框以便于您随时启用/禁用。要查看任意一条给定规则的内部脚本格式描述，请点击此项规则，将鼠标光标停留在上面 (移动鼠标将使得描述消失)。每当一封邮件经由内容过滤器处理，那么这些规则将以其列出的顺序来应用。这使您能够安排您的规则以到达一个更高的多功用性级别成为可能。

例如：如果您有一个删除包含 "这是垃圾邮件！"这句话的所有邮件的规则，和一个类似的发送这些邮件到邮件管理员的规则，则将它们放入正确的顺序将会启用这两个规则应用到邮件。假定没有 "停止执行规则"的规则应用到列表中较高位置的邮件。如果是这样，那么您可以使用*上移/下移*按钮来移动另两个规则下方的 "停止"规则。那么，任何包含 "这封是垃圾邮件！""的邮件将会被复制到 "邮件管理员"，然后进行删除。

MDaemon 有能力创建将会执行多个任务的规则和/或使用逻辑规则。参考上述例子，您可以创建一个能够完成那些所有及更多任务的规则，来替换使用多个规则

新建规则
点击此按钮来创建新的内容过滤器规则。这将打开 "创建规则 542"对话框。

编辑规则
点击此按钮来打开 "修改规则 546"编辑器中选定的规则。

复制规则
点击此按钮来复制选定的内容过滤器规则。将会创建一个同样的规则，并添加到此列表中。新规则将会使用 "Copy of [OriginalRule Name]"作为默认名称。如果你希望创建多个类似的规则，这是非常有用的。您可以创建一个单独的规则，然后复制它们几次，并根据需要调整这些副本。

删除规则
点击此按钮来删除选定的内容过滤器规则。在 MDaemon 这么做之前，您将被要求确认你的决定来删除规则。

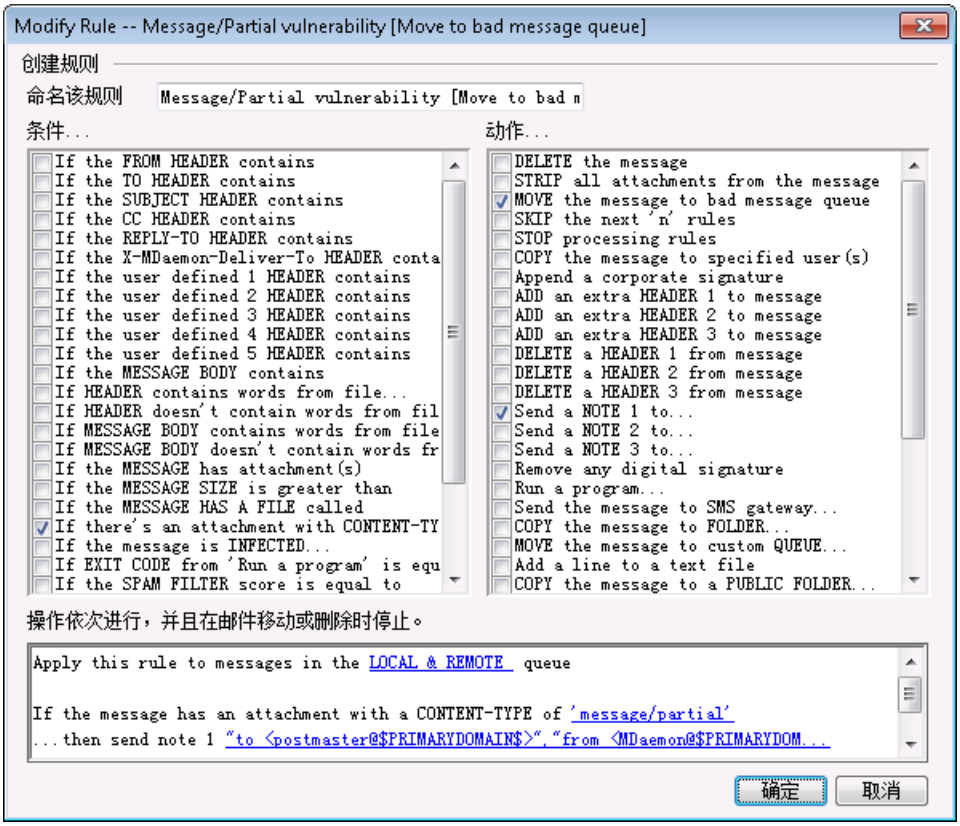
上移
点击此按钮上移所选规则。

下移
点击此按钮下移所选规则。

还请参阅：

创建新的内容过滤器规则 542
修改现有的内容过滤器规则 546
在您的过滤器规则中使用正则表达式 546

4.5.1.1.1 创建新的内容过滤器规则



此对话框用来创建 "内容过滤器规则"。可以点击在内容过滤器对话框上的 *"新建规则"*按钮来获取此对话框。

创建规则

命名该规则
在此为您的新规则输入一个描述性的名字。默认名称为 "New Rule #n"。

条件...

此框列出可能应用到您新规则中的条件。对于您希望应用到新规则的任意条件，请点击相应的选框。每一个启用的条件将会出现在下方的 "规则描述"框中。大多数条件需要附加信息，而这些信息您需要点击 "规则描述"框中条件的超链接来指定。

如果 [HEADER] 含有——点击这些选项中的任意一个来创建基于您规则指定的报头内容。您必须指定检查的文本。此条件现在支持正则表达式。请参阅 "在您的过滤器规则中使用正则表达式 546"。

如果用户定义的 [# HEADER] 中含有——点击这些选项中的任意一个来创建基于您规则指定的报头内容。您必须指定新报头，并且指定检查的文本。此条件现在支持正则表达式。请参阅 "在您的过滤器规则中使用正则表达式 546"。

如果邮件正文含有——此选项把邮件正文内容作为条件之一。此条件要求您指定检查的文本字符串。此条件现在支持正则表达式。请参阅 "在您的过滤器规则中使用正则表达式 546"。

如果邮件含有附件——选中此项后，该规则只扫描一个或者多个邮件附件。不需要附加信息。

如果邮件大于——如果您希望规则基于邮件的大小，点击此选项。邮件大小必须指定为 *KB*。默认值为 10 KB。

如果邮件所含文件名为——此选项将会对一个有指定名称的文件附件进行检测。此文件名必须指定。允许 "*.exe 和 file*.*"这类的通配符。

如果邮件受感染...——当 MDaemon 确定了一封邮件感染了病毒，那么此条件为 TRUE。

如果来自先前 "运行进程" 的 EXIT CODE（退出代码）等同于——如果您列表中先前的规则利用了 *"运行进程"*操作，您可以使用此条件来查找处理过程中指定的退出代码。

如果邮件含数字签名——此条件应用于已进行数字签名的邮件。此条件无需更多信息。

如果发件人是群组成员...——当发送邮件的账户是规则中所指定的账户群组中的一员，那么此条件将应用于该邮件。

如果收件人是群组成员...——当邮件的收件人是规则中所指定的账户群组中的一员，那么此条件将应用于该邮件。

所有邮件——如果您希望规则应用到所有邮件，请点击此选项。不需要更多的信息；此规则将会影响除了那些在过去的规则中，应用 "停止处理中的规则"或者 "删除消息"规则的消息外，操作每一个邮件。

操作...

如果一封邮件匹配规则条件，那么 MDaemon 可以执行这些操作。一些操作要求您通过点击 "规则描述"框中 "操作"的超链接，来指定附加信息。

删除邮件——选择此项操作将使邮件被删除。

剔除邮件中的所有附件——此操作将会使得所有附件从邮件中被去除。

将邮件移至坏邮件队列——点击此操作导致一个邮件被移动到坏邮件队列。会将 X-MDBadQueue-Reason 报头添加到这封邮件。

跳过 n 规则——选择此操作将导致跳过指定数量的规则。在您可能希望一条规则被应用到某些环境但不应用到其他的这种情况时，这是非常有用的。

例如：您可能希望删除某些含有 "垃圾邮件"字样的邮件，但是不删除那些含有 "好的垃圾邮件"的邮件。要完成此操作，您可能创建一条规则来删除含有 "垃圾邮件"的邮件，然后将其放到所有规则之上，陈述为 "如果邮件包含 '好的垃圾邮件'那么跳过规则 1"。

停止处理中的规则——此操作将跳过所有保留的规则。

将邮件复制到指定用户——使得邮件的一个副本被发送到一个或者多个收件人。您必须指定哪些收件人将收到邮件。

附加公司签名——此操作使得您能够创建少量文本作为邮件页脚。也可以选择添加一个文本文件的内容。如果您希望在您的签名文本中包含 HTML 代码，我们为您提供了一个 *"使用 HTML"*勾选框。该操作支持$CONTACT...$ 签名宏 1101。

例如：你可能使用此规则来包含一个为 "此邮件来自于我所在的公司，如有任何投诉或者疑问请直接发送到 user01@example.com "的表述。

为邮件添加额外报头——此操作将会添加一个额外的报头到邮件。您必须指定新报头的名称和它的值。

删除邮件中的报头项目——此操作将会从邮件中删除报头。您必须指定希望删除的报头。

发送便笺至...——此操作将会发送一封邮件到特定地址。您可以指定收件人、发件人、主题和少量文本。你也可以配置此动作，附加原始邮件到记录中。**请注意：**该操作跳过没有返回路径的所有邮件。因此像 "投递状态通知"(DSN)这样的邮件无法触发此操作。

例如：您可能希望创建移动所有包含 "这封是垃圾邮件！"的邮件到坏邮价目录的规则，以及发送记录到一些人，使他们知道完成了此动作的规则。

删除数字签名——点击此操作可以从邮件中移除数字签名。

运行进程...——当一封邮件符合规则条件时，该操作将用来运行一个特定的程序。您必须指定您希望运行的程序的路径。您可以使用 $MESSAGEFILENAME$ 宏将邮件的名称传递到处理进程，而且您可以指定当等待处理进程终止时，MDaemon 应该暂时或无限地延缓它的运行。而且，您可以强制处理进程终止，并且/或者将其运行在一个隐藏窗口。

通过 SMS 网关服务器发送邮件...——点击此项，通过一个 SMS 网关服务器发送邮件。您必须提供主机或者 IP 地址以及 SMS 电话号码。

将邮件复制到文件夹...——使用此项将邮件副本放置到指定的文件夹。

将邮件移至自定义队列...——使用此操作将邮件移动到一个或多个先前创建的自定义邮件队列。当移动邮件到自定义远程队列时候，您可以使用在时间调度上的自定义调度选项来控制这些邮件什么时候处理。

将行添加至文本文件——此项可以使得一行文本被添加到指定文本文件中。当选择此动作，您将指定文件的路径，以及您希望附加到其上面的文本。您可以在文本中使用某些 MDaemon 宏，使得内容过滤器动态包含关于邮件的发件人、收件人、邮件 ID 和其他信息。点击 "将行添加至文本文件"对话框上的 "宏"按钮，显示可使用的宏列表。

[复制|移动]邮件到公共文件夹...——使用此操作使得邮件被复制（或移动）到一个或者多个公共文件夹。

搜索并替换报头中的文本——使用此选项对指定报头检查某些单词，然后将其删除或替换。创建此规则时，点击"规则描述"中的"指定信息"链接来打开"报头 - 搜索并替换"对话框，您可以在其中指定要替换或者删除的报头和单词。此操作现在支持正则表达式。请参阅"在您的过滤器规则中使用正则表达式 546"。

搜索并替换邮件正文中的文本——使用该选项来扫描邮件正文并且以任何想要的文本来替换。此操作现在支持正则表达式。请参阅"在您的过滤器规则中使用正则表达式 546"。

跳至规则...——使用此操作立即跳转到列表中更靠下的规则，将跳过所有在这两个规则之间的规则。

发送即时邮件...—当邮件与规则的条件匹配时，此操作会向某人发送即时邮件。您将指定"收件人:"电子邮件、"发件人:"地址和邮件内容。

添加到 Windows 事件日志...—使用此操作可将文本字符串记录到 Windows 事件日志中。您可以在字符串中使用宏，并且有一个按钮来显示允许的宏。

提取附件到文件夹...—使用此操作可从邮件中提取附件。您将指定要将附件复制到的文件夹，并且可以选择在提取后从邮件中删除附件。您还可以设置条件，以根据文件名、内容类型和附件的大小来确定要提取的附件。

更改邮件处理优先级...—此操作用于设置邮件的处理优先级，从"10（紧急）"到"90（重试）"。默认设置为"50（常规）"。

使用 DKIM 选择器签名...——如果您希望该规则使一封邮件中包含一个DKIM 签名 445，请使用此操作。如果您希望使用一个服务器来签名一些邮件而不是在 DKIM 对话框中指定的签名，您同样可以使用此操作。

为 REQUIRETLS 标记邮件—指示该邮件应使用 REQUIRETLS 493。

使用用户的[私人|公共]密钥来[签名|加密|解密]邮件...—使用这些操作可以使用私钥或公钥对邮件进行签名，加密或解密。还请参阅：MDPGP 527 来了解更多信息。**请注意：**即使禁用了 MDPGP，也将执行这些操作。

在邮件顶部添加警告...—如果您希望在邮件顶部添加某种警告，请使用此操作。您可以输入纯文本字符串或输入 HTML 代码，然后勾选"使用 HTML"复选框。或者，您可以从文件中加载文本。

添加附件...—如果您希望将文件附加到符合规则条件的邮件，请使用此操作。该文件必须包含在 ./MDaemon/CFilter/Attachments/ 文件夹中。

提取附件并添加链接...—如果您希望从符合规则条件的邮件中提取附件并添加指向它们的链接，请使用此操作。还请参阅：附件链接 305。

规则描述

此框显示了新规则的内部脚本格式。点击任何规则的条件或操作（作为超链接列出）并将打开相应的编辑器来指定任何需要的信息。

还请参阅：

内容过滤编辑器 540
修改现有的内容过滤器规则 546
在您的过滤器规则中使用正则表达式 546

4.5.1.1.2 修改现有的内容过滤器规则

要修改一项现有的内容过滤器规则，选中该规则然后点击“内容过滤器”对话框上的“*编辑规则*”按钮。此规则将被打开，再在规则编辑器中进行编辑。此编辑器上的控件等同于“创建规则对话框 542”上的控件。

还请参阅：

内容过滤编辑器 540
创建新的内容过滤器规则 542
在您的过滤器规则中使用正则表达式 546

4.5.1.1.3 在您的过滤器规则中使用正则表达式

内容过滤系统支持*正则表达式*搜索，它是一个功能全面的系统，不仅您让您搜索特定的文本字符，也可以搜索到文本*类型*。正则表达式包含纯文本和特殊字符的组合来指示进行哪种类型的匹配，从而使您的“内容过滤器”规则变得更加强大和准确。

什么是规则表达？
一个正则表达式（regexp）是由*元字符*和文字数字的文本字符，或者“*文字的*”（abc，123，及其他）混合组合而成的文本模式。该类型用于匹配文本字符——并附有匹配的结果，是成功还是失败。Regexps 主要用于规则文本匹配以及搜索和替换。

在正则表达式中，元字符是有特定功能及用途的特殊字符。在 MDaemon“内容过滤”系统中的 Regexp 实施允许以下特殊字符：

```
\ | () [] ^ $ * + ? . <>
```

元字符	描述
****	若在一元字符钱使用反斜线（“\”），将使元字符被处理为文字字符。若您希望正则表达式搜索其中一个用作元字符的特殊字符，这一点是有必要的。例如，要搜索“+”您的表达式中必须包含“\+”。
|	使用*交替*字符（亦叫做“*或*”或者“*竖线*”），当您希望字符两侧的其中一个表达式符合目标字符。正则表达式是“abc|xyz”。搜索一个文本字符时，会出现符合条件的“abc”或“xyz”。
[...]	框（“[”及“]”）内包含的字符组就表示该组中的任意字符都可能符合所查找的文本字符。括号里字符间的破折号（“-”）表示了字符的范围。例如，在表达式“[a-z]”中搜索字符“abc”将生

成三个匹配项：*"a," "\b,"*以及 *"c。"*使用表达式 "[az]"只会生成一个匹配项：*"a。"*

^ 表示字符串的开头。在目标字符串中，"abc ab a"表达式 "^a"将生成一个匹配项—目标字符串中的第一个字符。正则表达式 "^ab"也将生成一个匹配项—*目标字符串中的*第一第二个字符。

[^...] 紧跟左括号（"["）后的插入记号（"^"）有不同的含义。用于将括号内剩余的字符排除在符合条件的目标字符串之外。表达式 "[^0-9]"表明目标字符不是数字。

(...) 圆括号影响了样式估计的顺序，也可作为*带标记的*表达式，用于*搜索和替换*表达式。

正则表达式的搜索结果可以暂时保存，也可用于*替换*表达式以建立新的表达式。在*替换*表达式中，您可以包含一个 "$0"字符，将会以正则表达式搜索过程中所找到的子字符串来替换。所以，如果*搜索*表达式 "a(bcd)e"找到了一个子字符串匹配项，那么 "123-$0-123"的*替换*表达式将以 "123-abcde-123"来替换符合条件的文本。

同样地，在替换表达式中您也可以使用特殊字符 "$1," "$2," "$3,"*等等*。这些字符只会被*已标记*表达式的结果所替代，而不是整个子字符串的匹配项。紧跟反斜线的数字表明您想要引用的带标记表达式 (如果正则表达式中包含了不知一个带标记的表达式)。例如，如果您的*搜索*表达式是 "(123)(456)"并且您的*替换*表达式是 "a-$2-b-$1"，那么一个符合的子字符将由 "a-456-b-123"替代，而 "a-$0-b"的一个*替换*表达式将以 "a-123456-b"替代。

**$** 美元记号（"$"）代表字符串的结尾。在文本字符串中，"13 321 123"表达式 "3$"将生成一个匹配项—字符串中的最后一个字符。正则表达式 "123$"也将生成一个匹配项——*目标字符串中的*最后三个字符。

***** 星号（"*"）量词表明星号左边的字符*在一行字符中出现的次数*必须大于等于零次。那么 "1*abc"将符合文本 "11abc"以及 "abc"。

+ 与星号量词类似，"+"量词表明加号左边的字符*在一行字符中出现的次数*必须大于等于一次。那么，"1+abc"将符合文本 "11abc"而不符合文本 "abc"。

? 问号（"?"）量词表明问号左边的字符必须匹配*零或*一次。因此 "1?abc"将匹配文本 "abc"，并且匹配 "11abc"的 "1abc"部分。

. 句号或者点（"."）元字符将符合任何其他字符。那么 ".+abc"将符合 "123456abc"，且 "a.c"将符合 "aac"，"abc"，"acc"等等。

符合的条件和操作
正则表达式可用于任何 *"报头"*过滤器规则 *"条件"*。例如，任何使用 "If the FROM HEADER contains"条件的规则。正则表达式同样可以使用 "If the MESSAGE BODY"条件。

正则表达式可用于两个 "内容过滤器"规则 *"操作"*: "搜索并替换报头中的文字"以及 "搜索并替换邮件正文中的文字。"

在 "内容过滤器"规则*条件中所使用的正则表达式*是不区分大小写的。因此不考虑大小写。

可以选择在 "内容过滤器"规则*操作中所使用的正则表达式*是否区分大小写。在规则的操作中创建正则表达式时，将有选项让您启用/禁用区分大小写。

在规则条件中配置 Regexp

配置邮件头或者邮件主体条件使用规则表达：

1. 在创建规则对话框中上，点击相应复选框以加入你希望插入到你的规则当中的，邮件头或者邮件主体条件。
2. 在 "创建规则"对话框底部的摘要区域，点击与此条件相应的您在步骤一中所选择的 **"包含特定字符串"**链接。这将打开 "指定搜索文本"对话框。
3. 在 "当前指定的字符串..."区域，点击 "包含..."链接。
4. 从下拉列表框中选择 **"匹配正则表达式"**，然后点击 **"确定"**。
5. 如果您需要帮助来创建您的 regexp 或希望对其进行测试，请点击 **"测试正则表达式"**。如果您不需要使用 "测试正则表达式"对话框，则在提供的文本框中输入您的 regexp，点击 **"添加"**，并跳到步骤 8。
6. 在 "搜索表示式"文本框中输入您的正则表达式。简单化处理过程，我们已经提供了一个快捷菜单，可以用来方便的插入渴望的特殊字符到您的 regexp。点击 "›"按钮进入此菜单。当您选择了这个菜单中的一个选项，会将其对应的特殊字符插入到表达式中，并将文本插入点移至字符所需的合适位置。
7. 在提供的文本区域，输入任何你希望用来测试你表达式的文本，然后点击**测试**。当你完成对你的表达的测试时，点击 **"确定"**。
8. 点击 **"确定"**。
9. 继续正常的创建你的规则。

在规则的操作中配置 Regexp

要配置一个 "搜索并替换文字…"操作来使用正则表达式：

1. 在 "创建规则"对话框中，点击您希望插入到您规则中与 *"搜索并替换文字..."*操作相对应的复选框。

2. 在 "创建规则"对话框底部的摘要区域，点击与此操作相应的您在步骤1中选择的 "**指定信息**"链接。这将打开 "搜索和替换"对话框。

3. 如果您在步骤1中选择了 "*搜索...报头*"，则使用提供的下拉列表框来选择您希望搜索的报头，未列出所需报头时，在此框中输入一个报头。如果您在步骤 1 中没有选择 "*搜索...报头*"操作，请跳过这一步。

4. 输入您希望用于此操作的*搜索*表达式。简单化处理过程，我们已经提供了一个快捷菜单，可以用来方便的插入渴望的特殊字符到您的 regexp。点击 "**>**"按钮进入此菜单。当您选择了这个菜单中的一个选项，会将其对应的特殊字符插入到表达式中，并将文本插入点移至字符所需的合适位置。

5. 输入您希望用于此操作的*替换*表达式。除了*搜索*表达式以外，我们还为此选项提供了一个元字符快捷方式菜单。如果您希望删除一个匹配的子字符串而不是用更多地文本替换，则留此文本框为空。

6. 如果您希望表达式区分大小写，则点击 "**匹配大小写**"。

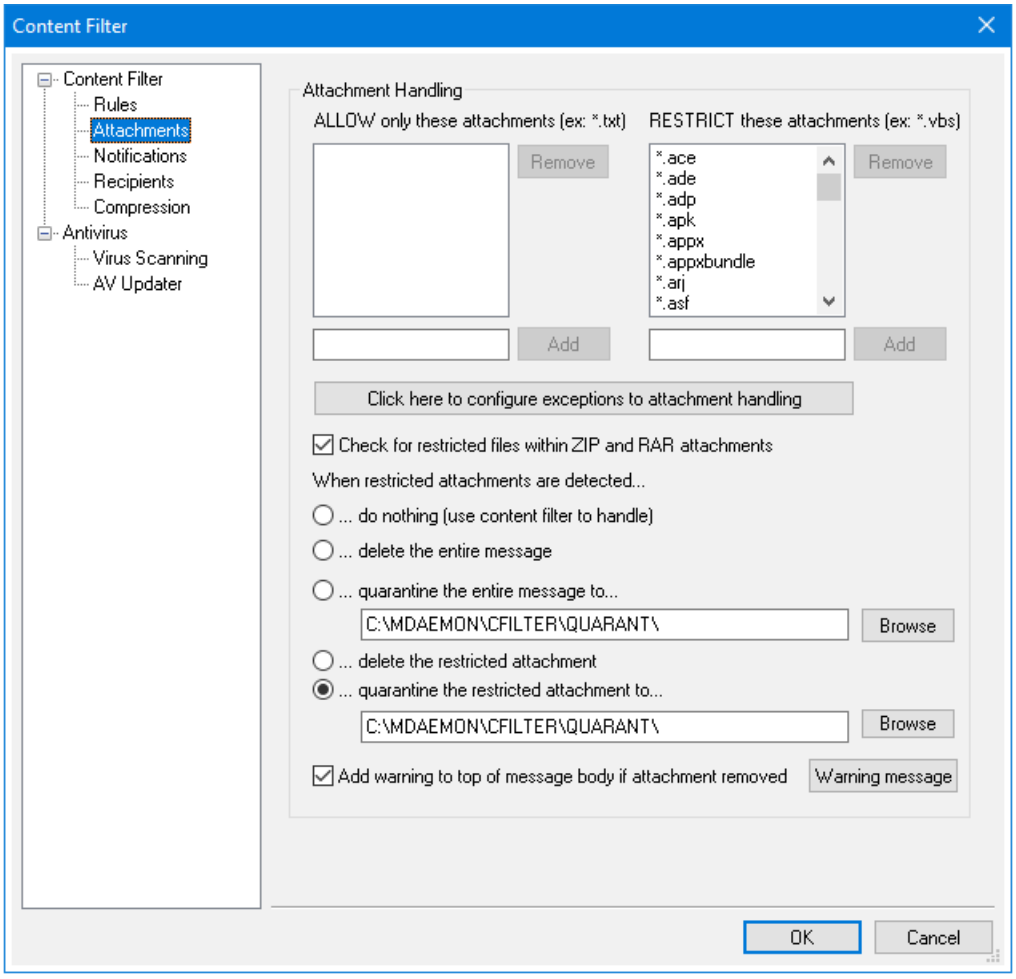
7. 如果您希望搜索和替换被作为正则表达式，则点击 "**正则表达式**"。否则其将被作为一个简单的子字符串搜索和替换—它将对文本的额外的文字匹配进行查找，而不是将其作为正则表达式来处理。

8. 如果您不需要测试您的表达式，请跳过这一步。如果您需要测试你的表达式，点击 "**运行测试**。"在搜索和替换测试者对话框， 输入您的搜索和替换表达式，以及你希望测试的文本，点击**测试**。当你完成对 regexps 的测试时，点击**确定**。

9. 点击 "**确定**"。

10. 继续正常的创建你的规则。

4.5.1.2 附件



使用此标签指定你希望区分为允许和限制的附件。不被允许的附件将自动从邮件中移除。

附件处理

在 *"限制这些附件"*列表中所指定的文件名，在 MDaemon 对其进行处理时，将从邮件中自动除去。若您在 *仅允许这些附件*列表中列出了任何文件，那么只会允许这些列出的文件—任何其他的附件将从邮件中除去。在附件除去之后，MDaemon 将会正常的继续并递送没有附件的邮件。但遇到这些受限制的附件之一时，你可以使用在通知标签上的选项使得一封通知邮件被发送到不同的地址。

在列表条目中，允许通配符。例如，一个 "*.exe"条目，将使所有以 EXE 文件扩展名结尾的附件被允许或者移除。要添加一个条目到任意一个列表，在提供的空白处输入文件名并点击 "添加"。

点击此处来配置附件处理例外

点击这个按钮来指定你希望排除在附件限制之外的地址。当从这些地址之一种直接收到一个邮件，MDaemon 将会允许邮件通过，即使它包含一个受限制的附件。

检查 ZIP 和 RAR 附件内受限的文件
点击这个按钮来对 Zip、7-Zip 和 RAR 压缩文件内容进行扫描以检查受限文件。此外，如果在一个经过压缩的附件内找到一个匹配文件，将触发设置成查找特定文件名的任何 "内容过滤器"规则。

监测到受限制的附件时...
当邮件包含受限的附件时，点击要执行的操作。

...无操作（使用内容过滤器来处理）
如果您不希望基于附件设置采取指定操作，不过希望按内容过滤器规则 540 采取操作，请选择此项。

...删除整封邮件
在邮件包含受限制的附件时，此选项将会删除整封邮件。

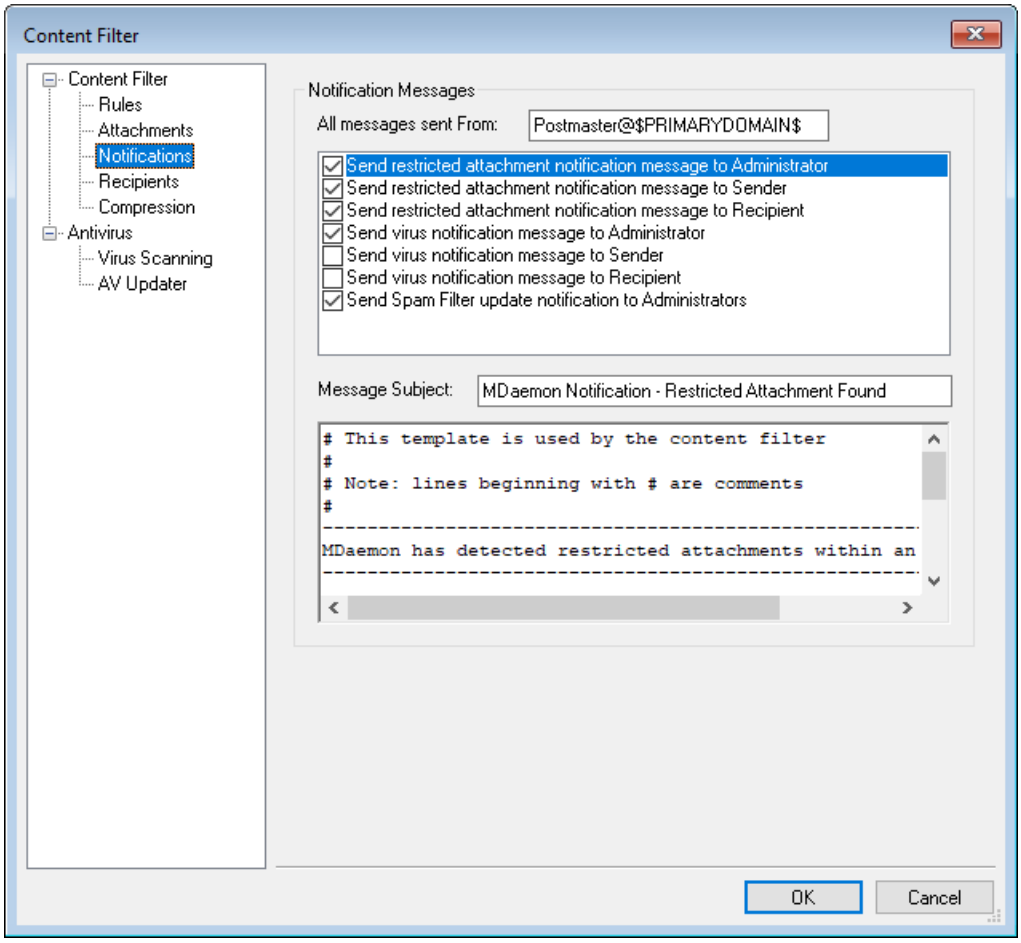
...隔离整个邮件到...
此选项将导致包含受限附件的邮件被隔离到指定的位置。

...删除受限制的附件
如果您希望删除任何受限制的附件，而不是删除整封邮件，请选择此选项。

...隔离受限制的附件到...
点击这个按钮来指定你希望隔离限制附件的地方。而不是简单地删除这些附件。这是默认设置。

如果附件被删除，则在邮件顶部添加警告
在 MDaemon 从邮件中删除附件时，例如因为检测到病毒而将其删除，它会在邮件正文的顶部添加一条警告消息。如果您希望审核或修改该邮件的模板，请点击 **警告**"按钮。默认情况下启用此项。

4.5.1.3 通知



使用该屏幕来指定在检测到病毒或受限附件时，或者在反病毒或垃圾邮件过滤器文件更新时应接收通知消息的人员。

通知邮件

所有邮件发自：
使用此选项指定发送通知邮件的邮件地址。

发送病毒通知邮件到…
当一封邮件带着病毒的附件到达时，一封警告邮件将会被发送到在此部分中指定的个人。一封自定义警告邮件可以被发送到发件人、收件人、以及您在收件人555屏幕上已经指定的管理员。为了对此三者的任意之一自定义邮件，从列表中选择他们其中之一，然后编辑出现在此屏幕中部的邮件。然而每一个条目都有其自己的邮件，尽管在默认值下，由于一些都是一样的，这并不明显。

发送受限制的附件通知邮件到…
当抵达达一封有文件附件的邮件，且此附件匹配受限制附件条目（在“附件”选项卡上所列）时，一封警告邮件将会被发送到在此部分指定的个人。一封自定义警告邮件可以被发送到发件人，收件人，以及你在收件人标签上已经指定的管理员。为了对此三者的任意之一自定义邮件，从列表中选择他们其中之一，然后编辑出现在此标签中部的邮件。

然而每一个条目都有其自己的邮件，尽管在默认值下，由于三者都是一样的，这并不明显。

向管理员发送垃圾邮件过滤器更新通知
如果您希望每次在更新垃圾邮件过滤器时，向管理员发送一封含有更新结果的邮件，请使用此项。此项与*"发送含有更新结果的通知邮件"*这一选项相同，该选项位于：垃圾邮件过滤器» 更新。

邮件主题：
此文本将显示在 已发送的通知邮件 "主题："报头中。

邮件
当与此条目相关的复选框被启用时，这是将被发送给在以上列表中所选的条目的邮件。您可以从显示邮件的此框中直接编辑邮件。

包含该文本的实际文件位于 MDaemon\app\ 目录中。它们是：

cfattrem[adm].dat - 受限制的附件邮件 -管理员
cfattrem[rec].dat - 受限制的附件邮件 -收件人
cfattrem[snd].dat - 受限制的附件邮件 -发件人
cfvirfnd[adm].dat - 发现有病毒的邮件 -管理员
cfvirfnd[rec].dat - 发现有病毒的邮件 -收件人
cfvirfnd[snd].dat - 发现有病毒的邮件 -发件人

如果您想要存储其中一封邮件到其初始面貌，只需删除相关的文件，然后 MDaemon 将会以它的默认状态对其进行重建。

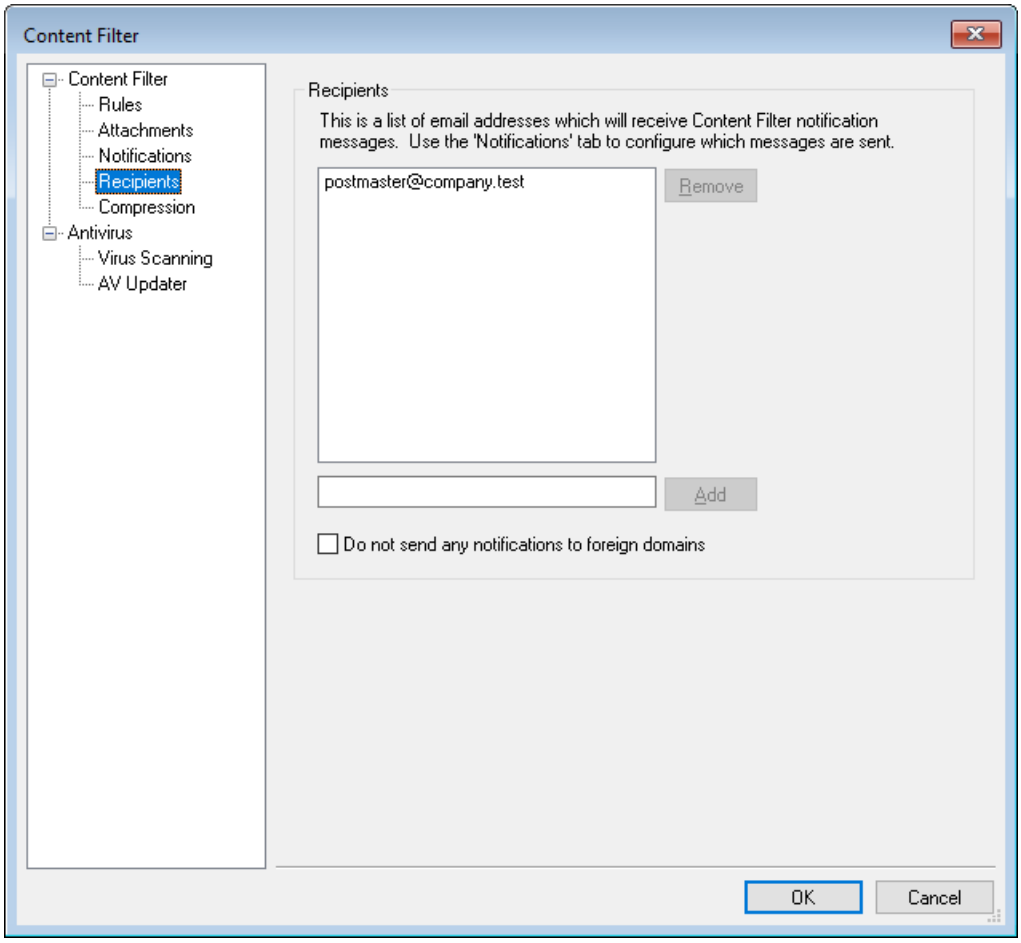
4.5.1.3.1 邮件宏

方便起见，在通知邮件和其他某些 "内容过滤器"生成的邮件中可以使用某些宏。您可以使用以下任意宏：

$ACTUALTO$	某些邮件可能包含 "ActualTo"字段，一般表示由原来用户在任何格式重定或别名转换之前输入的目标邮箱和主机。此宏用来替换所提到的值。
$AV_VERSION$	列出您正在使用的 AntiVirus 的版本。
$CURRENTTIME$	在处理邮件时，此宏用来替换当前时间。
$ACTUALFROM$	某些邮件可能包含 "ActualFrom"字段，一般表示任何格式重定或别名转换之前的原始邮箱和主机。此宏用来替换所提到的值。
$FILTERRULENAME$	此宏用来替换规则的名称，此邮件匹配规则的标准。
$FROM$	扩展为邮件 "发件人："报头中包含的完整地址。
$FROMDOMAIN$	此宏将插入邮件 "发件人："报头中找到的地址中包含的域名 (电子邮件地址中 "@"右侧的值)。

$FROMMAILBOX$	列出在邮件“发件人：”报头中找到的地址的邮箱部分（电子邮件地址中“@”左侧的值）。
GEN_GUID	使用 11 个字母和数字字符生成唯一 ID。示例：0XVBASADTZC
$HEADER:XX$	该宏可以使“xx”中指定的报头值在重定格式后的邮件中扩展。例如：如果原始邮件拥有“收件人：user01@example.com”，那么会将 $HEADER:TO$ 宏扩展成“user01@example.com”。如果原始邮件拥有“主题：这是主题”，则使用“这是主题”替换 $HEADER:SUBJECT$ 宏。
$HEADER:MESSAGE-ID$	与上方的 $HEADER:XX$ 类似，此宏将扩展成 Message-ID 报头值。
$LIST_ATTACHMENTS_REMOVED$	当从邮件中删除一个或多个附件时，此宏将列出这些附件。
$LIST_VIRUSES_FOUND$	当在邮件中发现一个或多个病毒时，此宏将列出这些病毒。
$MESSAGEFILENAME$	此宏扩展成当前正在处理的邮件的文件名。
$MESSAGEID$	除了该宏是从邮件 ID 值中去除$HEADER:MESSAGE-ID$“<>”以外，其他都与 $HEADER:MESSAGE-ID$ 一样。
$PRIMARYDOMAIN$	扩展成 MDaemon 的“默认域”名，在“域管理器 149”上指定。
$PRIMARYIP$	此宏扩展成 IPv4 地址 151（属于您的默认域 149）。
$PRIMARYIP6$	此宏扩展成 IPv6 地址 151（属于您的默认域 149）。
$RECIPIENT$	此宏解析成邮件收件人的完整地址。
$RECIPIENTDOMAIN$	此宏将插入邮件收件人的域名。
$RECIPIENTMAILBOX$	列出收件人的邮件箱（在邮件地址中，此值在“@”左侧）。
$REPLYTO$	此宏扩展成邮件的“Reply-to”报头值。
$SENDER$	扩展成发送邮件的完整地址。
$SENDERDOMAIN$	此宏将插入邮件发件人的域名（在邮件地址中，此值在“@”右侧）。
$SENDERMAILBOX$	列出发件人的邮件（在邮件地址中，此值在“@”左侧）。
$SUBJECT$	显示邮件主题中包含的文本。

4.5.1.4 收件人



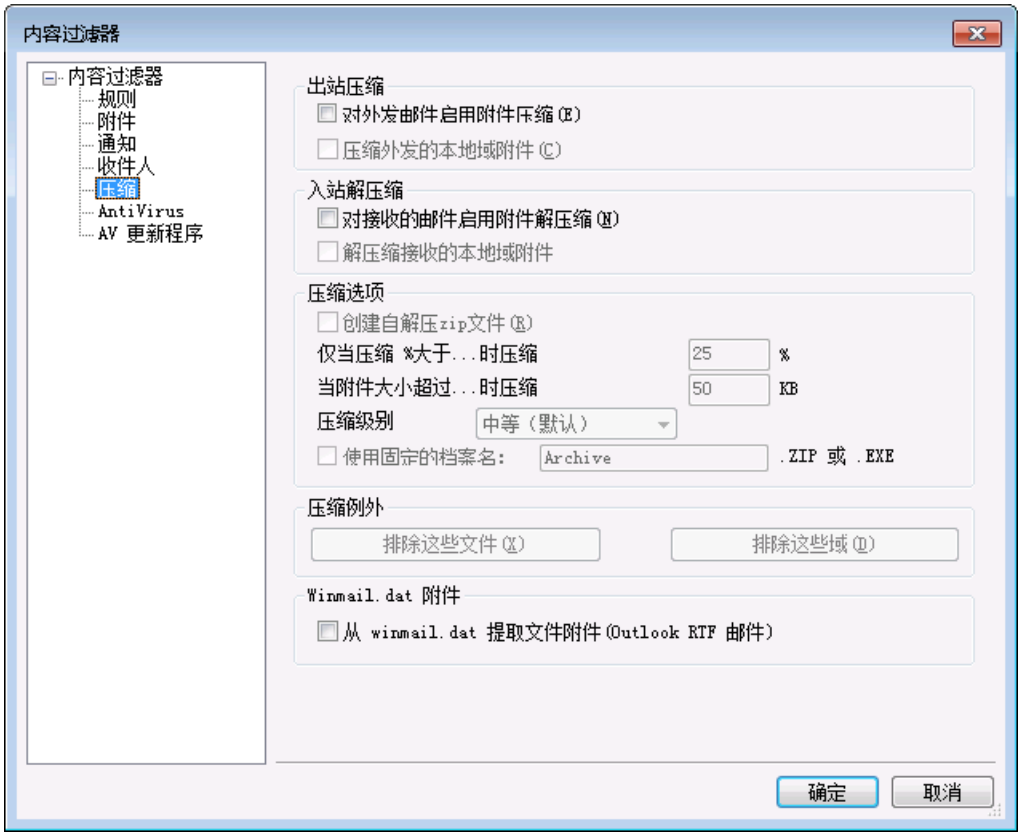
收件人

收件人列表和位于 "通知"选项卡上的多个 *"发送...到管理员"*选项相对应。当在那个标签上的管理员选项一个或多个被选择的时候，通知邮件将发送到这些地址。要添加一个地址到此部分，在给出的空白处输入并点击 *"添加"*。要删除一个地址，从列表中将其选中然后点击 *"删除"*。

不向外域发送任何通知

如果您希望将 "内容过滤器"通知邮件限制到本地域收件人，请勾选此框。默认情况下，禁用该选项。

4.5.1.5 压缩



利用这个选项卡上的控件，在邮件投递前，您可以使得邮件附件自动被压缩或者解压缩。压缩的级别也可以由其他几个参数和例外所控制。此功能可以明显减少带宽消耗量，以及投递你的出站邮件所需要的吞吐量。

出站压缩

为出站邮件启用附件压缩
如果您希望对出站远程邮件消息启用自动邮件附件压缩，点击此复选框。启用此控制将不会使所有邮件附件被压缩；它方便的打开此功能。一封出站邮件的文件是否被压缩由此选项卡上的保留设置决定。

压缩出站的本地域附件
启用此控件将会使得文件压缩设置应用到所有出站邮件——即使那些文件的最终目标是另外一个本地地址。

入站压缩

为入站邮件启用附件解压缩
如果你希望对入站的远程邮件附件启用自动解压缩，点击此复选框。当到达一封含有压缩附件的邮件时，MDaemon 将会在投递它到本地用户的邮件箱前对其进行压缩。

解压缩入站的本地域附件
如果你希望自动解压缩也应用到本地邮件，启用此控制。

压缩选项

创建自解压 zip 文件
如果您希望 MDaemon 创建的压缩文件能够成为有 EXE 文件扩展名的自解压 zip 文件，点击此复选框。如果你顾及到邮件的接收人可能不能访问解压缩软件，则这是非常有用的。自解压文件能够通过对其进行双击很方便地解压缩。

如果压缩率大于 xx% 才进行压缩
在发送邮件前，除非附件的压缩率能够高于在此控件中指定的一个百分比，否则 MDaemon 将不会压缩邮件的附件。例如，如果你指定此值为20，并且给定的附件在压缩率至少为21% 前，不能被压缩，那么 MDaemon 将不会在发送邮件前压缩附件。

MDaemon 必须先压缩一个文件来确定它所能被压缩的百分比。因此，此功能不会阻止文件被压缩——当这些文件不能被压缩到指定值之上时，即阻止文件附件以压缩格式发送。换言之，如果在压缩文件之后，MDaemon 发现它不能被压缩得超过此值，压缩将被忽视，并且邮件将和它未作改变的附件一起投递。

如果附件大小超过这个值 XX KB
启用 "自动附件压缩"时，当邮件的总大小超过在此指定的值时，MDaemon 将只尝试压缩一封邮件的附件。附件大小在以下阈值的邮件将会和未更改的附件一同被正常投递。

压缩级别
使用下拉列表框来选择您希望 MDaemon 应用到自动压缩附件的压缩级别。你可以选择3个级别的压缩：最小 (最快的压缩处理过程及最差的压缩)，中级 (默认值)，或者最大 (最慢的压缩过程，但是最高级别的压缩)。

使用固定的归档名称：[归档名称]
如果你希望自动压缩附件有一个指定文件名，点击此复选框，并且选择一个名称。

压缩例外

排除这些附件...
点击此按钮来指定您想从自动压缩功能中排除的文件。当一封邮件附件匹配这些文件名之一，那么它将不被压缩，无论压缩设置为何。在这些条目中允许通配符。因此，例如您可以指定 "*.exe"，并且所有以 ".exe"结尾的文件将会保持未压缩状态。

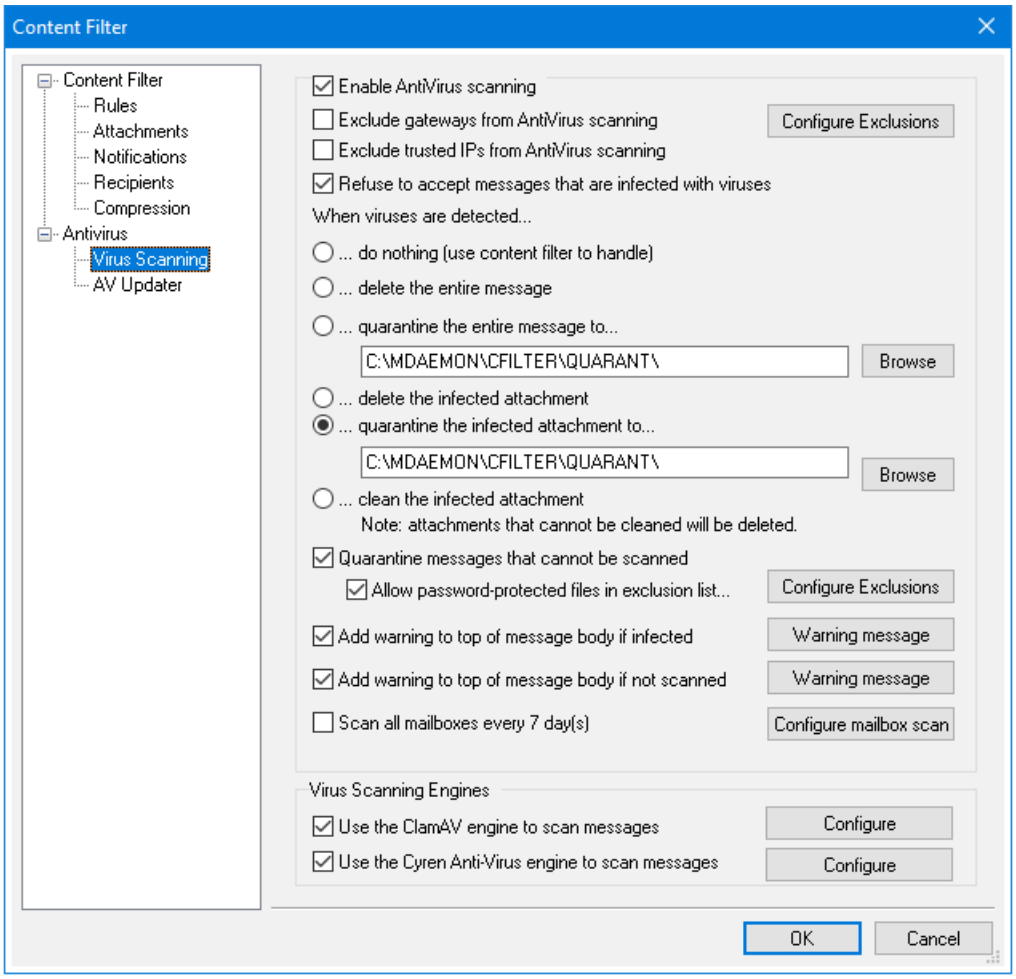
排除这些域...
点击此按钮指定收件人的域，这些域的邮件是你希望从自动压缩中排除的。对这些域的邮件发送将不会把他们的文件附件压缩，无论您的压缩设置如何。

Winmail.dat 附件

从 winmail.dat 提取文件附件 (Outlook RTF 邮件)
如果您希望从 winmail.dat 附件中提取文件并将其转换为标准的 MIME 邮件附件，请启用此选项。

4.5.2 AntiVirus

4.5.2.1 病毒扫描



只有在使用可选的 MDaemon AntiVirus 558 功能时此屏幕上的选项才可用。初次启用 MDaemon AntiVirus 将开始 30 天试用。如果您希望购买此功能，请联系您的授权 MDaemon 经销商或访问：www.mdaemon.com。

启用反病毒扫描

点击此复选框启用 AntiVirus 邮件扫描。当 MDaemon 收到一封带有附件的邮件时，在递送邮件到其最终目标前，将对它们进行病毒扫描。

从反病毒扫描中排除网关

若您希望对 MDaemon的域网关之一绑定的邮件免除病毒扫描，点击此选择框。对于那些希望将邮件扫描给给域所在的自身邮件服务器来完成的人来说，这一点是非常理想的。更多域网关信息，请参阅网关管理 206。

配置例外
点击配置例外按钮来指定无需进行病毒扫描的收件人地址。不对与这些地址绑定的邮件进行病毒扫描。在这些地址中允许通配符。因此你可以使用此功能来排除所有域或者交叉在全部所有域上的特殊的邮箱。例如，“*@example.com”或者“VirusArchive@*”。

从 AntiVirus 扫描排除可信 IP
如果您希望在邮件来自可信 IP 地址[435]时，将其从 AntiVirus 扫描中排除，请点击此勾选框。

拒收受病毒感染的邮件
如果您希望在 SMTP 会话过程中对入站邮件进行病毒扫描，而不是会话结束才进行，然后拒收包含病毒的邮件，请点击此选项。由于每封入站邮件在 MDaemon 官方地接受该邮件并结束会话之前已进行扫描，且发件服务器仍然对其负责—该邮件从技术上来说仍未投递。因此如果发现病毒，可彻底拒收该邮件。此外，因为该邮件被拒收，在此对话框中所列出的与反病毒相关的任何操作将不再执行。将不会执行隔离或者清除步骤，也不会发送通知邮件。这样可以大大减少受感染的邮件数量以及用户收到的病毒通知邮件的数量。

SMTP-(入站)日志将会反应出反病毒的过程。您可能会看到以下可能的结果：

- 扫描了邮件后发现该邮件受病毒感染
- 扫描了邮件后未发现有病毒
- 无法扫描邮件 (通常是由于无法打开/访问一个压缩文件或其他类型文件或者附件)
- 无法扫描邮件 (超出最大的尺寸限制)
- 在扫描过程中出错

当检测到病毒时...
点击在此部分中的此选项按钮之一来指定 MDaemon 在 AntiVirus 检测到病毒时，将会执行的操作。

...无操作 (使用内容过滤器来处理)
如果您不希望执行上述任何操作，而是希望在内容过滤规则中设置一些其他的操作，请使用此选项。

...删除整封邮件
在发现病毒时，此选项将会删除整封邮件，而不仅仅是附件。由于这样做是删除整封邮件，那么*“添加一个警告...”*选项将不能应用。但是，你仍可以通过使用通知标签上的控件，发送一封通知邮件给收件人。

...隔离整个邮件到...
此选项类似于上述*“删除整封邮件”*选项，但是邮件将会被隔离到指定位置并非删除。

...删除受感染的附件
此选项将会删除受感染的附件。邮件仍会被递送到收件人，但是将不会有感染的附件。您可以使用此对话框底部的*“添加一个警告...”*控制来添加文本到邮件中，以告知用户受感染的附件已被删除。

...隔离受感染的附件到...
如果你希望受感染的附件被隔离到一个位置，而不是删除或者清除，选择此选项并在提供的空白处指定那个位置。与 *"删除受感染的附件"* 选项类似，邮件将投递至收件人，但是其中不包括受感染的附件。

...清除受感染的附件
当选择此选项，AntiVirus 将会尝试清除（如禁用）此受感染的附件。如果附件无法被清除，那么它将被删除。

隔离无法扫描的邮件
启用此项时，MDaemon 将隔离无法进行扫描的任何邮件，例如一些邮件含有受密码保护的文件。

允许在例外列表中添加受密码保护的文件...
如果您希望允许那些含有受密码保护且无法扫描文件（这些文件名位于例外列表中）的邮件通过 AntiVirus 扫描程序，请使用此项。

配置例外
点击此按钮来打开并管理文件例外列表。将不扫描此列表中含有的文件名和文件类型。

如果受感染，将警告添加到邮件正文顶部
当选择了上方 *"...附件"* 选项之一时，如果你希望在曾经受感染的邮件递送到收件人之前，添加一些警告文本到曾受感染的邮件顶部，点击此选项。因此你可以通知收件人附件已经被除去，以及为什么这么做。

警告邮件...
当 *"添加一封警告邮件..."* 功能被使用时，点击此按钮显示将会被添加到邮件的警告文本。对此文本做出所需变更后，请点击 **"确定"** 来关闭此对话框并保存变更。

如果未扫描，将警告添加到邮件正文顶部
如果启用此项，MDaemon 将在无法扫描的任何邮件的顶部添加一些警告文本。

警告邮件...
点击此按钮即可显示在无法扫描的邮件中添加的警告文本。对此文本做出所需变更后，请点击 **"确定"** 来关闭此对话框并保存变更。

扫描所有邮箱的间隔为每隔*n*天
如果您希望定期扫描所有存储的邮件，请选中此框以检测可能通过系统传播的任何受感染邮件，然后病毒定义更新可用于捕获邮件。受感染的邮件将被移至隔离文件夹并添加 X-MDBadQueue-Reason 报头，因此在 MDaemon 中查看时您可以看见相关说明。不会隔离无法扫描的邮件。

配置邮箱扫描。
点击此按钮可以指定您希望扫描邮箱的频率，以及您是希望扫描所有邮件还是只扫描那些小于特定天数的邮件。您也可以立即手动运行邮箱扫描。

病毒扫描引擎

MDaemon AntiVirus 配备了两款病毒扫描引擎：ClamAV 和 IKARUS Anti-Virus。启用这两个反病毒引擎时，将使用它们扫描邮件，IKARUS Anti-Virus 优先于 ClamAV 对邮件进行扫描。这提供了额外的保护层，因为在更新其他引擎的病毒定义之前，可能由其中一个引擎识别病毒。

使用 ClamAV 引擎来扫描邮件

如果您希望使用 ClamAV 引擎来扫描邮件是否存在病毒，请点击此选框。

配置

点击此按钮可访问一个选项，以激活 ClamAV 的调试日志记录。该日志文件将位于 MDaemon 的日志文件夹。

使用 IKARUS Anti-Virus 引擎来扫描邮件

如果您希望使用 IKARUS Anti-virus 引擎来扫描邮件是否存在病毒，请点击此选框。

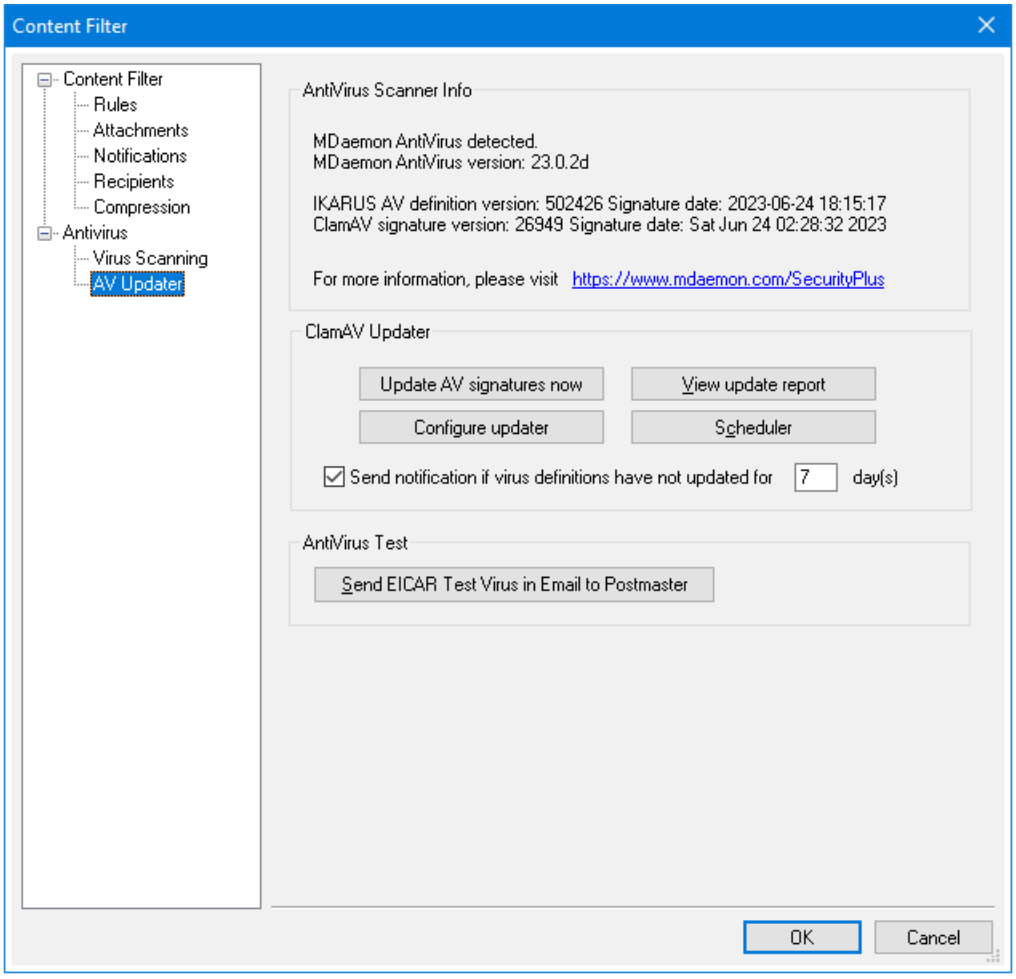
配置

如果您希望将所含文档带有宏的附件标记为病毒，请使用此选项。您可以在 -1 到 5 之间设置启发式级别。“1”是自动，“0”是禁用，并且 1-5 是从最低到最高的启发式级别。

还请参阅：

反病毒更新程序 562
内容过滤器与反病毒 539

4.5.2.2 反病毒更新程序



只有在使用可选的 MDaemon AntiVirus 558 功能时此屏幕上的一些选项才可用。初次启用 MDaemon AntiVirus 将开始 30 天试用。如果您希望购买此功能，请联系您的授权 MDaemon 经销商或访问：www.mdaemon.com。

使用此屏幕上的控制来手动或自动地更新您的病毒定义。这里有自动更新的调度程序，报告查看器可使您查看何时以及哪一个更新已经被下载，测试功能用来确认您的病毒扫描正在正常的工作。

反病毒扫描程序信息

这部分告诉您反病毒功能是否可用以及您正在运行哪个版本。它也将列出您最新病毒定义更新的日期。

ClamAV 更新程序

立即更新 AV 签名
点击此按钮手动更新病毒定义。在按下此按钮后，更新程序将会立即连接。

配置更新程序
点击此按钮打开更新程序配置对话框[564]。该对话框包含了四个选项卡：更新 URL、连接、代理服务器和其他。

查看更新报告
AntiVirus 日志查看器可以通过点击 *"查看更新报告"*按钮来打开。此查看器列出了次数，采取的动作，以及关于每个更新的其他信息。

调度程序
点击此按钮来打开 AntiVirus 调度[316]屏幕，用于在特定日期的特定时间安排对于病毒签名更新的检查或定期检查。

如果病毒定义在 xx 天未更新，则发送通知
默认情况下，如果 ClamAV 病毒定义在指定天数内未更新，管理员将收到通知。

反病毒测试

以邮件形式向管理员发送 EICAR 测试病毒
点击此按钮向管理员发送一封附有 EICAR 病毒文件的测试邮件。此附件是无害的——它仅仅用于反病毒测试。通过观察在 MDaemon 主界面上的 "内容过滤器"日志窗口，在接收邮件时，您可以看到 MDaemon 对其如何操作。例如，根据您的设置，您可以看到就像以下列出一样的一个日志摘录：

```
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 25.02.02 18:14:50: Processing complete (matched 0 of 12 active
rules)
```

还请参阅：

更新程序配置对话框 564
AntiVirus 558
内容过滤器与反病毒 539

4.5.2.2.1 更新程序配置对话框

点击 *"配置更新程序"*按钮（位于AV 更新程序 562）来打开 "更新程序配置"对话框。其中包含以下四个选项卡：

更新 URL
"更新 URL"选项卡是用来指定 AntiVirus 将检查更新的服务器。您可以设置检查服务器的顺序或以随机顺序检查这些服务器。

连接
"连接"选项卡用来指定您希望在连接更新站点时，AntiVirus 将使用的互联网连接配置文件。*"从控制面板中使用互联网设置"*选项使用您的默认互联网设置。可以使用 *"手动设置互联网设置"*选项和随后的控件来手动选择 "连接配置文件"，并指定其用户名和密码设置。

代理服务器
"代理服务器"选项卡包含用来配置任何 HTTP 或 FTP 代理服务器设置的选项，您当前的网络配置可能需要这些设置来连接更新站点。

其他
"其他"选项卡包含控制更新程序日志的选项。您可以选择将更新程序的行为记录到日志文件中，而且可以指定该文件的大小。

还请参阅：

反病毒更新程序 562
AntiVirus 558
内容过滤器与反病毒 539

4.6 垃圾邮件过滤器

4.6.1 垃圾邮件过滤器

"垃圾邮件过滤器"是 MDaemon 丰富的垃圾邮件防范工具组中的一项主要功能。它整合了启发式功能来检查入站邮件，以便基于一套复杂的规则系统来计算 "分数"。然后使用该分

数来确定邮件是否为垃圾邮件的可能性，并可基于该分数执行某些操作 — 拒绝邮件、将其标记为可能的垃圾邮件等等。

可以允许或阻止地址，或者将地址指定为完全免于垃圾邮件过滤器检查。您可将垃圾邮件报告插入邮件，以显示它们的垃圾邮件得分及其评判方式，或者您可将报告生成为单独的电子邮件并以原始垃圾邮件为附件。不仅如此，您甚至可以使用 "贝叶斯 568"学习来帮助 "垃圾邮件过滤器"随时间推移学习更为准确的识别垃圾邮件，并由此增强它的可靠性。

最后，通过检查数以千计的已知垃圾邮件，规则已随时间推移进行了优化，能非常可靠地检测出垃圾邮件的特征。不过，您可通过编辑 "垃圾邮件过滤器"的配置文件来定制或者添加新规则来满足特定需求。

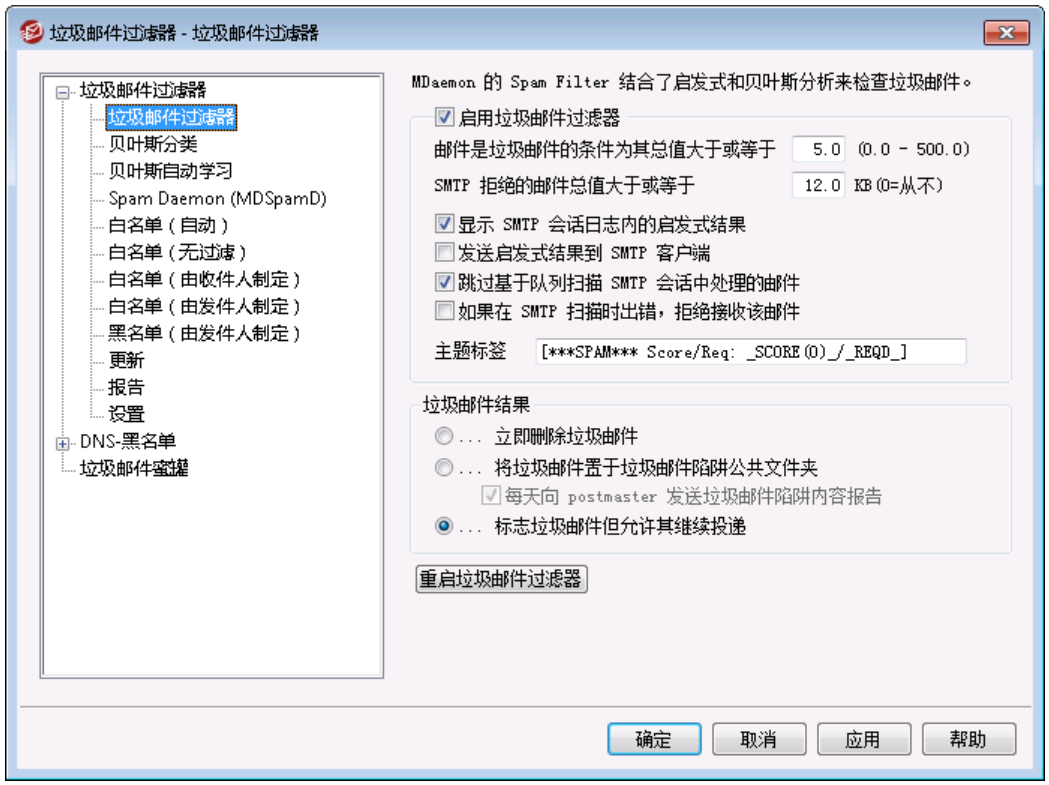
MDaemon 的 "垃圾邮件过滤器"使用集成的流行开源启发式技术。开源项目主页为：

http://www.spamassassin.org

还请参阅：

垃圾邮件过滤器 565
DNS 阻止列表 586

4.6.1.1 垃圾邮件过滤器



启用垃圾邮件过滤器

点击该复选框激活启发式邮件评分、垃圾邮件过滤系统。只有启用了该选项才能使用屏幕上的其他垃圾邮件过滤器选项。

如果邮件总分不小于 [XX] (0.0 - 500.0)则为垃圾邮件
在此指定的数值是所需的垃圾邮件阀值，MDaemon 将它与每封邮件的垃圾邮件总值进行比较。垃圾邮件总值不小于该数值的任何邮件将被视作垃圾邮件，然后基于其他垃圾邮件过滤器设置采取相应的操作。

SMTP 拒收总值不小于 XX 的邮件 (0= 从不)
使用该选项指定垃圾邮件拒收阀值。当邮件的垃圾邮件总值不小于该分数时，它将被彻底拒绝，而不是继续执行其余选项并有可能投递出去。该选项的数值应始终高于上述 *"如果邮件总分不小于…"*选项的数值。否则，邮件绝不会被视作垃圾邮件并应用垃圾邮件过滤器的其余选项——它将在投递过程中被直接拒收。如果希望在 SMTP 处理过程中禁用扫描，且不论邮件得分高低 Mdaemon 都不会拒收任何邮件，请在该选项中使用 "0"。如果禁用 SMTP 扫描，则在接收邮件后仍将对其执行基于队列的扫描。该选项的默认设置是 "12.0"。

举例来说，

如果垃圾邮件阈值设为 5.0，且拒收阈值设为 10.0，那么垃圾邮件总值在 10.0 以下但不低于 5.0 的任何邮件将被视作垃圾邮件，并根据垃圾邮件过滤器的其余设置进行处理。MDaemon 在投递过程中将拒收垃圾邮件总值不低于 10.0 的任何邮件。

您应监控垃圾邮件过滤器的长期性能，并调整垃圾邮件和拒收阈值以满足需求。然而，对于更多人，5.0这个垃圾邮件分数阀值能捉住更多的垃圾邮件，只具有极少漏检 (垃圾邮件未被识别)并且几乎没有任何误判 (邮件被错误的认为垃圾邮件)。10－15 的拒收阀值将使得只有那些几乎可以肯定的垃圾邮件被拒收。合法邮件得分会那么高的情况极其少见。默认拒收阈值是 12。

显示 SMTP 会话日志内的启发式结果
点击此选项即可将 SMTP 会话期间的启发式处理结果记录到 SMTP 会话日志 143。

将启发式结果发送至 SMTP 客户端
点击该选项显示在 SMTP 会话记录中内嵌的启发式处理结果。当垃圾邮件拒收阈值设为 "0"时该选项不可用，设为 "0"意味着垃圾邮件决不会因其分值而被拒收。更多信息，请参见上述的 *"SMTP 拒收总值不小于 XX 的邮件 (0=从不)"*。

跳过基于队列扫描 SMTP 会话中处理的邮件
默认情况下，MDaemon 在 SMTP 会话期间扫描邮件以确定是否因其垃圾邮件总值高于拒收阈值而拒收该邮件。对于被接受的邮件，MDaemon 还会执行另一个基于队列的扫描并根据其得分和垃圾邮件过滤器配置作相应处理。点击该选项，MDaemon 将忽略基于队列的扫描而将垃圾邮件过滤器初始扫描结果视为最终结果。这可能显著降低 CPU 占用率并提高反垃圾邮件系统的效率。然而当基于队列的扫描被忽略时，只有默认的 SpamAssassin 报头会被添加到邮件中。如果更改了默认的 SpamAssassin 报头或在 local.cf 文件中指定了自定义报头，这些更改和补充将被忽略。

如果在 SMTP 扫描时出错，拒绝接收该邮件
如果希望在 SMTP 处理过程中扫描邮件出错时拒收该邮件，请点击该选项。

主题标签
对于达到或超过所需垃圾邮件阈值的所有邮件，在其主题报头开头插入该标记。它可包含有关垃圾邮件总值的信息。您可使用 IMAP 邮件过滤器对其进行搜索并相应地过滤邮件（假设垃圾邮件过滤器配置为继续投递垃圾邮件）。这种简单的方法可自动路由垃圾邮件到指定的"垃圾邮件"文件夹。如果想要动态插入邮件的垃圾邮件总值和所需的垃圾邮件阈值，则可分别使用"_HITS_"标记（邮件总值）和"_REQD_"标记（所需阈值）。另外，可使用"_SCORE(0)_"代替"_HITS_"——它将在较低的分值前插入前导零，从而有助于确保在某些邮件客户端中按主题排列邮件时有正确的排列顺序。

举例来说，

如果主题标记设为：***SPAM*** Score/Req: _HITS_/_REQD_ -
则分值为 6.2 的垃圾邮件其主题："嘿，这里有些垃圾邮件！"将被更改为
"***SPAM*** Score/Req: 6.0/5.2 - 嘿，这里有些垃圾邮件！"

如果用"_SCORE(0)_"代替"_HITS_"，则将改为"***SPAM*** Score/Req: 06.2/5.0 - 嘿，这里有些垃圾邮件！"

如果不想更改主题报头，则将该选项留空。这样不会插入任何主题标记。

如果 MDaemon 已配置为使用其他服务器的 MDaemon Spam Daemon (MDSpamD) 来进行垃圾邮件过滤处理，则该选项不可用。主题标记的配置将取决于其他服务器的设置。还请参阅：垃圾邮件守护进程 573 了解更多信息。

垃圾邮件处理

如果邮件的垃圾邮件分数大于或等于在上方指定的垃圾邮件分数，垃圾邮件过滤器将会执行以下选定操作。

...立即删除垃圾邮件
如果希望简便地删除垃圾邮件分数等于或超过指定限值的所有入站邮件，请选择该选项。

...将垃圾邮件置于垃圾邮件陷阱公共文件夹
如果想要标记邮件为垃圾邮件，然后将其移入垃圾邮件公共文件夹，而不是允许其被投递，请选择该选项。

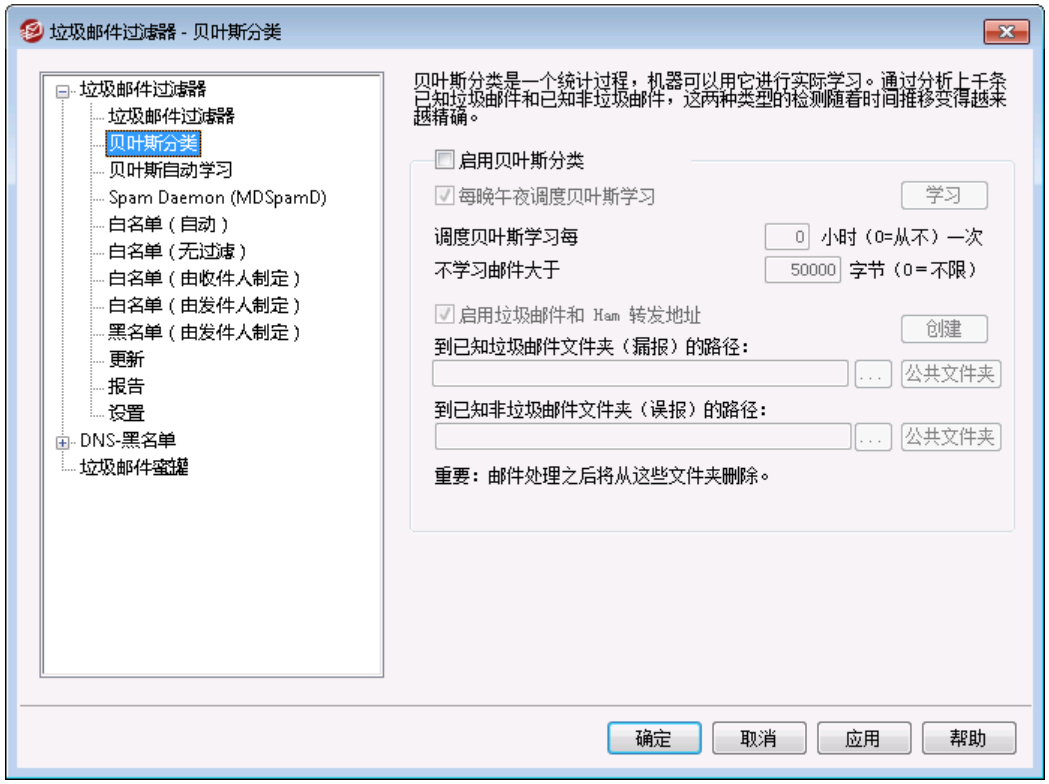
每天向邮件管理员发送垃圾邮件陷阱内容报告
当使用上述*...将垃圾邮件置于垃圾邮件陷阱公共文件夹*选项时，如果想让 postmaster 每天收到有关该文件夹内容摘要的邮件，请选中该复选框。

...标志垃圾邮件但任其继续向下传递
如果希望继续投递每封垃圾邮件到其预定收件人，同时通过插入报告 583 屏幕上指定的各种垃圾邮件报头和/或标记，将其标记为垃圾邮件，请选择该选项。这是默认选项，为用户提供更多选择，例如将邮件过滤到垃圾邮件文件夹以便查看，这样就避免了可能丢失被错误标记为垃圾邮件的邮件（例如误报）。

重启垃圾邮件过滤器

点击此按钮来重启“垃圾邮件过滤器”引擎。

4.6.1.2 贝叶斯分类



如果 MDaemon 已配置为使用其他服务器的 MDaemon Spam Daemon (MDSpamD) 来进行垃圾邮件过滤处理，则贝叶斯分类不可用。所有的贝叶斯学习将在另一台服务器上执行。要了解更多信息，请参阅垃圾邮件守护进程 573。

垃圾邮件过滤器支持贝叶斯学习，这是一个统计过程，可选择用于分析垃圾邮件和非垃圾邮件以便随着时间的推移提高垃圾邮件识别的可靠性。可以为垃圾邮件和非垃圾邮件指定文件夹，对其进行手动或定期的自动扫描。对这些文件夹中的所有邮件将作分析和索引，以便与新邮件进行统计比较，来确定其为垃圾邮件的可能性。然后垃圾邮件过滤器可以基于贝叶斯比较结果增加或者减少邮件的垃圾邮件分数。

垃圾邮件过滤器不会对邮件应用贝叶斯分类，直到对在贝叶斯自动学习 571 屏幕上指定数目的垃圾邮件和非垃圾邮件执行了贝叶斯分析。这样垃圾邮件过滤器才能有充足的统计信息库供进行贝

叶斯比较时来析取。一旦为系统提供了这些邮件供分析，就一切就绪可以开始将贝叶斯比较结果应用到每封入站邮件的垃圾邮件分数中。通过不断分析更多的邮件，贝叶斯分类将随着时间的推移变得更为准确。

贝叶斯分类

启用“贝叶斯”分类
如果希望基于同当前已知的贝叶斯统计信息的比较结果调整每封邮件的垃圾邮件分数，请点击该复选框。

每晚午夜调度“贝叶斯”学习
该选项有效时，每晚午夜垃圾邮件过滤器将会分析然后删除在下面指定的垃圾邮件和非垃圾邮件文件夹中包含的所有邮件。如果希望以其他时间间隔调度贝叶斯学习，请清除该选项并使用下面的*每隔 XX 小时调度贝叶斯学习*选项。如果不希望贝叶斯学习会自动发生，请清除该选项并在下面的选项中指定“0”小时。

每隔 XX 小时调度贝叶斯学习（0=从不）
如果希望贝叶斯学习以其他时间间隔而不是于每晚午夜发生，请清除上述选项并改在该选项中指定小时数。每次一到指定时间，垃圾邮件过滤器会分析然后删除在下面指定的垃圾邮件和非垃圾邮件文件夹中的所有邮件。如果不希望贝叶斯学习会自动发生，请清除上述选项并在该选项中指定“0”小时。

如果由于某些原因不希望邮件在分析后被删除，则可通过将 LEARN.BAT 复制到 \MDaemon\App\ 子目录中的 MYLEARN.BAT，然后删除靠近文件末尾以 "if exist" 开头的两行文本来实现。当文件夹中存在 MYLEARN.BAT 文件时，MDaemon 将使用该文件而不是 LEARN.BAT。更多信息，请参见 \MDaemon\SpamAssassin\ 子目录中的 SA-Learn.txt。

有关启发式垃圾邮件过滤技术和贝叶斯学习的更多详情，请访问：

http://www.spamassassin.org/doc/sa-learn.html

不要学习大于 XX 字节的邮件（0＝不限）
使用该选项为贝叶斯分析指定最大邮件尺寸。对大于该值的邮件不作分析。在该选项中指定“0”则不会应用任何尺寸限制。

学习
点击该按钮，启动对指定文件夹的手动贝叶斯分析，而不是等待进行自动分析。

启用垃圾邮件和非垃圾邮件转发地址
如果想让用户将垃圾邮件和非垃圾邮件（ham）转发到指定地址，以便贝叶斯系统可从中进行学习，请点击该复选框。MDaemon 使用的默认地址是“SpamLearn@<domain>”和“HamLearn@<domain>”。发往该地址的邮件必须通过 SMTP 从经 SMTP AUTH 验证过的会话上进行接收。不仅如此，MDaemon 希望该邮件作为

"message/rfc822"类型的附件转发给上述地址。发往该地址的邮件如果是其他类型则不作处理。

通过向 CFilter.INI 文件中添加以下键值可更改 MDaemon 使用的地址：

```
[SpamFilter]
SpamLearnAddress=MySpamLearnAddress@
HamLearnAddress=MyNonSpamLearnAddress@
```

请注意：最后一个字符必须为"@"。

创建
点击该按钮自动创建垃圾邮件和非垃圾邮件公共 IMAP 文件夹[95]，并配置 MDaemon 加以使用。将会创建以下文件夹：

\Bayesian Learning.IMAP\	IMAP 根文件夹
\Bayesian Learning.IMAP\Spam.IMAP\	该文件夹用于漏报（垃圾邮件得分不够高，未能被标记为垃圾邮件）。
\Bayesian Learning.IMAP\Non-Spam.IMAP\	该文件夹用于误报（非垃圾邮件错误地获得高分数，而被标记为垃圾邮件）。

默认情况下，这些文件夹的访问权限只授予本地域的本地用户，并仅限于查找和插入。邮件管理员的默认权限是查找、读取、插入和删除。

到已知垃圾邮件文件夹（漏报）的路径：
这是用于对已知垃圾邮件进行贝叶斯分析的文件夹路径。仅将您所认为的垃圾邮件复制到此文件夹。不应自动执行把邮件复制到此文件夹的过程，除非通过贝叶斯自动学习[571]或垃圾邮件蜜罐[592]选项来进行。以其他方式自动执行该过程可能会导致非垃圾邮件被作为垃圾邮件来分析，这会降低贝叶斯统计的可靠性。

到已知非垃圾邮件文件夹（误报）的路径：
这是用于对决非垃圾邮件的合法邮件进行贝叶斯分析的文件夹路径。只有您认为非垃圾邮件的合法邮件才应复制到此文件夹。不应自动执行把邮件复制到此文件夹的过程，除非通过贝叶斯自动学习[571]选项来进行。以其他方式自动执行该过程可能会导致垃圾邮件被作为非垃圾邮件来分析，这会降低贝叶斯统计的可靠性。

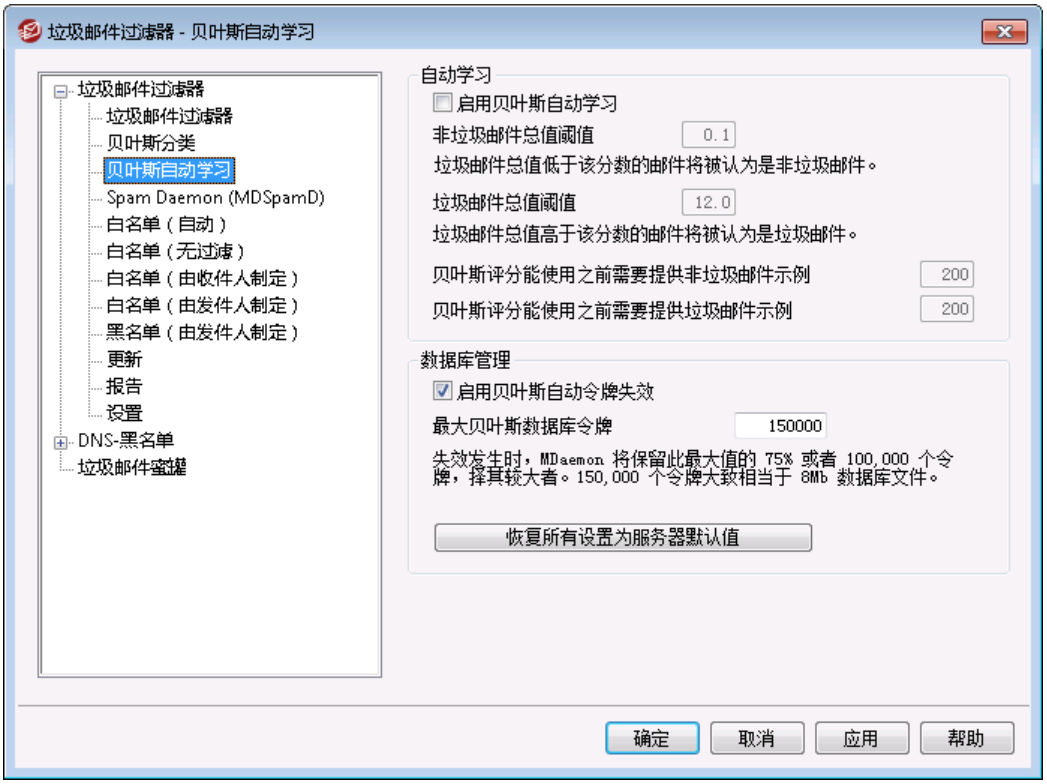
公共文件夹
点击这些按钮可将某个现有公共文件夹指定为贝叶斯目录。这使得用户可方便地将归类有误的垃圾邮件和非垃圾邮件放入贝叶斯目录供分析。但是，请注意，获得权限的人越多，因邮件被放入错误的文件夹而误导统计并降低可靠性的概率就越大。

如果通过邮件客户端、Windows 资源管理器或其他方式重命名公共文件夹，则必须手动将该路径重置为相应的新文件夹名称。如果您重命名一个文件夹但没有在此改变它的路径，垃圾邮件过滤器将会为贝叶斯文件夹继续使用此路径而替代新的。

还请参阅：

贝叶斯自动学习 571
垃圾邮件蜜罐 592

4.6.1.3 贝叶斯自动学习



如果 MDaemon 已配置为使用其他服务器的 MDaemon Spam Daemon (MDSpamD) 来进行垃圾邮件过滤处理，则贝叶斯自动学习不可用。所有的贝叶斯学习将在另一台服务器上执行。要了解更多信息，请参阅垃圾邮件守护进程 573。

自动学习

启用“贝叶斯”自动学习
使用自动贝叶斯学习，可指定垃圾邮件和非垃圾邮件评分阈值，从而使贝叶斯学习系统能自动学习邮件，而无需手动将邮件放入垃圾邮件和非垃圾邮件文件夹。得分低于非垃圾邮件阈值的任何邮件将被自动学习系统视作非垃圾邮件，而得分高于阈值的邮件将被视作垃圾邮件。使用自动学习，可自动替换从数据库中删除的过期旧令牌 *参见下面的数*

据库管理)。这样可以阻止手动训练覆盖过期标记的需求。如果您仔细设置阈值以避免在文件夹中不合适地分类邮件，自动学习十分有用。

非垃圾邮件总值阈值
垃圾邮件分数低于该值的邮件将会被贝叶斯分类系统视作非垃圾邮件。

垃圾邮件总值阈值
垃圾邮件分数高于该值的邮件将会被贝叶斯分类系统视作垃圾邮件。

"贝叶斯"评分实施之前需要非垃圾邮件样本
垃圾邮件过滤器不会对邮件应用贝叶斯分类，直到贝叶斯系统已经分析了这些数量的非垃圾邮件（以及在下一个选项中指定的垃圾邮件）。这样垃圾邮件过滤器才能有充足的统计信息库供进行贝叶斯比较时来析取。一旦为系统提供了这些邮件供分析，就一切就绪可以开始将"贝叶斯"比较结果应用到每封入站邮件的垃圾邮件分数中。通过不断分析更多的邮件，贝叶斯分类将随着时间的推移变得更为准确。

"贝叶斯"评分实施之前需要垃圾邮件样本
正如上一选项应用于非垃圾邮件，此选项用于指定在垃圾邮件过滤器开始对邮件应用贝叶斯分类之前必须分析的*垃圾邮件*数量。

数据库管理

启用贝叶斯自动令牌过期
如果希望每当达到以下指定的令牌数时，贝叶斯系统能使数据库令牌自动失效，请点击该选项。设置令牌限额可以防止贝叶斯数据库变得过大。

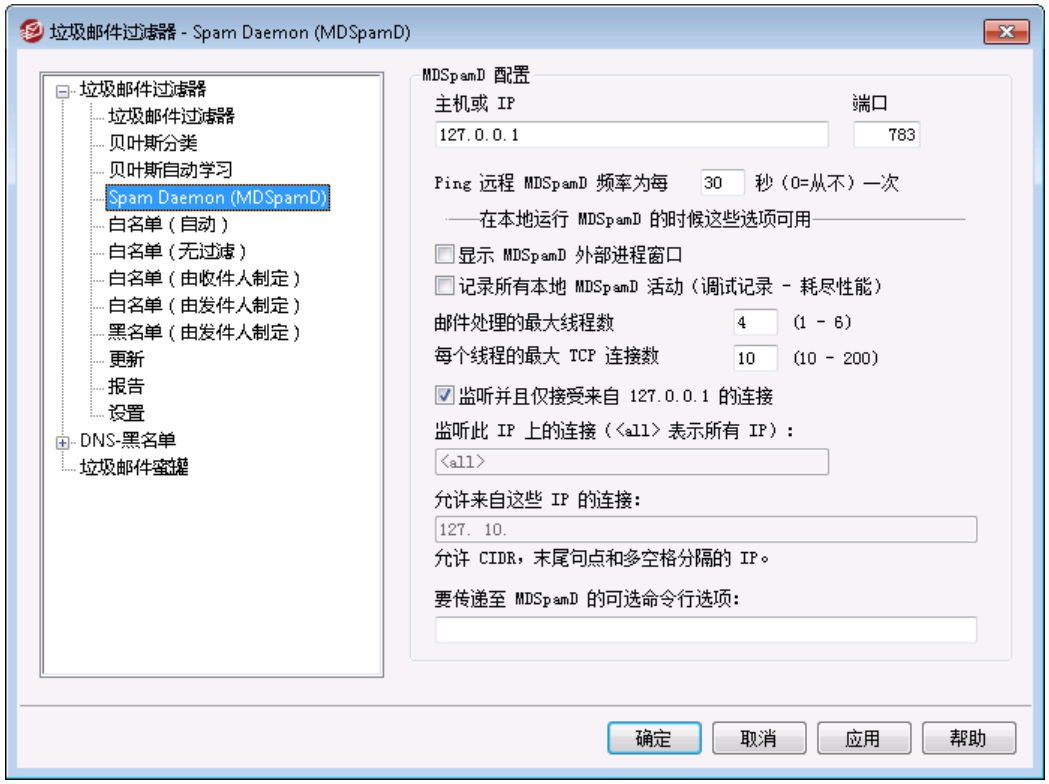
最大贝叶斯数据库令牌
这是所允许的最大贝叶斯数据库令牌数。当令牌数达到该限额时，贝叶斯系统会删除最旧的令牌，从而将令牌总数降至该值的 75% 或 100,000（二者取大）。无论有多少令牌过期，令牌数决不会低于此二值中的较大值。请注意：150,000 个数据库令牌约为 8MB。

恢复所有设置为服务器默认值
点击该按钮可将所有贝叶斯高级选项恢复为其默认值。

还请参阅：

贝叶斯分类 568
垃圾邮件蜜罐 592

4.6.1.4 垃圾邮件守护进程 (MDSpamD)



MDaemon 的垃圾邮件过滤系统作为独立的守护进程——MDaemon Spam Daemon (MDSpamD)——单独运行，可通过 TCP/IP 向其输送邮件供扫描。这极大地提高了垃圾邮件过滤器的性能，并使您得以在本地或另一台计算机上运行 MDSpamD，或让 MDaemon 使用在别处运行的其他 MDSpamD 或任何其他启用了 SpamD 的产品）。默认情况下，MDSpamD 在本地运行并使用地址 127.0.0.1 于端口 783 上接收邮件，但也可配置别的端口和 IP 地址，以将邮件发送到在别的位置或端口上运行的其他垃圾邮件守护进程。

MDSpamD 配置

主机或 IP
MDaemon 向该主机或 IP 地址发送邮件以供 MDSpamD 扫描。如果 MDSpamD 在本地运行，则使用 127.0.0.1。

端口
这是发送邮件使用的端口。默认的 MDSpamD 端口为 783。

每隔 XX 秒 Ping 远程 MDSpamD (0＝从不)
如果使用在远程位置上运行的垃圾邮件守护进程，可使用该选项定期 ping 其位置。如果不想 ping 该位置请使用 "0"。

在本地运行 MDSpamD 的时候这些选项可用

显示 MDSpamD 外部处理窗口
当 MDSpamD 在本地运行时，如果想让它运行在外部进程窗口，请启用该选项。该选项将导致 MDSpamD 的输出结果被输送到外部进程窗口，而不是 MDaemon 的内部用户界

面或日志系统。因为不必将 MDSpamD 的数据输送到 MDaemon 并记入日志，因此使用该选项可能会提高性能。不过日志文件不会被创建，因此该功能无法与下面的日志选项一起使用，同时 MDSpamD 数据也不会出现在 MDaemon 的 *"安全»MDSpamD"* 选项卡上。

记录所有本地 MDSpamD 活动 (调试记录——性能耗尽)
点击该选项将记录所有的 MDSpamD 活动。如果您正在使用上方的 *"显示 MDSpamD 外部进程窗口"*，则此项不可用。此外，如果使用 Windows 服务 341 对话框上的用户凭证而不是在 SYSTEM 账户下运行 MDaemon，则不会记录 MDSpamD 活动日志。

当使用该日志选项时，可能会发现邮件系统性能降低了，这取决于具体系统和活动程度。一般此选项被用来调试记录。

最大邮件处理线程数 (1-6)
这是 MDaemon 用于内部处理的最大线程数。可将该值设为 1 到 6 个线程。

每个线程的最大 TCP 连接数 (10-200)
这是一个 MDSpamD 线程在分支成另一线程前可接受的最大 TCP 连接数。可将该值设为 10 到 200 个线程。

监听并且仅接受来自 127.0.0.1 的连接
如果不想让本地 MDSpamD 接受任何源自外部的连接，请点击该选项。仅允许来自运行 MDSpamD 的同一台计算机的连接。

监听该 IP 上的连接
如果禁用了上一选项，则可使用该选项绑定或限制连接到特定的 IP 地址。仅允许到指定 IP 地址的连接。如果不想限制 MDSpamD 到任何特定的 IP 地址，请使用 "<all>"。

允许来自这些 IP 的连接
MDSpamD 将接受来自这些 IP 地址的入站连接。来自其他 IP 地址的连接将被拒绝。如果希望允许来自其他服务器的连接以便共享垃圾邮件过滤器的处理，该选项将非常有用。

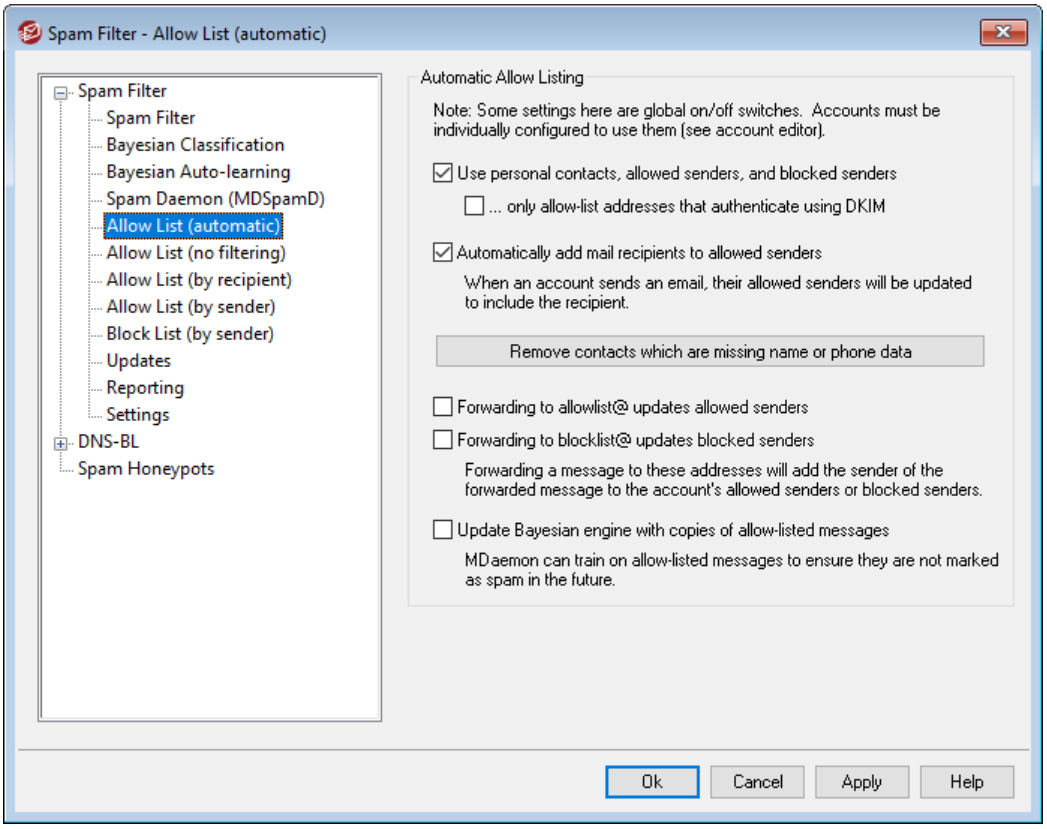
传递到 MDSpamD 可选命令行选项：
MDSpamD 可接受多种命令行选项，它们记录在：

http://spamassassin.apache.org/

如果要使用这些选项，请构建包含所需选项的字符串并放在这里。

其中某些选项可通过该对话框上的设置进行配置，因而无需使用命令行选项来手动设置。

4.6.1.5 允许列表（自动）



自动允许列表

使用个人联系人、已允许发件人和已阻止发件人
点击此选项，可使用每个用户的个人联系人，以及该用户垃圾邮件过滤的已允许和已阻止发件人。对于每封入站邮件，MDaemon 将在收件人账户的联系人、已允许和已阻止发件人列表中搜索邮件的发件人。如果找到发件人，则该邮件将被自动允许或阻止。如果您不希望将自动列入允许和阻止列表应用于每个 MDaemon 用户，则可通过清除 *"垃圾邮件过滤器"使用私人联系人、已允许发件人和已阻止发件人*选项（位于"账户编辑器"[允许列表](#) 637屏幕上），为个别用户禁用该功能。

...仅允许列表地址使用 DKIM 进行验证
启用该选项时，MDaemon 只将通过[域名秘钥标识邮件](#) 442（DKIM）"验证了发件人的那些邮件列入允许列表。该选项有助于避免将含有欺诈性地址的邮件列入允许列表。默认情况下，禁用该选项。

自动添加指向已允许发件人的邮件收件人
启用此选项后，每当用户向任何非本地电子邮件地址发送邮件时，MDaemon 都会自动将该收件人添加到用户的已允许发件人列表中。当结合使用上述 *"使用私人联系人、已允许发件人和已阻止发件人"*选项时，可大幅减少"垃圾邮件过滤器"的误报数量。

如果您不希望将此项应用于每个 MDaemon 用户，则可通过清除 *"自动添加指向已允许发件人的邮件收件人"*选择框（位于"账户编辑器"的[允许列表](#) 637屏幕上）。

为使用自动应答器的账户禁用该选项。

删除缺少姓名或电话数据的联系人
如果您希望将仅包含电子邮件地址的每位联系人从用户默认的联系人文件夹中删除，请点击此按钮。如果联系人连姓名或电话数据都没，则会将其删除。该选项主要是帮助那些在版本11之前已使用 MDaemon 自动列入允许列表选项的用户，纯粹作为用以清理联系人的允许列表功能而添加。在之前版本的 MDaemon 中，将地址添加到主要联系人而不是专用的已允许发件人文件夹。这可能导致用户在其联系人中拥有大量本不应位于那里的条目。

慎用此选择项，因为仅包含电子邮件地址的联系人也有可能是合法的。

转发到允许列表@ 更新已允许发件人
启用此项时，使用“账户编辑器”中“设置”屏幕上的“*垃圾邮件过滤器使用私人联系人、已允许发件人和已阻止发件人*”的账户可以将邮件转发至“allowlist@<domain>”，而且 MDaemon 会将原始邮件的发件人添加到此账户的已允许发件人中。已允许的地址取自转发邮件的 From 报头。

转发到“allowlist@<domain>”的邮件必须作为“message/rfc822”类型的附件转发，且必须由 MDaemon 通过 SMTP 从经身份验证的会话上来接收。转发的邮件达不到这些要求将不作处理。

通过编辑 CFilter.INI 文件中的下列键值可更改 MDaemon 使用的地址：

```
[SpamFilter]
WhiteListAddress=MyAllowListAddress@
```

请注意： 最后一个字符必须为“@”。

转发到阻止列表@ 更新已阻止发件人
启用此项时，使用“账户编辑器”中“设置”屏幕上的“*垃圾邮件过滤器使用私人联系人、已允许发件人和已阻止发件人*”的账户可以将邮件转发至“blocklist@<domain>”，而且 MDaemon 会将原始邮件的发件人添加到此账户的已阻止发件人中。已阻止的地址取自转发邮件的 From 报头。

转发到“blocklist@<domain>”的邮件必须作为“message/rfc822”类型的附件转发，且必须由 MDaemon 通过 SMTP 从经身份验证的会话上来接收。转发的邮件达不到这些要求将不作处理。

用允许列表上的邮件副本更新贝叶斯引擎
选中该复选框会导致合格邮件被自动复制到贝叶斯非垃圾邮件学习文件夹（在贝叶斯 568 屏幕上指定）。这有助于自动化为贝叶斯引擎提供非垃圾邮件样本的流程。定期为贝叶斯引擎提供非垃圾邮件的新实例供学习将会随时间推移提高其可靠性并有助于减少误报（即错误地归类为垃圾邮件的正常邮件）数量。

要应用该功能，入站邮件必须是发给一个本地用户，且发件人必须在其地址簿文件或已允许发件人文件夹中。如果是出站邮件，则必须是收件人在地址簿或已允许发件人中。

如果希望任何出站邮件都不够格，则可使用记事本来编辑 CFILTER.INI 文件中的如下设置：

```
[SpamFilter]
UpdateHamFolderOutbound=No （默认 = Yes）
```

当邮件够格时，即使在贝叶斯屏幕上禁用了贝叶斯调度学习，该邮件也将被复制到贝叶斯非垃圾邮件学习文件夹中。因此，当稍后启用调度学习时，或当手动激活学习时，即预备好了一组非垃圾邮件随时可供分析。然而，不是每封合格的邮件都被复制到学习文件夹中。当激活该功能时，Mdaemon 将复制合格邮件直到达到指定数量。随后将以指定间隔复制单个邮件。默认情况下，最初的 200 封合格邮件将被复制，接着在之后的每十封合格邮件中复制第十封。初始复制数目等于在 *"贝叶斯评分前所需的非垃圾邮件样本"*选项 (位于贝叶斯自动学习 571 屏幕)中指定的数量。更改该设置也会更改此数值。如果想要更改后续邮件的复制间隔，则可编辑 MDaemon.ini 文件中的如下设置：

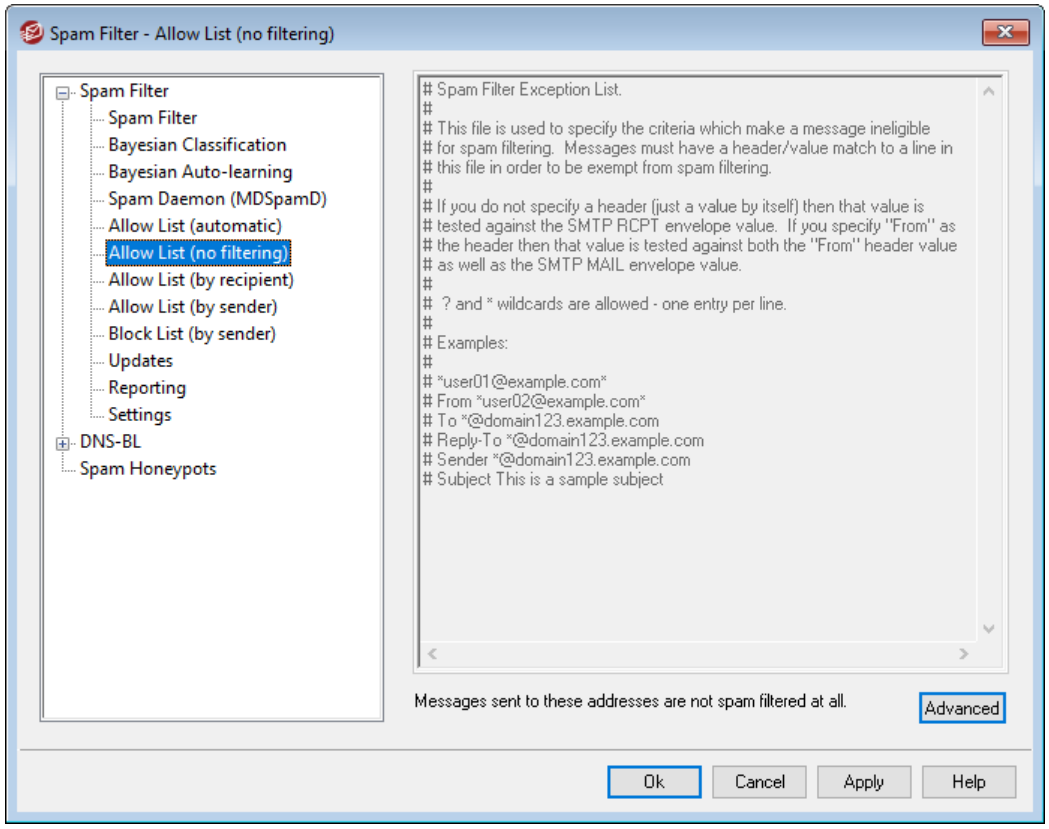
```
[SpamFilter]
HamSkipCount=10 （默认 = 10）
```

最后，一旦复制的邮件总数达到了指定值，整个过程将重新开始——200 封邮件将被复制，然后在每 10 封邮件中复制第 10 封 (或其他值，如果更改了设置的话)。默认情况下，当复制了 500 封合格邮件后，该过程将重新启动。要更改此数值，可编辑 MDaemon.ini 文件中的如下设置：

```
[SpamFilter]
HamMaxCount=500 （默认 = 500）
```

如果 MDaemon 已配置为使用其他服务器的 MDaemon Spam Daemon (MDSpamD) 来进行垃圾邮件过滤处理，则该选项不可用。所有的贝叶斯学习功能将取决于其他服务器的设置，并在其他服务器上执行。更多信息，请参阅垃圾邮件守护进程 573。

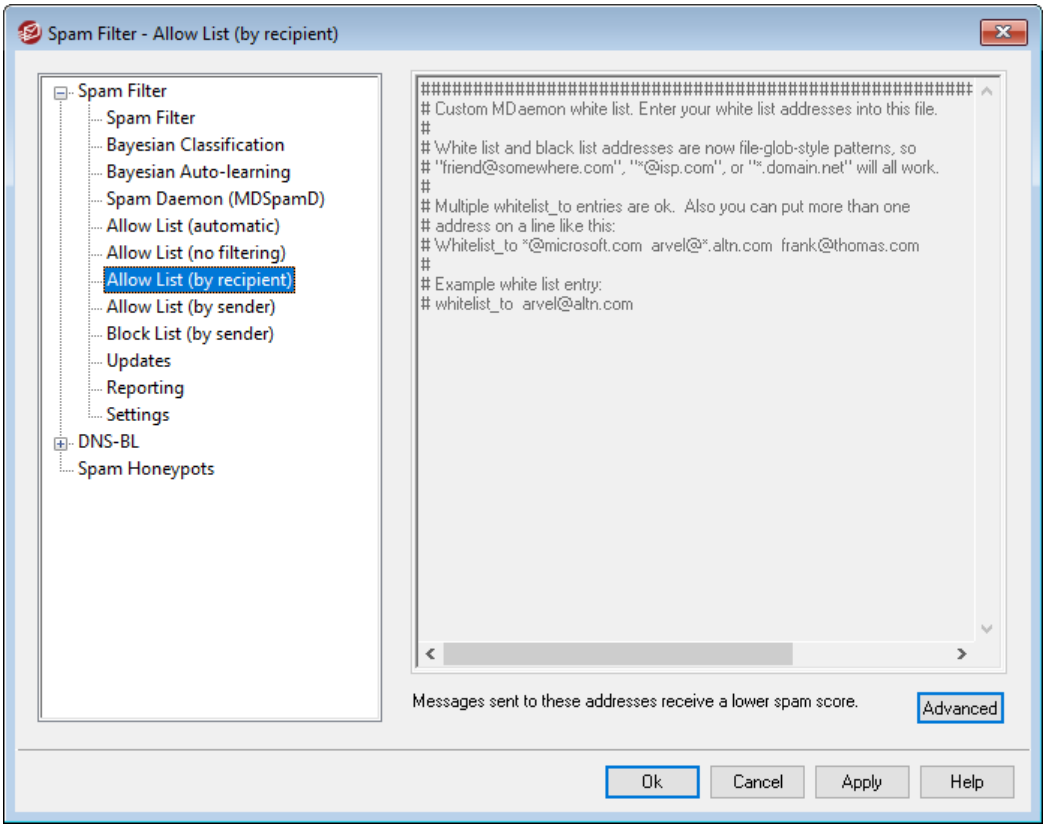
4.6.1.6 允许列表（无过滤）



完全不过滤发送至这些地址的邮件
点击此屏幕上的 **"高级"**来指定您希望免于垃圾邮件过滤的收件人地址。发送到这些地址的邮件不会经由垃圾邮件过滤器来处理。

如果 MDaemon 已配置为使用其他服务器的 MDaemon Spam Daemon (MDSpamD) 来进行垃圾邮件过滤处理，则该屏幕不可用。该垃圾邮件过滤器名单将保留在其他服务上。更多信息，请参阅垃圾邮件守护进程 573。

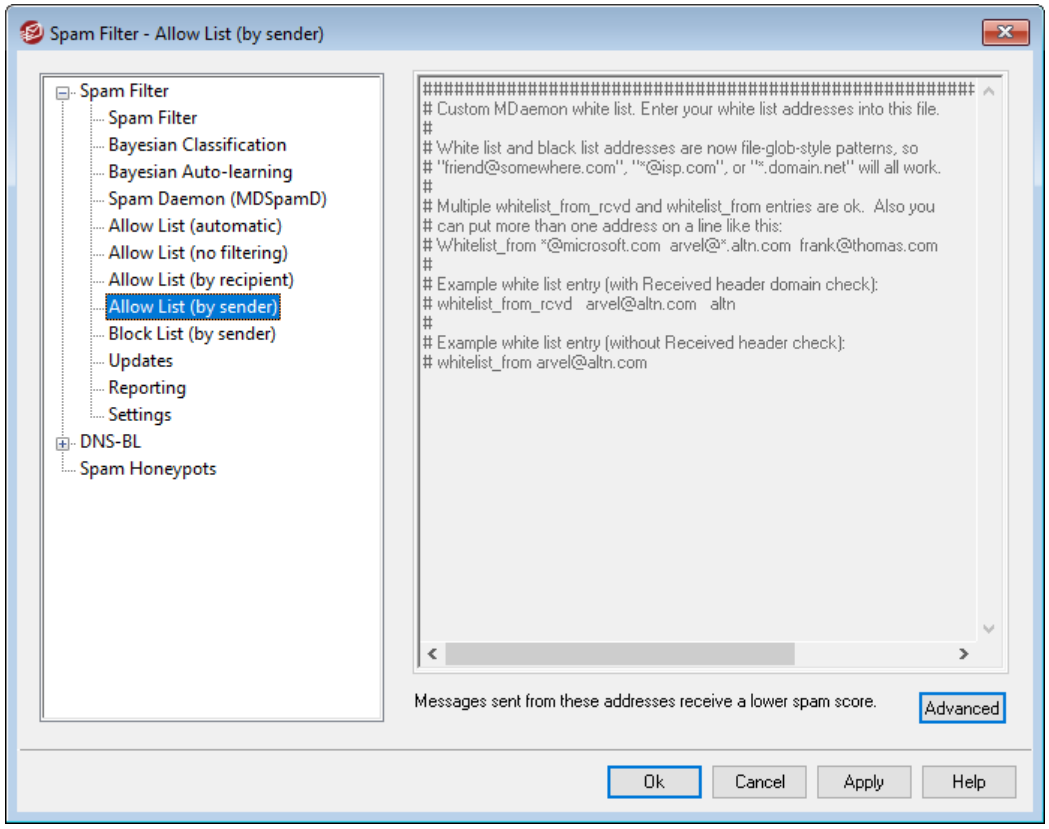
4.6.1.7 允许列表（按收件人）



发往这些地址的邮件获得有利的分数
点击 **"高级"**来将地址添加到这个列表。该列表与 *允许列表（无过滤）*[578]类似，除了该功能不使收件人的邮件免于 "垃圾邮件过滤器"处理，这些邮件将经过处理，不过将使其 "垃圾邮件过滤器总值"[565]按照在 "垃圾邮件过滤器设置"[584]屏幕上指定的值相应减少。因此，将地址包括在此允许列表上并不会自动保证发往该地址的邮件不会被视作垃圾邮件。例如，如果垃圾邮件阈值设为 5.0，且允许列表的值设为 100，然后传来一封特别恶劣的垃圾邮件，其垃圾邮件总值在减去允许列表分值之前为 105.0 或更高，那么该邮件最终的垃圾邮件总值将至少为 5.0，由此标志其为垃圾邮件。不过这种情况很罕见，因为垃圾邮件很少会有这么高的分值，除非它包含其他某些得分极高的元素，例如列入阻止列表的地址。

如果 MDaemon 已配置为使用其他服务器的 MDaemon Spam Daemon (MDSpamD) 来进行垃圾邮件过滤处理，则该屏幕不可用。该垃圾邮件过滤器名单将保留在其他服务上。更多信息，请参阅垃圾邮件守护进程[573]。

4.6.1.8 允许列表（按发件人）

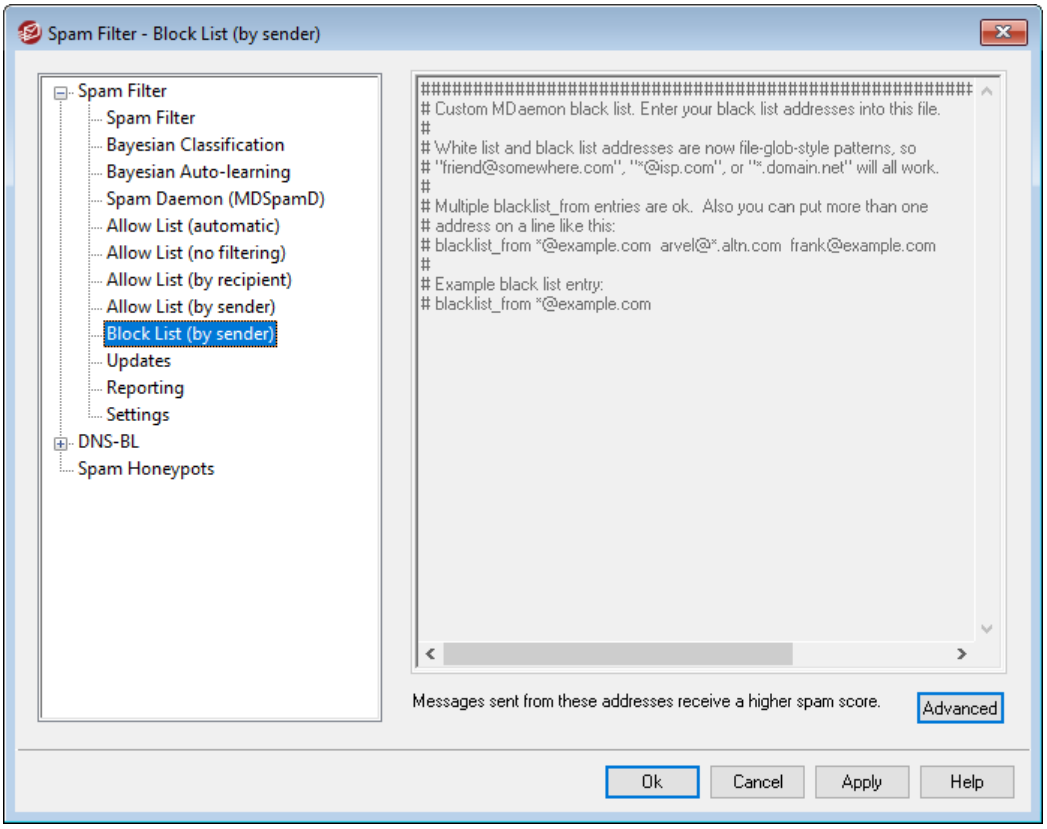


发自这些地址的邮件获得有利的分数

点击 "高级"来将地址添加到这个列表。这个允许列表与*允许列表（按收件人）*[579]类似，除了基于邮件的*发件人*而不是收件人来减少垃圾邮件分值以外。来自这些发件人的邮件将使其垃圾邮件过滤器总值[565]按照在 "垃圾邮件过滤器设置[584]"屏幕上指定的值相应减少。因此，将地址包括在此允许列表上并不会自动保证发往该地址的邮件不会被视作垃圾邮件。例如，如果垃圾邮件阈值设为 5.0，且允许列表的值设为 100，然后传来一封特别恶劣的垃圾邮件，其垃圾邮件总值在减去允许列表分值之前为 105.0 或更高，那么该邮件最终的垃圾邮件总值将至少为 5.0，由此标志其为垃圾邮件。不过这种情况很罕见，因为垃圾邮件很少会有这么高的分值，除非它包含其他某些得分极高的元素，例如列入阻止列表的地址。

如果 MDaemon 已配置为使用其他服务器的 MDaemon Spam Daemon (MDSpamD) 来进行垃圾邮件过滤处理，则该屏幕不可用。该垃圾邮件过滤器名单将保留在其他服务上。更多信息，请参阅垃圾邮件守护进程[573]。

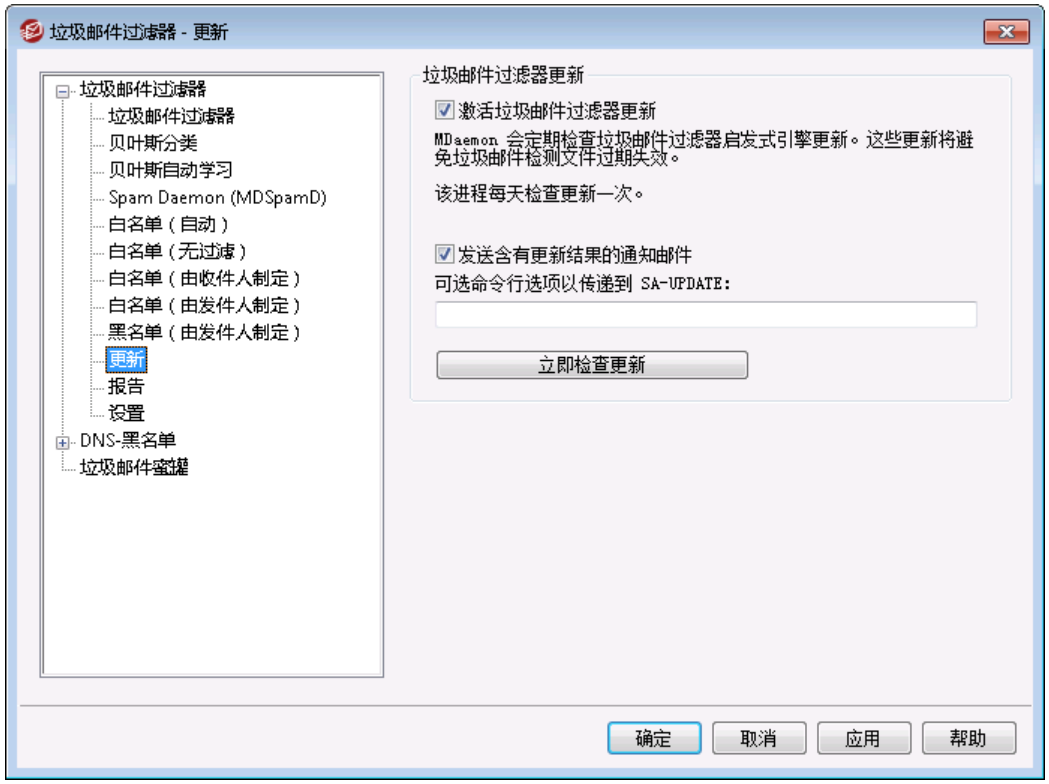
4.6.1.9 允许列表（按发件人）



发自这些地址的邮件将收到不利的分数
点击 **高级**”来将地址添加到该列表。邮件的发送地址被列于这个阻止列表，将使其 “垃圾邮件过滤器总值 565”按照在 “垃圾邮件过滤器设置 584”屏幕上指定的总量增加，这通常使其被标记为垃圾邮件。不过，将地址添加到该黑名单中并不会自动保证来自该地址的邮件将被视作垃圾邮件。例如，如果一封邮件来自被阻止的发件人，但是它指向允许的收件人，那么评分调整程序可以采取相互抵消的操作，并使该邮件的最终分值低于垃圾邮件的分值阈值。如果您将阻止列表评分调整程序设置得极低，也会发生这种情况。

如果 MDaemon 已配置为使用其他服务器的 MDaemon Spam Daemon (MDSpamD) 来进行垃圾邮件过滤处理，则该屏幕不可用。该垃圾邮件过滤器名单将保留在其他服务上。更多信息，请参阅垃圾邮件守护进程 573。

4.6.1.10 更新



垃圾邮件过滤器更新

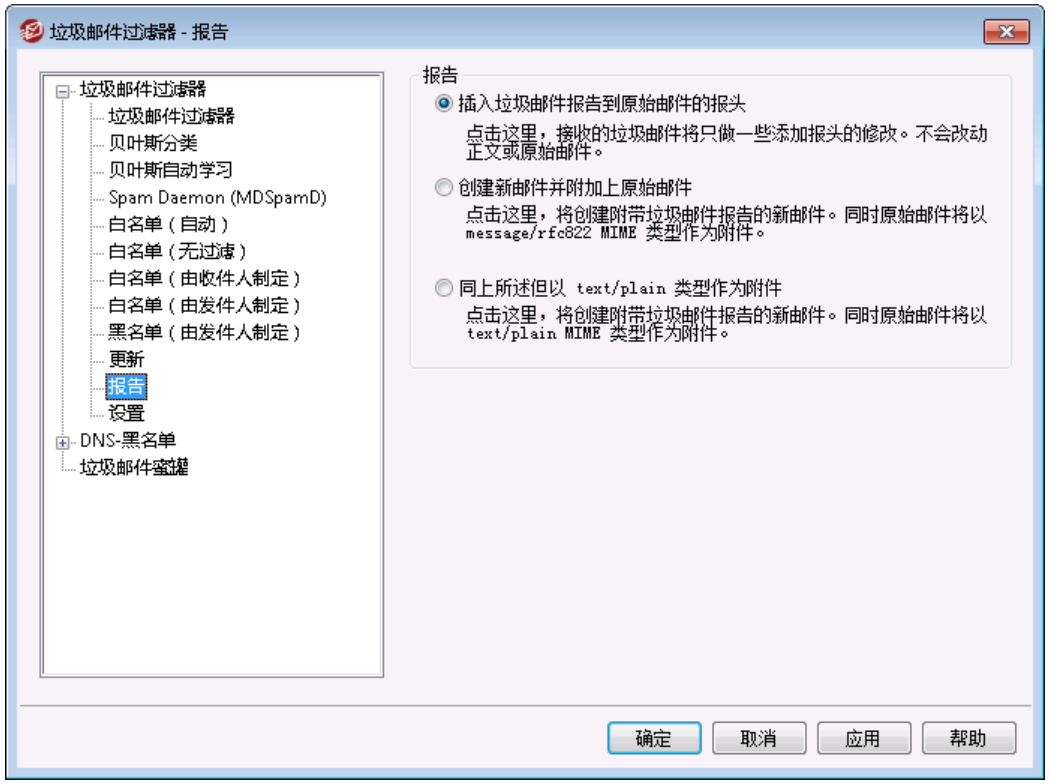
激活垃圾邮件过滤器更新
如果要自动更新垃圾邮件过滤器，请点击该复选框。MDaemon 每日一次检查是否有垃圾邮件过滤器启发式引擎的更新，如果有，将自动下载并安装更新。

发送含有更新结果的通知邮件
如果您希望每次在更新垃圾邮件过滤器时，向管理员发送一封含有更新结果的邮件，请使用此项。此项与 *"向管理员发送垃圾邮件过滤器更新通知"* 这一选项相同，该选项位于：内容过滤器» 通知。

传递到 SA-UPDATE 的可选命令行选项
如果您希望将任何命令行选项传递到 SA-UPDATE，请使用这个高级选项。

立即检查更新
点击该按钮立即检查垃圾邮件过滤器规则更新。

4.6.1.11 报告



如果 MDaemon 已配置为使用其他服务器的 MDaemon Spam Daemon (MDSpamD) 来进行垃圾邮件过滤处理，则垃圾邮件过滤器报告选项不可用。垃圾邮件过滤器报告将由其他服务器的设置来控制。要了解更多信息，请参阅垃圾邮件守护进程 573。

报告

插入垃圾邮件报告到原始邮件的报头
这是默认报告选项。如果想让垃圾邮件过滤器向每封垃圾邮件的报头插入垃圾邮件报告，请使用该选项。以下是一个简单的垃圾邮件报告示例：

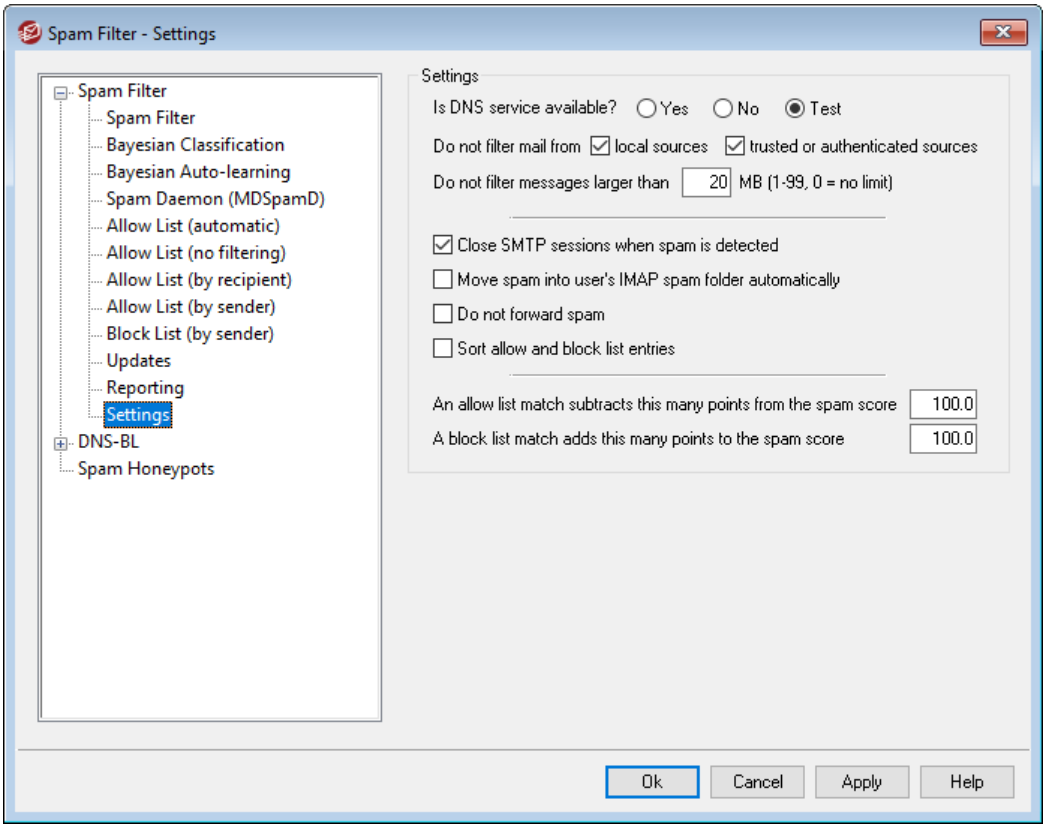
```
X-Spam-Report: ---- 垃圾邮件过滤器结果开始
 共 5.30 分，所需为 5 分；
 * -5.7 -- Message-Id 表明邮件发自 MS Exchange
 * 2.0 -- 主题包含大量空格
 * -3.3 -- 具有 In-Reply-To 报头
  *  3.0 -- MDaemon 的 DNS-BL 已对邮件作标记
  *  2.9 -- 正文：无效对策
  *  2.2 -- 正文：谈论活动时使用惊叹号！
  *  0.5 -- 正文：Message 80% 到 90% 是 HTML
  *  0.1 -- 正文：邮件包含 HTML
  *  1.6 -- 正文：HTML 邮件是保存的网页
  *  2.0 -- 日期：比 Received: 日期早 96 小时以上
```

---- 垃圾邮件过滤器结果结束

创建新邮件并附加上原始邮件
如果想让垃圾邮件创建包含垃圾邮件报告的新电子邮件，请选择该报告选项。原始垃圾邮件将作为附件包含在其中。

同上所述但以文本/纯文本类型作为附件
类似于前面的报告选项，该选项将为垃圾邮件报告生成新的邮件，并以原始垃圾邮件为附件。不同之处在于附加原始邮件时将使用 text/plain MIME 类型。因为垃圾邮件有时会包含 HTML 代码（它对于每封邮件都是独一无二的，并可能会向垃圾邮件制造者泄露将其打开的邮件和 IP 地址），因此该方法通过将 HTML 代码转换为纯文本可避免发生这种现象。

4.6.1.12 设置



设置

DNS 服务可用吗？
这些选项让您选择在垃圾邮件过滤器处理邮件时 DNS 是否可用。可以从如下选项中选择：

是——DNS 可用。SURBL/RBL 和其他需要 DNS 连接的规则因此可以使用。

否——DNS 不可用。需要用到 DNS 的垃圾邮件过滤器规则将无法使用。

测试——测试 DNS 的可用性，如果可用，将使用 DNS。这是默认设置。

不要过滤邮件，来自...

本地源
如果想让来自本地用户和域的邮件免于过滤，请点击该复选框。

可信或经验证的源
如果想让来自可靠域或已验证发件人的邮件免于垃圾邮件过滤，请启用该选项。

不过滤大于 [XX] MB 的邮件 (1-99, 0 = 无限制)
通常垃圾邮件制造者的目的是在最短的时间内投递尽可能多的邮件，因此垃圾邮件往往都非常短小。如果想让大于特定尺寸的邮件免于垃圾邮件过滤，则可在此指定大小（KB 为单位）。如果您不希望设置垃圾邮件过滤的邮件大小限制，则使用 "0"。

检测到垃圾邮件时关闭 SMTP 会话
默认情况下启用该选项，如果内联的扫描检测到垃圾邮件，则关闭 SMTP 会话。

将垃圾邮件自动移入用户的 IMAP 垃圾邮件文件夹
点击该选项，MDaemon 将自动把垃圾邮件过滤器确定的每封垃圾邮件放入每个用户的 "垃圾邮件" IMAP 文件夹中（如果此文件夹存在的话）。它还会为添加的每个新用户账户自动创建该文件夹。

当您点击该选项时，还会询问您是否想让 MDaemon 为每个业已存在的用户账户创建该文件夹。如果选择 "是"，则会为所有用户创建一个文件夹。如果选择 "否"，则只有在添加每个新用户时，才会创建文件夹。某些或所有用户业已存在的文件夹不会以任何方式被更改或者受到影响。

不转发垃圾邮件
如果不希望转发垃圾邮件，请点击该复选框。

排序允许和阻止列表条目
如果您希望排序垃圾邮件过滤器的允许和阻止列表条目，请使用此项。**请注意：**如果您已为文件添加了您自己的备注（以 # 开头的行），请启用此项来将这些行整理排序到文件顶部。默认情况下禁用此功能。如果您启用此项，将在您的允许或阻止列表文件下一次发生变化时执行排序。

如果已将 MDaemon 配置成使用其他服务器的 MDaemon Spam Daemon (MDSpamD) 来处理垃圾邮件过滤，此屏幕上的其余选项不可用。要了解更多信息，请参阅垃圾邮件守护进程 573。

一个允许列表匹配将在垃圾邮件总值里添加这些点数
将地址置于垃圾邮件过滤器的允许列表（按收件人）579或允许列表（按发件人）580屏幕并不会自动保证由该地址收发的邮件不会被视作垃圾邮件。相反，这些地址将只是从垃圾邮件总值中减去在该控件中指定的数值。例如，如果垃圾邮件总分阈值设为 5.0，而该值设成 100，然后传来一封特别恶劣的垃圾邮件，其垃圾邮件总值在减去允许列表分值之前为 105.0 或更高，那么该邮件的最终垃圾邮件总值将至少为 5.0 ——因此指示其为垃圾邮件。然而，这种情况很罕见，因为垃圾邮件很少有这么高的分值，除非它包含

其他某些得分极高的元素，例如其地址位于阻止列表上。当然，如果您将允许列表的减数设得极低，则这种情况的发生概率就会高很多。

如果想让发往特定收件人的邮件彻底规避垃圾邮件过滤器，而不只是调整其分数，请在 允许列表（无过滤）[578]屏幕上包括这些收件人地址。通过使用允许列表（自动）[575]屏幕上的选项，还可基于发件人为邮件免除垃圾邮件过滤器评分。

一个阻止列表匹配将在垃圾邮件总值里添加这些点数
该值将添加到来自阻止列表（按发件人）[581]屏幕上所列地址的邮件的垃圾邮件总值中。正如上述允许列表选项，将地址包括在“垃圾邮件过滤器”的阻止列表中并不保证来自该地址的邮件会被视作垃圾邮件。相反，在此选项中指定的分值将被添加到该邮件的垃圾邮件总值中，然后将用于确定是否是垃圾邮件。

4.6.2 DNS 阻止列表（DNS-BL）

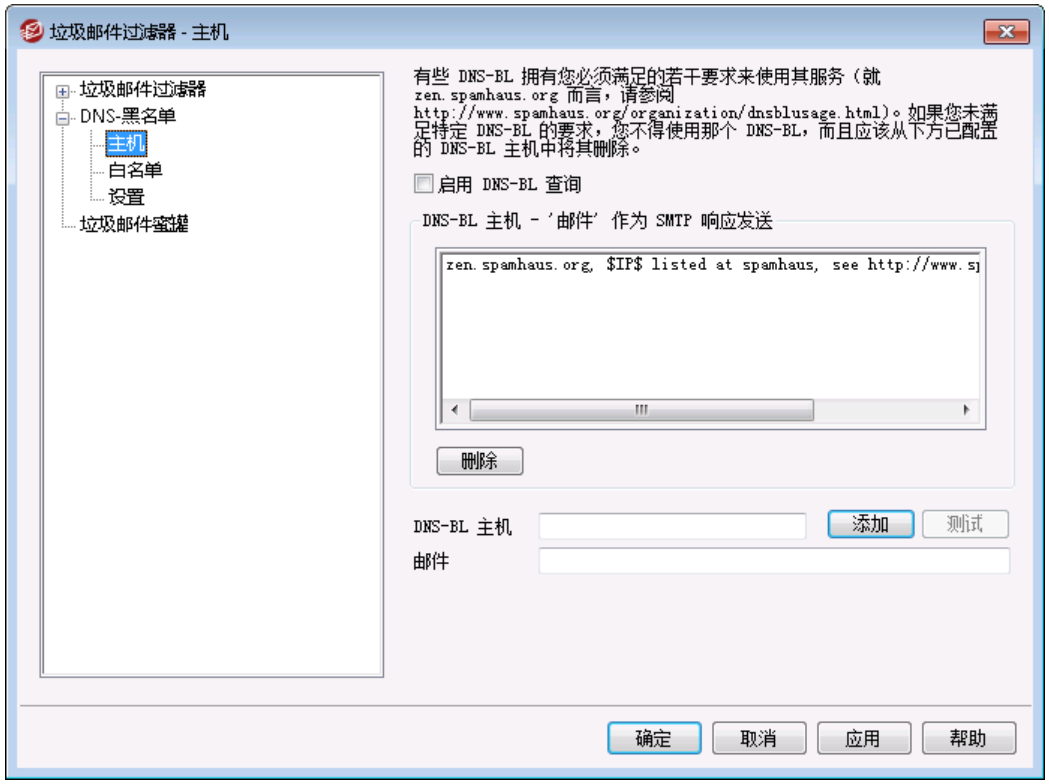
DNS 阻止列表（DNS-BL）能被用于防止大多数“垃圾邮件”到达您的用户。该安全功能允许您指定若干个 DNS 阻止列表服务（它们维持了中继垃圾邮件所知的服务器列表），每次有人试图发送邮件到您的服务器时，都将对该邮件进行安全性检查。如果连接 IP 已被这些服务的其中之一列入阻止列表，那么将根据设置[589]屏幕上的设置来拒收或标记邮件。

DNS 阻止列表包含一个“允许列表”来指定您希望豁免于 DNS-BL 查询的 IP 地址。在激活 DNS-BL 之前，您应该确保您的本地 IP 地址范围是在“允许列表”上的，从而防止对这些地址进行查询。"127.0.0.1"是被免除的，因此它不必被添加到此列表中。

还请参阅：

DNS-BL 主机[587]
DNS-BL 设置[589]
DNS-BL 允许列表[588]

4.6.2.1 主机



DNS-BL 主机

启用 DNS-BL 查询
如果您希望对照 阻止列表来检查入站邮件，请激活此项。MDaemon 在对一个发送 IP 地址执行 DNS-BL 查找时，将查询每个列出的主机。如果一个主机响应查询为一个正面的结果，MDaemon 可以标记或拒收该邮件，这取决于您在 DNS-BL 设置 589 屏幕上所启用的选项。

删除
从 DNS-BL 服务列表中选中一个条目，然后点击此按钮将它从列表中删除。

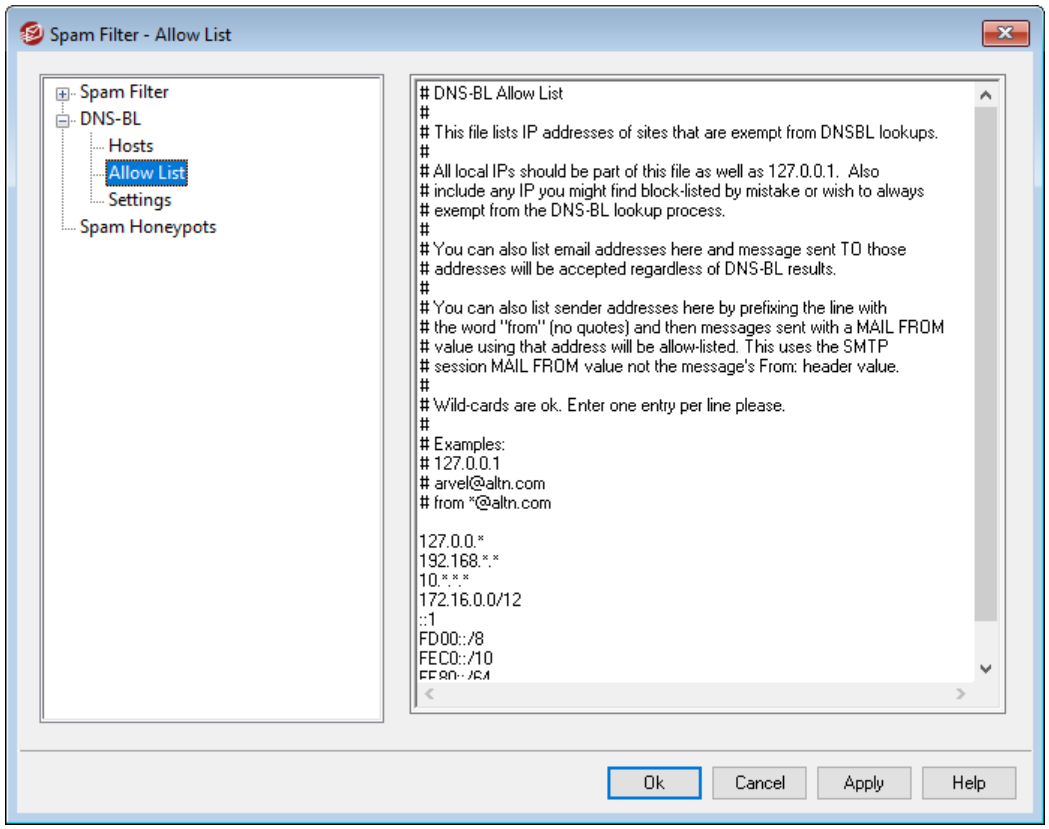
DNS-BL 主机
如果您希望添加一个新主机，它会被查询被列入阻止列表的 IP 地址，请在此输入。

测试
在 *"DNS-BL 主机"*选项中输入一个主机，并点击此按钮来通过查询 127.0.0.2 对其进行测试。

邮件
当一个 IP 地址被上方列出的相应 DNS-BL 主机列入上方的列表时，可以在 SMTP 会话中发送这封邮件。该邮件响应了...*应答 "邮件"而不是 "未知用户"*选项，该选项位于DNS-BL 设置 589 屏幕。

添加
在输入一个主机和返回邮件后，点击这个按钮来将其添加到 RBL 主机列表。

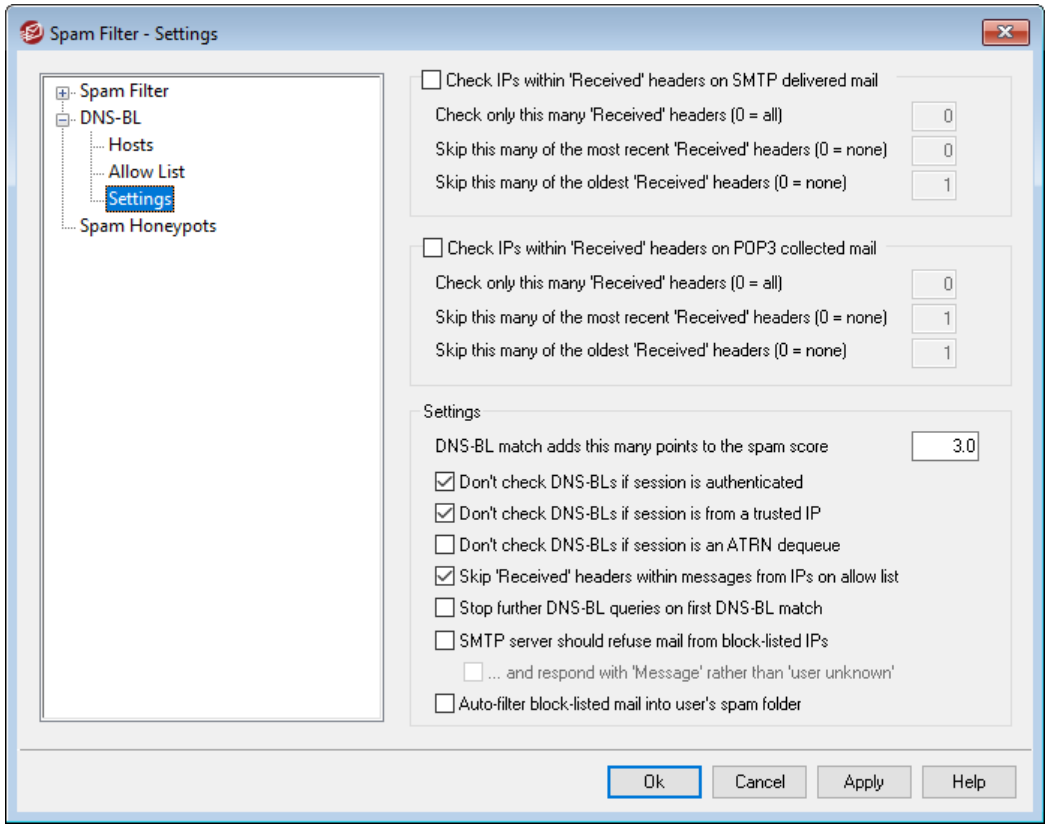
4.6.2.2 允许列表



使用此屏幕来指定从 DNS 阻止列表查询中将被豁免的 IP 地址。您应该总是包括您的本地 IP 地址范围来阻止 DNS-BL 查询来自本地用户和域的邮件（如 127.0.0.*, 192.168.*.* 等）。您也可以包含此列表上的邮件地址。存在一封指向这些地址的邮件时，将无论 DNS-BL 查询结果接收这封邮件。最后，您还可以在此列表上输入 "from *sender@example.com*"来使特定的发件人免于 DNS-BL 结果。该地址必须匹配 SMTP 会话的 "MAIL FROM"值，而不是邮件的 "From:"报头中的地址。

每行只放置一个条目。允许通配符。

4.6.2.3 设置



检查以 SMTP 投递的邮件中“已接收”报头内的 IP。
如果您希望 DNS 阻止列表检查通过 SMTP 收到的邮件中“已接收”报头内标出的 IP 地址，请点击此项。

仅检查这些数量的“已接收”报头（0 = 所有）
指定您希望 DNS-BL 检查的最近“已接收”报头的数目。“0”值表示将检查所有的“已接收”报头。

跳过这些最近的“已接收”报头（0 =都不）
如果您希望在 DNS-BL 检查 SMTP 邮件时，让其跳过一个或多个最近的已接收报头，请使用此选项。

跳过这些最旧的“已接收”报头（0 = 都不）
如果您希望在 DNS-BL 检查 SMTP 邮件时，让其跳过一个或多个最旧的“已接收”报头，请使用此选项。

检查以 POP3 收集的邮件中“已接收”报头内的 IP。
启用此切换时，DNS-BL 将检查通过 DomainPOP 与 MultiPOP 收集的邮件中“已接收”报头内标出的 IP 地址。

仅检查这些数量的“已接收”报头（0 = 所有）
指定您希望 DNS-BL 检查的最近“已接收”报头的数目。“0”值表示将检查所有的“已接收”报头。

跳过这些最近的“已接收”报头 (0=都不)
如果您希望在 DNS-BL 检查 DomainPOP 与 MultiPOP 邮件时，让其跳过一个或多个最近的已接收报头，请使用此选项。通常很有必要跳过通过 POP3 收集的邮件 (例如 DomainPOP)中最近的已接收报头，此选项的默认设置为“1”。

跳过这些最旧的“已接收”报头 (0 = 都不)
如果您希望在 DNS-BL 检查 DomainPOP 与 MultiPOP 邮件时，让其跳过一个或多个“已接收”报头，请使用此选项。

设置

DNS-BL 匹配将在垃圾邮件总值里添加这些点数
使用此项来指定在找到 DNS-BL 匹配时，被添加到邮件的垃圾邮件分值 565 中的值。有时，垃圾邮件过滤器对邮件的启发式检查可能不会使其分数高到足以被视作垃圾邮件，但 DNS-BL 查询会显示它可能是垃圾邮件。因此，向垃圾邮件分值添加这个值有助于捕获未被检测到的一些遗漏的垃圾邮件。默认情况下 DNS-BL 匹配向垃圾邮件分值添加 3.0 点。

不检查 DNS-BLs 的前提为如果会话是...

已验证
如果您希望那些使用 AUTH 命令进行验证的会话免于 DNS-BL 查询，请点击此选择框。

来自可信 IP
如果您希望那些列在可信主机 434 屏幕上的地址免于 DNS-BL 查询，请点击此选择框。

ATRN 出队
如果您不希望对通过 ATRN 出队会话收集的邮件进行 DNS-BL 查询，请启用此选项。默认情况下，此设置为禁用状态，但是如果您的智能主机已经在对存储的邮件进行 DNS-BL 检查，则可以启用此设置。

跳过来自允许列表中 IP 的邮件内的“已接收”报头
启用此选项时，DNS-BL 不会检查从您列在 DNS-BL 允许列表 588 的 IP 地址所发送邮件内的“已接收”报头。

首次 DNS-BL 匹配后停止进一步 DNS-BL 查询
经常有多个主机被包含在 DNS-BL 处理的每封邮件的报头中，还存在多个被查询的 DNS-BL 服务。默认情况下，DNS-BL 将为邮件中的所有主机继续查询这些服务，无论找到多少个匹配。如果您希望 DNS-BL 一找到匹配就对任何给定的邮件停止查询这些服务，请点击此选项。

SMTP 服务器应拒收来自列入阻止列表 IP 的邮件
默认情况下不勾选此框，这就表示来自于列入阻止列表的 IP 地址的邮件在 SMTP 会话中将不会被拒收，不过会插入一个 X-MDDNSBL-Result 报头。您可以使用“内容过滤器”来搜索拥有此类报头的邮件，并根据您的需要来处理它们。您也可以使用以下*“将阻止列表中的邮件自动过滤到用户的垃圾邮件文件夹”*选项，将这些邮件自动过滤到每位用户的垃圾邮件文件夹。如果您希望 MDaemon 拒收来自阻止列表 IP 地址的邮件，而不是标记它们，请勾选此框。

因为某些 IP 地址会被错误地列入阻止列表，请慎用此选项。值得一提的是，除了标志邮件之外，您也可以基于 DNS-BL 结果调整其垃圾邮件总值，这可通过 *若匹配 DNS-BL 则添加这些点值到垃圾邮件总值*选项实现，其位于垃圾邮件过滤器 565屏幕上。

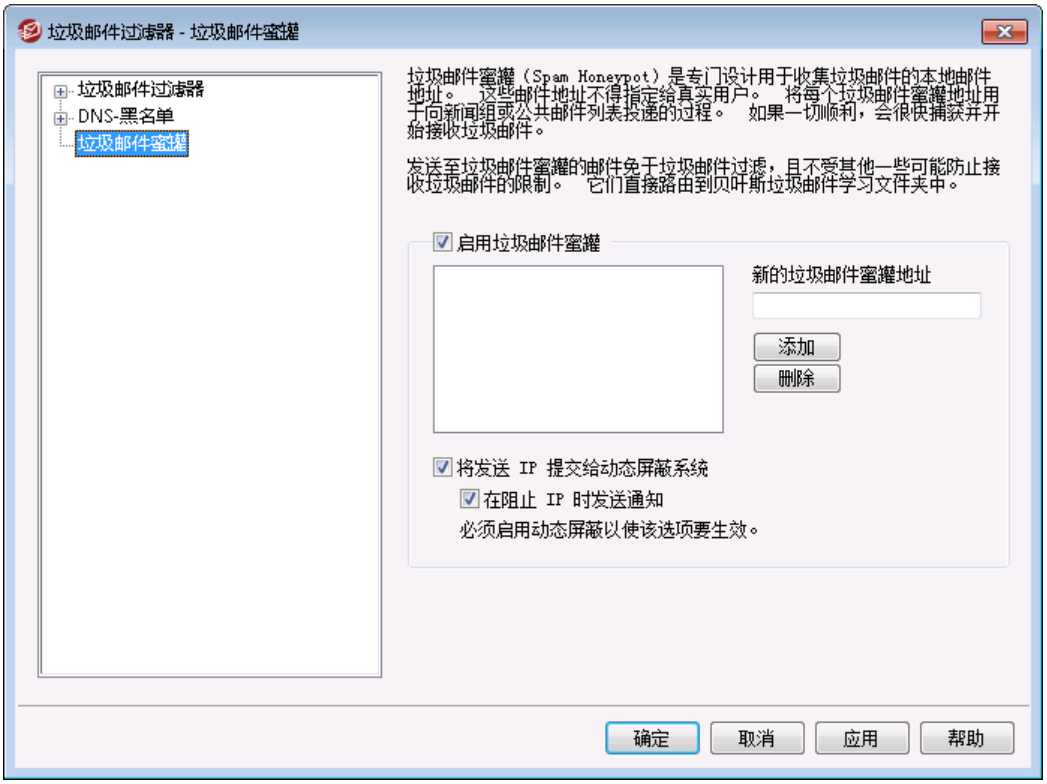
...使用 "邮件"而非 "用户未知"回应
如果您希望每当找到阻止列表中的 IP 地址，就在 SMTP 会话期间发送已分配到 DNS-BL 主机 587的特定邮件，请点击此选项。否则，将发送 "用户未知"邮件。此选项可用的前提是，您已选择使用了以上 *"SMTP 服务器应拒收发自阻止列表 IP 的邮件"*选项。

将被列入阻止列表的邮件自动过滤到用户的垃圾邮件文件夹
点击此选项将会创建一个 "Junk E-mail (垃圾邮件)"IMAP 文件夹，用于今后您添加到 MDaemon 的所有用户账号。MDaemon 还会为每个用户创建一个邮件过滤器，这将搜索 X-MDDNSBL-Result 报头并将包含该标题的邮件放置到用户的垃圾邮件文件夹。点击此选项时，将询问您是否希望 MDaemon 为每位现有的用户账号创建这个文件夹和过滤器。请参阅以下的*为每个账户自动生成垃圾邮件文件夹和过滤器*。

为每个账户自动生成 "垃圾邮件文件夹"和 "过滤器"

MDaemon 能为每一个账户自动创建一个 "Junk E-mail" IMAP 邮件文件夹，并生成一个邮件过滤器，每当发现 X-MDDNSBL-Result 报头就会将邮件转移到那个文件夹中。当您点击了 *"将阻止列表中的邮件自动过滤到用户的垃圾邮件文件夹"*选项时，将向您显示为所有账户创建文件夹与过滤器的选项。只要在对话框中选择 "是"就能创建文件夹和过滤器。这种简单可靠的方式帮助您的用户快速识别垃圾邮件——它能有效阻止混杂在所有合法邮件中的垃圾邮件。他们只需偶尔查看一下垃圾邮件文件夹的内容，以确保没有任何重要邮件被意外放置其中 (这种情况有时可能发生)。在为您的账号创建文件夹和过滤器时，如果 MDaemon 发现某个账户已拥有过滤器来检查是否存在 X-MDDNSBL-Result 报头，就不会对该账户采取任何操作也不会创建过滤器。如果您不希望将 IMAP 文件夹命名为 "Junk E-mail (垃圾邮件)"，您可以更改默认设置，这可通过编辑*默认垃圾邮件文件夹名称*选项 (位于系统 414屏幕，在 设置» 首选项中)来实现。

4.6.3 垃圾邮件蜜罐



垃圾邮件蜜罐（位于"安全» 垃圾邮件过滤器» 垃圾邮件蜜罐"），是特意设计用于收集垃圾邮件的本地邮件地址。这些垃圾邮件蜜罐不是有效的 MDaemon 账户或地址别名，且永远不得用于发送或接收合法的邮件。但通过将蜜罐地址发布到新闻组、公共邮件列表或其他的源（垃圾邮件发送者经常从这些地方获取地址），便应该可以发现不断接收到发往这些垃圾邮件蜜罐的邮件——您也可以从接收到的发往其他无效本地地址的垃圾邮件中拖出这些地址。由于蜜罐绝不会收到合法的电子邮件，所有入站邮件都将直接指向您的 贝叶斯垃圾邮件学习文件夹[568]进行处理。此外，可选择将发送服务器的 IP 地址添加到动态屏蔽[472]系统，在指定期限内禁止来自这些地址的后续连接。所有这些都有助于提高今后识别并阻止垃圾邮件的可能性。

垃圾邮件蜜罐
该列表包括所有指定为垃圾邮件蜜罐的地址。

启用垃圾邮件蜜罐
默认情况下，启用该选项。如果您希望禁用垃圾邮件蜜罐功能，请取消勾选此框。

新建垃圾邮件蜜罐
要添加垃圾邮件蜜罐，请在此输入地址并点击*添加*。

删除
要移除垃圾邮件蜜罐，请选择要删除的地址然后点击"删除"。

将发送 IP 提交给“动态屏蔽”系统
如果要将垃圾邮件蜜罐邮件所来自的全部 IP 地址提交给动态屏蔽[472]系统，请选中该复选框。必须在服务器上启用动态屏蔽（位于“安全» 安全设置» 屏蔽» 动态屏蔽”）才能使用该功能。

在阻止 IP 时发送通知
默认情况下，当“动态屏蔽”系统阻止提交的 IP 地址时，“动态屏蔽”的“*IP 地址阻止报告*[517]”选项将用于通知您相关操作。如果由于“垃圾邮件蜜罐”提交功能阻止 IP 地址时不希望收到通知，请清除此复选框。

章节

5

5 账户菜单

5.1 账户管理器

为了更好地管理您的账户操作（选择、添加、删除或者修改），MDaemon 中包含了账户管理器。此对话框提供账户信息访问，并且可根据邮箱、域、实际名称者邮件文件对账户进行排序。“账户管理器”位于“账户”菜单下的：“账户» 账户管理器..”

账户管理

在账户列表上方您可以看见有关此列表的两个数据统计。第一个数字是当前在您系统上的 MDaemon 用户账户总数。第二个数字是目前在列表中所显示的账户数。将显示的账户取决于您在列表下方 *“仅显示该域中的账户”*选项里所选中的内容。如果您选择了“所有域”，则将在列表中显示您所有的 MDaemon 账户。对话框顶部有一个搜索选项，您可以使用它来准确定义除了已选择的账户所在域之外，还将显示哪些账户。

列表中的每个条目都包含了一个“账户状态图标”（见下），邮箱、所属域、账户持有人的“实际姓名”，账户所属的任何群组、邮件计数、已用磁盘空间（单位是 MB）、上次访问的账户、以及存储账户邮件的邮件文件夹。此列表可以按照您的需要升序和降序排列。点击任何栏目的标题来以升序排列列表。再次点击该列，对其进行降序排列。

默认情况下，一次最多只能在此列表中显示 500 个账户。如果您希望从当前所选域中看到更多账户（或者“所有域”，如果您已选中此选项的话），那么您必须点击 *“显示更多账户”*按钮来显示后 500 个账户。如果您希望能够一次显示超过 500 个账户，那么请打开 MDaemon.ini 文件，然后将 MaxAccountManagerEntries=500 的键值更改为所需值。

账户状态图标


账户为全局或域管理员。


完全访问账户。同时启用 POP 和 IMAP 访问。


受限访问账户。禁用 POP、IMAP 或同时禁用两者。


账户被冻结。MDaemon 仍将接收该账户的邮件，不过该用户无法发送或检查邮件。


禁用账户。禁用该账户的所有访问。

新建
点击此按钮打开“账户编辑器[598]”来创建一个新账户。

编辑
从列表中选择一个账户然后点击此按钮，在“账户编辑器[598]”中将其打开。您还可以双击此账户来将其打开。

删除
从列表中选择一个账户然后点击此按钮将其删除。在 MDaemon 执行删除账户的操作中，将要求您确认此决定。

仅显示来自此域的账户
从下拉式列表框中选择“所有域”以显示所有的 MDaemon 账户。选择一个特定域，仅显示来自此域的账户。

显示更多账户
该账户列表一次只能显示 500 个账户。如果您在该域中已选中超过 500 个账户，那么点击此按钮来显示后 500 个。参见上方的注意事项，它指导应如何增加可以显示的最大账户数。

顶部
点击此按钮快速移至账户列表顶部。

导入
如果您希望从一个以逗号分隔的文本文件中导入账户，请点击此按钮。该按钮等同于“账户» 导入» 从一个逗号分隔的文本文件导入账户”的菜单选项。

模板
点击此按钮来打开“群组 & 模板[657]”对话框，您可以从中管理“新建账户[667]”的默认设置，并控制账户群组成员。

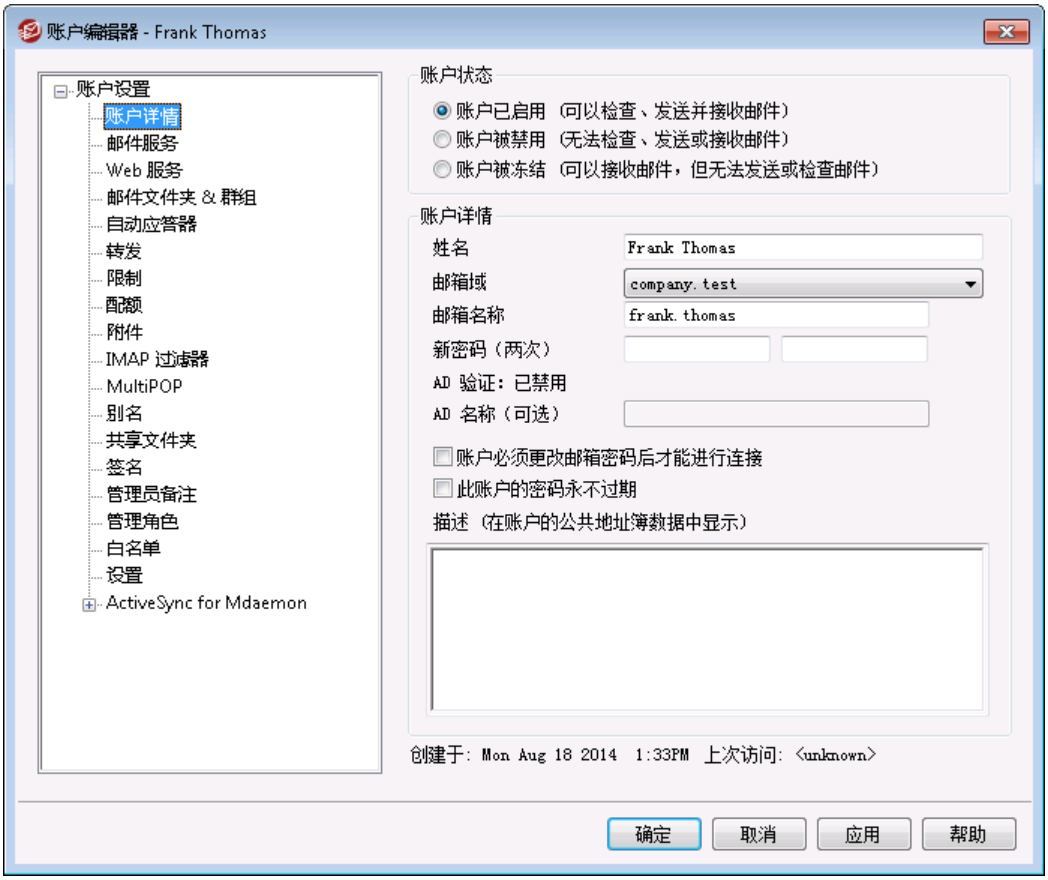
默认列表
如果您希望取消订阅托管于服务器上的所有“邮件列表[228]”，可以选择一个或多个账户，然后点击此按钮。接着会打开一个对话框，要求您确认是否删除列表中的这些地址。

还请参阅：

账户编辑器 598
新建账户模板 667

5.1.1 账户编辑器

5.1.1.1 账户详细信息



账户状态

已启用账户 (可以检查、发送和接收电子邮件)
这是默认选项，账户可以检查、发送和接收电子邮件。

已禁用账户 (无法检查、发送和接收电子邮件)
如果您希望禁用对于该账户的一切访问，可选择此项。用户将不能通过任何方法访问此账户，MDaemon 也将不能为其接收邮件。它不会被删除，仍然会计入许可证账户限制中使用的账户数，但 MDaemon 会像该账户不存在一样运行，除非其他用户共享了该账户的任何文件夹，则其他用户仍能按照该文件夹的 ACL 权限 260 对其进行访问。

已冻结账户（可以接收但无法发送或检查电子邮件）
如果您希望允许账户接收入站邮件，但阻止其检查或发送邮件，请选择此项。在您怀疑账户是否被劫持时这很有用。冻结账户将防止恶意用户访问其邮件或使用该账户来发送邮件，不过这个账户仍然能接收其入站邮件。

账户详细信息

名和姓
在此输入用户的名和姓。在新建账户时，输入名和姓并选择*"邮箱域"*的时候，将自动填写"账户编辑器"各种屏幕上的某些字段（例如*邮箱名称*和*邮箱文件夹*）。不过，您也可以更改任何默认值。名和姓字段不能包含"!"或"|"。

邮箱域
使用这个下拉列表框来指定该账户所属域，此域将用于其邮件地址。默认情况下，MDaemon 的"默认域[149]"将出现在下拉式列表中。

邮箱名称
这是账户的电子邮件地址中使其区别于域中其他账户的部分。完整的邮件地址（例如[*邮箱名称*]@[*邮箱域*]）用作账户唯一的标识符，以及 POP3、IMAP、Webmail 等的登录信息。邮件地址中不能包含空格或者"!"或者"|"的字符。不要在此选项中使用"@"。例如，使用"frank.thomas"而不是"frank.thomas@"。

新建密码（两次）
如果要更改账户的密码，请在此处输入一个新密码，一次填写一个框。当连接到 MDaemon 通过 POP3 或者 IMAP 来收发邮件时，当在 SMTP 会话过程中进行验证时，又或者在使用 Webmail, Remote Administration 或 MDaemon Connector 时，该账户将使用此密码。如果密码不匹配或者违反密码限制[717]，这两个框都将以红色亮显。否则这些框将呈现绿色状态。

如果您为此账户使用"活动目录验证[727]"，您必须输入两个反斜杠，后接用户所属域，而不是输入密码（例如：应输入\\ALTN 而不是 123Password）。下方密码字段有简短的说明来指示是否为此账户启用或禁用了 AD 验证。

即使您不希望允许 POP3/IMAP 访问该邮件账户，该账户仍然应该持有密码。除了邮件会话验证之外，还使用邮件地址和*"邮箱密码"*值来允许远程账户配置和检索远程文件。如果您希望阻止 POP/IMAP 访问，请使用位于邮件服务[602]屏幕上的选项。如果您希望阻止所有访问，请使用上述的*"已禁用账户"*或*"已冻结账户"*选项。

活动目录名称（可选）：
如果要指定可选的活动目录账户名来访问该账户，请使用此设置。

账户在可以进行连接前必须更改邮箱密码
如果您希望账户在可以访问 POP、IMAP、SMTP、Webmail 或 Remote Administration 之前，必须更改其*"邮箱密码"*，请勾选此框。该用户可以连接到 Webmail 或 Remote Administration，但只有在这名用户更改他或她的密码后才能继续操作。注意 为了让用户能够通过 Webmail 或 Remote Administration 更改其密码，他们必须先被授予*"...编辑密码"*web 访问权限（位于 Web 服务[603]屏幕。）密码更改完毕后，将取消激活这个选项。

因为更改密码对某些用户而言可能不是易事，您应该慎用此项。

此账户的密码从不过期
如果您希望此账户免于“密码[717]”对话框中的密码过期选项，请勾选此框。

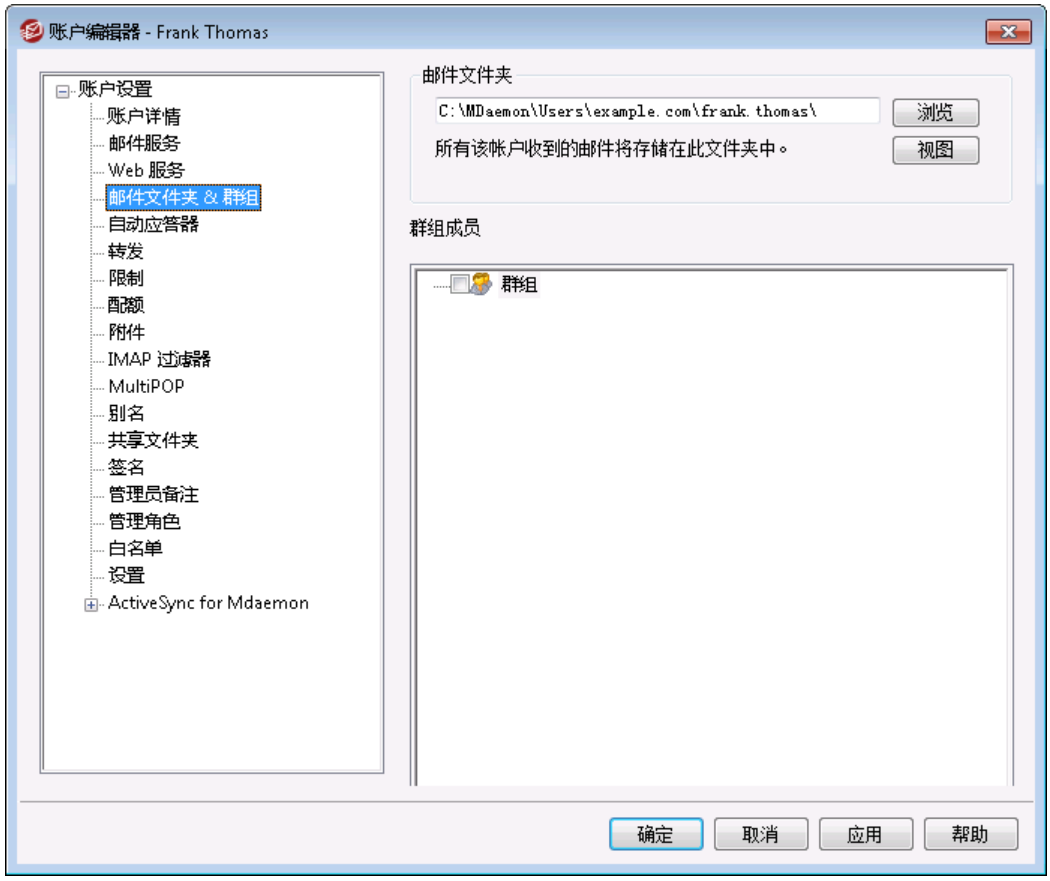
描述
如果您希望为账户添加公共描述，请使用此文本区域。

此账户的公共联系人记录中将含有这个描述，而且可供其他人查看。不要在此字段中包含私人或敏感信息。有关此账户的私人注释或评论，请使用管理员角色[636]屏幕上提供的空格。

还请参阅：

AD 验证[727]
密码[717]
账户编辑器 » Web 服务[603]

5.1.1.2 邮件文件夹 & 群组



邮件文件夹

输入您希望存储该账户邮件的文件夹。创建一个新账户时，该文件夹的默认位置是基于*邮件文件夹*设置，在新建账户模板[667]上指定。

视图

点击此按钮来打开队列/统计管理器[742]并转至用户的*"邮件文件夹"*。

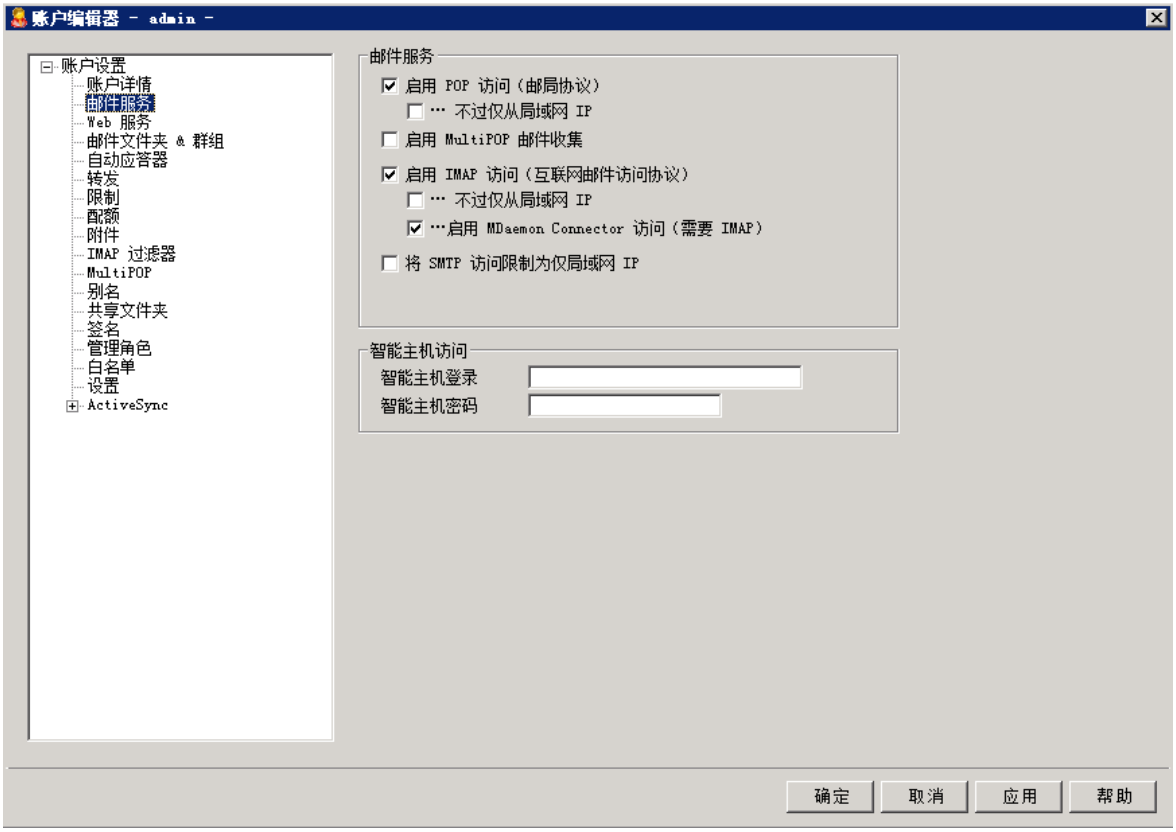
群组成员

使用此框添加账户到一个或多个群组[657]。勾选您希望账户加入的各个群组旁的选框。

还请参阅：

新建账户模板[667]
群组[657]

5.1.1.3 邮件服务



此屏幕上的选项控制允许账户使用哪些邮件服务：POP、IMAP、MultiPOP 和 MDaemon Connector。可以从 Web 服务 603 屏幕控制通过a Webmail进行的邮件访问。该屏幕还含有用于为账户指定可选智能主机访问凭证的选项。

邮件服务

启用邮局协议（邮局协议）
勾选此框时，可以通过“邮局协议（POP3）”访问账户的邮件。事实上所有电子邮件客户端软件都支持此协议。

...不过仅从局域网 IP
如果您希望在用户从局域网 IP 地址 508 建立连接时，允许仅通过 POP 访问该账户，请勾选此框。

启用 MultiPOP 邮件收集
如果您希望允许该账户使用 MultiPOP 620，请勾选此框。MultiPOP 允许用户收集来自其他邮件账户的电子邮件，并在其他邮件服务器上保留这些邮件。

启用互联网邮件访问协议（互联网邮件访问协议）
勾选此框时，可以通过“互联网邮件访问协议（IMAP）”访问账户的邮件。IMAP 的功能多于 POP3，允许在服务器上管理电子邮件，并使用多种客户端访问邮件。大多数电子邮件客户端软件都支持此协议。

...不过仅从局域网 IP
如果您希望在用户从局域网 IP 地址[508]建立连接时，允许仅通过 IMAP 访问该账户，请勾选此框。

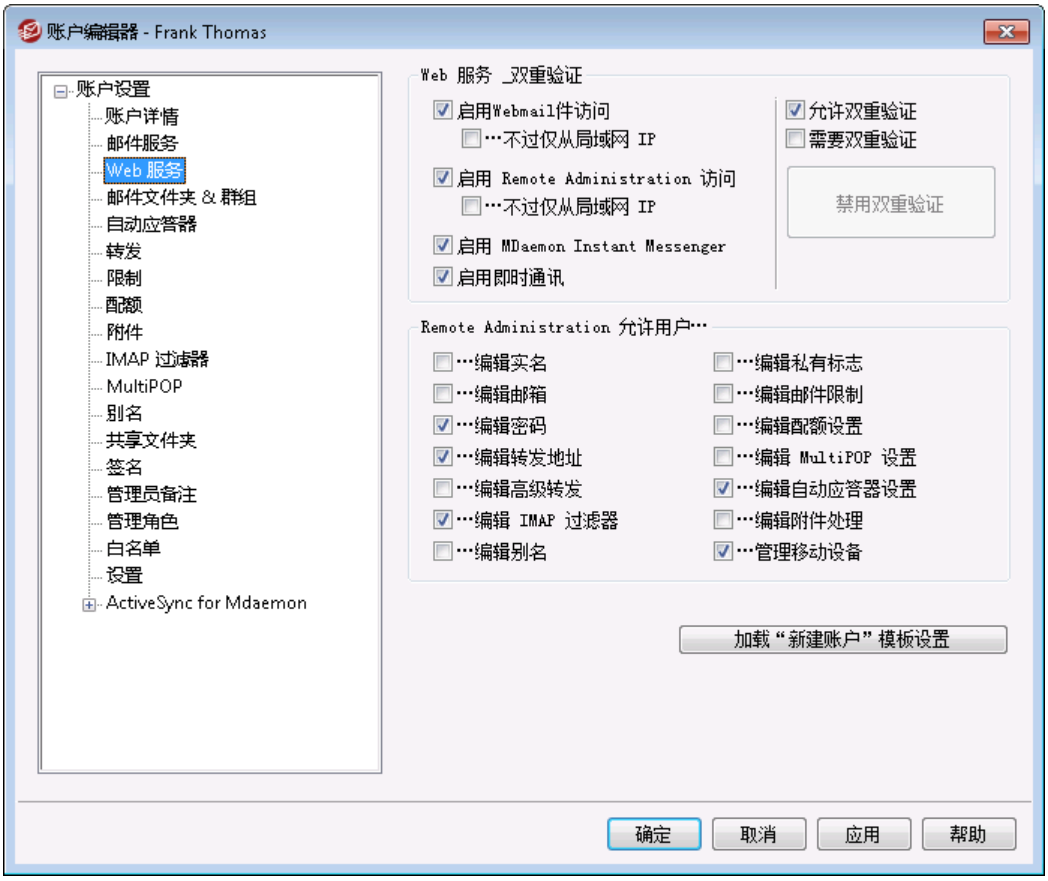
...启用 MDaemon Connector 访问（需要 IMAP）
如果您希望允许账户使用 MDaemon Connector[323] 进行连接，请点击此项。**请注意：**此选项仅在您的服务器上激活对 MDaemon Connector 的支持时才可用。

仅限制 SMTP 访问到 LAN IP
如果您希望仅将 SMTP 访问限制为 LAN IP，请选中此框。这将防止账户发送邮件，除非它们已连接到您的网络。如果该账户尝试从外部 IP 地址发送邮件，则连接将被拒绝并断开。

智能主机访问

智能主机登录/密码
如果您已启用了*"允许按账户验证"*选项（位于"设置 » 服务器设置"的"投递[76]"屏幕上），并且您希望对此账户使用"按账户验证"，而不使用该屏幕上所指定的凭证，那么请在此指定账户的可选智能主机凭证。如果您不希望对此账户使用"按账户验证"，则留空这些选项。

5.1.1.4 Web 服务



Web 服务

启用 Webmail访问
如果您希望此账户能够访问 Webmail[266]，请启用此选框来使用户能够使用 web 浏览器访问其电子邮件、日历和其他功能。

...不过仅从局域网 IP
如果您希望在账户从局域网 IP 地址[508]建立连接时，允许此账户访问 Webmail，请勾选此框。

启用 Remote Administration 访问
如果您希望允许该用户通过 Remote Administration[293] 来修改他或她的账户设置，请勾选此框。用户只能够编辑以下您所指定的设置。

当启用该功能且 Remote Administration 服务器处于活动状态时，用户通过将浏览器指向指定的 MDaemon 域以及 分配给 Remote Administration 的端口[294] (例如 http://example.com:1000)，用户便可登录到 Remote Administration。首先显示登录界面，然后将看到有权限编辑的设置。只需编辑所选设置并点击 *"保存更改"*按钮即可。然后可以注销并关闭浏览器。如果他能访问 Webmail，也可通过 Webmail中的高级选项菜单访问 Remote Administration。

如果用户是 "全局管理员"或 "域管理员"(在 "账户编辑器"的 "管理角色[636]"屏幕上指定)，在登录到 Remote Administration 后他将看到一个不同的屏幕。

...不过仅从局域网 IP
如果您希望在账户从局域网 IP 地址[508]建立连接时，允许此账户访问 Remote Administration，请勾选此框。

启用 MDaemon InstantMessenger
如果您希望为此账户启用 MDIM[267] 支持，请点击此框。

启用即时通讯
在为此账户启用 MDIM 支持时，如果您还希望启用对于 MDIM 的即时通讯系统的支持，请点击此项。取消勾选此框时，您将能访问 MDIM 的其他功能，不过无法使用即时通讯。

双重验证

MDaemon 为登录 Webmail或 MDaemon 的 Remote Administration web 界面的用户支持 "双重验证"(2FA)。通过 HTTPS 登录到 Webmail的账户可以在 Webmail中的 **"选项» 安全"**屏幕上为账户激活 "双重验证"。然后用户在登录 Webmail或 Remote Administration 时必须输入验证码。可以从安装在用户的移动设备或平板电脑上的验证器应用程序获取该代码。该功能专为支持 Google Authenticator 的任何客户端而设计。请参阅 Webmail帮助文件获得有关为一个账户设置 2FA 的更多信息。

允许双重验证
默认情况下，允许新账户[672]设置和使用 Webmail的 "双重验证"(2FA) 功能。如果您不希望这个账户使用 2FA，请取消勾选这个选框。

请求双重验证
如果您希望强制账户在登录到 Webmail时使用 "双重验证"(2FA),请启用此项。如果尚未对此账户配置 2FA,那么下一次当这名账户登录到 Webmail时,会将其重定向到设置页面。请参阅 Webmail帮助文件获得有关为一个账户设置 2FA 的更多信息。

禁用双重验证
如果您需要为此账户禁用 "双重验证",则点击这个按钮。这在用户丢失其设备而且不能访问认证数据时很必要。

Remote Administration 允许用户...

...编辑实名
启用该功能后,将使用户能够修改账户的*姓与名*[598]设置。

...编辑邮箱
启用此功能将允许用户修改账户的 "*邮箱名称*[598]"。

> 因为*邮箱名称*是账户电子邮件地址的一部分,它是账户唯一的标识符与登录值,修改它就表示用户将要更改他或她的实际邮件地址。这会导致将来任何一封指向此旧地址的邮件被拒收、删除或其他相应操作。

...编辑密码
如果您希望允许该用户修改其账户的*邮箱密码*,请点击此选择框。有关密钥要求的更多信息,请参阅:密码[717]。

...编辑转发地址
启用该功能后,用户就能修改转发[610]地址设置。

...编辑高级转发
启用了该功能后,用户就能够修改*高级转发设置*[610]。

...编辑 IMAP 过滤器
使用此控件让用户能够创建并管理他们自己的 "IMAP 过滤器[617]"。

...编辑别名
如果您希望允许账户持有人使用 Remote Administration 来编辑与其账户相关联的别名[622],请启用此项。

...编辑应用程序密码
默认情况下,用户可以编辑其应用程序密码[630]。如果您不希望允许用户编辑它们,请清除该复选框。

...编辑私人旗标
该选项管理该用户是否被允许使用 Remote Administration 来编辑 "*从"所有人"列表、共享日历和 VRFY 中隐藏的账户*"选项 (其位于 "账户编辑器"的设置[639]屏幕上)。

...编辑邮件限制
该选择框用于控制账户是不是能够编辑位于限制[611]屏幕上的入站/出站邮件限制。

...编辑配额设置
如果您希望允许用户修改配额[613]设置，请点击此选择框。

...编辑 MultiPOP 设置
如果您希望授予账户权限来添加新的 MultiPOP[620] 条目，并在 MDRA[293] 中为这些条目启用/禁用 MultiPOP 收集，请点击此勾选框。如果同时启用了此项和该账户的*启用 MultiPOP*[620]选项，则在 Webmail[266] 中提供一个邮箱页面，供用户管理其 MultiPOP 邮箱设置。最后，用于启用/禁用 MultiPOP 服务器的全局选项位于：设置» 服务器设置» MultiPOP[118]。

...编辑自动应答器设置
如果您希望让用户能够为其账户添加、编辑或者删除自动应答器[607]，请点击此选择框。

...编辑附件处理
如果您希望允许该用户编辑位于附件[616]屏幕上的账户附件处理选项，请勾选此框。

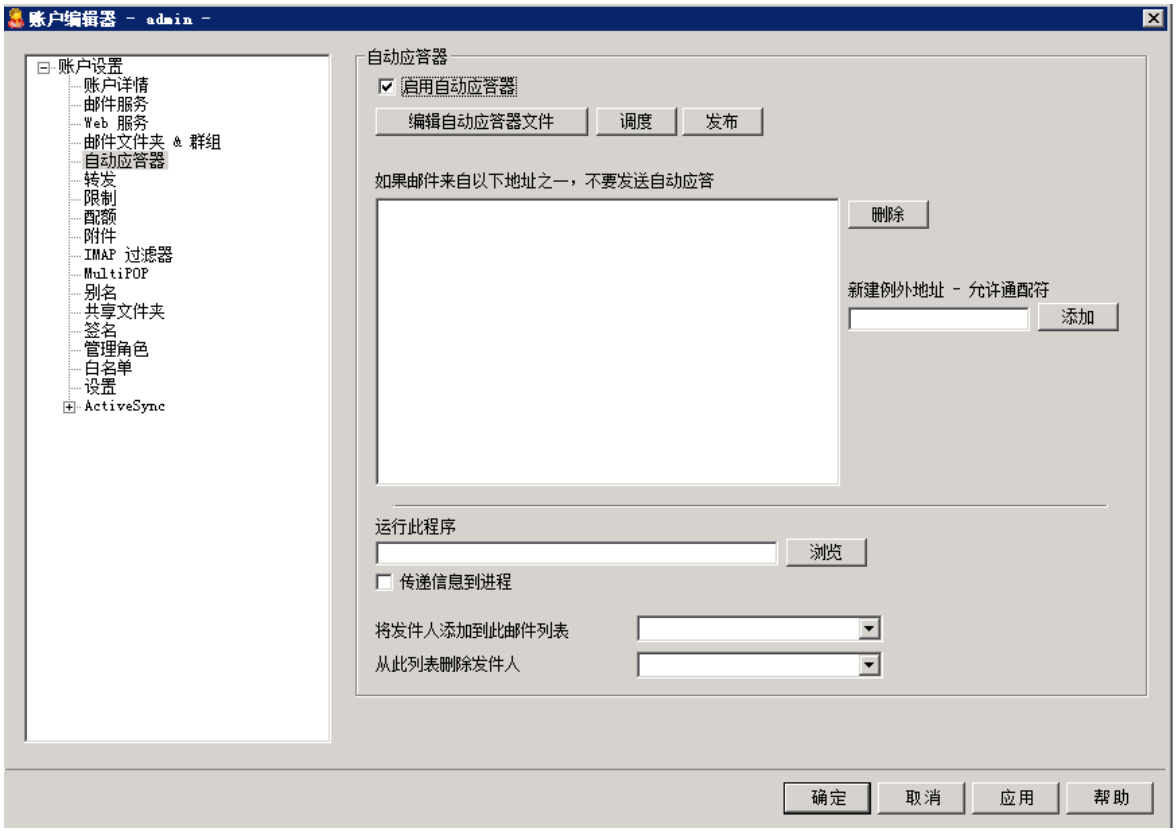
...管理移动设备
如果您希望允许账户持有人使用 Remote Administration 来管理其特定的设备（例如 ActiveSync 设备）设置，请点击此项。

加载“新建账户”模板设置
点击此按钮将该屏幕上的设置还原为默认值，这些默认值在 Web 服务[672]屏幕（位于*新建账户*模板中）指定。

还请参阅：

Webmail[266]
Remote Administration[293]
模板管理器 » Web 服务[672]

5.1.1.5 自动应答器



自动应答器是非常有用的工具，使得入站邮件自动触发某些特定事件，例如运行一个程序，添加发件人到邮件列表，以一封自动生成的邮件来应答等等。自动应答器最常见的用途就是以一封用户自定义邮件自动应答入站邮件，声称收件人正在休假目前无法回应，将尽快答复，诸如此类。使用 web 访问[603]和 Webmail[266] 或 Remote Administration[293] 的 MDaemon 用户可以使用所提供的选项来为自己编写自动应答邮件并且安排邮件将要使用的日期。最后，自动应答邮件基于 OOF.mrk 文件的内容，可以在每名用户的根 \data\ 文件夹中找到。此文件支持大量的宏，这些宏可用于引起动态生成邮件的许多内容，从而使自动应答器具有多种用途。

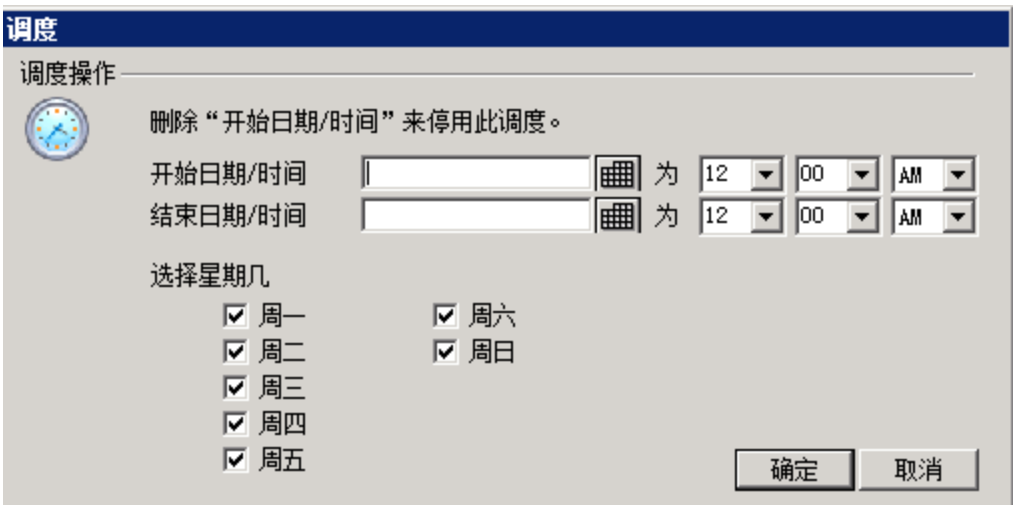
当触发一封来自远程来源的邮件时，总会准许自动应答事件。不过，对于来自用户相同域地邮件，只有在您启用了 *"自动应答器由域内邮件触发"*这个选项后（位于 "自动答器» 设置[706]"屏幕），才会触发自动应答器。您也可以使用该屏幕上的一个选项来限制每个发件人每天针对一个应答的自动应答邮件。

自动应答器

启用自动应答器
启用该控件来激活此账户的自动应答器。有关 WebAdmin 的更多信息，请参阅：自动应答器[703]。

编辑自动应答文件
点击此按钮来编辑账户的自动应答文件。此文件是 oof.mrk 文件，位于这个账户的 \data\ 文件夹。

调度
点击此按钮打开 "调度"对话框，在此您可以设置自动应答器处于活动状态的起始和结束日期和时间，并设置使其处于活动状态的工作日。如果您希望自动应答器始终处于活动状态，请将此 "调度"留空。



发布
如果您希望将此账户的自动应答文件和设置复制到一个或多个其他账户，请点击此按钮。选择您要将自动应答器复制到的账户，然后点击 "确定"。

如果邮件来自以下地址，请不要发送自动应答
您可以在此列出您希望排除在 (自动应答器所启动的)应答之外的地址。

有时，自动应答邮件可能会发送到一个返回本身自动应答的地址。这样就会引起 "乒乓"效应，使得邮件在这两个服务器之间不断来回。若您碰到这种地址，请在此输入以防止这种情况发生。这同样是一个位于自动答器» 设置 706 屏幕上的选项，可用来将自动应答邮件限制为每天应答每位发件人一次。

删除
点击此按钮，从已排除地址的列表中删除任何所选条目。

新建排除地址—通配符可用
如果您希望添加一个地址到排除地址列表中，请在此输入地址然后点击 *添加*按钮。

运行程序

运行该程序
使用该字段来指定当此账户收到新邮件时，您希望为其运行的程序路径和文件名。必须确保该程序可以正常终止并能在无人职守的情况下运行。若有需要，可以在可执行路径后立即输入可选的命令行参数。

传递邮件到进程
选择该选项与进程（在*运行该程序*字段中指定）将传递触发邮件的名称，而该名称将作为第一个可用的命令行参数。当自动应答器在为将邮件转发至另一位置但未在其自身邮箱中保留本地副本的账户进行设置时，（参见转发 610）那么此功能将被禁用。

默认情况下，MDaemon 会将邮件文件的名称用作命令行中的最后一个参数。您可以通过使用 $MESSAGE$ 宏覆盖这一行为。在邮件文件名称应该放置的位置使用此宏。允许更为灵活地使用该功能，这样便能使用以下如此复杂的命令行：
logmail /e /j /message=$MESSAGE$ /q.

邮件列表

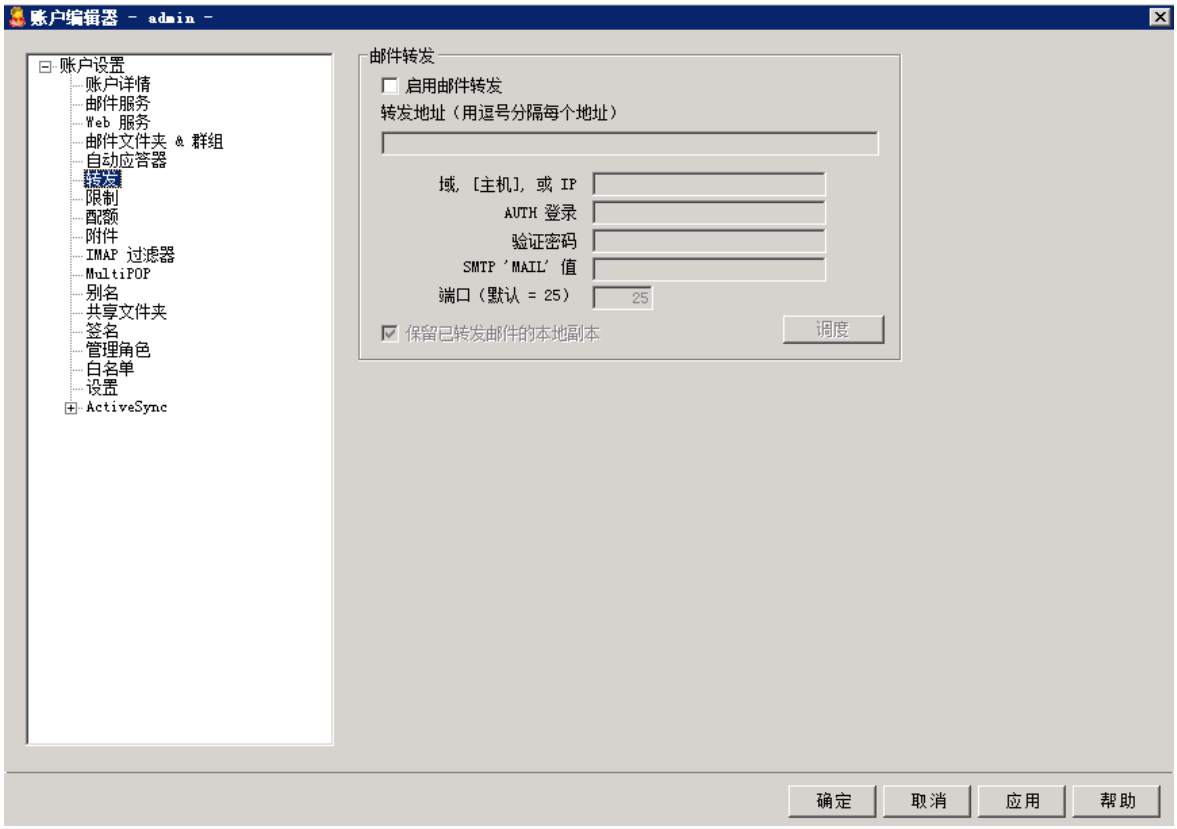
添加发件人到邮件列表
若在该字段中输入一个邮件列表，那么入站邮件的发件人将自动添加到此邮件列表中的一员。对于自动构建列表，这是一个非常简便的功能。

从此邮件列表删除发件人
如果在该字段中输入一个邮件列表，则自动从指定的邮件列表中删除该入站邮件的发件人。

还请参阅：

自动应答器 » 账户 703
自动应答器 » 豁免列表 705
自动应答器 » 设置 706
创建自动应答脚本 707

5.1.1.6 转发



邮件转发

启用邮件转发
如果您希望将该账户的入站邮件转发到一个地址或者在*"转发邮件"*选项中所指定的地址，那么请勾选此框。拥有 web 访问 603 到 Webmail 266 或者 Remote Administration 293 的 MDaemon 用户可以使用所提供的选项来为自己设置转发选项，无需管理员设置。

转发地址（用逗号分隔每个地址）
如果您希望当账户的入站邮件到达时转发邮件副本，那么请使用该字段来指定邮件地址。如果已勾选上方的*"启用邮件转发"*选项，每一封新到达邮件服务器的邮件将被自动生成一个副本并被转发到在此字段中指定的地址。当转发到多个地址时，使用逗号将每个地址隔开。

域、[Host]或 IP
如果您希望通过其他服务器路由已转发的邮件，例如特定域的 MX 服务器，请在此处指定域或 IP 地址。如果您希望通过指定主机路由转发的邮件，把值放入[]中（例如[host1.example.com]）。

AUTH 登录/密码
请在此处输入要将用户的邮件转发到服务器的所有必需登录名/密码凭证。

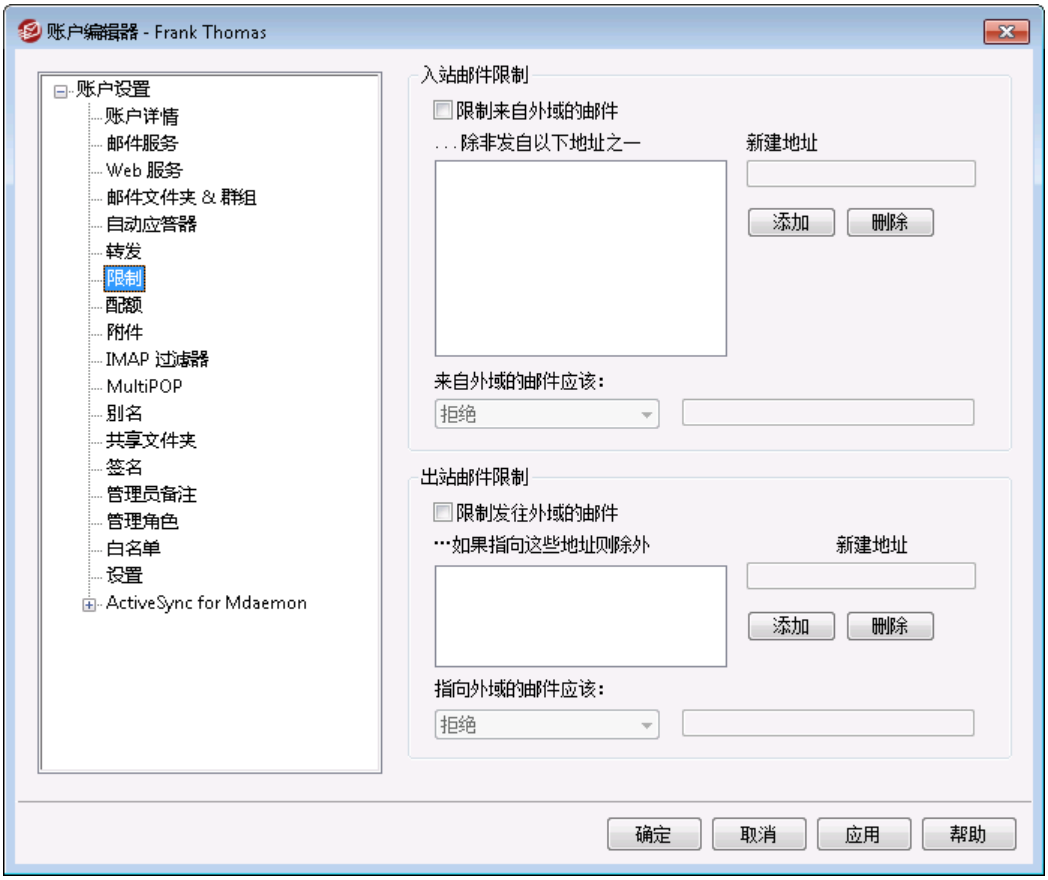
SMTP "MAIL"值
如果在此指定一个地址，会将其用于（在与接受主机的 SMTP 会话期间发送的 "MAIL From"语句中，而不使用邮件的实际发件人。若您需要一个空的 SMTP "MAIL From"语句（例如 "MAIL FROM <>"）则在此选项中输入 "[trash]"。

端口（默认值 = 25）
MDaemon 会使用在此所指定的 TCP 端口来发送转发邮件。默认的 SMTP 端口是 25。

保留已转发邮件的本地副本
默认情况下，每封转发邮件的副本都会正常投递到本地用户邮箱。若您未勾选此框，则不会保留任何本地副本。

调度
点击此按钮可为您创建何时转发该账户的电子邮件的调度时间表。您可以设置开始日期和时间、结束日期和时间，并指定在一周中的哪几天转发邮件。

5.1.1.7 限制



使用此屏幕上的选项来管理账户是否能够发送或接收来自于非本地域的邮件。

入站邮件限制

限制来自域外的邮件
点击此选框来阻止这个账户接收来自非本地域的电子邮件。

...除非发自以下地址之一
在此区域中指定的地址免于入站邮件限制。允许通配符。如果您指定 "*@altn.com"免于限制，那么发自 altn.com 任意地址的所有入站邮件都将被接收并投递到该账户。

新建地址
如果您希望添加一个地址特例到 "入站邮件限制"列表，则在此输入并点击 *"添加"*按钮。

添加
在输入一个地址到 *"新建地址"*选项后，点击此按钮将其添加到例外列表。

删除
如果您希望从限制列表中删除一个地址，选择地址然后点击此按钮。

来自域外的邮件应...
下拉列表框中的选项控制 MDaemon 如何处理发往此账户、但来自非本地域的邮件。您可以选择以下选项：

拒收——受限制的邮件将被 MDaemon 拒收。

返回给发件人——来自受限域的邮件被退回给发件人。

发送给管理员——将会接收受限制的邮件，不过会投递给管理员而不是该账户。

发送至... - 会接收受限邮件，不过这些邮件将投递到您在文本框右边指定的地址。

出站邮件限制

限制发往域外的邮件
点击此选框来阻止这个账户将电子邮件发送至非本地域。

...除非发往以下地址之一
在此区域中指定的地址免于出站邮件限制。允许通配符。如果您指定 "*@altn.com"免于限制，那么发往 altn.com 任意地址的所有出站邮件都不会受到任何限制。

新建地址
如果您希望添加一个地址特例到 "出站邮件限制"列表，则在此输入并点击 *"添加"*这个按钮。

添加
在输入一个地址到 *"新建地址"*选项后，点击此按钮将其添加到例外列表。

删除
如果您希望从限制列表中删除一个地址，选择地址然后点击此按钮。

发往域外的邮件应...
下拉列表框中的选项控制 MDaemon 如何处理来自此账户、但指向非本地域的邮件。您可以选择以下选项：

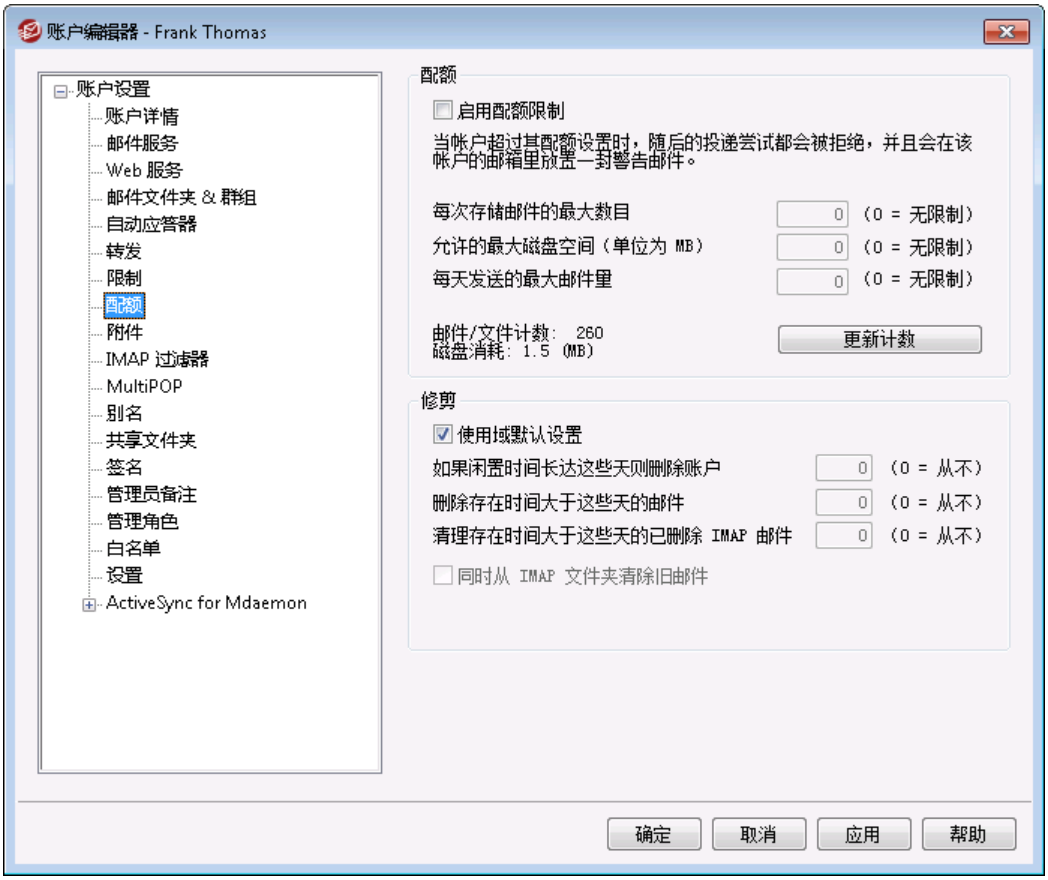
拒收——MDaemon 将绝收受限制的邮件。

返回给发件人——发往受限域的邮件被退回给发件人。

发送给管理员——将会接收受限制的邮件，不过会投递给管理员而不是指定的收件人。

发送至... -会接收受限邮件，不过这些邮件将投递到您在文本框右边指定的地址。

5.1.1.8 配额



配额

启用配额限制
如果您希望指定账户可存储的最大邮件数，或者设置账户可以使用的最大磁盘空间（包括在账户的 Documents 文件夹中所包含的一切文件附件），您可以勾选此框，并指定这些账户每天可以发送的最大邮件数。如果尝试投递到某个账户的邮件将超过最大邮件数或磁盘空间限制，则拒收此邮件，并将一封合适的警告邮件放置到用户的邮箱中。如果 MultiPOP 620 收集将超出账户的最大限制，则发送一封类似的警告邮件，并自动关闭该账户的 MultiPOP 条目（但不是从数据库中删除）。

使用 *"如果达到其配额的百分比，则向用户发送警告"*这个选项（位于 "账户» 账户设置» 配额 681"）后，当账户接近配额限制时就会发送警告消息。当账户超出了其 *"立即存储的最大邮件数"*或 *"允许的最大磁盘空间"*限制中指定的百分比数值时，会在午夜向该账户发送一封警告邮件。该邮件中将列出此账户所存储的邮件数，邮件箱的大小，以及所用和剩余百分数。此外，如果在账户的邮箱里找到现有警告，会以更新过的邮件进行替代。

每次存储邮件的最大数目
使用该选项为此账户指定可以存储的最大邮件数。在该选项中，使用 "0"表示对于已认可的邮件没有数量限制。

允许的最大磁盘空间（单位是 MB）
使用该选项来指定此账户可以使用的最大磁盘空间，包括可以存储在该账户的 Documents 文件夹中的任意文件附件。在该选项中，使用 "0"便是对于账户可以使用的磁盘空间，没有任何数量限制。

每天发送的最大邮件数
使用此项来指定该账户每天可以通过 SMTP 发送的最大邮件数。如果账户达到此限制，就会拒收来自该账户的新邮件，直到在午夜重置计数器为止。如果您不希望限制账户可以发送的邮件数量，请在此项中使用 "0"。

更新计数
点击此按钮来更新在左侧显示的*邮件/文件计数*和*磁盘消耗*统计。

清理

该区段下的选项是用来指定当账户不活动时何时被删除。你也可以指定该账户的旧邮件在一定时间后是否被删除。每晚午夜，MDaemon 将会删除所有超过时间限制的旧邮件，或者彻底删除达到闲置限制的账户。

使用域默认设置
认的清理设置视域而定，并且位于 "域管理器"的 "设置 175"屏幕上。如果您希望为此账户覆盖域的默认值，请清除该选择框并在下方选项中设置想要的值。

账户闲置这些天后将其删除（0=从不）
在删除账户前指定您允许该账户处于闲置状态的天数。此控件中的值 "0"意味着账户从不会因为不活动而被删除。

删除存在时间长于这些天的邮件 (0=从不)
这是邮件被 MDaemon 自动删除前在账户的邮箱里可以保留的天数。"0"值意味着邮件永远不会因其存在时间而被删除。**请注意：**此选项的设置不适用于包含在 IMAP 文件夹中的邮件，除非您还启用下方的*"也清理 IMAP 文件夹中的旧邮件"*这个选项。

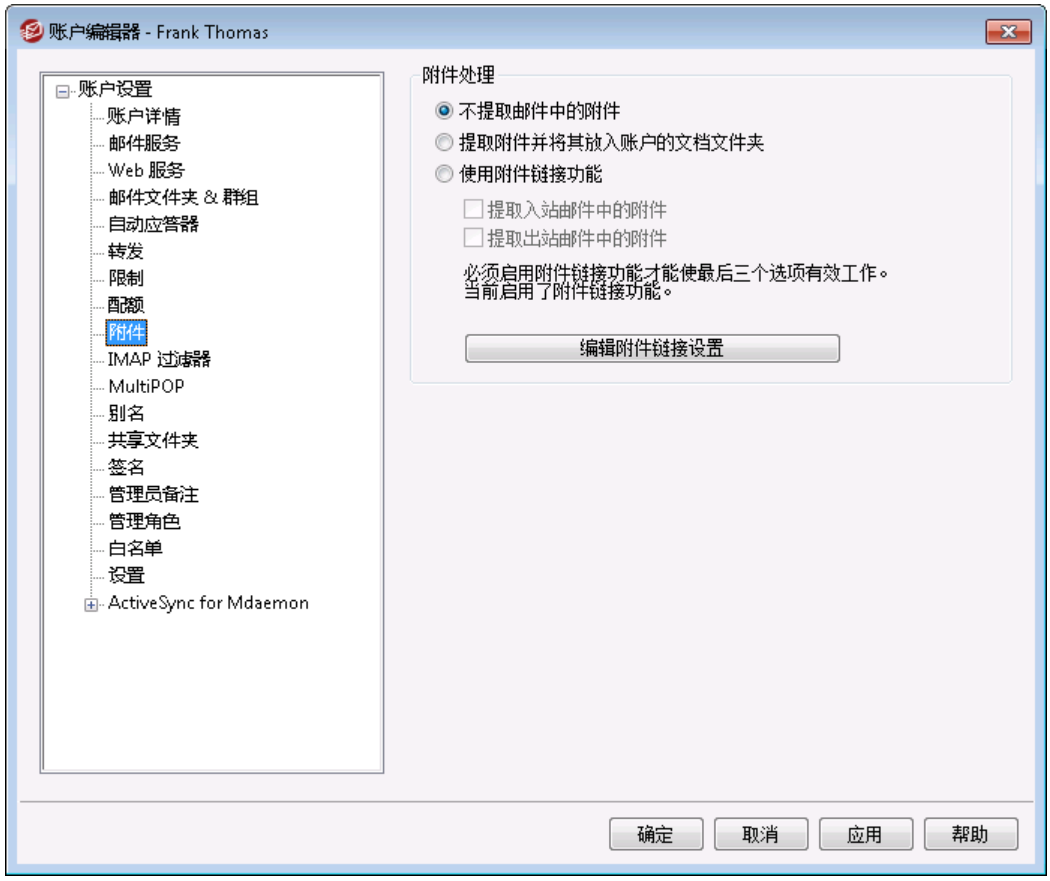
清理存在时间长于这些天的已删除 IMAP 邮件 (0=从不)
使用此控件来指定您允许标记为已删除的 IMAP 邮件在此用户的文件夹中可以保留的天数。对于已经标记为删除的 IMAP 邮件在到达指定天数前会被自动清理掉。值"0"表示带有删除标记的邮件从不会因为其存在天数而被删除。

同时从 IMAP 文件夹清理旧邮件
如果您希望*"删除存在时间超过以下天数的邮件"*这个选项同样应用于 IMAP 文件夹中邮件，请点击此选择框。禁用该选项时，IMAP 文件夹中的常规邮件将不会因为其存在时间而被删除。

还请参阅：

模板管理器 » 配额 681
账户设置 » 配额 721

5.1.1.9 附件



附件处理

此屏幕用于控制 MDaemon 是否提取账户电子邮件中的附件。您可以使用 "模板管理器"[683] 来为这些选项指定默认设置。

不提取邮件中的附件
如果选中此选项，将不会提取该账户邮件中的附件。将正常处理含有附件的邮件，并将附件完整保留。

提取附件并将其放置在账户的文档文件夹
如果设置，此选项使得 MDaemon 自动提取在入站邮件中发现的任何 Base64 MIME 内嵌文件附件。提取的邮件会从入站邮件中删除，并在解码后将其放置在账户的 文档文件夹中。邮件正文中放置了一个便笺，列出了已提取文件的名称。该选项不提供转至已存储附件的链接，不过用户可以使用 Webmail[266] 来访问其文档文件夹。

使用附件链接功能
如果您希望为含有附件的入站或出站邮件使用 "附件链接"功能，请选择此项。

如果已选择该选项，不过在附件链接[305]对话框上禁用了附件链接功能，则不会提取附件。

提取入站邮件中的附件
启用此项时，能够提取账户入站邮件中的附件并将其存储在 "附件链接[305]"对话框中指定的位置。然后将 URL 链接置于邮件正文，该用户可以点击此链接以下载文件。鉴于对安全的考虑，这些 URL 链接不包含直接文件路径。而是包含该服务器所使用的独特标识符 (GUID)来映射文件到实际路径。GUID 映射图存储在 `AttachmentLinking.dat` 文件中。默认情况下启用此项。

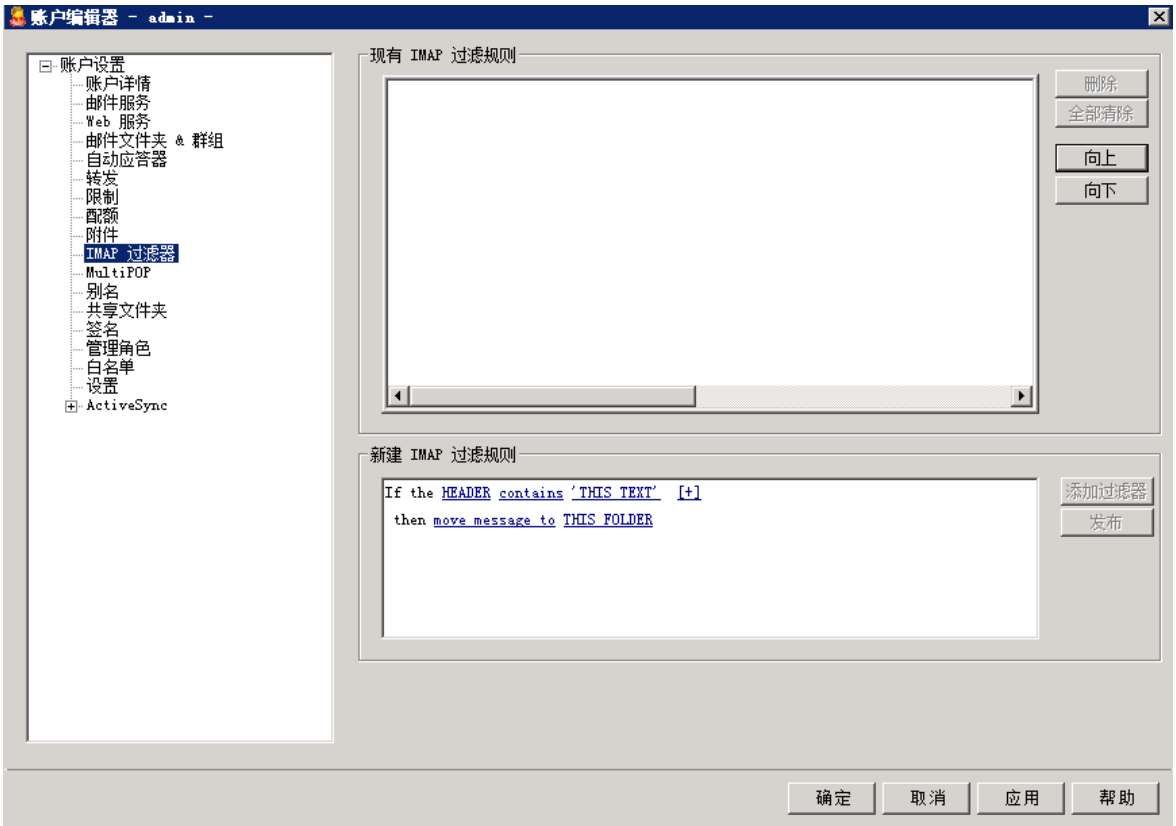
提取出站邮件中的附件
如果您希望使用 "附件链接"功能来提取账户出站邮件中的附件，则勾选此框。在账户发送电子邮件时，附件链接将提取文件，进行存储，并使用一个 URL 进行替换来下载此文件。

编辑 "附件链接"设置
点击此按钮来打开 "附件链接[305]"对话框。

还请参阅：

附件链接[601]
模板管理器 » 附件[683]

5.1.1.10 IMAP 过滤器



IMAP 和 Webmail[266] 用户通过使用过滤器能够将他们的邮件自动路由到服务器上的特定文件夹。与内容过滤器[540]类似，MDaemon 会检查账户的每封入站邮件报头并与账户的过滤器进行比较。当账户的邮件与其过滤器匹配时，MDaemon 会将其移至过滤器中指定的文件夹，删除该邮件或将其重定向或转发至您选择的电子邮件地址。 对于客户端和服务器来说)这种方法要比试图在客户端过滤邮件有效得多，而且由于一些邮件客户端甚至不支持本地邮件规则或过滤，IMAP 过滤器不向其提供此选项。

管理员可通过 "账户编辑器"的 "IMAP 过滤"屏幕，或者使用 Remote Administration[293] 来创建过滤器。不过，您同样可以授予用户权限让他们在 Webmail或 Remote Administration 中为自己创建和管理过滤器。这些权限可以在 Web 服务[603]屏幕上进行设置。

现有的 IMAP 过滤器规则

此框显示为用户账户创建的所有过滤器规则列表。根据过滤器的排列顺序对其进行处理，直到发现匹配。因此，一旦邮件与其中一个过滤器匹配，该邮件将移至该过滤器所指定的文件夹内，然后将终止对此邮件进行过滤处理。使用*向上*和*向下*按钮将过滤器移动到列表中的不同位置。

删除

在列表中点击一个过滤器然后点击*删除*将其从列表中删除。

全部删除

点击此按钮删除该用户的所有过滤器。

正常运行

点击列表中的一个过滤器然后点击此按钮将其移至列表中的更高位置。

停机

点击列表中的一个过滤器然后点击此按钮将其移至列表中的较低位置。

新建 IMAP 过滤器规则

使用这块区域中的链接来构建新的过滤器规则。完成您的规则后，请点击 **"添加过滤器"**来将其加入*"现有 IMAP 过滤规则"*。

过滤器条件

点击过滤规则第一部分中的链接来设置过滤条件。当邮件符合过滤条件时，将执行过滤操作。

报头

点击 **"HEADER"**来选择作为过滤器规则一部分而进行检查的报头或其他邮件组件。您可以选择：**TO**、**CC**、**FROM**、**SUBJECT**、**SENDER**、**LIST-ID**、**X-MDMAILING-LIST**、**X-MDRCPT-TO**、**X-MDDNSBL-RESULT**、**X-SPAM-FLAG**、**MESSAGE SIZE** **MESSAGE BODY**或**其他...** 如果您选择 "Other... (其他)"，则会打开一个 "过滤条件"框，由此来指定未列出的报头名称。如果您点击 MESSAGE SIZE (邮件大小)，则 "包含"和 "此文本"链接将分别被替换为 "大于"和 "0 KB"。

包含/大于

点击 **"包含"**或 **"大于"**来选择在检查报头时设置什么类型的条件。例如：报头是否存在，包含或不包含某些文本，以某些文本开始或结束等。您可从以下操作中进行选择：**以此开头**、**以此结尾**、**等于**、**不等于**、**包含**、**不包含**、**存在**、**不存在**、**大于**或**小**

于。 "大于"和 "小于"选项仅在 "HEADER"链接被设置为 "MESSAGE SIZE (邮件大小)"时可用。

此文本/0 KB
当扫描您为过滤器所指定的报头时，请输入您希望 MDaemon 搜索的文本。当 HEADER 选项设置为 MESSAGE SIZE 时，链接会显示 "0 KB"，"过滤器条件"对话框将显示一个框，用于表示 "邮件大小 (KB)"。

[+] [x]和
如果您希望为过滤器规则设置两个或更多条件，请点击 "**[+]**"。这将添加包含 "报头"、"包含"和 "此文本"组件的另一行来扩展这个过滤器。在针对具有多个条件的过滤器规则测试邮件时，默认情况下，该邮件必须通过每个条件才能符合规则。如果您希望邮件在通过任何条件时都匹配规则，请点击 "**和**"并选择 "**或**"。当过滤规则有多行时，您可以点击希望删除的任何行附近的 "**[x]**"。

过滤操作

点击过滤规则底部的链接，指定在邮件符合过滤条件时采取的操作。

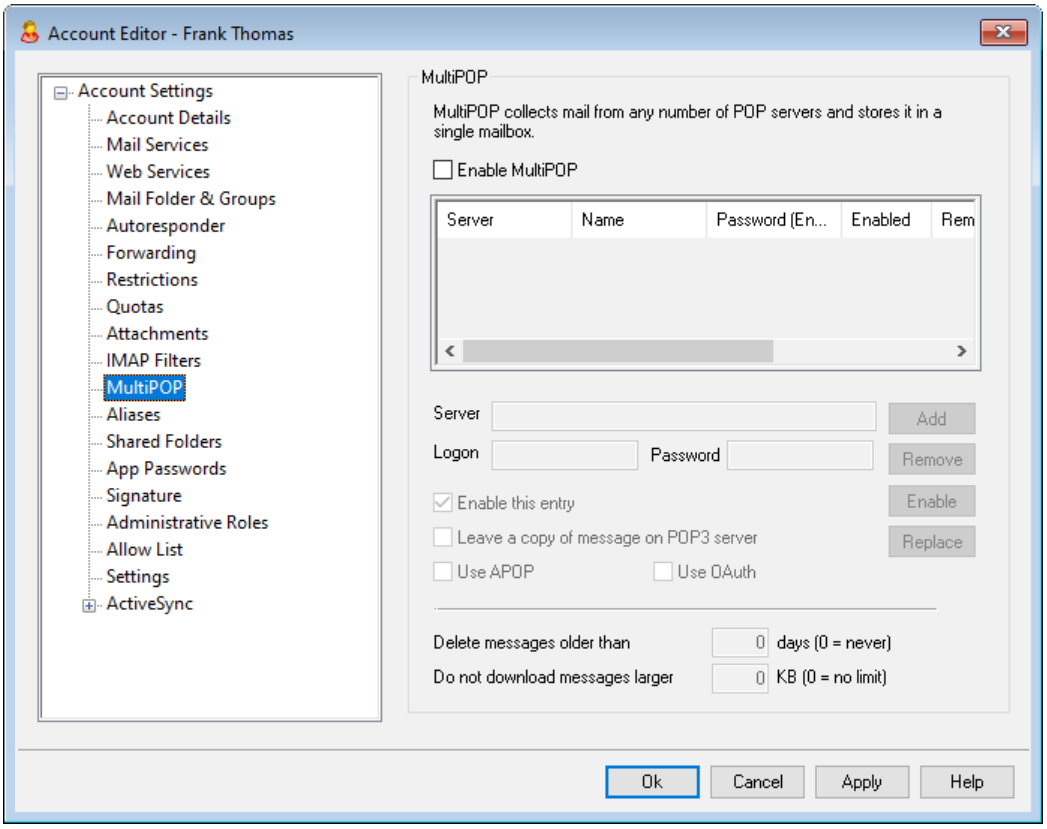
将邮件移至
点击 "**将邮件移至**"来指定过滤器操作。您可以选择：**将邮件移至**、**删除邮件**、**将邮件重定向至**或**将邮件转发至**。

此文件夹/电子邮件
如果您选择 "将邮件移至"操作，则点击 "**此文件夹**"来指定将邮件移至哪个文件夹。如果您选择重定向或转发此邮件，请点击 "**电子邮件**"并输入收件人的邮件地址。对于重定向的邮件，不会对邮件报头或正文做出任何变更。唯一改变的是 SMTP 的信封收件人。对于转发的邮件，将会创建和发送一封新邮件，其主题报头和正文内容都来自那封初始邮件。

添加过滤器
完成创建新过滤器后，请点击此按钮将其添加到 *"现有的 IMAP 过滤规则"*。

发布
创建规则后，如果您希望将该规则复制到属于此账户域的所有其他用户账户，请点击 "**发布**"。系统将要求您确认将规则复制到其他账户的决定。

5.1.1.11 MultiPOP



MultiPOP 功能帮助您为多种来源的邮件集创建无限数量的 POP3 主机/用户/密码组合。这对那些在多个服务器上拥有邮件账户，而又希望将邮件收集并保存在一个地方的用户来说，非常有用。邮件在被放置到用户的邮箱之前，MultiPOP 所收集的邮件首先放置到本地队列中，以使它能像其他拥有自动应答器和内容过滤器的邮件一样被处理。MultiPOP 的调度选项位于：设置» 事件调度» 邮件调度选项» MultiPOP 收集[320]。

启用 MultiPOP
为此账户启用 MultiPOP 处理，请勾选此框。如果您希望允许用户在 MDRA[293] 中编辑他自己的 MultiPOP 设置，请启用 *"...编辑 MultiPOP 设置"* 选项，位于该账户的 Web 服务[603]页面上。如果同时启用了此项和 web 服务选项，则在 Webmail[266] 中提供一个邮箱页面，供用户管理其 MultiPOP 邮箱设置。用于启用/禁用 MultiPOP 服务器的全局选项位于：设置» 服务器设置» MultiPOP[118]。如果禁用此项，则无法使用 MultiPOP，即使启用了这个账户选项也是如此。

创建或编辑一个 MultiPOP 条目

服务器
输入您要从中收集邮件的 POP3 服务器。如果此服务器要求您连接除标准 POP3 端口以外的其他特定端口，请在服务器名中附加 ":[port]"。例如："mail.example.com:1000"。在从 Gmail 或 Microsoft (Office) 365 收集时，请分别使用 "pop.gmail.com:995" 或 "outlook.office365.com:995"。

登录
输入 POP3 用户名或者与上方所指定服务器上的邮件账户相关联的登录名。

密码
输入 POP3 或 APOP 密码来访问指定服务器的邮件账户。

使用 APOP
如果你想使用 APOP 这个认证方法来从其相应的主机收取邮件，请点击这个勾选框。

使用 OAuth
在从 Gmail或 Office365 收集邮件时，请选择这种验证方式。还请参阅 MultiPOP OAuth 2.0 指南 118来获取更多信息，它位于服务器设置 » MultiPOP 页面。**请注意：**还必须为用户启用 *"..编辑 MultiPOP 设置"*这个选项，它位于账户的 Web 服务 603页面，以便使用户能将 OAuth 用于 Gmail或 Office 365，因为用户必须登录 Webmail并前往**邮箱**页面来验证 Gmail或 Office 365 邮箱条目。

在 POP3 服务器上保留邮件副本
如果您希望在服务器上保留邮件副本，请点击此选择框。如果你希望以后在别的地方还要收取邮件，这是非常有用的。如果您希望为所有用户覆盖此选项，这意味着邮件被下载到 MDaemon 后，将始终从 POP 服务器中删除，您可以通过启用 *"MultiPOP 在收集后始终删除所有服务器中的邮件"*这个选项来实现这点，它位于设置» 服务器设置» MultiPOP 118。

添加
为新的 MultiPOP 条目输入所有信息后，点击此按钮将其添加到列表中。

删除
若您希望删除其中一个 MultiPOP 条目，请选中所需条目然后点击此按钮。

启用/禁用
点击此按钮切换所选 MultiPOP 条目的状态，在 MDaemon 执行 MultioPOP 处理时，此切换帮助您控制 MDaemon 是否为此条目收集邮件还是忽略邮件。

替换
要编辑一个条目，请点击列表中的条目，做出任何所需更改，并点击此按钮来保存对于这个条目的更改。

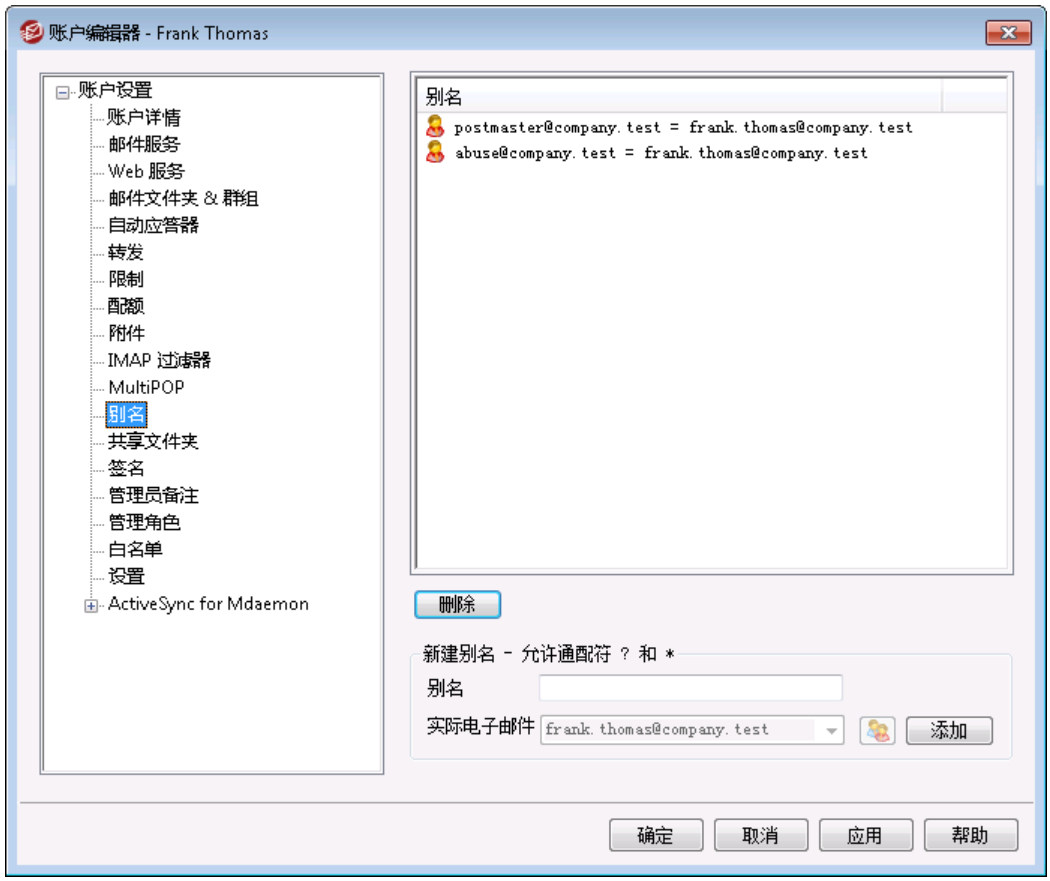
删除存在时间大于 [XX]天的邮件 (0 = 从不)
这是邮件在删除以前可以保留在 MultiPOP 主机上的天数。若您不希望删除旧的邮件，请使用 "0"。

不要下载大于 [XX]KB的邮件 (0=不限)
在此输入一个值来指定不下载多大的邮件。

还请参阅：

服务器设置 » MultiPOP 118
调度 MultiPOP 收集 320

5.1.1.12 别名



该屏幕上列出了与该账户相关联的所有地址别名 699，并且可用来添加或删除别名。

删除别名

要删除该账户中的某个别名，请选择列表中的别名并点击 **"删除"**。

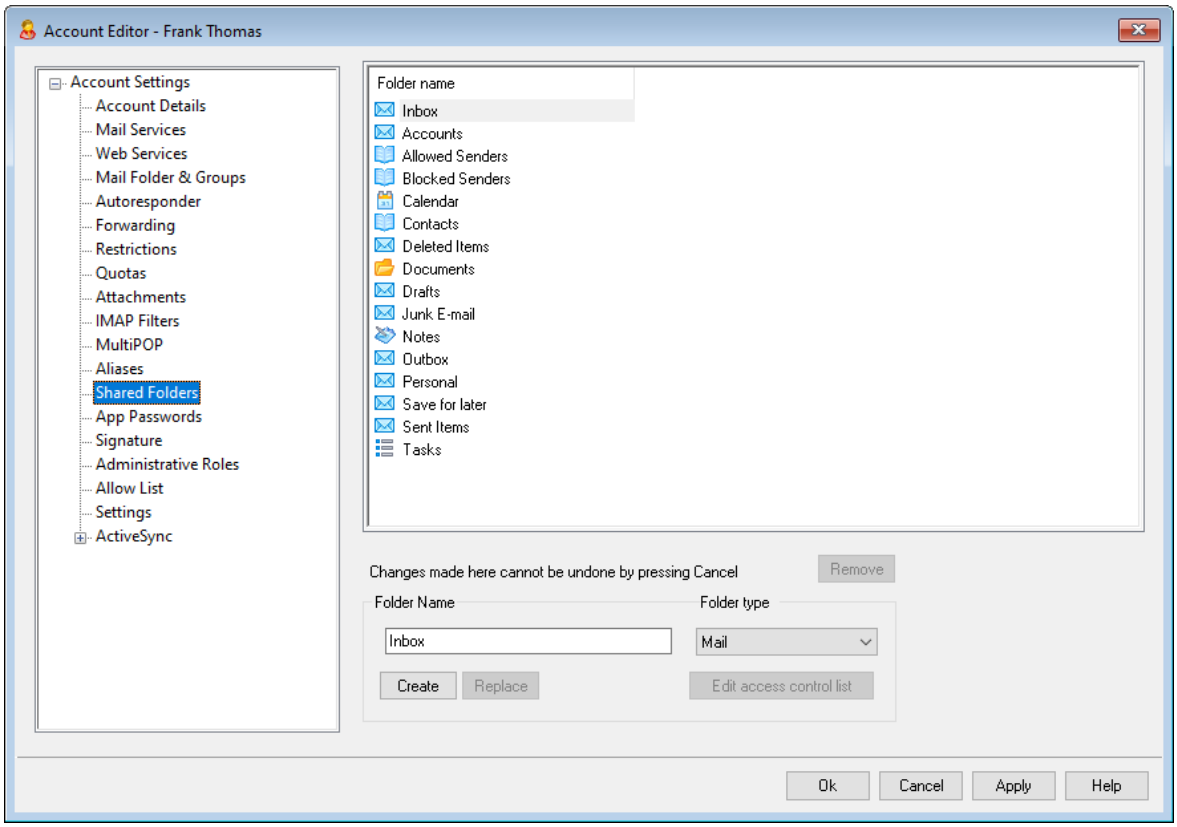
添加别名

要添加新别名到该账户，请在 *"别名"*框内输入您希望与该账户相关联的地址然后点击 **"添加"**。允许 **"?"**和 **"*"**通配符，分别代表单个字符和单个单词。

还请参阅：

账户设置 » 别名 699

5.1.1.13 共享文件夹



这个屏幕只有在您启用了 *"启用公共文件夹"*选项（在 *"公共 & 共享文件夹* 97 *"*屏幕上）才可用，位于 *"设置» 服务器设置» 公共& 共享文件夹"*。可以从 *"公共文件夹管理器* 258 *"*管理 *"公共文件夹"*。

最高区段显示了用户所有的 IMAP 文件夹，而且可以用来与其他 MDaemon 用户或群组 657 共享访问。当刚创建好一个账户时，个区域中只列出了收件箱，直到您使用了 *"文件夹名称"*以及 *"创建"*选项（两者位于 *"IMAP 过滤器* 617 *"*上的选项）来添加文件夹到该区域。该列表中的子文件夹将会以一条斜杠将文件名与子文件名隔开。

删除
要从列表中删除共享 IMAP 文件夹，选择文件夹，然后点击 *"删除"*按钮。

文件夹名称
要添加新文件夹到此列表，在此选项中为其指定名称并点击 *"创建"*。如果您希望新文件夹作为此列表中一个文件夹的子文件夹，使用父文件夹名称和斜杠为新建文件夹添加前缀。例如，如果父文件夹是 "My Folder"，则新建的子文件夹名将为 "My Folder/My New Folder"。如果你不希望它作为一个子文件夹，那么新文件夹名称应为 "My New Folder"，而没有前缀。

文件夹类型
使用此下拉式列表来选择您希望创建的文件夹类型：邮件、日历和联系人等。

创建
在指定了一个文件夹的名称后。点击此按钮添加文件夹到该列表。

替换
如果您希望编辑其中的一个共享文件夹，点击条目，做出更改，然后点击 *"替换"*。

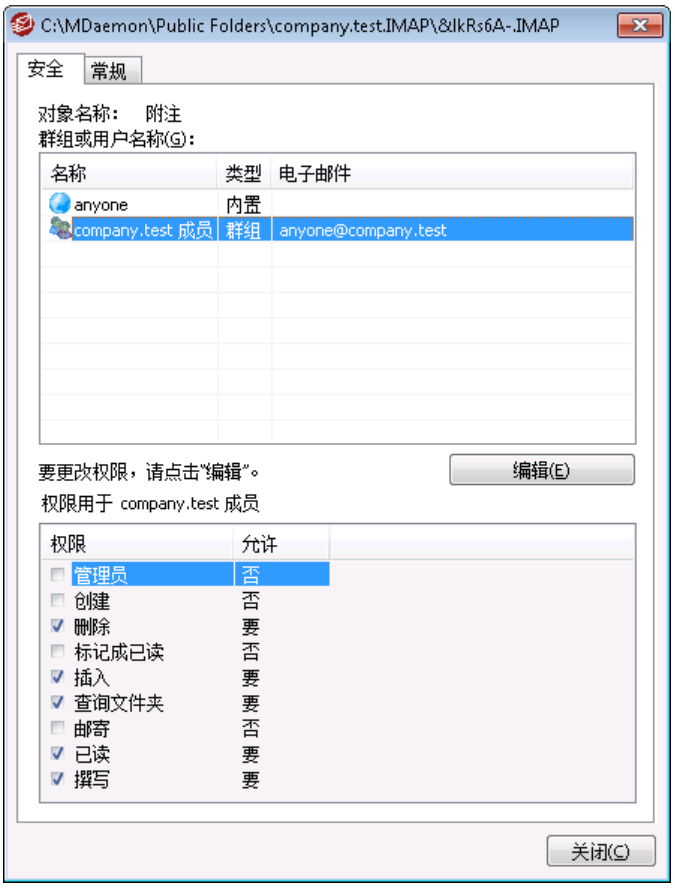
编辑访问控制列表
选择一个文件夹，然后点击该按钮打开此文件夹的 "访问控制列表[260]" 对话框。使用 "访问控制列表" 来指定能访问此文件夹的用户或群组，以及每个用户或群组的权限。

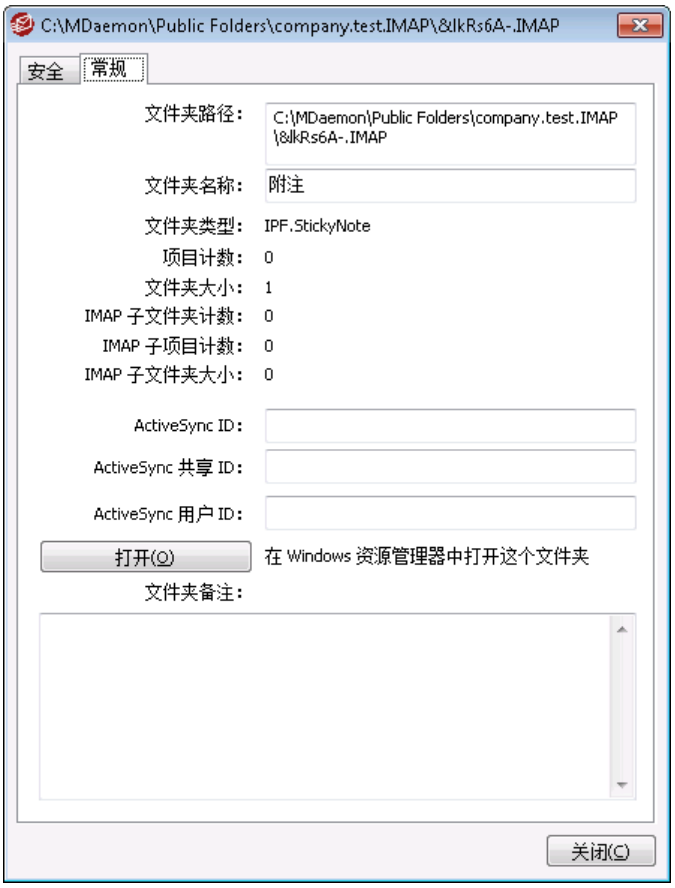
还请参阅：

访问控制列表[260]
公共文件夹管理器[258]

5.1.1.13.1 访问控制列表

访问控制列表 (ACL) 用来为您的公共和共享文件夹[95]设置用户或群组访问权限。可以从 *"编辑 ACLs"* 按钮 (位于公共文件夹管理器[258]) 或 *"编辑访问控制列表"* 按钮 (位于 "账户编辑器" 的 "共享文件夹[623]" 屏幕) 访问此项。





安全

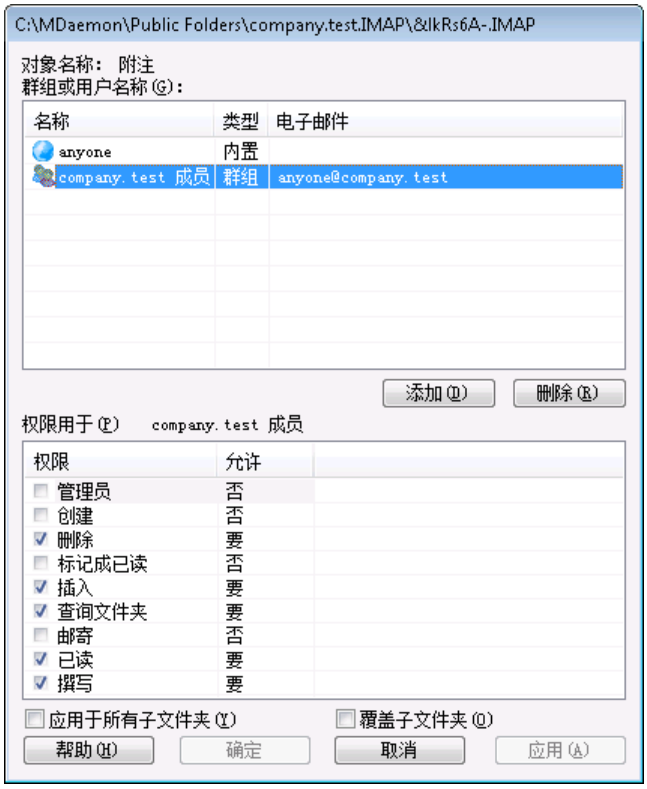
此选项卡显示与文件夹相关联的群组或用户列表，以及授予各自的特定访问权限。选择此列表中的一个群组或用户来显示其权限[263]，以便在下方的 "权限"窗口中审核。要编辑这些权限，请点击 "编辑[262]"。

常规

该选项卡显示文件夹的属性，例如其路径、名称、类型和大小等。

ACL 编辑器

点击 ACL "安全"选项卡上的 "编辑"来打开 ACL 编辑器修改访问权限。



对象名称
这是将应用 ACL 权限的对象或文件夹的名称。

群组或用户名
这些是将授予一些访问权限级别的群组或用户。选择群组或用户，以便在下方的 *"群组或用户>权限"*窗口中显示。对于您希望授予群组或用户的任何访问权限，请勾选其附近的选框。

添加
要向未列于上方的群组或用户授予访问权限，请点击 "添加"。

删除
要删除一个群组或用户，请选择上方列表中相应的条目并点击 "**删除**"。

<群组或用户>(<group oruser>)权限
对于您希望授予上方选定的群组或用户的任何访问权限，请勾选其附近的选框。

您可以授予以下访问控制权限：

管理员——用户可管理该文件夹的访问控制列表。

创建——用户可在该文件夹中创建子文件夹。

删除——用户可从该文件夹中删除项目。

标记已读——用户可更改该文件夹中邮件的已读/未读状态。

插入——用户可以添加或复制项目到该文件夹中。

查询文件夹——用户在其个人 IMAP 文件夹列表中可以看到该文件夹。

投递——用户可直接发送邮件到该文件夹中（如果文件夹运行的话）。

读取——用户可打开该文件夹并查看其内容。

写入——用户可以更改该文件夹中邮件的标记。

应用于所有子文件夹
如果您希望向文件夹当前包含的任何子文件夹应用这个文件夹的访问控制权限，请勾选此框。这将向这些子文件夹添加这个文件夹的用户和群组权限，并在发生任何冲突时进行替换。不过它不会删除当前对这些文件夹拥有访问权限的任何其他用户或群组权限。

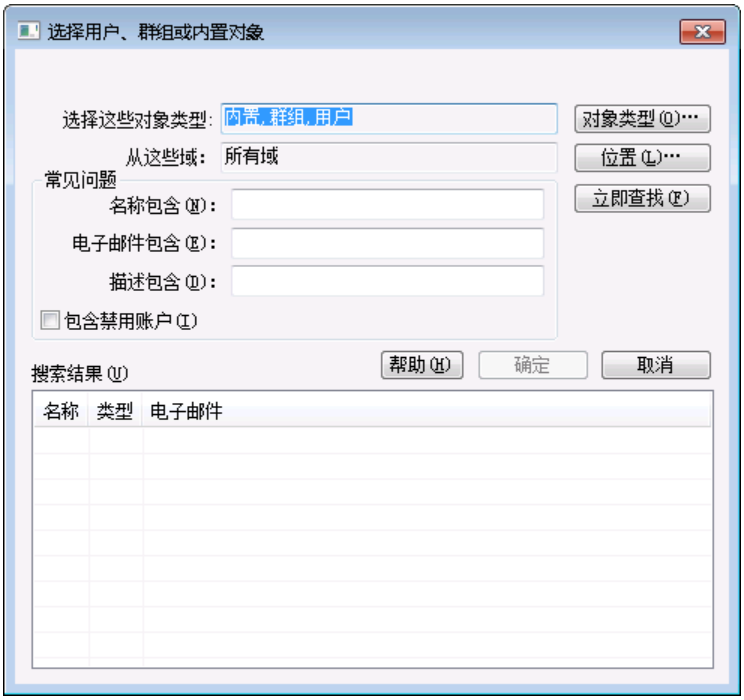
举例来说，

父文件夹向 User_A 和 User_B 授予特定权限。子文件夹向 User_B 和 User_C 授予访问权限。此项会将 User_A 权限添加到子文件夹，并使用父文件夹的权限来替换子文件夹的 User_B 权限，对 User_C 的权限不做任何操作。因此，这个子文件夹将拥有 User_A、User_B 和 User_C 的权限。

覆盖子文件夹
如果您希望使用父文件夹的当前权限来替换所有子文件夹的访问权限，请勾选此框。子文件夹的权限将与父文件夹的权限相同。

添加群组或用户

如果您希望将其他群组或用户添加到“访问控制列表”，请点击“ACL 编辑器”上的“添加”。这将打开“添加群组”或“用户”屏幕，您可以使用这两个屏幕来进行添加。



选择这些对象类型
点击 "**对象类型...**"来选择您希望为要添加的群组或用户搜索的对象类型。您可以选择："内置"、"群组"和 "用户"。

从这些位置
点击 "**位置...**"来选择您希望搜索的域。您可以选择所有 MDaemon 域或特定的域。

常规查询
使用这一部分的这些选项，通过指定所有或部分用户名、邮件地址或账户描述[598]的内容来缩小您的搜索范围。如果您希望这些搜索结果包含与上方指定的 "对象类型"和 "位置"相匹配的各个群组和用户，请留空这些字段。

包含 "禁用账户"
如果您希望在搜索中包含 "禁用账户[598]"，请勾选此框。

立即查找
在您指定了所有搜索条件之后，请点击 "**立即查找**"来执行搜索。

搜索结果
执行完搜索后，请在 "搜索结果"中选择任何所需群组或用户，并点击 "**确定**"来将其添加到 ACL。

访问权限可通过 MDaemon 对访问控制列表 (ACL) 的支持进行控制。ACL 是 Internet 邮件访问协议 (IMAP4)的扩展，它使您得以为每个 IMAP 邮件文件夹创建访问列表，从而将文件夹访问权限授

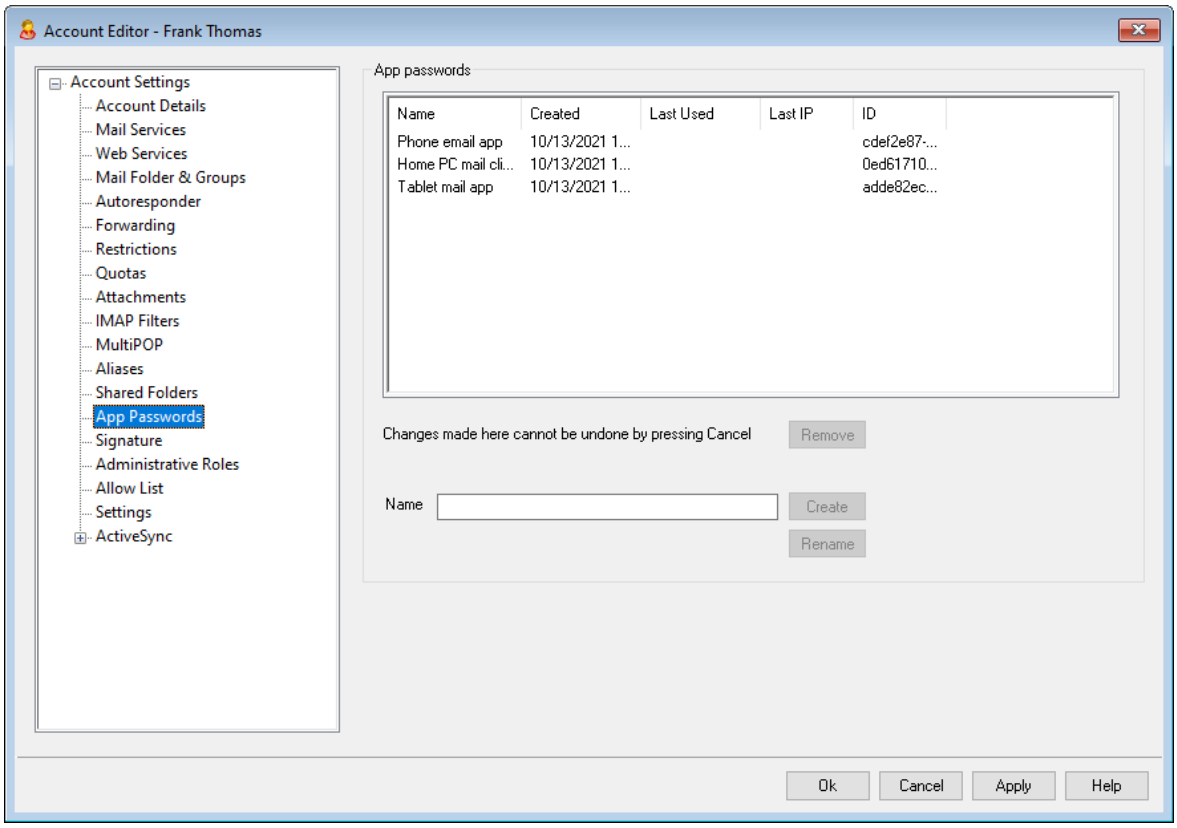
予在您的邮件服务器上拥有账户的其他用户。如果您的邮件客户端不支持 ACL，您仍可通过本对话框内的控件设置权限。

在 RFC 2086 中对 ACL 作了完整讨论，可访问以下网址来查阅该文档：http://www.rfc-editor.org/rfc/rfc2086.txt。

还请参阅：

公共文件夹管理器 258
公共文件夹概述 95
公共文件夹和共享文件夹 97
账户编辑器 » 共享文件夹 623
邮件列表 » 公共文件夹 248

5.1.1.14 应用程序密码



应用程序密码

应用程序密码是随机生成的强密码，用于电子邮件客户端和应用程序，有助于使您的电子邮件应用程序更加安全，因为它们无法受到双重验证 603 (2FA) 的保护。2FA 是用户登录 Webmail 或 MDaemon Remote Administration (MDRA) 的一种安全方式，但电子邮件应用程序无法使用它，因为该应用程序必须能够在后台访问您的电子邮件，无需您输

入身份验证器应用程序中的代码。这个应用程序密码功能允许您创建强大、安全的密码，以在您的应用程序中使用，同时仍然通过 2FA 保护您的账户密码。应用密码只能在电子邮件应用程序中使用，不能用于登录 Webmail或 MDRA。这意味着即使应用程序密码以某种方式被泄露，未经授权的用户仍然无法进入您的账户来更改您的密码或其他设置，但是您仍然可以使用账户和密码来登录您的账户，在需要时也能使用 2FA 来删除已泄露的应用程序密码，并创建一个新密码。

如果您不希望允许用户使用应用程序密码，您可以通过禁用 *"...编辑应用程序密码* 603 "选项（位于用户的 Web 服务页面）来实现这点。如果您希望为所有用户禁用对应用程序密码的支持，您可以使用*启用应用程序密码* 717选项，位于"密码"页面上。

应用程序密码要求和推荐

- 要创建应用程序密码，必须为账户启用 2FA（您也可以选择关闭该要求 717）。
- 应用密码只能在电子邮件应用程序中使用，不能用于登录 Webmail或 MDRA。
- 每个应用程序密码在创建时仅显示一次。以后无法检索它，因此用户应该准备好在创建时将其输入到他们的应用程序中。
- 用户应该为每个电子邮件应用程序使用不同的应用程序密码，并且当他们停止使用该应用程序或设备丢失或被盗时，他们应该撤销（删除）其密码。
- 每个应用程序密码都会列出它的创建时间、上次使用时间、以及上次访问账户邮件的 IP 地址。如果用户发现"上次使用"或"上次 IP 数据"有可疑之处，该用户应该撤销该"应用程序密码"，并为他或她的应用创建一个新密码。
- 更改账户密码后，所有应用程序密码都会被自动删除——用户无法继续使用旧的应用程序密码。

创建和使用应用程序密码

用户通常会按照以下概述的步骤在 Webmail中创建和管理他们自己的应用程序密码（此信息包含在 Webmail帮助文件中）。在用户开始操作之前，他应该让他的电子邮件应用程序或客户端准备好输入密码，因为应用程序密码在创建时只会显示一次。

1. 让应用程序或电子邮件客户端准备好输入应用程序密码。
2. 登录 Webmail并点击**"选项 » 安全"**。
3. 请在**"当前密码"**输入账户密码。
4. 点击**"新建应用程序密码"**。
5. 输入将使用此密码的应用程序的名称（例如"电话电子邮件应用程序"），然后点击**"确定"**。
6. 将显示的密码复制/粘贴或手动输入到您的邮件应用程序中，或者将其粘贴到文本文件中，或在必要时将其写下来。如果有人复制密码以备后用，他应在将其输入电子邮件客户端后删除该副本。完成后请点击**"确定"**。

如果出于某些原因，您需要为您的一位用户创建或删除应用程序密码，您可以使用此页面上的选项来执行此操作。就像在 Webmail中一样，应用程序密码在创建时只会显示一次，因此应立即将其输入到应用程序中，或复制到某个地方以供以后使用。

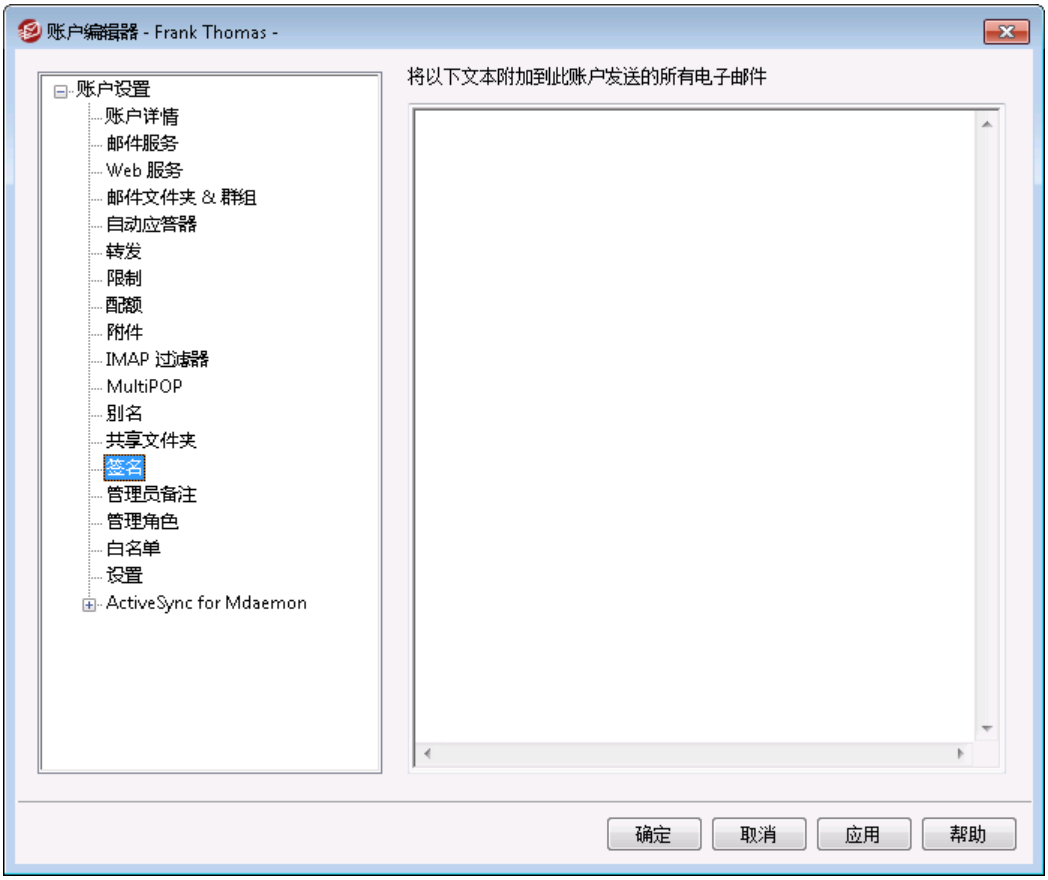
账户编辑器设置[639]页面上有一个账户选项，您可以使用它来要求*"需要应用程序密码才能登录 SMTP、IMAP、ActiveSync 等。"*。

"需要应用程序密码"有助于保护账户密码免受字典和通过 SMTP、IMAP 等进行的暴力攻击。这样更安全的原因是因为即使这种攻击是猜测账户的实际密码，它也不会不起作用，因为 MDaemon 只会接受正确的应用程序密码。此外，如果 MDaemon 中的账户正在使用活动目录[689]验证，"活动目录"又在达到失败的尝试次数后锁定了账户，该选项有助于防止账户被锁定，因为 MDaemon 只会检查应用程序密码，而不尝试对"活动目录"进行身份验证。

还请参阅：

密码[717]
账户编辑器 » 设置[639]

5.1.1.15 签名



账户签名

使用此屏幕来指定一个签名，此签名将会添加到账户所发送的每封邮件底部。除了添加此签名外，还有一些通过其他选项添加的签名或者脚注，例如 Webmail或者其他邮件客户端所包含的签名选项，"默认[109]"签名和 "域[166]"签名选项，以及邮件列表脚注[246]。默认/域签名和邮件列表脚注总是位于 "账户签名"下方。

能够访问 Webmail或 Remote Administration[293] 的用户可以从那里编辑自己的签名。

签名宏

MDaemon 签名支持将发件人的联系信息插入签名的宏，该签名取自位于其域的公共联系人文件夹中的发件人联系人。这允许使用发件人的信息对默认和域签名进行个性化。例如 $CONTACTFULLNAME$ 插入发件人的全名，$CONTACTEMAILADDRESS$ 插入发件人的邮件地址。使用 Webmail、MDaemon Connector 或 ActiveSync 来编辑公共联系人。如果发件人不存在联系人，则使用空值。可用的宏如下所示。

用户可以通过使用 $SYSTEMSIGNATURE$ 宏放置默认/域签名，并使用 $ACCOUNTSIGNATURE$ 放置账户签名来控制 MDaemon 签名在其邮件中的位置。

Signature Selector	
$SYSTEMSIGNATURE$	Places the Default Signature[109] or Domain Signature[166] in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature[113] or Domain Client Signature[170] in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature[632] in the message.
姓名和 ID	
全名	**$CONTACTFULLNAME$**
名	**$CONTACTFIRSTNAME$**
中间名	**$CONTACTMIDDLENAME$,**
姓	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
后缀	**$CONTACTSUFFIX$**
昵称	**$CONTACTNICKNAME$**
Yomi名	**$CONTACTYOMIFIRSTNAME$**
Yomi姓	**$CONTACTYOMILASTNAME$**
账户名称	**$CONTACTACCOUNTNAME$**
客户 ID	**$CONTACTCUSTOMERID$**
政府 ID	**$CONTACTGOVERNMENTID$**

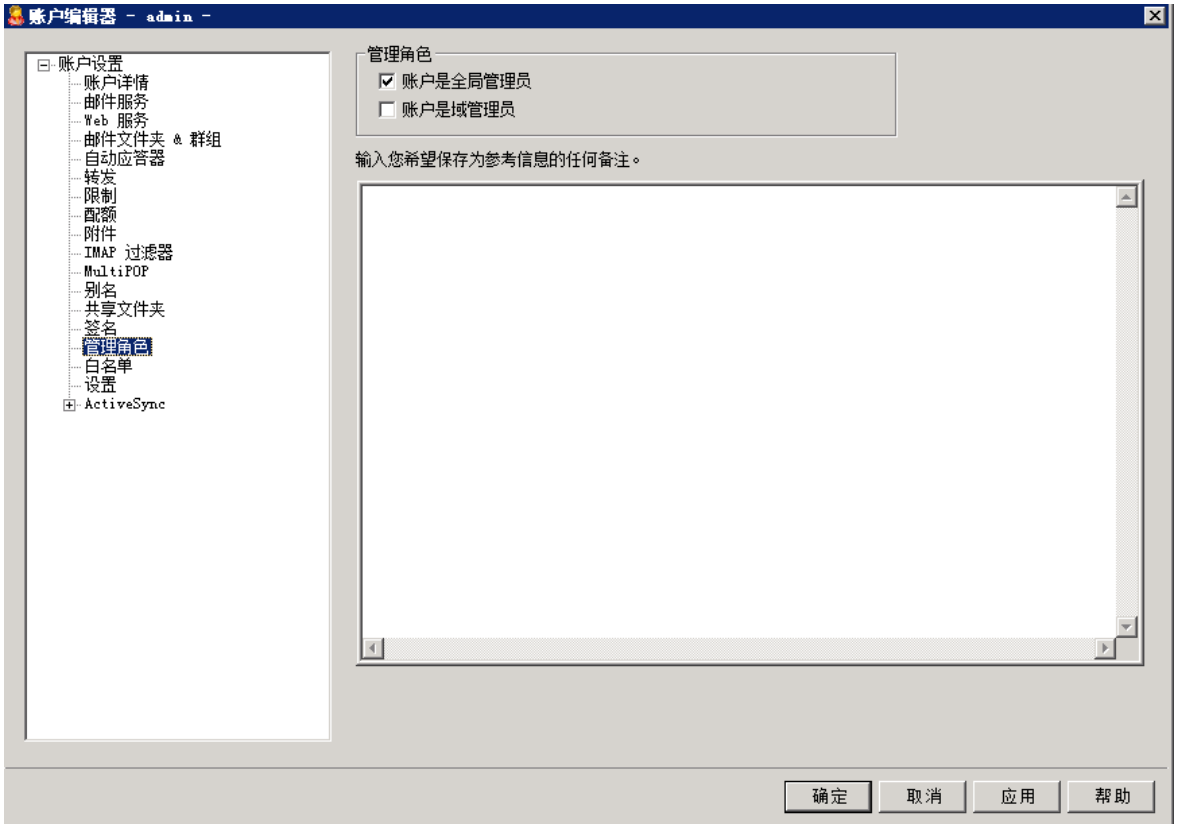
文件作为	**$CONTACTFILEAS$**
电子邮件地址	
电子邮件地址	**$CONTACTEMAILADDRESS$**
电子邮件地址 2	**$CONTACTEMAILADDRESS2$**
电子邮件地址 3	**$CONTACTEMAILADDRESS3$**
电话和传真号码	
手机号码	**$CONTACTHOMEMOBILE$**
手机 2	**$CONTACTMOBILE2$**
车载电话	**$CONTACTCARPHONENUMBER$**
家庭电话	**$CONTACTHOMEPHONE$**
家庭电话 2	**$CONTACTHOMEPHONE2$**
家庭传真	**$CONTACTHOMEFAX$**
其他电话	**$CONTACTOTHERPHONE$**
即时通讯和 W eb	
IM 地址	**$CONTACTIMADDRESS$**
IM 地址 2	**$CONTACTIMADDRESS2$**
IM 地址 3	**$CONTACTIMADDRESS3$**
M M D 地址	**$CONTACTMMSADDRESS$**
家庭网址	**$CONTACTHOMEWEBADDRESS$**
地址	
家庭地址	**$CONTACTHOMEADDRESS$**
家乡城市	**$CONTACTHOMECITY$**
家乡州	**$CONTACTHOMESTATE$**
家乡邮政编码	**$CONTACTHOMEZIPCODE$**
家乡国家	**$CONTACTHOMECOUNTRY$**
其他地址	**$CONTACTOTHERADDRESS$**
其他城市	**$CONTACTOTHERCITY$**
其他州	**$CONTACTOTHERSTATE$**
其他邮政编码	**$CONTACTOTHERZIPCODE$**
其他国家	**$CONTACTOTHERCOUNTRY$**

公司相关	
公司名称	**$CONTACTBUSINESSCOMPANY$**
Yomi公司名称	**$CONTACTYOMICOMPANYNAME$**
公司职位	**$CONTACTBUSINESSTITLE$**
公司办公室	**$CONTACTBUSINESSOFFICE$**
公司部门	**$CONTACTBUSINESSDEPARTMENT$**
公司经理	**$CONTACTBUSINESSMANAGER$**
公司助理	**$CONTACTBUSINESSASSISTANT$**
公司助理电话	**$CONTACTBUSINESSASSISTANTPHONE$**
公司总机	**$CONTACTBUSINESSMAINPHONE$**
公司电话	**$CONTACTBUSINESSPHONE$**
公司电话 2	**$CONTACTBUSINESSPHONE2$**
公司 IP 电话	**$CONTACTBUSINESSIPPHONE$**
公司传真	**$CONTACTBUSINESSFAX$**
公司寻呼机	**$CONTACTBUSINESSPAGER$**
公司无线电	**$CONTACTBUSINESSRADIO$**
公司地址	**$CONTACTBUSINESSADDRESS$**
公司所在城市	**$CONTACTBUSINESSCITY$**
公司所在州	**$CONTACTBUSINESSSTATE$**
公司邮政编码	**$CONTACTBUSINESSZIPCODE$**
公司所在城市	**$CONTACTBUSINESSCOUNTRY$**
公司网址	**$CONTACTBUSINESSWEBADDRESS$**
其他	
配偶	**$CONTACTSPOUSE$**
孩童	**$CONTACTCHILDREN$**
类别	**$CONTACTCATEGORIES$**
备注	**$CONTACTCOMMENT$**

还请参阅：

默认签名 109
域签名 166
邮件列表脚注 246

5.1.1.16 管理角色



管理角色

账户是全局管理员
启用该选择框来赋予用户服务器级别的管理员访问。全局管理员可以：

- 对于服务器配置的完全访问，通过 Remote Administration 对于所有域和所有用户的完全访问。
- 可以作为即时通信好友来访问所有 MDaemon 域的所有用户。
- 即使邮件列表标记为“只读”，仍可投递邮件到所有邮件列表。
- 即使管理员不是其中成员，仍可投递邮件到所有邮件列表。

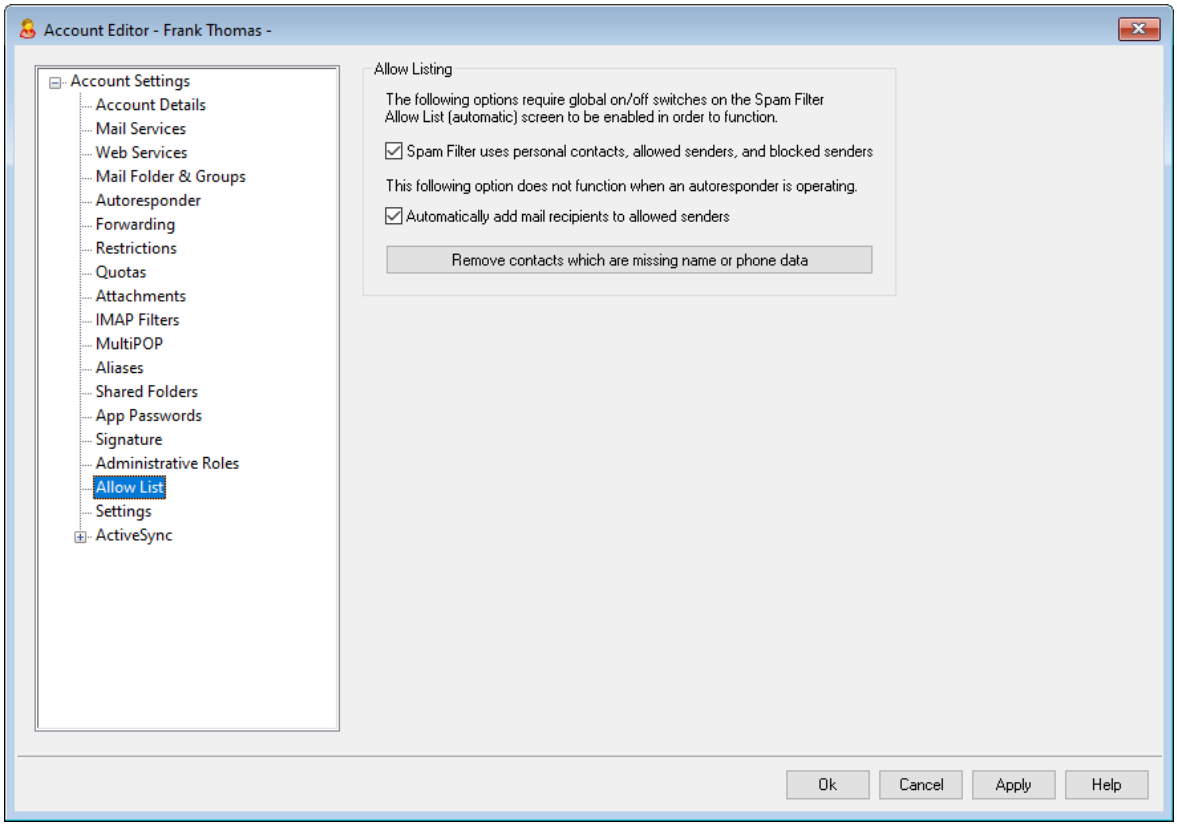
此用户可以对 MDaemon 的所有文件和选项进行完全访问。要了解 Remote Administration 的 web 界面内各种管理选项的详细信息，请参阅 Remote Administration 293。

账户是域管理员
点击此选择框来指定一个用户为域管理员。域管理员和全局管理员类似，不过其管理访问权限受到此域和 "Web 服务[603]"页面上所授权限的限制。

如果您希望允许该账户管理一个不同的域，您可以从 "Remote Administration[293]"的 "域管理器 » 管理"页面上实现这点。

输入您希望保存以供参考的任何注解
如果您希望为此账户添加您需要的任何备注或其他信息来供您参考，请使用此空间。此便笺与 *"描述"*字段（位于账户详细信息[598]屏幕）不同，不会被同步到公共联系人或映射到 "活动目录"中的任何字段。

5.1.1.17 允许列表



允许列表

垃圾邮件过滤器使用个人联系人、已允许发件人和已阻止发件人
"垃圾邮件过滤器"的 "允许列表（自动）[575]"屏幕上含有一个全局选项，如果在本地收件人的私人联系人或已允许发件人文件夹中找到邮件的发件人，那么使垃圾邮件过滤器将自动允许该邮件。如果在用户的已阻止发件人文件夹中找到发件人，就将自动阻止该邮件。如果您已启用了 "垃圾邮件过滤器"的全局选项，但不希望将此功能应用到该账户，请清除此框来覆盖全局设置。如果禁用了全局选项，此项将不可用。

自动将邮件收件人添加到已允许发件人
如果您希望在每次该账户地址簿发送一封出站邮件到一个非本地邮件地址时，更新此账户的已允许发件人文件夹，请点击此选项。当结合使用上述*"垃圾邮件过滤器使用私人联系人、已允许发件人和已阻止发件人"*选项时，可大幅减少垃圾邮件过滤器误报数量。在您使用*"自动将邮件收件人添加到已允许发件人"*选项(位于允许列表（自动）575屏幕上)之前，您必须已启用该功能。

在账户使用自动应答器时，该选项是禁用的。

删除缺少姓名或电话数据的联系人
如果您希望将仅包含电子邮件地址的每位联系人从账户默认的联系人文件夹中删除，请点击此按钮。如果联系人连姓名或电话数据都没，则会将其删除。该选项主要是帮助那些在版本 11 之前已使用 MDaemon允许列表选项的用户，纯粹作为用以清理联系人的允许列表功能而添加。在之前版本的 MDaemon 中，将地址添加到主要联系人而不是专用的允许列表文件夹。这可能会造成该账户在联系人文件夹中生成多个条目，而用户可能压根不需要这些条目的存在。

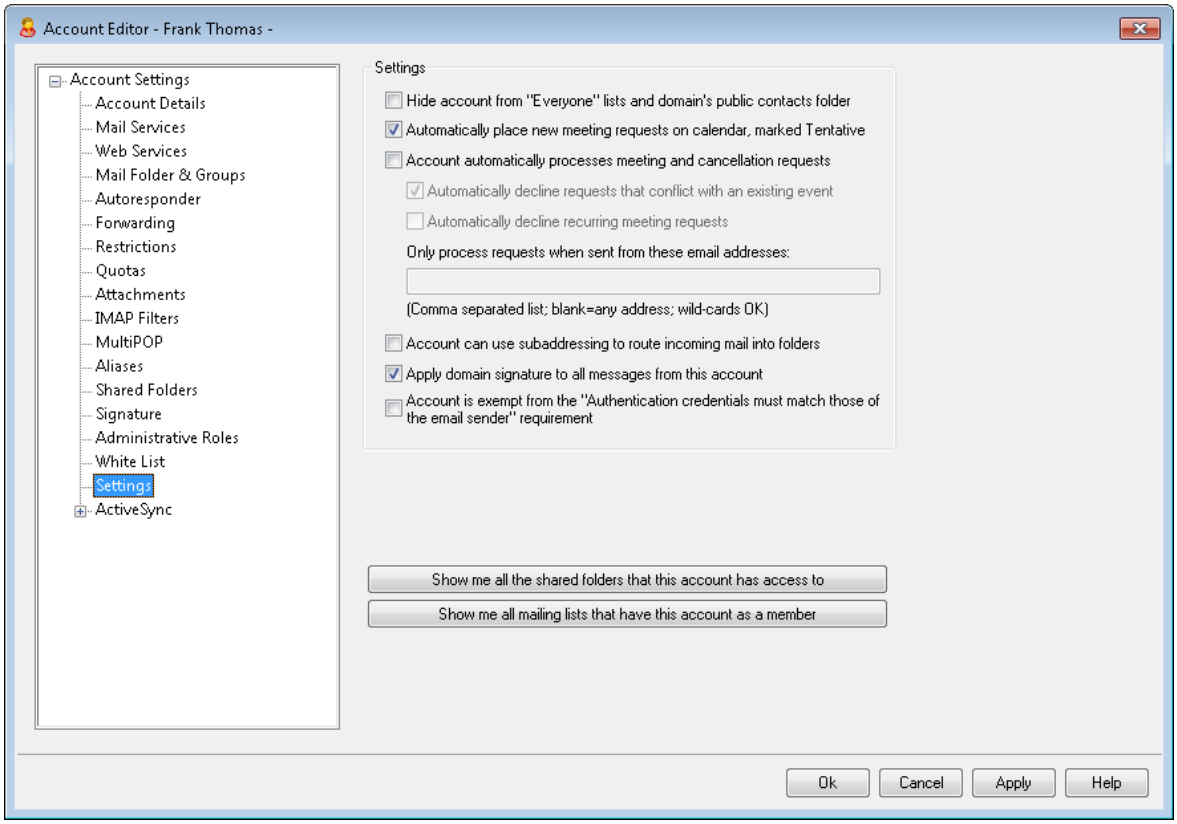
慎用此选择项，因为仅包含电子邮件地址的联系人也有可能是合法的。

为新账户和群组设置默认值
该屏幕上的这些选项对应位于"模板属性 » 允许列表686"屏幕上的选项，用来为新账户667设置默认值，并为所属特定群组657的账户设置值。

还请参阅：

允许列表（自动）575
模板管理器666
模板属性 » 允许列表686

5.1.1.18 设置



设置

从 "所有人"列表和域的公共联系人文件夹中隐藏账户
MDaemon 可以自动创建和维护 "Everyone@"和 "MasterEveryone@"邮件列表 225，能用来将一封邮件分别发送至域的所有用户和所有 MDaemon 用户。默认情况下这些列表包含各个域的所有账户，不过如果您希望从这些列表隐藏这个账户，您可以勾选此框。这也将从域的公共联系人文件夹中隐藏该账户。

自动在日历上放置标记为 "临时"的新会议请求
默认情况下，当一个账户收到新的会议请求时，会议将被放置在用户的日历上并标记为 *"临时"*。

账户自动处理会议和取消请求
如果您希望为该账户进行自动处理会议请求、更改及取消，请点击此选择框。当账户接收到一封包含会议请求的邮件，那么将自动更新账户的日历中。默认情况下为所有账户禁用该选项。

自动拒绝与现有事件相冲突的请求
如果为此账户启用了自动处理会议请求和取消，默认情况下，在这些会议请求与现有事件相冲突时将自动拒绝这些请求。如果您允许创建相冲突的事件，请取消勾选此框。

自动拒绝循环会议请求
如果已为此账户启用了自动处理会议请求和取消，不过您又希望拒绝那些循环会议请求，请点击此框。

只在从这些邮件地址发送时处理请求
如果您只想自动处理来自某些电子邮件地址的请求，请在这里列出这些地址。使用逗号来分隔多个地址。在地址中允许通配符（例如 *@example.com)。如果您将此框留空，则允许任何地址。

账户可以使用子寻址来将入站邮件路由到文件夹
如要允许对该账户进行子寻址 640，可点击该选择框。

向来自这个账户的所有邮件应用域签名
存在此账户所属域的“域签名 166”时，此项允许您将这个签名添加到该账户发送的所有电子邮件中。默认情况下，启用该选项。

账户免于“身份验证凭证必须匹配这些电子邮件发件人”要求
如果您希望此账户免于*“身份验证凭证必须匹配这些电子邮件发件人”*这个位于“SMTP 验证 438”屏幕的全局选项，则使用此项。默认情况下，禁用该选项。

需要应用程序密码才能登录 SMTP、IMAP、ActiveSync 等
如果您希望账户必须使用邮件客户端中的应用程序密码 630来登录 SMTP、IMAP、ActiveSync 或其他邮件服务协议，请勾选此框。不过，该账户的常规密码 717必须仍被用来登 Webmail或 Remote Admin。

“需要应用程序密码”有助于保护账户密码免受字典和通过 SMTP、IMAP 等进行的暴力攻击。这样更安全的原因是因为即使这种攻击是猜测账户的实际密码，它也不会不起作用，因为 MDaemon 只会接受正确的应用程序密码。此外，如果 MDaemon 中的账户正在使用活动目录 689验证，“活动目录”又被设置成在达到失败的尝试次数后锁定了账户，该选项有助于防止账户被锁定，因为 MDaemon 只会检查应用程序密码，而不尝试对“活动目录”进行身份验证。

向我显示该账户有权访问的所有共享文件夹
点击此按钮来显示该账户已被授予访问权限的所有共享文件夹。

显示该账户所属的所有邮件列表
点击此按钮来打开将该账户用作其中一员的所有邮件列表 223。

子寻址

子寻址这种系统用来将文件夹名称包含在账户邮件地址的邮箱部分中。利用该系统后，指向 *mailbox+folder* 名称组合的邮件将自动路由到该地址中所包含的账户文件夹中（假定该文件夹实际存在），无需创建特定的过滤器规则使其发生。

例如，如果 bill.farmer@example.com 有一个 IMAP 邮件文件夹名为 “stuff”，那么指向 “bill.farmer+stuff@example.com”的到达邮件将自动路由到该文件夹中。通过额外的 “+”号字符来分隔文件夹和子文件夹，以此指定子文件夹，在文件夹名称中可使用下划线来取代空格。所以，使用上述示例，如果 Bill的 “Stuff”文件夹有一个名为 “my older stuff”的子文件夹，那么指

向 "bill.farmer+stuff+my_older_stuff@example.com"的邮件将会自动路由到 Bill 的 "stuff\my older stuff"邮件文件夹中。

由于子寻址需要使用 "+"字符，包含 "+"的邮箱无法进行子寻址。因此，在上述示例中，如果实际地址为 "bill+farmer@example.com"而不是 "bill.farmer@example.com"，那么它将无法进行子寻址。此外，您不能在一个子地址中使用地址别名。不过，您可以创建引用整个子地址格式的别名。因此，即使不允许 "alias+stuff@example.com"，但可使用 "alias@example.com"来指向 "bill.farmer+stuff@example.com"。

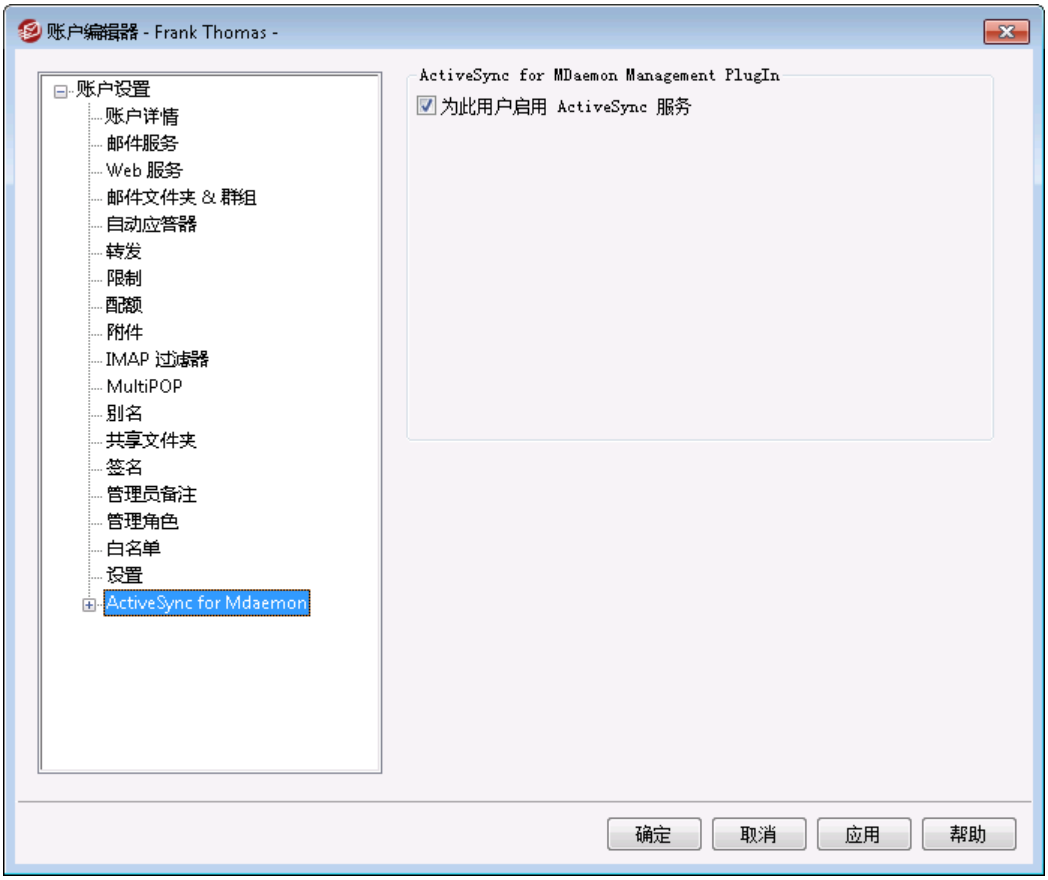
要防止漏洞或者滥用，在该子地址中所包含的 IMAP 文件夹必须是有效的。若有一封子寻址邮件到达一个账户，而该账户没有文件夹匹配子地址中所定义的文件名，那么该子地址将被视为一封未知的邮件地址并且根据您 MDaemon 的其他设置进行相应处理。例如：如果 bill.farmer@example.com 没有一个名为 "stuff"的文件夹，而一封到达邮件是 "bill.farmer+stuff@example.com"，那么该邮件将被视为是指向一个未知用户，并且很有可能会被拒收。

默认情况下，每个账户都已个别禁用了此功能。不过，您可以通过 *"为所有账户禁用子寻址功能"*选项来全局禁用此功能，此选项位于首选项对话框上的 "其他 421"屏幕。如果通过此选项禁用子寻址，那么无论个人账户设置如何，任何账户都不允许使用该功能。

还请参阅：

允许列表（自动） 575
Remote Administration 293
模板管理器 666
密码 717

5.1.1.19 ActiveSync for MDaemon



ActiveSync for MDaemon 屏幕位于"账户编辑器",用于为账户启用或禁用 ActiveSync、配置特定账户设置[643]、分配默认策略[648]、以及管理账户的 ActiveSync 客户端[649]。

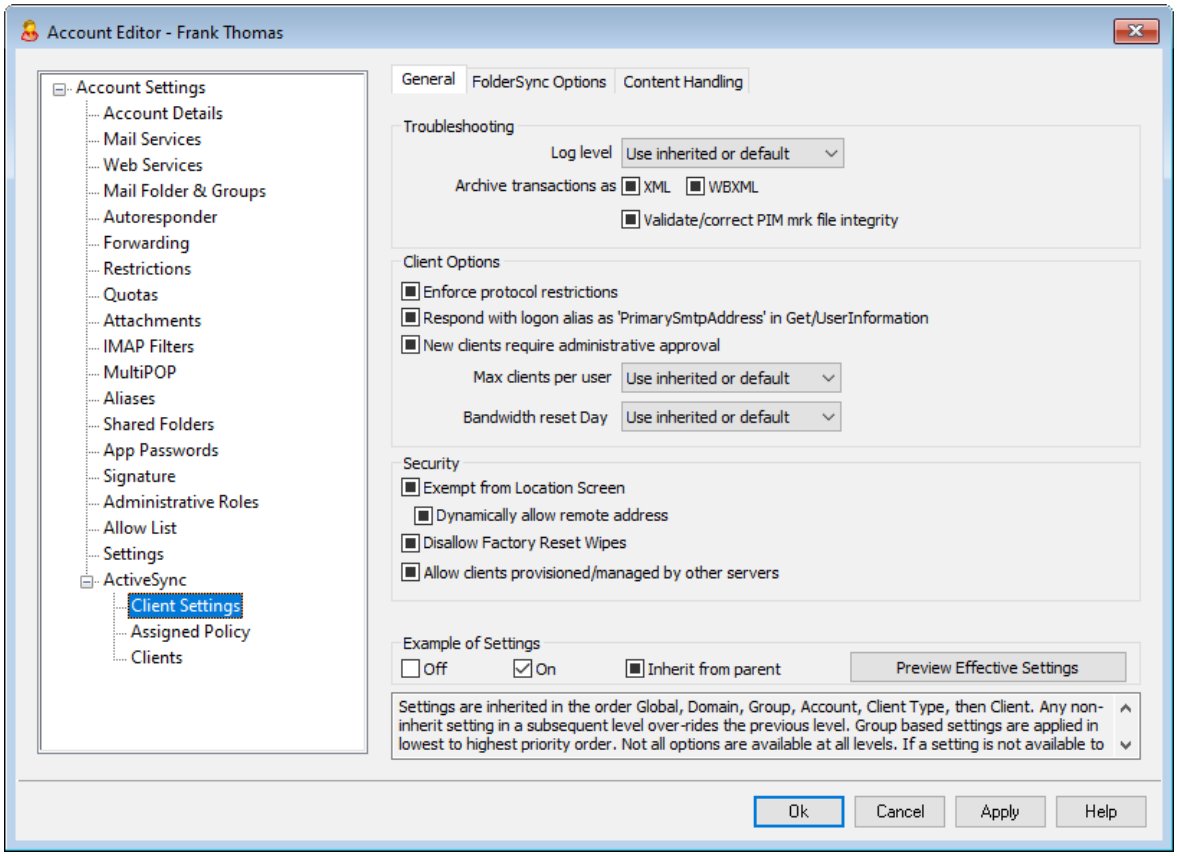
为账户启用/禁用 ActiveSync

如果您希望允许这个账户使用 ActiveSync 客户端来访问其电子邮件和 PIM 数据,请启用此项。

还请参阅:

账户编辑器 » ActiveSync » 客户端设置[643]
账户编辑器 » ActiveSync » 已分配策略[648]
账户编辑器 » ActiveSync » 客户端[649]

5.1.1.19.1 客户端设置



此屏幕上的选项用来为与此账户相关联的客户端控制 ActiveSync 客户端设置。默认情况下，会将各个选项配置成从账户所属的相应域继承其设置。更改此屏幕上的任何设置将覆盖这个账户的域设置 365。此外，如果您希望为特定客户端覆盖这些账户级别的设置，您可以使用 *"设置"*选项（位于 *"客户端* 649*"*屏幕）。

常规

故障诊断

日志级别

ActiveSync for MDaemon 支持 6 种日志级别，按所记录数据数量的多少分级，以下是从高到低的级别一览：

调试 这是最丰富的日志级别。记录所有可用条目，而且通常只在诊断问题时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键　记录关键错误和开机/关机事件。

无　只记录开机和关机事件。

Inherit　默认情况下，"日志级别"设置是从"客户端设置"层次结构继承的。因此，客户端从客户端类型继承，账户从客户端类型继承，群组从账户等继承其设置。此选项的"全局客户端设置"由故障诊断[361]对话框上的"日志级别"设置确定。

归档处理为 [XML | WBXML]
如果您希望保存此数据，请使用*"归档 XML..."*和*"WBXML"*选项，而且有时这些数据对调试很有帮助。默认情况下，禁用这些全局选项。

验证/修复 PIM mrk 文件完整性
该选项对客户端的 PIM 数据运行验证和修复进程来查询有碍正确同步的已知问题，例如重复的 iCalUID 或空的必填字段。默认情况下，禁用这个全局选项。

客户端选项

强制执行协议限制
如果有连接来自尝试使用指定的*"允许的协议版本"*以外的其他协议的客户端，您希望拒绝这些连接时请启用此项。默认情况下禁用此项，这就表示协议限制不防止客户端使用不同的协议：它们只是告诉客户端使用哪些协议。如果客户端无论如何都要尝试使用限制的协议，MDaemon 仍然允许这个连接。还请参阅：协议限制[363]来了解更多信息。

使用登录别名响应，作为 GetUserInformation 中的"PrimarySmtpAddress"
这允许该服务返回别名/次要地址作为主要地址来响应"设置/获取/用户信息"请求。这有助于解决 iOS9.x 更新所引起的一个问题：即导致客户端无法使用别名发送邮件。使用此项将导致对于"设置/获取/用户信息"不规范的响应。

新建客户端需要管理批准
如果您希望要求新的客户端必须先由管理员授权，才能开始与账户同步，请启用此选项。The 客户端[388]列表指示等候授权的任何客户端，管理员可以从相同的屏幕对其进行授权。默认情况下，禁用该设置。

每用户的客户端最大值
如果您希望限制 MDaemon 账户可以关联的 ActiveSync 客户端或设备的数量，请在此项中指定所需数量。默认情况下将这个全局选项设成"无限"。"全局"、"域"和"账户"客户端设置屏幕提供此项，但是个别客户端屏幕不提供此项。

带宽重置日期
如果您希望在每个月指定的一天为 ActiveSync 设备重置带宽使用统计，请使用此项。重置事件作为常规夜间维护过程的一部分进行，而且像其他维护例程一样被记录到系统日志中。默认情况下将这个全局选项设置成"0"（从不），这就意味着从不重置使用统计。如果您希望重置的那一天与用户或客户端无线运营商计费的重置日期一致，请将子项设置成不同的一天。

安全

从“位置屏蔽”豁免
启用此项（位于 ActiveSync 客户端的设置屏幕）允许您将设备绕过位置屏蔽[477]。这使得有效的用户有可能通过 ActiveSync 继续访问他或她的账户，例如当前往一个阻止验证尝试的位置时。为了免除设备，它必须使用 ActiveSync 在配置的时间范围内进行连接和验证，请在位于“微调”屏幕的这些天后删除闲置的客户端[351]这个设置中进行配置。

动态允许远程地址
当从“位置屏蔽”豁免设备时，如果您还希望允许其连接的远程 IP 地址，请启用此选项。这对允许其他可能从相同 IP 地址连接的客户端很有用。

允许由其他服务器配置/管理的客户端
默认情况下，当 ActiveSync 服务器向特定客户端发送数据/策略，并报告它也受其他 ActiveSync 服务器管理时，也允许那个客户端连接到 MDaemon。不过在这种情况下，无法确保在与其他 ActiveSync 服务器的策略发生冲突时将应用您的策略。通常默认客户端在策略冲突时使用最具有限制性的选项。如果您不希望允许这些客户端进行连接，请禁用此项。

不允许出厂重置擦除
如果将其设置成启用/是，就不提供完全擦除 ActiveSync 客户端的功能。如果您希望能够完全远程擦除客户端，您必须先禁用此项。默认情况下，禁用该选项。要了解更多详情，请参阅：“客户端”页面上的完全擦除 ActiveSync 客户端[388]。

FolderSync 选项

FolderSync 选项

例外

已允许/已阻止发件人文件夹
默认情况下，无法和设备同步用户的“已允许发件人和已阻止发件人”联系人文件夹。它们通常只能由 MDaemon 用来吸住自动防止垃圾邮件。出于这个原因，它们无需在设备上显示为联系人。

非默认邮件文件夹
默认情况下能与设备同步所有由用户创建和默认的邮件文件夹。如果您仅希望允许同步默认的邮件文件夹（例如收件箱、已发送项目、已删除项目和草稿等），请启用此项。不会包含由用户创建的文件夹。默认情况下，禁用该选项。

非默认 PIM 文件夹
默认情况下，将与设备同步用户的所有 PIM 文件夹（例如联系人、日历、便笺和任务等）。如果您希望仅允许同步默认的 PIM 文件夹，请启用此项。例如，如果启用此项，而且用户拥有多个日历文件夹，将仅同步默认的日历。默认情况下，禁用该选项。

包括

公告文件夹层次结构
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的公共文件夹[258]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的公共文件夹[258]。默认情况下允许搜索操作。

公共文件夹遍历（显示文件夹名称）
默认情况下，为了让客户端同步/访问公共子文件夹，该账户必须拥有查询权限[260]，而且必须对子文件夹和所有父代公共文件夹[258]拥有该权限。如果该账户没有权限查看父文件夹，那么该账户也不能查看子文件夹，即使该账户有查看子文件夹的权限也是如此。如果您希望允许客户端访问这些子文件夹，请启用此项。**请注意：**启用此项必须向客户端显示父文件夹的名称，这会被视为安全风险。默认情况下，禁用该选项。

允许的公共文件夹数量最大值
如果您希望限制在设备上允许的"公共文件夹"的数量，请使用此项。在设置了限制时，该服务器遍历文件夹列表，直到达到这个限制为止，不会再将更多项目发送到设备。无法确保以何顺序处理这些文件夹。默认情况下未设置全局限制。

共享文件夹
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的共享文件夹[97]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的共享文件夹[623]。默认情况下允许搜索操作。

内容处理

内容处理选项

在被客户端标记时为邮件项目创建任务/提醒
该选项可以在客户端请求时，使 MDaemon 通过为各个已标记的邮件创建任务项目来向用户提醒已标记的项目。。默认情况下，此控件的全局选项处于启用状态。

在事件被修改时始终发送会议更新
某些客户端在修改会议时未正确发送会议更新电子邮件。这指示 ActiveSync 服务在组织者更新会议项目时发送会议更新。这仅能在客户端[388]和无法恰当发送会议更新的客户端类型[402]上设置，否则将导致发送重复的会议更新。因此，此选项仅在"客户端"和"客户端类型"的设置页面上可用。

对所有已发送邮件请求已读回执
如果您希望服务器为客户端发送的所有邮件请求已读确认，请启用此项。默认情况下，禁用该选项。

当邮件被标记为已读时，以及发件人请求时，从服务器发送已读回执
如果您希望服务器支持已读确认请求，并在客户端将邮件标记为已读时发送已读回执，请启用此项。默认情况下，禁用该选项。

发送为在 ReplyTo 地址中指定的别名
某些客户端可能不允许发件人使用别名发送邮件。已在 Exchange ActiveSync (EAS) 协议[363] 16.x 中添加该功能，不过一些客户端不支持 16.x。例如，Windows 版的 Outlook

仅使用 EAS 14.0，虽然它允许用户指定要发送的备用地址，但生成的邮件并不能正确反映用户的选择。该选项允许使用 ReplyTo（答复）字段来发送电子邮件，只要 ReplyTo 地址是该用户的有效别名[699]即可。默认情况下启用这个全局选项。

虚拟地将公共联系人合并为默认联系人
如果您希望将设备上的公共联系人与用户的默认联系人合并在一起，请启用此项。这仅仅是一个虚拟合并，实际上未将它们复制到用户的联系人文件夹。这对不支持"全局地址列表"(GAL)搜索的客户端而言极其有用。默认情况下，禁用该选项。

在将邮件移入垃圾邮件文件夹时阻止发件人
启用后，当客户端将电子邮件移动到账户的垃圾邮件文件夹时，该服务将该电子邮件的发件人或从地址添加到阻止的发件人联系人文件夹。

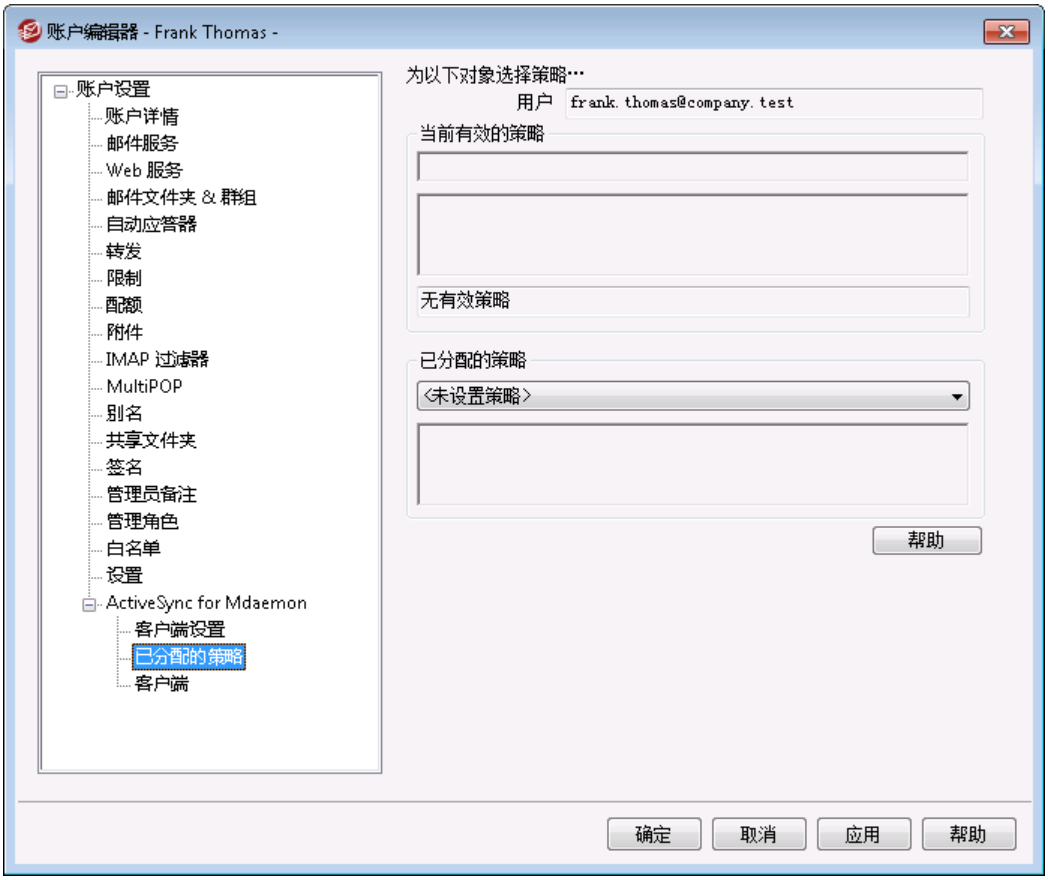
在会议请求被接受/拒绝等时强制发送会议请求。
启用后，当客户端接受、拒绝或以其他方式选择响应会议请求的操作时，服务将向会议组织者发送会议响应。这是针对没有正确发送这些更新本身的特定客户端。

预览有效设置
该按钮在所有子"客户端设置"屏幕上可用（例如域[365]、账户[380]和客户端[388]）。由于默认情况下，已将这些屏幕上的选项都设置成从父屏幕继承其设置，使用该功能来查看当前向显示的屏幕应用了什么设置。

还请参阅：

ActiveSync » 域[365]
账户编辑器 » ActiveSync » 客户端[649]

5.1.1.19.2 已分配策略



使用此屏幕来指定默认的 ActiveSync 策略[372]，这些策略将用于使用此账户进行连接的任何 ActiveSync 客户端。默认情况下，这个策略设置从域的策略[190]设置继承，不过您可以在此处更改它来覆盖这个账户的设置。此外，您也可以覆盖特定的账户设置，并将不同的策略分配至特定的客户端[649]。

分配 ActiveSync 策略

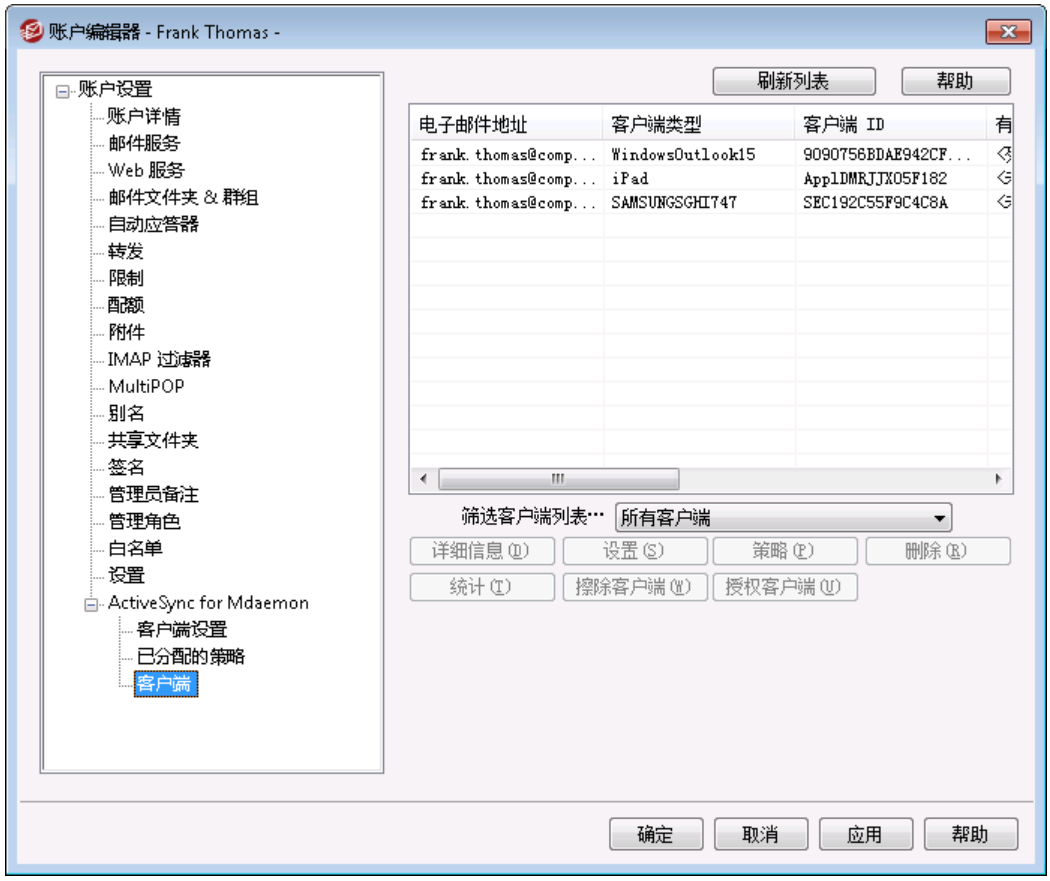
要为此账户分配策略，请点击**待分配策略**"下拉列表，选择策略，并点击 **确定**"或 **应用**"。

并非所有的 ActiveSync 设备都识别这些策略或按设置应用策略。有些设备可能忽略这些策略或一些策略元素，有些设备可能必须在重启后才能使策略设置生效。此外，在尝试分配一个新策略时，只有在该设备自身下一次连接到 ActiveSync 服务器时才会应用这个策略；而且只有在建立连接时才能将这些策略 "推送"到设备。

还请参阅：

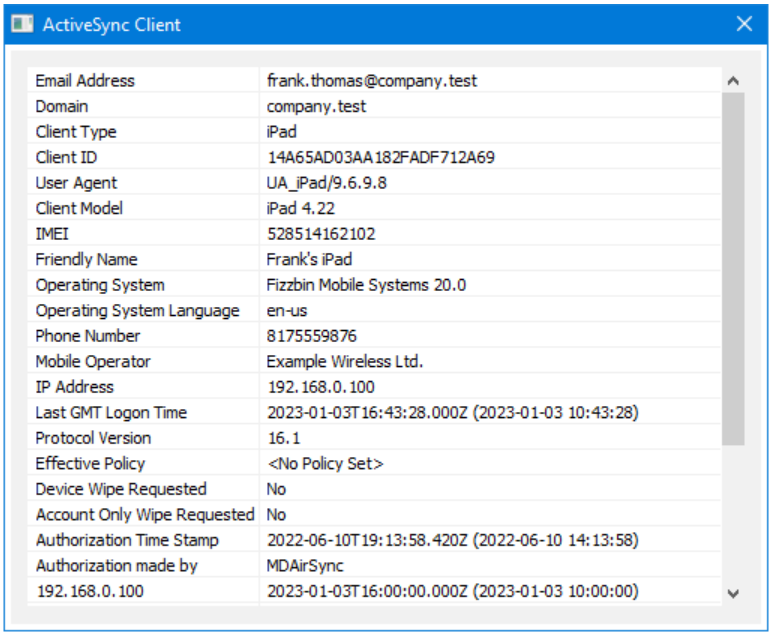
ActiveSync » 策略管理器[372]
ActiveSync » 域[365]
账户编辑器 » ActiveSync » 客户端[649]

5.1.1.19.3 客户端



此屏幕显示与此用户账户相关联的任何 ActiveSync 客户端的信息。您可以从此处为每个客户端分配 ActiveSync 策略 648、控制各种客户端设置、远程擦除这些客户端，并在 MDaemon 内重置客户端统计。

ActiveSync 客户端详细信息



双击一个条目，或右键单击该条目并点击 **"查看详细信息"**来打开 "客户端详细信息"对话框。此屏幕包含有关客户端的信息，例如其客户端类型、客户端 ID 和上次登录时间等。

客户端设置

右键点击一个客户端并点击 **"自定义客户端设置"**来管理其 "客户端设置"。默认情况下，这些设置是从 "客户端类型"设置继承的，但是可以按需进行调整。请参阅下方的 管理设备的客户端设置 651 。

分配 ActiveSync 策略

要向设备分配一个策略 372:

1. 右键单击此列表中的一个设备。
2. 点击 **"分配策略"**。这会打开 "应用策略"对话框。
3. 点击 **"特分配策略"**下拉列表并选择所需策略。
4. 点击 **"确定"**。

统计

右键点击一个条目，并点击 **"统计"**来打开 "客户端统计"对话框，其中含有关于该客户端的各种使用统计。

重置统计

如果要重置客户端的统计信息，请右键单击该客户端，然后依次点击 **"重置统计"**和 **"确定"**来确认操作。

删除 ActiveSync 客户端

要删除 ActiveSync 客户端，右键单击客户端并点击**删除**，然后点击**是**。这将删除列表中的

客户端，并删除 MDaemon 中与其相关的所有同步信息。因此，如果该账户在未来使用 ActiveSync 来同步相同的客户端，MDaemon 会将该客户端视作从未在这台服务器上使用过的客户端；所有客户端数据必须重新与 MDaemon 进行同步。

完全擦除 ActiveSync 客户端

在将一个策略[372]应用到选定的 ActiveSync 客户端时，并且客户端已应用它并做出响应，则该客户端将有一个可用的 "完全擦除"选项。要进行完全擦除，请右键点击客户端（如果您使用 MDRA，请选择它），并点击 **"完全擦除"**。下次该客户端进行连接时，MDaemon 将告诉它擦除所有数据，或将自身重置成出厂默认状态。取决于该客户端，上述操作可能删除设备上的一切，包括已下载的应用程序。此外，只要客户端的 ActiveSync 条目存在，MDaemon 将在该设备日后进行连接的任何时候继续发送擦除请求。如果有时您希望删除客户端，请确保您先将其添加到阻止列表[359]，这样它以后就无法再次连接。最后，如果擦除的设备被恢复，并且您希望允许它再次连接，您应该选择该设备并点击 **"取消擦除操作"**。您也必须从 阻止列表将其删除。

账户擦除 ActiveSync 客户端

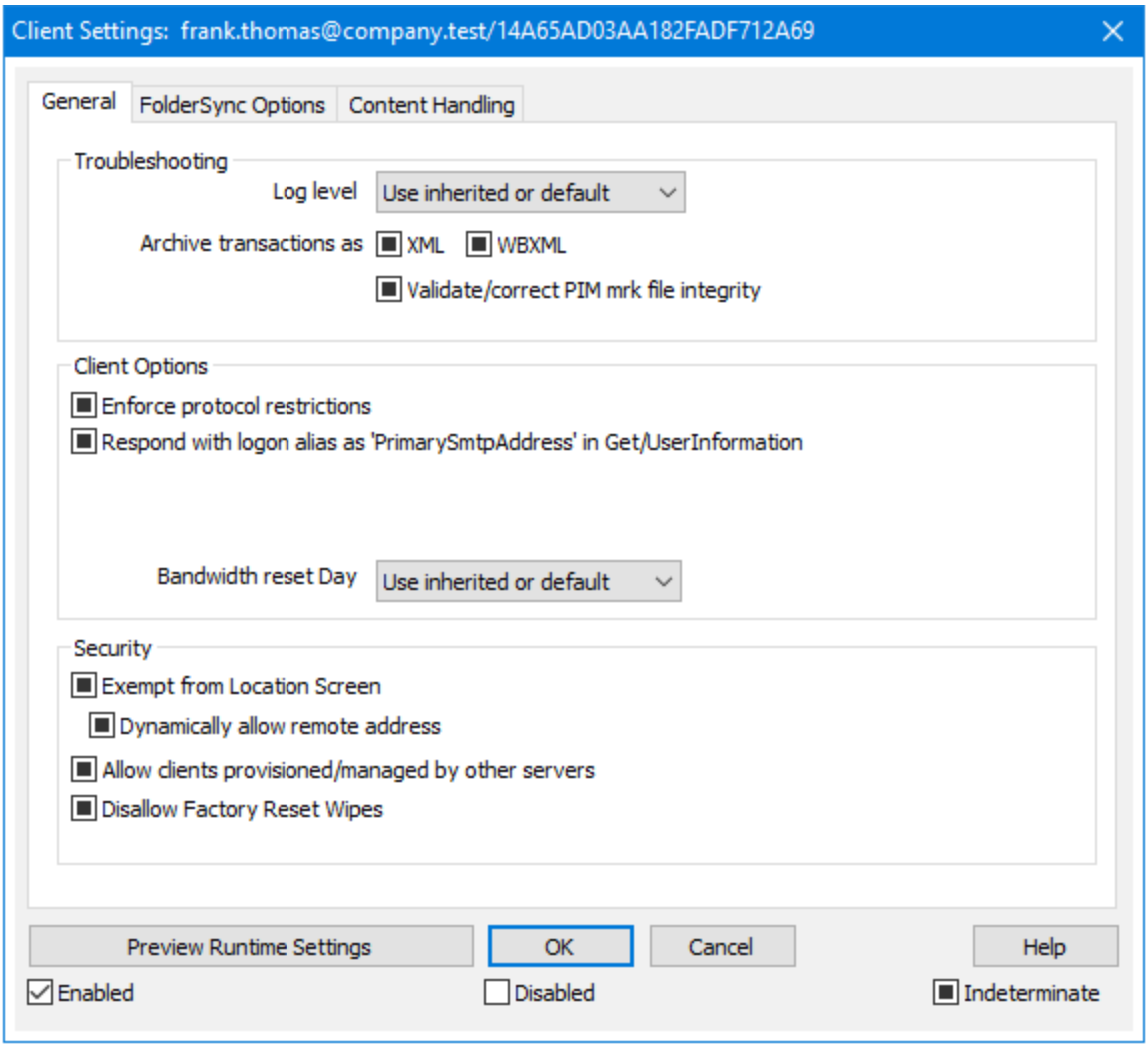
要从客户端或设备中擦除账户的邮件和 PIM 数据，请右键点击并选择 **"从客户端擦除账户邮件和 PIM"**。*"账户擦除"*选项与上述 *"完全擦除"*选项类似，不过该项不擦除所有数据，而是仅擦除这个账户的数据，例如其电子邮件、日历条目和联系人等。保留剩余所有项目，例如应用程序、照片或音乐。

授权客户端

如果将 *"新建客户端需要管理批准"*选项（位于 ActiveSync 客户端设置[353]屏幕）设置成需要批准，选择一个客户端并点击批准客户端进行同步来授权它与服务器进行同步。

管理设备的客户端设置

设备级别的 "客户端设置"屏幕允许您管理特定设备的设置。



默认情况下，此屏幕上的所有选项都被设置为 "使用继承或默认值"，表示每个选项都会从客户端类型客户端设置 402 屏幕上的相应选项中获取其设置。在此屏幕上对设置做出的任何变更都将在屏幕上反映。反之亦然，您在此屏幕上做出的任何变更将覆盖此设备的客户端类型级别的设置。

常规

故障诊断

日志级别

ActiveSync for MDaemon 支持 6 种日志级别，按所记录数据数量的多少分级，以下是从高到低的级别一览：

调试 这是最丰富的日志级别。记录所有可用条目，而且通常只在诊断问题时使用。

信息 适度记录。不含详细信息记录常规操作。这是默认的日志级别。

警告 记录警告、错误、关键错误和开机/关机事件。

错误 记录错误、关键错误和开机/关机事件。

关键 记录关键错误和开机/关机事件。

无 只记录开机和关机事件。

Inherit 默认情况下，"日志级别"设置是从"客户端设置"层次结构继承的。因此，客户端从客户端类型继承，账户从客户端类型继承，群组从账户等继承其设置。此选项的"全局客户端设置"由故障诊断[361]对话框上的"日志级别"设置确定。

归档处理为 [XML | WBXML]
如果您希望保存此数据，请使用*"归档 XML..."*和*"WBXML"*选项，而且有时这些数据对调试很有帮助。默认情况下，禁用这些全局选项。

验证/修复 PIM mrk 文件完整性
该选项对客户端的 PIM 数据运行验证和修复进程来查询有碍正确同步的已知问题，例如重复的 iCalUID 或空的必填字段。默认情况下，禁用这个全局选项。

客户端选项

强制执行协议限制
如果有连接来自尝试使用指定的*"允许的协议版本"*以外的其他协议的客户端，您希望拒绝这些连接时请启用此项。默认情况下禁用此项，这就表示协议限制不防止客户端使用不同的协议：它们只是告诉客户端使用哪些协议。如果客户端无论如何都要尝试使用限制的协议，MDaemon 仍然允许这个连接。还请参阅：协议限制[363]来了解更多信息。

使用登录别名响应，作为 GetUserInformation 中的"PrimarySmtpAddress"
这允许该服务返回别名/次要地址作为主要地址来响应"设置/获取/用户信息"请求。这有助于解决 iOS9.x 更新所引起的一个问题：即导致客户端无法使用别名发送邮件。使用此项将导致对于"设置/获取/用户信息"不规范的响应。

新建客户端需要管理批准
如果您希望要求新的客户端必须先由管理员授权，才能开始与账户同步，请启用此选项。The 客户端[388]列表指示等候授权的任何客户端，管理员可以从相同的屏幕对其进行授权。默认情况下，禁用该设置。

每用户的客户端最大值
如果您希望限制 MDaemon 账户可以关联的 ActiveSync 客户端或设备的数量，请在此项中指定所需数量。默认情况下将这个全局选项设成"无限"。"全局"、"域"和"账户"客户端设置屏幕提供此项，但是个别客户端屏幕不提供此项。

带宽重置日期
如果您希望在每个月指定的一天为 ActiveSync 设备重置带宽使用统计，请使用此项。重置事件作为常规夜间维护过程的一部分进行，而且像其他维护例程一样被记录到系统日志中。默认情况下将这个全局选项设置成"0"(从不)，这就意味着从不重置使用统计。如果您希望重置的那一天与用户或客户端无线运营商计费的重置日期一致，请将子项设置成不同的一天。

安全

从“位置屏蔽”豁免
启用此项（位于 ActiveSync 客户端的设置屏幕）允许您将设备绕过位置屏蔽[477]。这使得有效的用户有可能通过 ActiveSync 继续访问他或她的账户，例如当前往一个阻止验证尝试的位置时。为了免除设备，它必须使用 ActiveSync 在配置的时间范围内进行连接和验证，请在位于“微调”屏幕的这些天后删除闲置的客户端[351]这个设置中进行配置。

动态允许远程地址
当从“位置屏蔽”豁免设备时，如果您还希望允许其连接的远程 IP 地址，请启用此选项。这对允许其他可能从相同 IP 地址连接的客户端很有用。

允许由其他服务器配置/管理的客户端
默认情况下，当 ActiveSync 服务器向特定客户端发送数据/策略，并报告它也受其他 ActiveSync 服务器管理时，也允许那个客户端连接到 MDaemon。不过在这种情况下，无法确保在与其他 ActiveSync 服务器的策略发生冲突时将应用您的策略。通常默认客户端在策略冲突时使用最具有限制性的选项。如果您不希望允许这些客户端进行连接，请禁用此项。

不允许出厂重置擦除
如果将其设置成启用/是，就不提供完全擦除 ActiveSync 客户端的功能。如果您希望能够完全远程擦除客户端，您必须先禁用此项。默认情况下，禁用该选项。要了解更多详情，请参阅：“客户端”页面上的完全擦除 ActiveSync 客户端[388]。

FolderSync 选项

FolderSync 选项

例外

已允许/已阻止发件人文件夹
默认情况下，无法和设备同步用户的“已允许发件人和已阻止发件人”联系人文件夹。它们通常只能由 MDaemon 用来吸住自动防止垃圾邮件。出于这个原因，它们无需在设备上显示为联系人。

非默认邮件文件夹
默认情况下能与设备同步所有由用户创建和默认的邮件文件夹。如果您仅希望允许同步默认的邮件文件夹（例如收件箱、已发送项目、已删除项目和草稿等），请启用此项。不会包含由用户创建的文件夹。默认情况下，禁用该选项。

非默认 PIM 文件夹
默认情况下，将与设备同步用户的所有 PIM 文件夹（例如联系人、日历、便笺和任务等）。如果您希望仅允许同步默认的 PIM 文件夹，请启用此项。例如，如果启用此项，而且用户拥有多个日历文件夹，将仅同步默认的日历。默认情况下，禁用该选项。

包括

公告文件夹层次结构
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的公共文件

夹[258]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的公共文件夹[258]。默认情况下允许搜索操作。

公共文件夹遍历（显示文件夹名称）
默认情况下，为了让客户端同步/访问公共子文件夹，该账户必须拥有查询权限[260]，而且必须对子文件夹和所有父代公共文件夹[258]拥有该权限。如果该账户没有权限查看父文件夹，那么该账户也不能查看子文件夹，即使该账户有查看子文件夹的权限也是如此。如果您希望允许客户端访问这些子文件夹，请启用此项。**请注意：**启用此项必须向客户端显示父文件夹的名称，这会被视为安全风险。默认情况下，禁用该选项。

允许的公共文件夹数量最大值
如果您希望限制在设备上允许的“公共文件夹”的数量，请使用此项。在设置了限制时，该服务器遍历文件夹列表，直到达到这个限制为止，不会再将更多项目发送到设备。无法确保以何顺序处理这些文件夹。默认情况下未设置全局限制。

共享文件夹
如果您希望在 ActiveSync 设备上的用户文件夹列表中包含用户有权访问的共享文件夹[97]，则勾选此框。默认启用此项。

允许屏蔽
允许客户端搜索它有权访问的共享文件夹[623]。默认情况下允许搜索操作。

内容处理

内容处理选项

在被客户端标记时为邮件项目创建任务/提醒
该选项可以在客户端请求时，使 MDaemon 通过为各个已标记的邮件创建任务项目来向用户提醒已标记的项目。。默认情况下，此控件的全局选项处于启用状态。

在事件被修改时始终发送会议更新
某些客户端在修改会议时未正确发送会议更新电子邮件。这指示 ActiveSync 服务在组织者更新会议项目时发送会议更新。这仅能在客户端[388]和无法恰当发送会议更新的客户端类型[402]上设置，否则将导致发送重复的会议更新。因此，此选项仅在“客户端”和“客户端类型”的设置页面上可用。

对所有已发送邮件请求已读回执
如果您希望服务器为客户端发送的所有邮件请求已读确认，请启用此项。默认情况下，禁用该选项。

当邮件被标记为已读时，以及发件人请求时，从服务器发送已读回执
如果您希望服务器支持已读确认请求，并在客户端将邮件标记为已读时发送已读回执，请启用此项。默认情况下，禁用该选项。

发送为在 ReplyTo 地址中指定的别名
某些客户端可能不允许发件人使用别名发送邮件。已在 Exchange ActiveSync (EAS) 协议 363 16.x 中添加该功能，不过一些客户端不支持 16.x。例如，Windows 版的 Outlook 仅使用 EAS 14.0，虽然它允许用户指定要发送的备用地址，但生成的邮件并不能正确反映用户的选择。该选项允许使用 ReplyTo (答复) 字段来发送电子邮件，只要 ReplyTo 地址是该用户的有效别名 699 即可。默认情况下启用这个全局选项。

虚拟地将公共联系人合并为默认联系人
如果您希望将设备上的公共联系人与用户的默认联系人合并在一起，请启用此项。这仅仅是一个虚拟合并，实际上未将它们复制到用户的联系人文件夹。这对不支持 "全局地址列表" (GAL) 搜索的客户端而言极其有用。默认情况下，禁用该选项。

在将邮件移入垃圾邮件文件夹时阻止发件人
启用后，当客户端将电子邮件移动到账户的垃圾邮件文件夹时，该服务将该电子邮件的发件人或从地址添加到阻止的发件人联系人文件夹。

在会议请求被接受/拒绝等时强制发送会议请求。
启用后，当客户端接受、拒绝或以其他方式选择响应会议请求的操作时，服务将向会议组织者发送会议响应。这是针对没有正确发送这些更新本身的特定客户端。

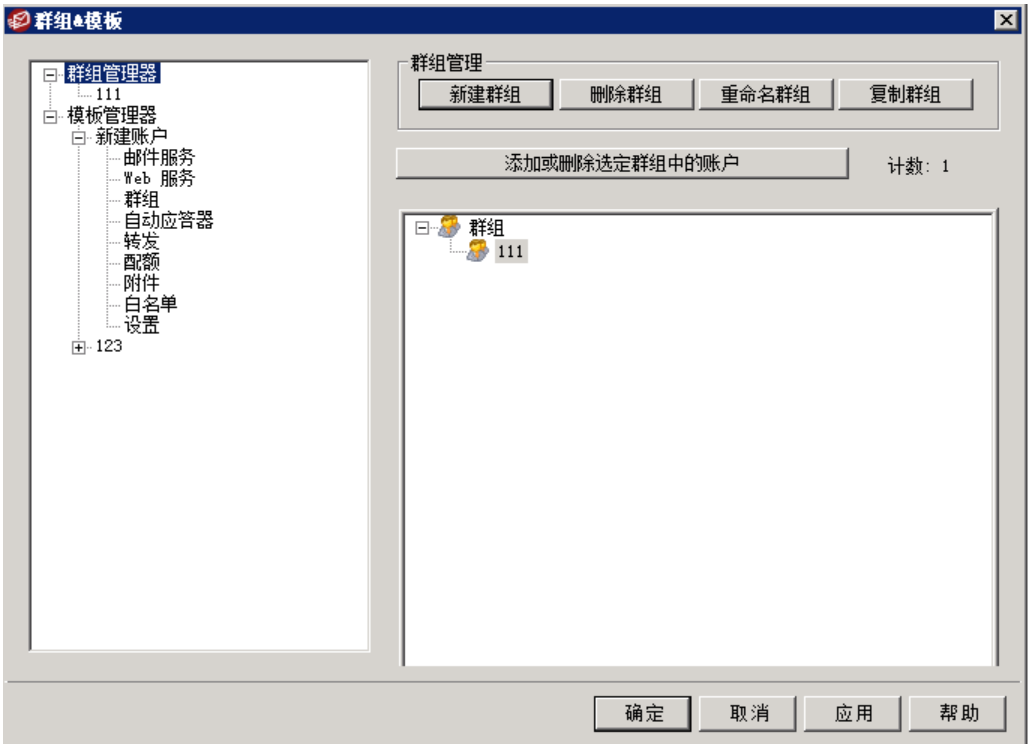
预览有效设置
该按钮在所有子 "客户端设置" 屏幕上可用 (例如域 365、账户 380 和客户端 388)。由于默认情况下，已将这些屏幕上的选项都设置成从父屏幕继承其设置，使用该功能来查看当前向显示的屏幕应用了什么设置。

还请参阅：

ActiveSync » 客户端设置 353
ActiveSync » 域 365
ActiveSync » 账户 380

5.2 群组 & 模板

5.2.1 群组管理器



群组管理器(账户» 群组& 模板.. » 群组管理器)用于创建账户群组，并管理属于这个群组的账户。群组拥有一些不同的用途和功能。例如，利用群组属性[658]屏幕，您可以将一个账户模板[666]分配到一个群组，允许您控制群组成员的多种账户设置。您还可以控制群组成员是否能访问 MDaemon Instant Messenger[267]和即时通讯。此外，内容过滤器支持群组，允许您基于邮件发件人或收件人是否是特定群组的成员，来创建规则条件[542]。最后，至于共享文件夹[95]，您可以将访问控制列表[260]权限分配给特定的群组，这就意味着该群组的所有成员将共享这些访问权限。

您可以从下方列表中选择一个群组，并点击 *"添加或删除账户..."*按钮来将账户添加到群组。您也可以从各个用户的邮件文件夹 & 群组[601]屏幕来将用户添加到群组中。

群组管理

新建群组

要创建一个新的账户群组，请点击*新建群组*，输入群组名称和相关描述，并点击*确定*。新的群组将出现在下方及左窗格内的群组列表中。

删除群组

要删除一个群组，请在下方列表中选定一个群组，点击 *"删除群组"*并点击 *"是"*来确认您的确要删除此群组。

重命名群组

要重命名一个群组，请在下方列表中选定一个群组并点击 *"重命名群组"*。为此群组输入一个新名称并点击 *"确定"*。

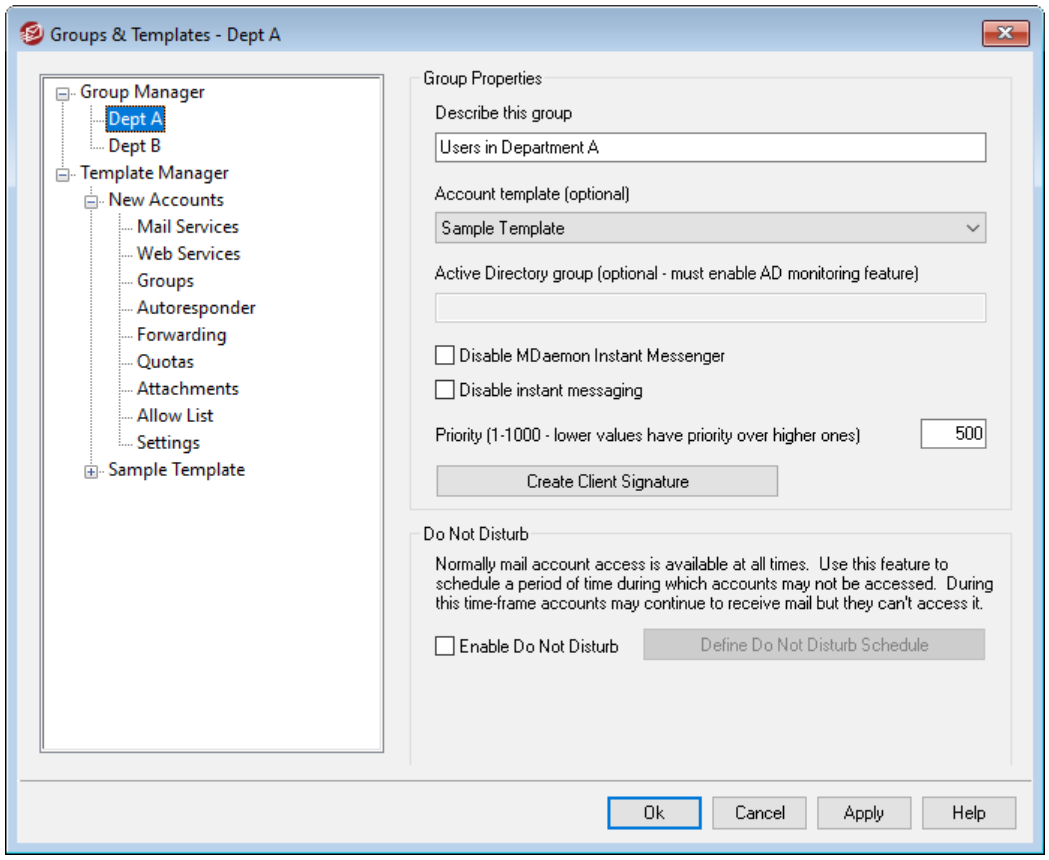
复制群组
如果您要创建具有与另一个群组匹配设置的新群组，请从列表中选择一个群组，点击此按钮，然后指定新群组的名称和描述。

添加或删除选定群组中的账户
要管理群组的成员，请从下方列表中选定一个群组并点击这个按钮。点击您希望加入群组的任何账户旁的选框，并取消勾选您要删除的任何成员旁的选框。点击*"确定"*。

还请参阅：

邮件文件夹& 群组 601
创建新的内容过滤器规则 542
共享文件夹 95

5.2.1.1 群组属性



"群组属性"屏幕（"账户» 群组& 模板..»[群组名称]）用于配置您使用群组管理器 657 创建的各个群组的设置。要从"群组管理器"打开"群组属性"，请双击您要编辑的群组，或在左窗格中点击此群组的名称。在此屏幕上，您可以将一个账户模板 666 分配到一个群组，允许您控制群组成员的各种账户设置。您还可以将群组链接到一个"活动目录"群组，控制群组成员是否能访问 MDaemon Instant Messenger (MDIM) 267 和实时通讯，并为此群组设置优先级。要控制群组成员，请使用"账户编辑器"上的"群组管理器"和邮件文件夹& 群组 601 屏幕。

群组属性

描述该群组
在此处为群组输入描述供您参考。通常在您创建群组时输入该信息，不过您可以随时通过此屏幕对其进行编辑。

账户模板（可选）
如果您已创建了一个用于控制群组成员一些账户设置的账户模板[666]，请使用此下拉列表来选择所需模板。将账户模板链接到一个群组时，在模板属性[667]中指定的任何账户设置分类将用于属于这个群组的所有账户。该模板将用来控制这些设置，而不是使用“账户编辑器”上的个别账户设置。如果从一个群组中删除了一个控制其账户设置的账户，会将这些设置恢复到在新建账户模板[667]中指定的值。

如果一个账户属于链接到不同模板的多个群组，那么所有这些模板将用于在指定的模板属性[667]中没有任何冲突的各种场合。如果多个模板被设置成控制相同的属性，那么将使用首个列出的模板。

活动目录群组（可选 -需要 AD 监控）
如果您希望将群组链接到一个视活动目录而定的群组，请使用此项。会自动将“活动目录”群组的成员添加到账户群组。不过您必须使用活动目录监控[694]功能才能使其有效工作。

您可以映射您希望用作将账户添加到群组的触发程序的任何“活动目录”属性，其中“memberOf”属性是最常用的。您可以通过在记事本中编辑 ActiveDS.dat 来对其进行配置。默认情况下禁用此功能。要实现这点，请编辑 ActiveDS.dat，并指定要将哪个属性用作您的群组触发程序，或取消评注“Groups=%memberOf%”这行（位于 ActiveDS.dat）来实现使用。

禁用 MDaemon InstantMessenger
如果您希望为所有群组成员禁用 MDIM 支持，请点击此框。

禁用即时通讯
如果您希望在支持 MDIM 的同时禁用即时通讯功能，请点击此框。

优先级（1-1000 -较低值的优先级高于较高值）
使用此项来为您的群组设置优先级（1-1000），这就允许账户可以是多个群组的成员，并避免两个群组设置之间可能存在的冲突。例如，在账户是多个群组（每个群组拥有一个相关联的控制相同设置的账户模板）的成员时，将使用具有第一优先级的群组设置。换言之，具有“1”优先级值的群组优先于具有“10”优先级值的群组。当各组间不存在任何设置上的冲突，则进行综合应用。在平局的情况下，则第一组胜出。如果从一个链接到账户模板的群组中删除了一个账户，则将此账户模板之前控制的账户设置更改成下一个“优先级”群组指定的账户设置。如果没有其他群组控制这些设置，则它们将被新建账户模板[667]还原为指定的设置。

创建客户签名
如果您希望添加用于组成员的客户端签名，请单击此按钮。请参阅：团体客户签名[661]

勿扰
使用“勿扰”功能来调度时间框架，在此期间账户无法发送邮件或被其用户访问。在“勿扰”期间不允许访问，而且会向 IMAP、POP、SMTP、ActiveSync 和 Webmail 访问请求返回合适的

错误响应。MDaemon 仍然为处于这种状态的账户接受入站邮件，不过这些账户无法发送电子邮件或被邮件客户端访问。

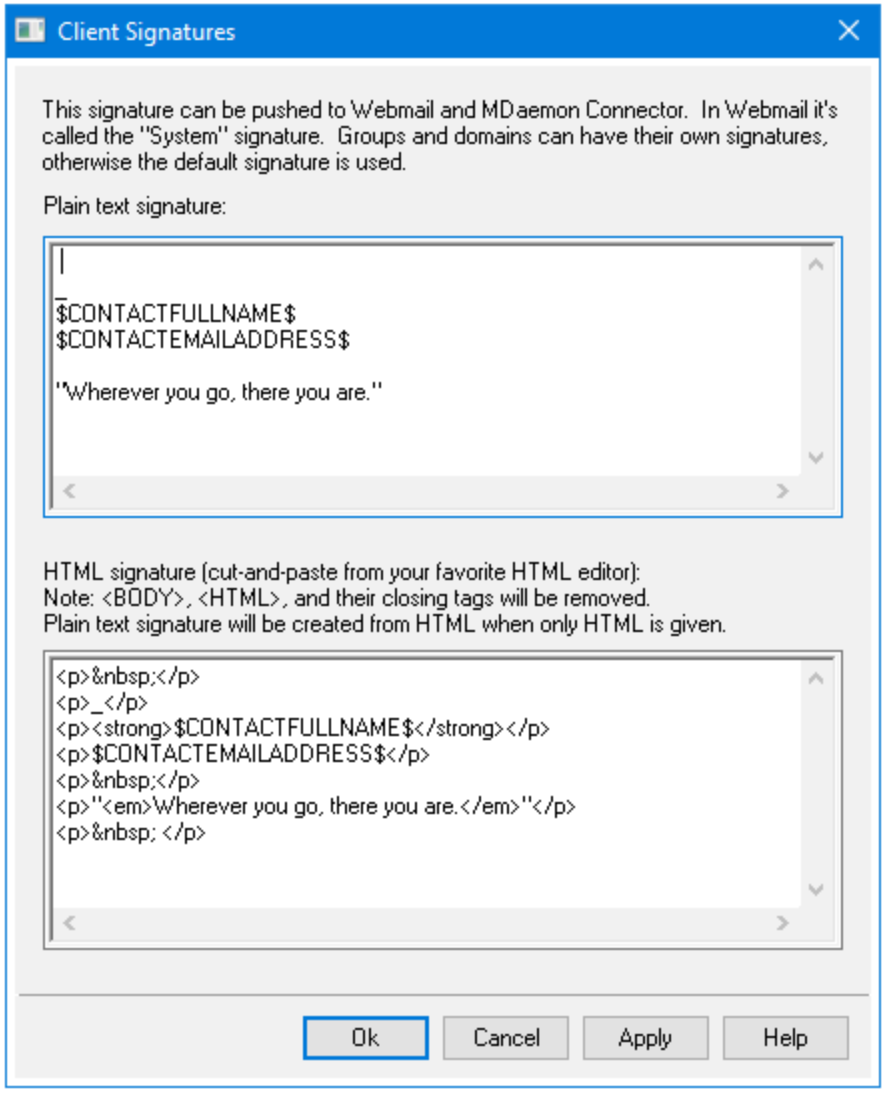
向一个或多个账户应用勿扰：

1. 点击 "启用勿扰"。
2. 点击 "定义勿扰调度"。
3. 设置开始/结束日期、开始/结束时间、以及使用 "勿扰"的天数。
4. 点击 "确定"。
5. 使用 "群组管理器 657"来将任何账户分配到您希望使用的群组。

还请参阅：

群组管理器 657
邮件文件夹& 群组 601
模板管理器 666
模板属性 667

5.2.1.1.1 客户端签名



现在可以为每个群组设置客户端签名。客户端签名将被推送给使用 MDaemon Webmail[289] 或 MDaemon Connector[339] 的成员。群组客户端签名会覆盖域客户端签名[170]，而域客户端签名会覆盖默认客户端签名[113]。在 MDaemon GUI 中，转至 "账户 | 群组 & 模板"来编辑一个群组并设置其客户端签名。清除编辑器中的文本来删除客户端签名。

纯文本签名

此区域用于插入纯文本签名。如果您希望在多部分邮件 (multipart message)的文本/html 部分中使用指定且相应的 html签名，请使用下方的 *"HTML 签名"*屏幕。如果一个签名同时存在于这两个位置，MDaemon 将为多部分邮件的各个部分使用正确的签名。如果未指定 html签名，就会在两个部分中都使用纯文本签名。

HTML 签名（剪贴自您首选的 HTML 编辑器）

此区域用于插入 HTML 签名，将在多部分邮件的文本/html部分使用。如果此处和上方的*"纯文本签名"*区域都包括同一个签名，MDaemon 将为多部分邮件的各个部分使用正确的签名。如果未指定纯本文签名，就会使用 html格式来创建一个签名。

要创建您的 html签名，可以在此处手动输入 html代码，也可直接从您首选的 HTML 编辑器对签名进行剪切和粘贴操作。如果您希望在您的 HTML 签名中包含内嵌图像，您可以使用 $ATTACH_INLINE:path_to_image_file$ 宏来实现这点。

例如：

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

还有多种从 MDaemon 的Remote Administration 293 web 界面，将内嵌图像插入签名的方法：

- 在 Remote Administration 的"客户端签名"屏幕上，点击 HTML 编辑器中的"图像"工具栏按钮并选择上传选项卡。
- 在 Remote Administration 的"客户端签名"屏幕上，点击 HTML 编辑器中的"添加图像"工具栏按钮。
- 将一个图像拖放到"客户端签名"屏幕的 HTML 编辑器（使用 Chrome、FireFox、Safari或 MSIE 10+）
- 借助 Chrome、FireFox 或 MSIE 11+，将剪贴板中的图像复制粘贴到"客户端签名"屏幕的 HTML 编辑器

签名中不允许 <body></body> 和 <html></html> 标签，而且在找到这些标签时会将它们删除。

签名宏

MDaemon 签名支持将发件人的联系信息插入签名的宏，该签名取自位于其域的公共联系人文件夹中的发件人联系人。这允许使用发件人的信息对默认和域签名进行个性化。例如 $CONTACTFULLNAME$ 插入发件人的全名，$CONTACTEMAILADDRESS$ 插入发件人的邮件地址。使用 Webmail、MDaemon Connector或 ActiveSync 来编辑公共联系人。如果发件人不存在联系人，则使用空值。可用的宏如下所示。

用户可以通过使用 $SYSTEMSIGNATURE$ 宏放置默认/域签名，并使用 $ACCOUNTSIGNATURE$ 放置账户签名来控制 MDaemon 签名在其邮件中的位置。

Signature Selector	
$SYSTEMSIGNATURE$	Places the Default Signature 109 or Domain Signature 166 in a message. If both exist, the Domain Signature is used.

$CLIENTSIGNATURE$	Places the Default Client Signature 113 or Domain Client Signature 170 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 632 in the message.
姓名和 ID	
全名	**$CONTACTFULLNAME$**
名	**$CONTACTFIRSTNAME$**
中间名	**$CONTACTMIDDLENAME$,**
姓	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
后缀	**$CONTACTSUFFIX$**
昵称	**$CONTACTNICKNAME$**
Yomi名	**$CONTACTYOMIFIRSTNAME$**
Yomi姓	**$CONTACTYOMILASTNAME$**
账户名称	**$CONTACTACCOUNTNAME$**
客户 ID	**$CONTACTCUSTOMERID$**
政府 ID	**$CONTACTGOVERNMENTID$**
文件作为	**$CONTACTFILEAS$**
电子邮件地址	
电子邮件地址	**$CONTACTEMAILADDRESS$**
电子邮件地址 2	**$CONTACTEMAILADDRESS2$**
电子邮件地址 3	**$CONTACTEMAILADDRESS3$**
电话和传真号码	
手机号码	**$CONTACTHOMEMOBILE$**
手机 2	**$CONTACTMOBILE2$**
车载电话	**$CONTACTCARPHONENUMBER$**
家庭电话	**$CONTACTHOMEPHONE$**
家庭电话 2	**$CONTACTHOMEPHONE2$**
家庭传真	**$CONTACTHOMEFAX$**
其他电话	**$CONTACTOTHERPHONE$**
即时通讯和 Web	

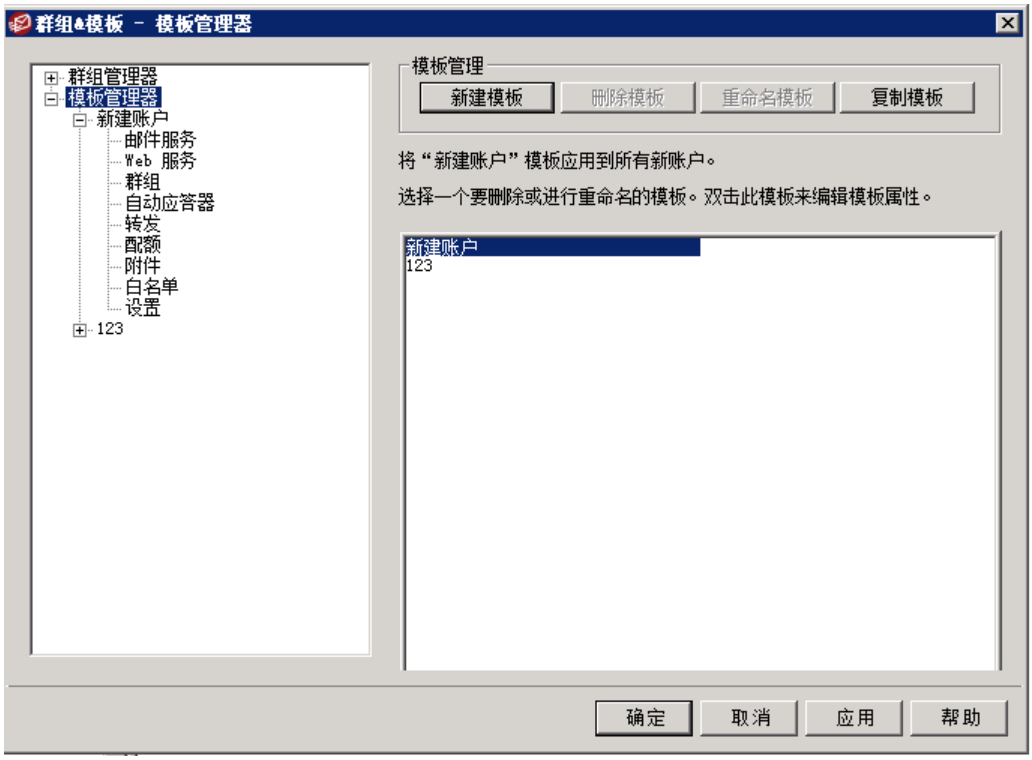
IM 地址	**$CONTACTIMADDRESS$**
IM 地址 2	**$CONTACTIMADDRESS2$**
IM 地址 3	**$CONTACTIMADDRESS3$**
MMD 地址	**$CONTACTMMSADDRESS$**
家庭网址	**$CONTACTHOMEWEBADDRESS$**
地址	
家庭地址	**$CONTACTHOMEADDRESS$**
家乡城市	**$CONTACTHOMECITY$**
家乡州	**$CONTACTHOMESTATE$**
家乡邮政编码	**$CONTACTHOMEZIPCODE$**
家乡国家	**$CONTACTHOMECOUNTRY$**
其他地址	**$CONTACTOTHERADDRESS$**
其他城市	**$CONTACTOTHERCITY$**
其他州	**$CONTACTOTHERSTATE$**
其他邮政编码	**$CONTACTOTHERZIPCODE$**
其他国家	**$CONTACTOTHERCOUNTRY$**
公司相关	
公司名称	**$CONTACTBUSINESSCOMPANY$**
Yomi公司名称	**$CONTACTYOMICOMPANYNAME$**
公司职位	**$CONTACTBUSINESSTITLE$**
公司办公室	**$CONTACTBUSINESSOFFICE$**
公司部门	**$CONTACTBUSINESSDEPARTMENT$**
公司经理	**$CONTACTBUSINESSMANAGER$**
公司助理	**$CONTACTBUSINESSASSISTANT$**
公司助理电话	**$CONTACTBUSINESSASSISTANTPHONE$**
公司总机	**$CONTACTBUSINESSMAINPHONE$**
公司电话	**$CONTACTBUSINESSPHONE$**
公司电话 2	**$CONTACTBUSINESSPHONE2$**
公司 IP 电话	**$CONTACTBUSINESSIPPHONE$**
公司传真	**$CONTACTBUSINESSFAX$**

公司寻呼机	**$CONTACTBUSINESSPAGER$**
公司无线电	**$CONTACTBUSINESSRADIO$**
公司地址	**$CONTACTBUSINESSADDRESS$**
公司所在城市	**$CONTACTBUSINESSCITY$**
公司所在州	**$CONTACTBUSINESSSTATE$**
公司邮政编码	**$CONTACTBUSINESSZIPCODE$**
公司所在城市	**$CONTACTBUSINESSCOUNTRY$**
公司网址	**$CONTACTBUSINESSWEBADDRESS$**
其他	
配偶	**$CONTACTSPOUSE$**
孩童	**$CONTACTCHILDREN$**
类别	**$CONTACTCATEGORIES$**
备注	**$CONTACTCOMMENT$**

还请参阅：

默认客户端签名 113
默认签名 109
域管理器 » 签名 166
账户编辑器 » 签名 632
域管理器 » Webmail设置 160
MC客户端设置 » 签名 339

5.2.2 模板管理器



使用模板管理器（“账户» 群组& 模板.. » 模板管理器”）您可以创建并管理账户模板，这些模板是一套指定的账户设置，可以分配到特定的群组[657]。属于那些（一个或多个）群组的任何账户将拥有指定的账户设置（被锁定），而且只能由其被分配到的模板（而不是“账户编辑器”）进行控制。可以在各个模板的属性[667]屏幕上（通过双击列表下方这个模板的名称，或点击左窗格中的模板抵达）指定该模板将控制的账户设置类别。

模板管理

新建模板
要创建一个新的账户模板，请点击*新建模板*，输入模板名称，并点击*确定*。新的模板将出现在下方及左窗格内的模板列表中。

删除模板
要删除一个模板，请在下方列表中选定一个模板，点击*“删除模板”*并点击*“是”*来确认您的确要删除此模板。

重命名模板
要重命名一个模板，请在下方列表中选定一个模板并点击*“重命名模板”*。为此模板输入一个新名称并点击*“确定”*。

复制模板
如果您希望使用与另一个模板匹配的设置来创建模板，请从列表中选择一个模板，点击此按钮，然后为新模板指定名称。

模板列表

"模板管理器"底部的列表含有您的所有模板。点击一个模板，并使用屏幕顶部的按钮来删除或重命名这个模板。双击一个模板即可打开其属性[667]屏幕，您可以在这个屏幕上指定该模板将控制的账户设置类别。您可以使用左侧窗格中的控件，直接跳转至任何其他模板及其账户设置。*"新建账户"*模板是始终在列表中位居第一的专用模板。

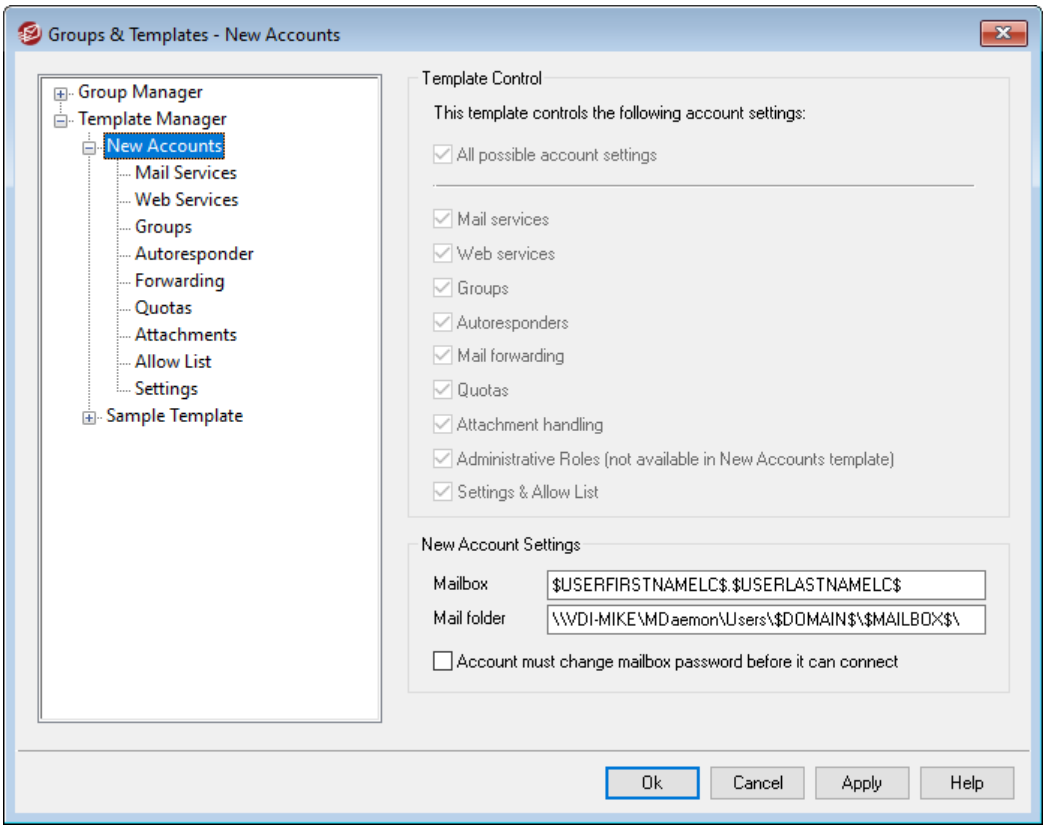
新建账户模板

"*新建账户*"模板是在创建新账户时应用到所有这些新账户的专用模板。*"新建账户"*不像其他模板那样，锁定和控制特定的账户设置，而是用来为新建账户指定初始设置。可以使用"账户编辑器"来编辑个别账户，从而更改这些初始设置。一些模板设置，例如位于"管理角色[685]"屏幕上的选项，不适用于"新建账户"模板。

还请参阅：

模板属性[667]
群组管理器[657]

5.2.2.1 模板属性



要访问模板的属性屏幕，请打开模板管理器[666]，并点击左侧窗格中模板的名称。使用各个模板的属性屏幕来指定该模板将控制的账户设置类别。所属使用此账户模板的群组[657]的任何账户，自这些设置受该模板控制起，其对应的"账户编辑器"屏幕将被锁定。如果一个账户

属于链接到不同模板的多个群组，那么所有这些模板将用于在指定的模板属性中没有任何冲突的各种场合。如果多个模板被设置成控制相同的属性，那么将使用首个列出的模板。

模板控制

所有可能的账户设置

如果您希望使用此模板来控制使用这个模板的群组[657]的所有可用账户设置，请点击此框。所有的模板屏幕（而不是"账户编辑器"上对应的同名屏幕）将用于各个群组成员的账户设置。如果您希望使用下方的*"账户设置"*选项来选择要控制的特定账户设置，请清除此选框。

账户设置

这一部分列出此模板可以为使用这个模板的群组控制的所有账户设置类别。各个选项对应同名的模板屏幕。选定此项时，将为相关联的群组成员使用这个模板屏幕上的设置，而不是对应"账户编辑器"屏幕上的设置。

新建账户设置

这些选项仅适用于新建账户模板[667]。它们使用大量专用宏[669]来自动生成邮件存储文件夹和新建账户邮件地址的邮箱部分。

邮箱

使用此字段来控制为新建账户生成的邮件地址的默认*邮箱名称*[598]部分。请参阅下方的模板宏[669]来查看可用于此模板字符串的宏列表。
"$USERFIRSTNAMELC$.$USERLASTNAMELC$"是这个选项的默认模板。因此，在 example.com 域中为"MichaelMason"创建一个账户的结果，会将其地址设置成"michael.mason@example.com"。

邮件文件夹

使用此字段来控制将用于新建账户的默认*邮件文件夹*[601]。每个账户的*邮箱文件夹*就是每封邮件存储在服务器上的位置。例如"..\$DOMAIN$\$MAILBOX$\"将为用户"michaelmason@example.com"创建路径"..\example.com\michael.mason\"。

MDaemon 支持一个用于散列文件夹的基本系统。在 NTFS 下，将大量文件夹放置在同一根目录下，有时将导致性能问题。如果您拥有大量用户，并希望不顾默认的 $DOMAIN$\$MAILBOX$\ 设置细分用户文件夹，您可以使用宏 $MAILBOXFIRSTCHARSn$ 来实现这点。使用这个宏时，"n"是 1 到 10 之间的数。它将随着邮件箱名称中第一个"n"字符而扩展。将您默认的*邮件文件夹*路径更改成类似以下式样，将得到一个出色的文件夹散列系统：

```
C:
\MailboxRoot\$MAILBOXFIRSTCHARS4$\$MAILBOXFIRSTCHARS
2$\$MAILBOX$\。
```

账户在可以进行连接前必须更改邮箱密码

此项控制新账户是否必须更改其*邮箱密码*才能访问 POP、IMAP、SMTP、Webmail或 Remote Administration。该用户可以连接到 Webmail或 Remote Administration，但只有在这名用户更改他或她的密码后才能继续操作。注意：为了让用户能够通过 Webmail或 Remote Administration 更改其密码，他们必须先被授予*"..编辑密码"*web 访问权限（位

于 Web 服务[672]屏幕。）更改完密码后，将在该账户的 "账户详细信息[598]"屏幕上取消激活此项。

因为更改密码对某些用户而言可能不是易事，您应该慎用此项。

模版宏

以下是对自动化您账户设置可用宏的快速参考：

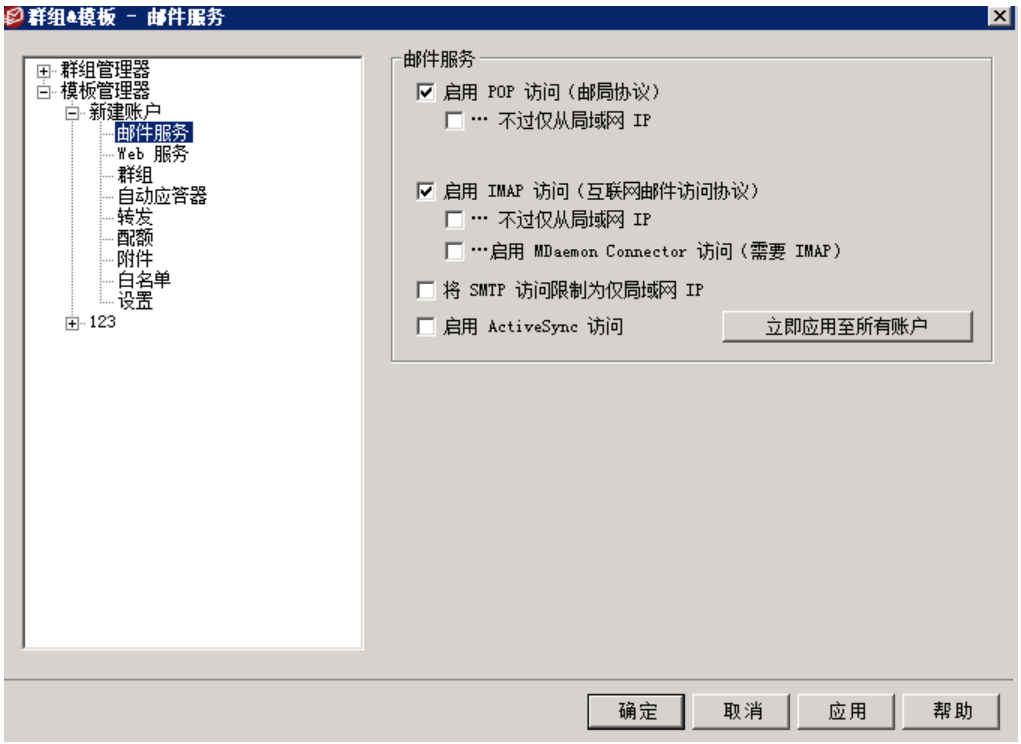
$DOMAIN$	此变量将为账户解析所选域名。
$DOMAINIP$	此变量将为账户解析与当前所选域相关联的 IPv4 地址。
$DOMAINIP6$	此变量将为账户解析与当前所选域相关联的 IPv6 地址。
$MACHINENAME$	此宏从 "域管理器"的 "主机名称 & IP"屏幕中返回 "默认域"的主机名称。该宏目前用于默认账户信息脚本 (NEW USERHELP.DAT)中，以便于新的安装。
$USERNAME$	该变量解析账户持有人的完整姓和名。该字段等同于 "$USERFIRSTNAME$ $USERLASTNAME$"
$USERFIRSTNAME$	该变量解析账户持有者的名字。
$USERFIRSTNAMELC$	该变量以小写字母解析账户持有人的名。
$USERLASTNAME$	该变量解析账户持有者的姓氏。
$USERLASTNAMELC$	该变量以小写字母解析账户持有人的姓。
$USERFIRSTINITIAL$	该变量解析账户持有人名的第一个字母。
$USERFIRSTINITIALLC$	该变量以小写字母解析账户持有人名的第一个字母。
$USERLASTINITIAL$	该变量解析账户持有人姓的第一个字母。
$USERLASTINITIALLC$	该变量以小写字母解析账户持有人的姓氏的第一个字母。
$MAILBOX$	该变量解析当前账户的邮箱名称。该值将作为 POP3 邮件会话过程中所通过的 USER 命令的值。

$MAILBOXFIRSTCHARSn$	此处的 "n"是 1 到 10 之间的数。它将随着邮件箱名称中第一个 "n"字符而扩展。

还请参阅：

模板管理器 666
群组管理器 657

5.2.2.1.1 邮件服务



此模板上的选项对应 "账户编辑器"邮件服务 602屏幕上的选项。在将一个模板设置成控制此屏幕 667时，该模板将控制所属使用此模板群组 658的任何账户的 "邮件服务"选项。

邮件服务

启用邮局协议（邮局协议）
勾选此框时，可以通过 "邮局协议（POP）"访问由此模板控制其设置的账户。事实上所有电子邮件客户端软件都支持此协议。如果您不希望允许 POP 访问，请清除该复选框。

...不过仅从局域网 IP
如果您希望在用户从局域网 IP 地址 508建立连接时，允许仅通过 POP 访问该账户，请勾选此框。

启用互联网邮件访问协议 (互联网邮件访问协议)
勾选此框时，可以通过“互联网邮件访问协议 (IMAP)”访问由此模板控制其设置的账户。IMAP 的功能多于 POP，允许在服务器上管理电子邮件，并使用多种客户端访问邮件。大多数电子邮件客户端软件都支持此协议。

...不过仅从局域网 IP
如果您希望在用户从局域网 IP 地址[508]建立连接时，允许仅通过 IMAP 访问该账户，请勾选此框。

...启用 MDaemon Connector访问 (需要 IMAP)
此选项仅适用于“新建账户”模板。如果您希望允许账户使用 MDaemon Connector[323]进行连接，请点击此项。**请注意：**此选项仅在您的服务器上激活对 MDaemon Connector 的支持时才可用。

仅限制 SMTP 访问到 LAN IP
如果您希望仅将 SMTP 访问限制为 LAN IP，请选中此框。这将防止账户发送邮件，除非它们已连接到您的网络。如果该账户尝试从外部 IP 地址发送邮件，则连接将被拒绝并断开。

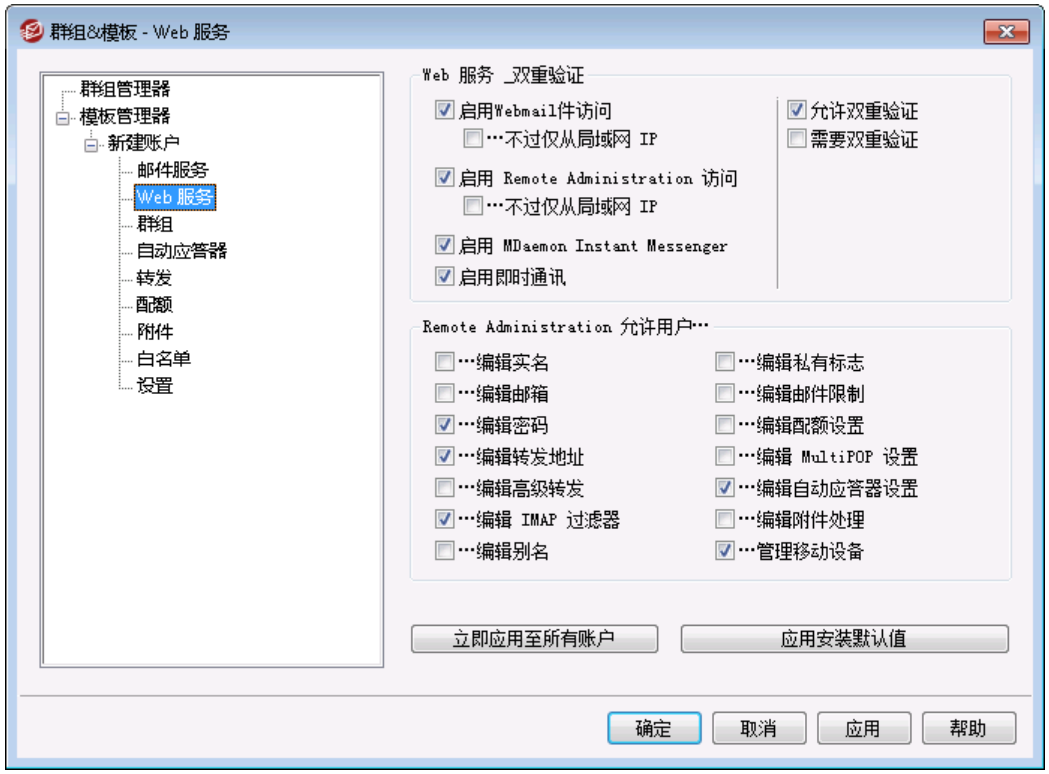
启用 ActiveSync 访问权限
此选项仅适用于“新建账户”模板。如果您希望允许这些新账户在移动设备上使用 ActiveSync 来将其电子邮件、联系人、日历和其他数据与 MDaemon/Webmail同步，请勾选此框。此设置对应“*为此用户启用 ActiveSync 服务*”选项 (位于“账户编辑器”的“ActiveSync for MDaemon[642]”屏幕)。

立即应用于所有账户
此选项仅适用于“新建账户”模板。点击此项来将这个屏幕的设置立即应用到所有现有 MDaemon 账户的“邮件服务[602]”和“ActiveSync for MDaemon[642]”屏幕。

还请参阅：

模板属性[667]
群组属性[658]
新建账户模板[667]
账户编辑器 » 邮件服务[602]

5.2.2.1.2 Web 服务



此模板上的选项对应 "账户编辑器" Web 服务 603 屏幕上的选项。在将一个模板设置成控制此屏幕 667 时，该模板将控制所属使用此模板群组 658 的任何账户的 "Web 服务"选项。

Web 服务 & 双重验证

启用 Webmail访问
如果您希望受此模板控制的账户能够访问 Webmail 266，请启用此选框来使用户能够使用 web 浏览器访问其电子邮件、日历和其他功能。

...不过仅从局域网 IP
如果您希望在账户从局域网 IP 地址 508 建立连接时，允许相关联的账户访问 Webmail，请勾选此框。

启用 Remote Administration 访问
如果您希望允许受此模板控制的账户通过 Remote Administration 293 修改其账户的一些设置，请勾选此框。这些账户只能够编辑您所指定的以下设置。

当启用该功能且 Remote Administration 服务器处于活动状态时，用户通过将浏览器指向指定的 MDaemon 域以及 Remote Administration 所指定的端口 294 （例如 http://example.com:1000），用户便可登录到 Remote Administration。首先显示登录界面，然后将看到有权限编辑的设置。只需编辑所选设置并点击 *"保存更改"*按钮即可。然后可以注销并关闭浏览器。如果他能访问 Webmail，也可通过 Webmail中的高级选项菜单访问 Remote Administration。

如果用户是 "全局管理员"或 "域管理员"（在 "账户编辑器"的 管理角色 636 "屏幕上指定），在登录到 Remote Administration 后他将看到一个不同的屏幕。

...不过仅从局域网 IP
如果您希望在账户从局域网 IP 地址[508]建立连接时，允许此账户访问 Remote Administration，请勾选此框。

启用 MDaemon InstantMessenger
如果您希望在默认情况下，为这些新账户启用 MDIM[267] 支持，请点击此框。此选项仅适用于新建账户模板[667]。可以使用 "群组属性[658]"上的一个类似选项来控制群组成员对于 MDIM 的访问。

启用即时通讯
如果您希望在默认情况下，为新建账户启用对于 MDIM 即时通讯系统的支持，请点击此项。此选项仅适用于新建账户模板[667]。可以使用群组属性[658]上的一个类似选项来控制群组成员对于 "即时通讯"的访问。

双重验证

MDaemon 为登录 Webmail或 MDaemon 的 Remote Administration web 界面的用户支持 "双重验证"(2FA)。通过 HTTPS 登录到 Webmail的账户可以在 Webmail中的 **"选项 » 安全"**屏幕上为账户激活 "双重验证"。然后用户在登录 Webmail或 Remote Administration 时必须输入验证码。可以从安装在用户的移动设备或平板电脑上的验证器应用程序获取该代码。该功能专为支持 Google Authenticator 的任何客户端而设计。请参阅 Webmail帮助文件获得有关为一个账户设置 2FA 的更多信息。

允许双重验证
默认情况下，允许新账户设置和使用 Webmail的 "双重验证"(2FA) 功能。如果您不希望新账户能默认使用 2FA，请取消勾选这个选框。您可以在各个账户的 Web 服务[603]页面为特定账户控制该设置。

请求双重验证
如果您希望强制所有新账户在登录到 Webmail或 MDaemon 的远程管理 web 界面时使用 "双重验证"(2FA)，请启用此项。在要求 2FA 时，未被配置成使用该功能的任何账户将被重定向到一个页面进行设置，以便在下一次该账户登录到 Webmail时应用此功能。请参阅 Webmail帮助文件获得有关为一个账户设置 2FA 的更多信息。

Remote Administration 允许用户...

...编辑实名
启用此功能将允许与此模板相关联的账户修改*姓名*[598]设置。

...编辑邮箱
启用此功能将允许用户修改*邮箱名称*[598]。

> 因为*邮箱名称*是账户电子邮件地址的一部分，它是账户唯一的标识符与登录值，修改它就表示用户将要更改他或她的实际邮件地址。这会导致将来任何一封指向此旧地址的邮件被拒收、删除或其他相应操作。

...编辑密码
如果您希望允许新用户修改*"邮箱密码"*设置，请点击此选择框。有关密钥要求的更多信息，请参阅：密码[717]。

...编辑转发地址
启用此功能时，与此模板相关联的账户可以修改转发[610]地址设置。

...编辑高级转发
启用此功能时，用户将能修改*高级转发设置*[610]。

...编辑 IMAP 过滤器
使用此控件则允许各个用户能够创建并管理他们自己的 IMAP 过滤器[617]。

...编辑别名
如果您希望允许账户持有人使用 Remote Administration 来编辑与其账户相关联的别名[622]，请启用此项。

...编辑应用程序密码
默认情况下，用户可以编辑其应用程序密码[630]。如果您不希望允许用户编辑它们，请清除该复选框。

...编辑私人旗标
该选项管理每个人是否被允许使用 Remote Administration 来编辑*"从'所有人'列表、共享日历和 VRFY 中隐藏的账户"*选项（其位于"账户编辑器"的设置[639]屏幕上）。

...编辑邮件限制
该选择框用于控制账户是不是能够编辑位于限制[611]屏幕上的入站/出站邮件限制。

...编辑配额设置
如果您希望允许用户修改配额[613]设置，请点击此选择框。

...编辑 MultiPOP 设置
若您希望授予账户权限来添加新的 MultiPOP[620] 条目，以及为这些条目启用/禁用 MultiPOP 集，请点击此选择框。

...编辑自动应答器设置
如果您希望让用户能够为其账户添加、编辑或者删除自动应答器[607]，请点击此选择框。

...编辑附件处理
如果您希望允许该用户编辑位于附件[616]屏幕上的账户附件处理选项，请勾选此框。

...管理移动设备
如果您希望允许账户持有人使用 Remote Administration 来管理其特定的设备（例如 ActiveSync 设备）设置，请点击此项。

立即应用于所有账户
此选项仅适用于新建账户模板[667]。点击此项来将这个屏幕上的选项设置应用到未专受"Web 服务账户模板"控制的现有 MDaemon 账户。

应用安装默认值

此选项仅适用于新建账户模板[667]。点击此项来将“新建账户模板”重置成安装默认值。该项只更改这个模板的设置，而不会更改任何现有账户。

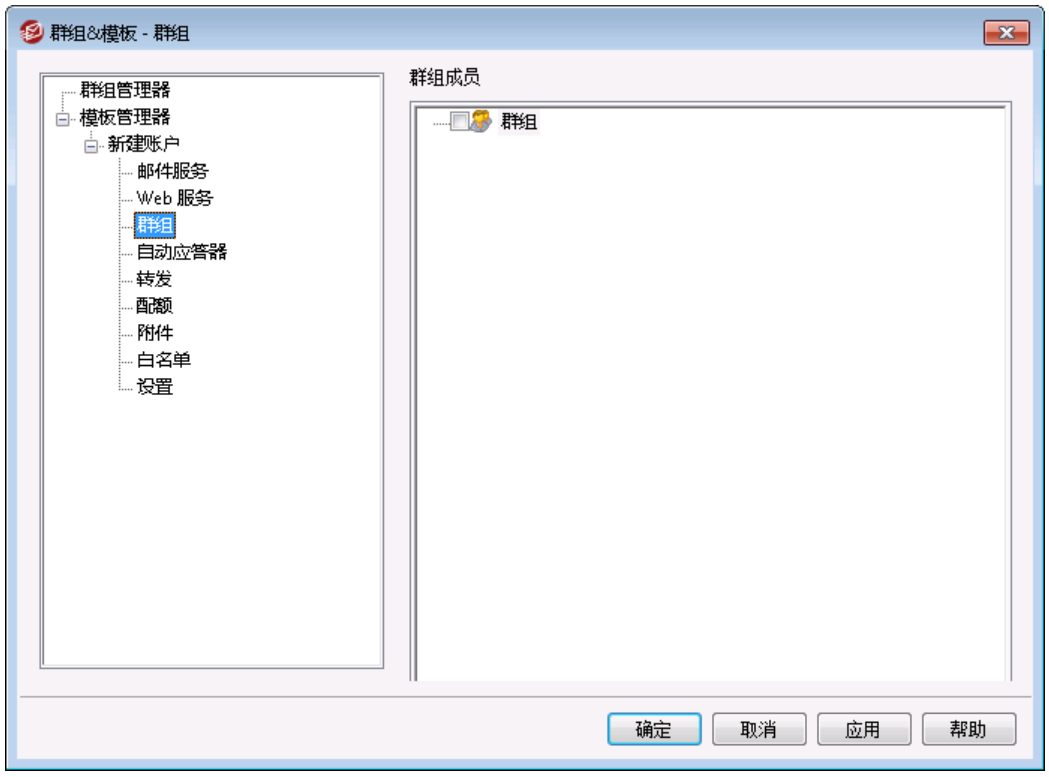
加载“新建账户”模板设置

此项仅适用于定制模板。点击此项来将这个屏幕上的选项设置成在新建账户模板[667]内“Web 服务”屏幕上指定的默认值。

还请参阅：

模板属性[667]
群组属性[658]
新建账户模板[667]
账户编辑器 » Web 服务[603]

5.2.2.1.3 群组



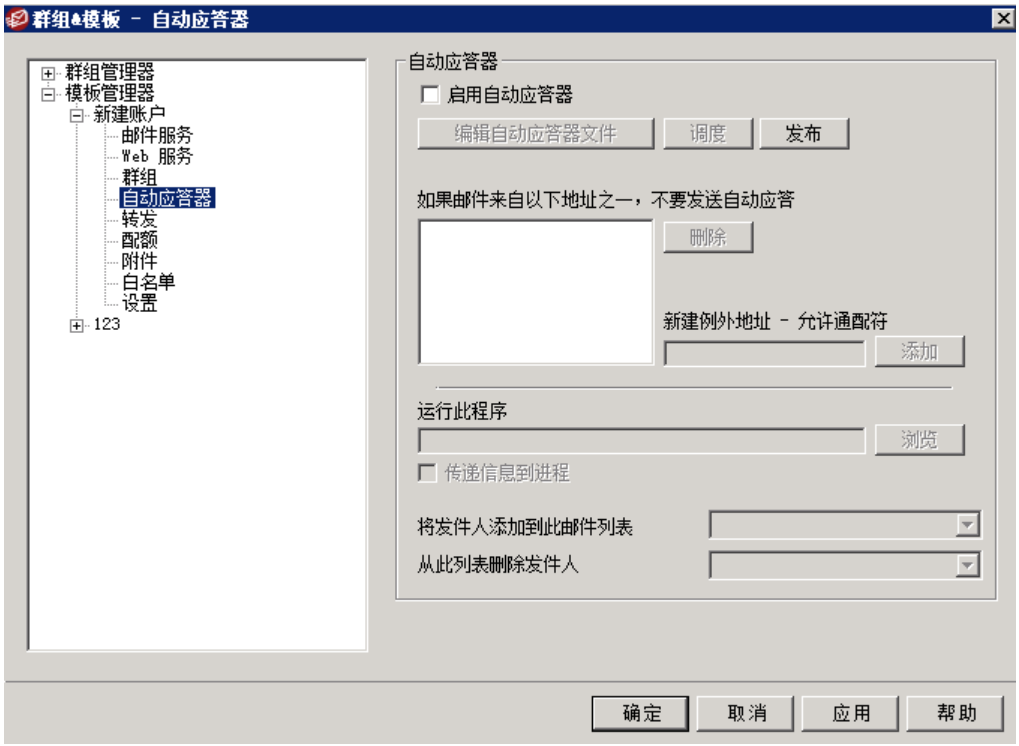
群组管理

该屏幕仅适用于新建账户模板[667]，而且对应“账户编辑器”的邮件文件夹 & 群组[601]屏幕的“群组成员”部分。在此屏幕上选择一个或多个群组时，新账户将被自动添加到这些组中。

还请参阅：

新建账户模板 667
群组管理器 657
群组属性 658

5.2.2.1.4 自动应答器



此模板上的选项对应"账户编辑器"自动应答器 607屏幕上的选项。在将一个模板设置成控制此屏幕 667时，该模板将控制所属使用此模板群组 658的任何账户的"自动应答器"选项。

自动应答器是非常有用的工具，使得入站邮件自动触发某些特定事件，例如运行一个程序，添加发件人到邮件列表，以一封自动生成的邮件来应答等等。自动应答器最常见的用途就是以一封用户自定义邮件自动应答入站邮件，声称收件人正在休假目前无法回应，将尽快答复，诸如此类。使用 web 访问 603和 Webmail 266或 Remote Administration 293的 MDaemon 用户可以使用所提供的选项来为自己编写自动应答邮件并且安排邮件将要使用的日期。最后，自动应答邮件基于 OOF.mrk 文件的内容，可以在每名用户的根 \data\ 文件夹中找到。此文件支持大量的宏，这些宏可用于引起动态生成邮件的许多内容，从而使自动应答器具有多种用途。

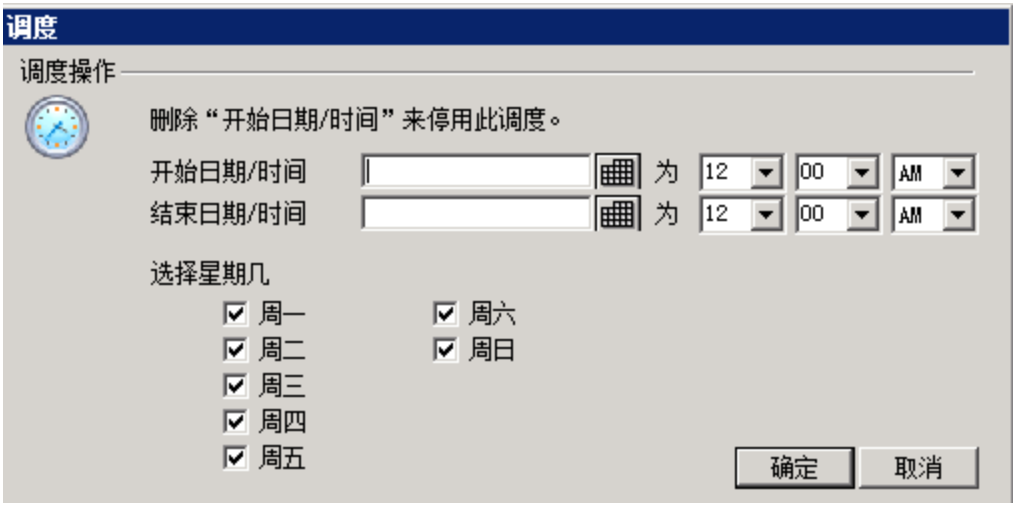
当触发一封来自远程来源的邮件时，总会准许自动应答事件。不过，对于来自用户相同域地邮件，只有在您启用了*"自动应答器由域内邮件触发"*这个选项后（位于"自动答器» 设置 706"屏幕），才会触发自动应答器。您也可以使用该屏幕上的一个选项来限制每个发件人每天针对一个应答的自动应答邮件。

自动应答器

启用自动应答器
启用此项来激活面向受此模板控制的所有群组的自动应答器。有关 WebAdmin 的更多信息，请参阅：自动应答器 703。

编辑自动应答文件
点击此按钮编辑将用于与此模板关联的文件的自动响应文件。

调度
点击此按钮打开“调度”对话框，在此您可以设置自动应答器处于活动状态的起始和结束日期和时间，并设置使其处于活动状态的工作日。如果您希望自动应答器始终处于活动状态，请将此“调度”留空。



发布
如果您希望将此模板的自动应答文件和设置复制到一个或多个其他账户，请点击此按钮。选择您要将自动应答器复制到的账户，然后点击“确定”。

如果邮件来自以下地址，请不要发送自动应答
您可以在此列出您希望排除在（自动应答器所启动的）应答之外的地址。

> 有时，自动应答邮件可能会发送到一个返回本身自动应答的地址。这样就会引起“乒乓”效应，使得邮件在这两个服务器之间不断来回。若您碰到这种地址，请在此输入以防止这种情况发生。这同样是一个位于自动答器» 设置 706屏幕上的选项，可用来将自动应答邮件限制为每天应答每位发件人一次。

删除
点击此按钮，从已排除地址的列表中删除任何所选条目。

新建排除地址—通配符可用
如果您希望添加一个地址到排除地址列表中，请在此输入地址然后点击*添加*按钮。

运行程序

运行该程序
使用该字段来指定当新邮件抵达受此模板控制的群组成员时，您希望为其运行的程序路径和文件名。必须确保该程序可以正常终止并能在无人职守的情况下运行。若有需要，可以在可执行路径后立即输入可选的命令行参数。

传递邮件到进程
选择该选项与进程（在*运行该程序*字段中指定）将传递触发邮件的名称，而该名称将作为第一个可用的命令行参数。当自动应答器在为将邮件转发至另一位置但未在其自身邮箱中保留本地副本的账户进行设置时，（参见转发 610）那么此功能将被禁用。

默认情况下，MDaemon 会将邮件文件的名称用作命令行中的最后一个参数。您可以通过使用 $MESSAGE$ 宏覆盖这一行为。在邮件文件名称应该放置的位置使用此宏。允许更为灵活地使用该功能，这样便能使用以下如此复杂的命令行：
logmail /e /j /message=$MESSAGE$ /q.

邮件列表

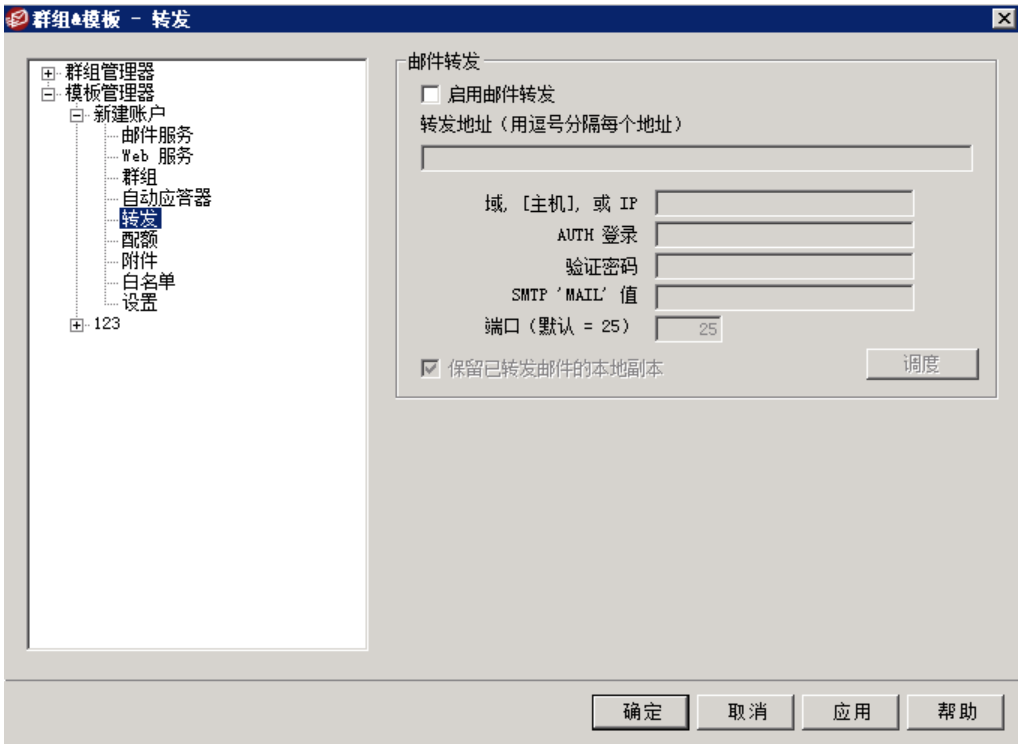
添加发件人到邮件列表
若在该字段中输入一个邮件列表，那么入站邮件的发件人将自动添加到此邮件列表中的一员。对于自动构建列表，这是一个非常简便的功能。

从此邮件列表删除发件人
如果在该字段中输入一个邮件列表，则自动从指定的邮件列表中删除该入站邮件的发件人。

还请参阅：

模板属性 667
群组属性 658
新建账户模板 667
账户编辑器 » 自动应答器 607

5.2.2.1.5 转发



此模板上的选项对应 "账户编辑器"转发[610]屏幕上的选项。在将一个模板设置成控制此屏幕[667]时，该模板将控制所属使用此模板群组[658]的任何账户的 "转发"选项。

邮件转发

启用邮件转发
如果您希望将相关账户的入站邮件转发到一个地址或者在 *"转发邮件"*选项中所指定的地址，那么请勾选此框。具有 web 访问权限[603]（针对 Webmail[266]或 Remote Administration[293]）的 MDaemon 用户可以使用提供的选项来为自己设置转发选项，无需管理员设置。

转发地址（用逗号分隔每个地址）
如果您希望当相关账户的入站邮件到达时转发邮件副本，那么请使用该字段来指定邮件地址。如果已勾选上方的 *"启用邮件转发"*选项，每一封新到达邮件服务器的邮件将被自动生成一个副本并被转发到在此字段中指定的地址。当转发到多个地址时，使用逗号将每个地址隔开。

域、[Host]或 IP
如果您希望通过其他服务器路由已转发的邮件，例如特定域的 MX 服务器，请在此处指定域或 IP 地址。如果您希望通过指定主机路由转发的邮件，把值放入[]中（例如 [host1.example.com]）。

AUTH 登录/密码
请在此处输入要将相关联用户的邮件转发到服务器的所有必需登录名/密码凭证。

SMTP "MAIL"值
如果在此指定一个地址，会将其用于（在与接受主机的 SMTP 会话期间发送的 "MAIL From"语句中，而不使用邮件的实际发件人。若您需要一个空的 SMTP "MAIL From"语句（例如 "MAIL FROM <>"）则在此选项中输入 "[trash]"。

端口（默认值 = 25）
MDaemon 会使用在此所指定的 TCP 端口来发送转发邮件。默认的 SMTP 端口是 25。

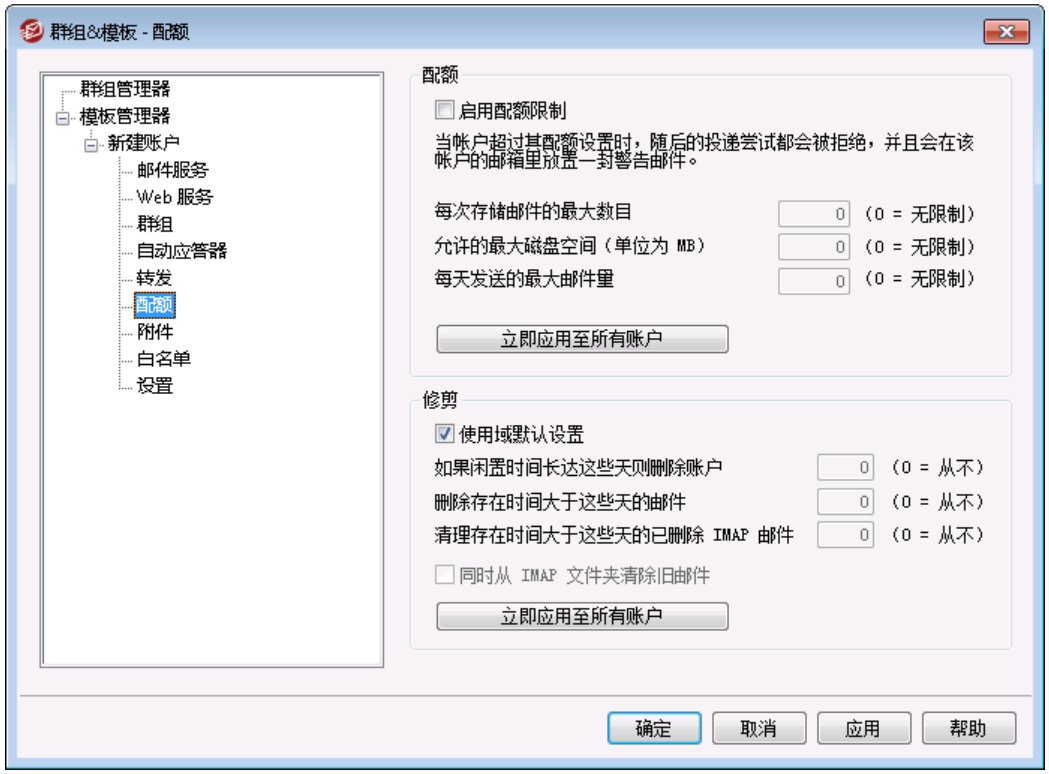
保留已转发邮件的本地副本
默认情况下，每封转发邮件的副本都会正常投递到本地用户邮箱。若您未勾选此框，则不会保留任何本地副本。

调度
点击此按钮可为您创建何时转发相关联账户的电子邮件的调度时间表。您可以设置开始日期和时间、结束日期和时间，并指定在一周中的哪几天转发邮件。

还请参阅：

模板属性 667
群组属性 658
新建账户模板 667
账户编辑器 » 转发 610

5.2.2.1.6 配额



此模板上的选项对应"账户编辑器"[配额](#)屏幕上的选项。在将一个模板设置成[控制此屏幕](#)时，该模板将控制所属使用此模板[群组](#)的任何账户的"配额"选项。

配额

启用配额限制
如果您希望指定受此模板控制的账户可存储的最大邮件数，或者设置账户可以使用的最大磁盘空间（包括在账户的"文档"文件夹中所包含的一切文件附件），或指定这些账户每天可以通过 SMTP 发送的最大邮件数，您可以勾选此框。如果尝试投递到某个账户的邮件将超过最大邮件数或磁盘空间限制，则拒收此邮件，并将一封合适的警告邮件放置到用户的邮箱中。如果 MultiPOP 收集将超出账户的最大限制，则发送一封类似的警告邮件，并自动关闭该账户的 MultiPOP 条目（但不是从数据库中删除）。

使用*"如果达到这个配额百分比则通过电子邮件向用户发送警告"*这个选项（位于"账户» 账户设置» 配额")来在账户接近其配额限制时发送警告邮件。当账户超出了其*"立即存储的最大邮件数"*或*"允许的最大磁盘空间"*限制中指定的百分比数值时，会在午夜向该账户发送一封警告邮件。该邮件中将列出此账户所存储的邮件数，邮件箱的大小，以及所用和剩余百分数。此外，如果在账户的邮箱里找到现有警告，会以更新过的邮件进行替代。

每次存储邮件的最大数目
使用该选项为这些账户指定可以存储的最大邮件数。在该选项中，使用"0"表示对于已认可的邮件没有数量限制。

允许的最大磁盘空间（单位是 MB）
使用该选项来指定这些账户可以使用的最大磁盘空间，包括可以存储在各个账户“文档”文件夹中的任意文件附件。在该选项中，使用“0”表示对于账户可以使用的磁盘空间，没有任何数量限制。

每天发送的最大邮件数
使用此项来指定各个账户每天可以通过 SMTP 发送的最大邮件数。如果账户达到此限制，就会拒收来自该账户的新邮件，直到在午夜重置计数器为止。如果您不希望限制账户可以发送的邮件数量，请在此项中使用“0”。

立即应用于所有账户
点击此按钮来将这个屏幕上的设置应用到所有现有的 MDaemon 账户（其配额设置并未专受账户模板的控制）。将账户重新设置为默认的配额值。此选项仅适用于新建账户模板 667。

清理
这一部分的选项是用来指定当受此模板控制的账户处于闲置状态时，是否或何时被删除。你也可以指定该账户的旧邮件在一定时间后是否被删除。每晚午夜，MDaemon 将会删除所有超过时间限制的旧邮件，或者彻底删除达到闲置限制的账户。

使用域默认设置
认的清理设置视域而定，并且位于“域管理器”的“设置 175”屏幕上。如果您希望为受此模板控制的这些账户覆盖域的默认值，清除该选择框并在下方选项中设置想要的值。

账户闲置这些天后将其删除（0=从不）
在删除账户前指定您允许该账户处于闲置状态的天数。此控件中的值“0”意味着账户从不会因为不活动而被删除。

删除存在时间长于这些天的邮件（0=从不）
这是邮件被 MDaemon 自动删除前在账户的邮箱里可以保留的天数。“0”值意味着邮件永远不会因其存在时间而被删除。**请注意：**此选项的设置不适用于包含在 IMAP 文件夹中的邮件，除非您还启用下方的*“也清理 IMAP 文件夹中的旧邮件”*这个选项。

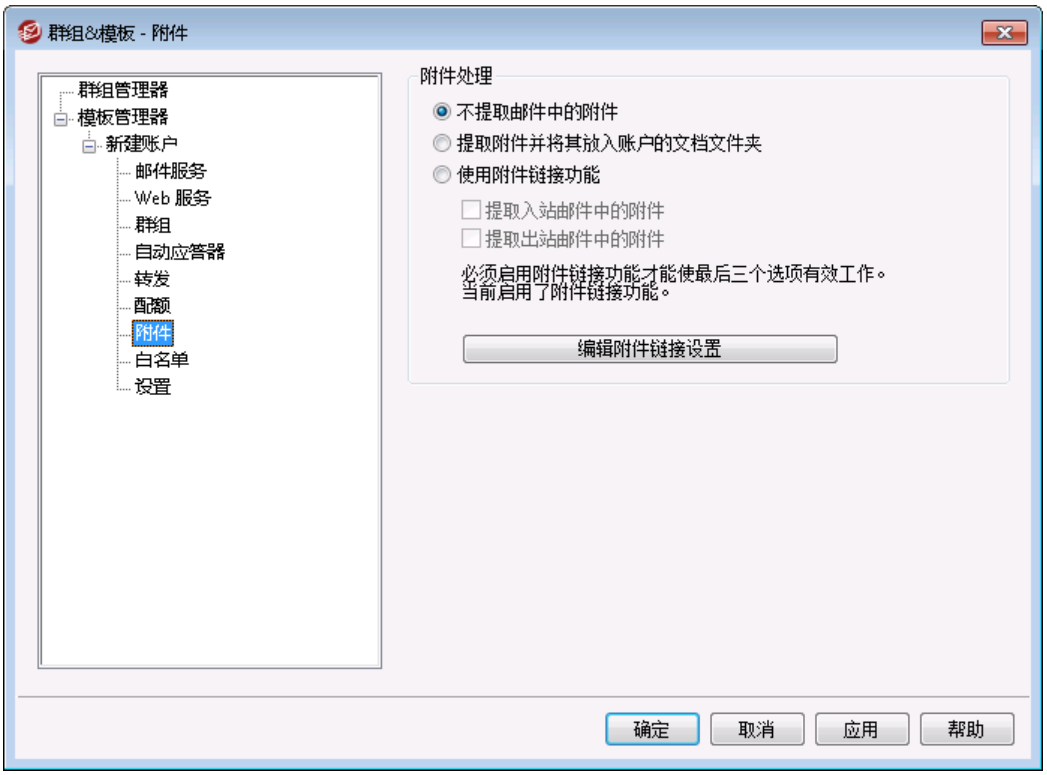
清理存在时间长于这些天的已删除 IMAP 邮件（0=从不）
使用此控件来指定您允许标记为已删除的 IMAP 邮件在此用户的文件夹中可以保留的天数。对于已经标记为删除的 IMAP 邮件在到达指定天数前会被自动清理掉。值“0”表示带有删除标记的邮件从不会因为其存在天数而被删除。

同时从 IMAP 文件夹清理旧邮件
如果您希望*“删除存在时间超过以下天数的邮件”*这个选项同样应用于 IMAP 文件夹中邮件，请点击此选择框。禁用该选项时，IMAP 文件夹中的常规邮件将不会因为其存在时间而被删除。

还请参阅：

模板属性 667
群组属性 658
新建账户模板 667
账户编辑器 » 配额 613
账户设置 » 配额 721

5.2.2.1.7 附件



此模板上的选项对应"账户编辑器"的"附件 616"屏幕上的选项。在将一个模板设置成控制此屏幕 667时，该模板将控制所属使用此模板群组 658的任何账户的"附件"选项。

附件处理

不提取邮件中的附件
如果选中此选项，将不提取受模板控制的这个账户邮件中的附件。将正常处理含有附件的邮件，并将附件完整保留。

提取附件并将其放置在账户的文档文件夹
如果设置，此选项使得 MDaemon 自动提取在入站邮件中发现的任何 Base64 MIME 内嵌文件附件。从经过解码并被放置在账户"文档"文件夹内的入站邮件中删除已提取的文

件。邮件正文中放置了一个便笺，列出了已提取文件的名称。该选项不提供转至已存储附件的链接，不过用户可以使用 Webmail[266] 来访问其文档文件夹。

使用附件链接功能
如果您希望为含有附件的入站或出站邮件使用 "附件链接"功能，请选择此项。

如果已选择该选项，不过在附件链接[305]对话框上禁用了附件链接功能，则不会提取附件。

从入站邮件提取附件
启用此项时，能够提取账户入站邮件中的附件并将其存储在 "附件链接[305]"对话框中指定的位置。然后将 URL 链接置于邮件正文，该用户可以点击此链接以下载文件。鉴于对安全的考虑，这些 URL 链接不包含直接文件路径。而是包含该服务器所使用的独特标识符 (GUID)来映射文件到实际路径。GUID 映射图存储在 `AttachmentLinking.dat` 文件中。

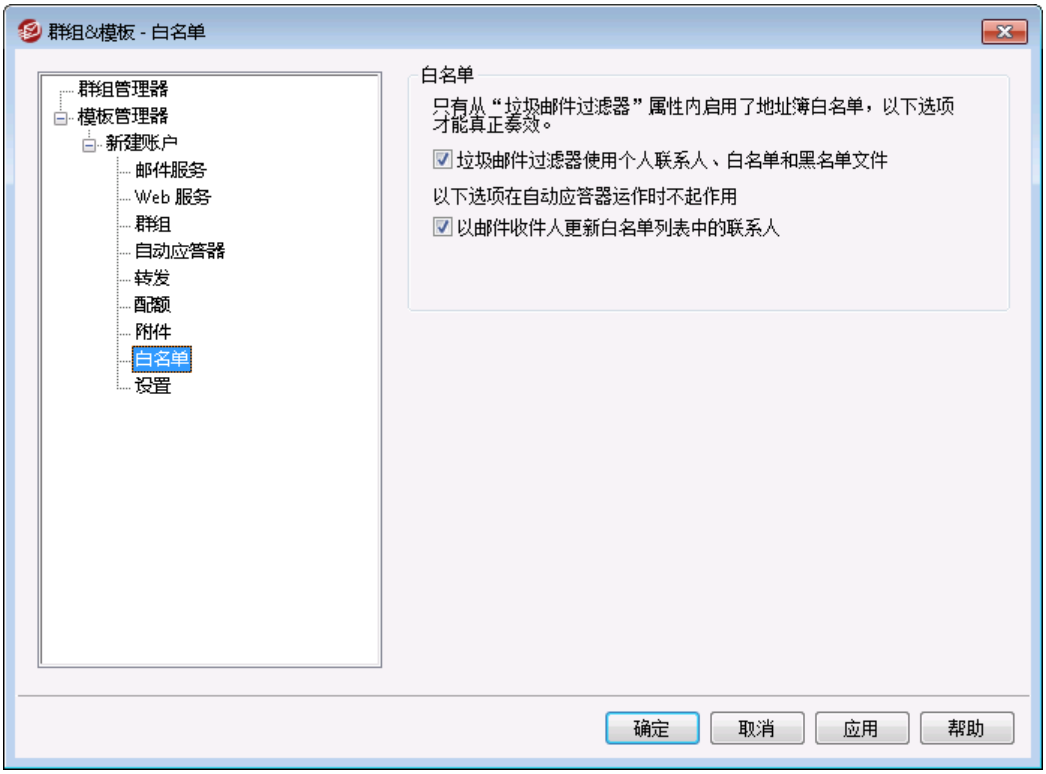
从出站邮件提取附件
如果您希望使用 "附件链接"功能来提取账户出站邮件中的附件，则勾选此框。在账户发送电子邮件时，附件链接将提取文件，进行存储，并使用一个 URL 进行替换来下载此文件。

编辑 "附件链接"设置
点击此按钮来打开 "附件链接[305]"对话框。

还请参阅：

模板属性[667]
群组属性[658]
新建账户模板[667]
附件链接[601]
用户编辑器 » 附件[616]

5.2.2.1.8 管理角色



管理角色

账户是全局管理员
启用该选择框来赋予这些用户服务器级别的管理员访问。全局管理员可以：

- 通过Remote Administration 完全访问服务器配置、全部用户以及全部域
- 可以作为即时通信好友来访问所有 MDaemon 域的所有用户。
- 即使邮件列表标记为“只读”，仍可投递邮件到所有邮件列表。
- 即使管理员不是其中成员，仍可投递邮件到所有邮件列表。

该用户将能完全访问 MDaemon 的文件和选项。要了解 Remote Administration 的 web 界面内各种管理选项的详细信息，请参阅 Remote Administration 293。

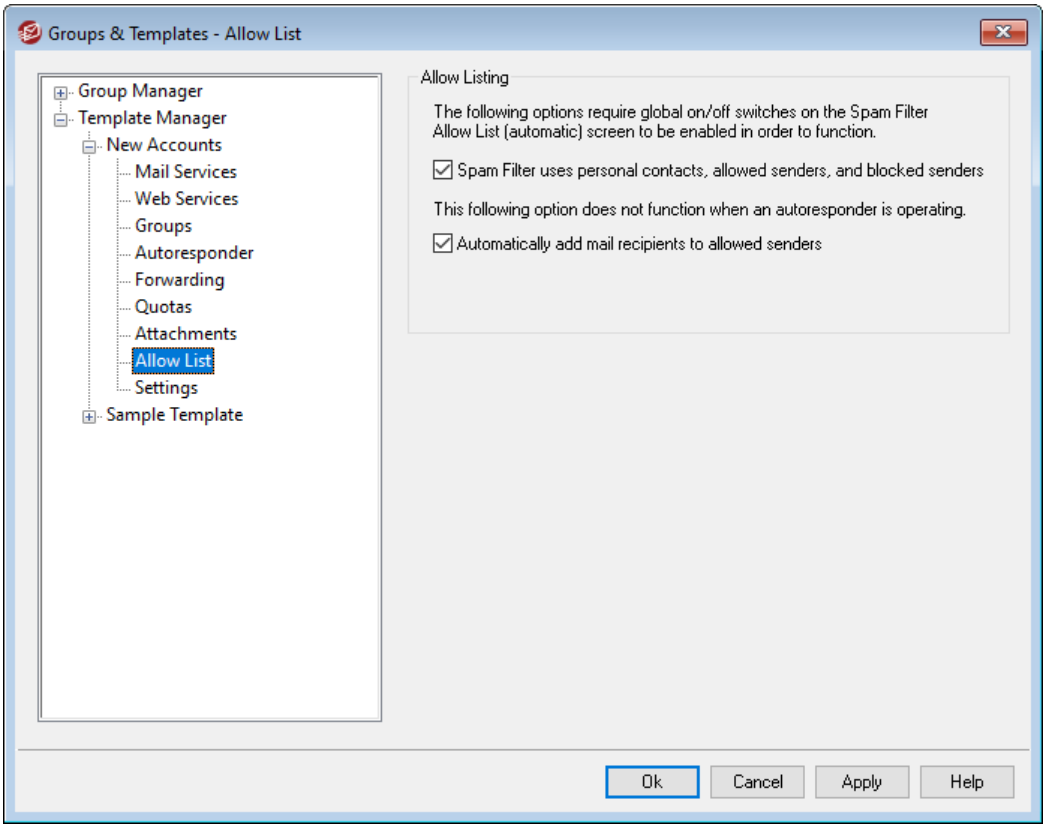
账户是域管理员
点击此勾选框来将您的用户指定为域管理员。域管理员和全局管理员类似，不过其管理访问权限受到此域和“Web 服务 603”页面上所授权限的限制。

此屏幕不适用于新建账户模板 667。不能为新建账户自动授予管理访问权限。要为账户授予管理访问权限，将此账户与使用此屏幕来授予访问权限的自定义模板相关联，或从“账户编辑器”的“管理角色 636”屏幕手动指定该账户为管理员。

还请参阅：

模板属性 667
群组属性 658
新建账户模板 667
账户编辑器 » 管理角色 636

5.2.2.1.9 允许列表



此模板上的选项对应"账户编辑器"的 允许列表 637屏幕。在将模板设置成控制此屏幕 667时，它将 为属于使用该模板的群组 658的任何账户控制"允许列表"屏幕的设置。

允许列表

垃圾邮件过滤器使用个人联系人、已允许发件人和已阻止发件人
"垃圾邮件过滤器"的"允许列表（自动）575"屏幕上含有一个全局选项，如果在本地收件人的私人联系人或已允许发件人文件夹中找到邮件的发件人，那么使垃圾邮件过滤器将自动允许该邮件。如果在用户的已阻止发件人文件夹中找到发件人，就将自动阻止该邮件。如果您已启用了"垃圾邮件过滤器"的全局选项，但不希望将此功能应用到这些账户，请清除此框来覆盖全局设置。如果禁用了全局选项，此项将不可用。

自动将邮件收件人添加到已允许发件人
如果您希望在每次该账户地址簿发送一封出站邮件到一个非本地邮件地址时，更新每个账户的已允许发件人文件夹，请点击此选项。当结合使用上述*"垃圾邮件过滤器使用私人联系人、已允许发件人和已阻止发件人"*选项时，可大幅减少垃圾邮件过滤器误报数

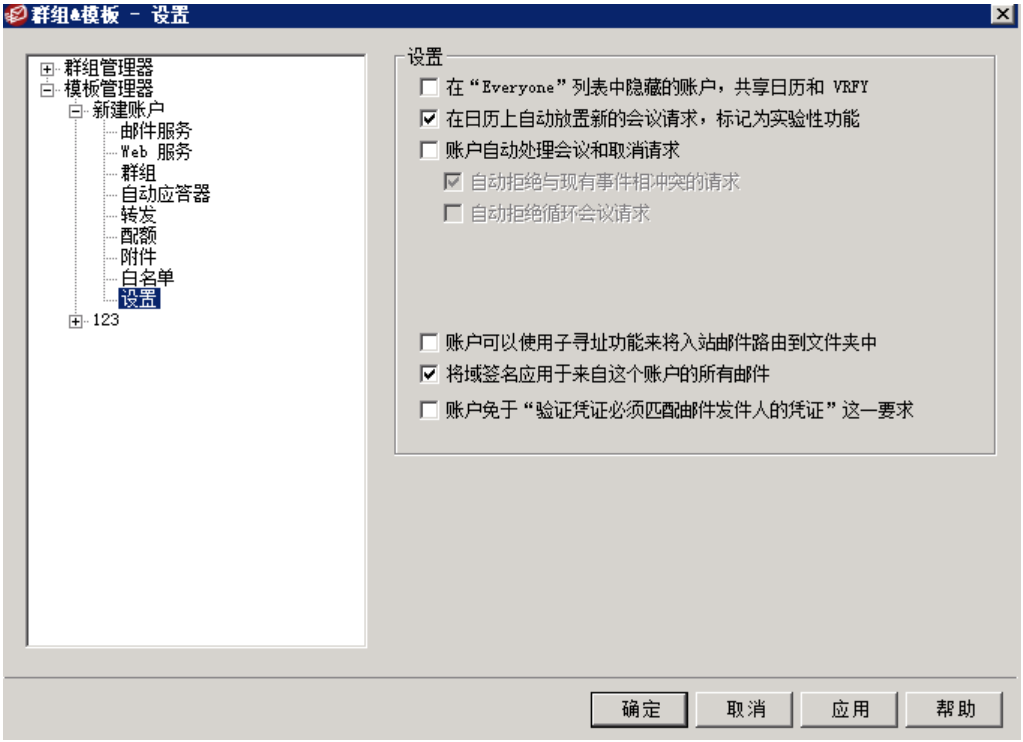
量。在您使用 *"自动将邮件收件人添加到已允许发件人"*选项(位于允许列表 (自动)575屏幕上)之前,您必须已启用该功能。

在账户使用自动应答器时,该选项是禁用的。

还请参阅:

模板属性667
群组属性658
新建账户模板667
账户编辑器 » 允许列表637

5.2.2.1.10 设置



此模板上的选项对应"账户编辑器"设置639屏幕上的设置。在将一个模板设置成控制此屏幕667时,该模板将控制所属使用此模板群组658的任何账户的"选项"屏幕设置。

设置

从"所有人"列表、共享日历和 VRFY 隐藏的账户
MDaemon 为每个域自动创建并维护一个"everyone@"邮件列表,可用于将一封邮件立即发送给所有人。默认情况下,当 MDaemon 构建此列表时,会将所有账户包含其中。

如果您希望将受此模板控制的这个账户排除在该列表之外，请勾选此框。这样做将在共享日历及 VRFY 74 结果中隐藏这些账户。

自动在日历上放置标记为 "临时"的新会议请求
默认情况下，当一个账户收到新的会议请求时，会议将被放置在用户的日历上并标记为 *"临时"*。如果您不希望这是新账户的默认设置，请清除此复选框。

账户自动处理会议和取消请求
如果您希望为各个账户自动处理会议请求、更改及取消，请点击此选择框。当一个账户接收到一封包含会议请求的邮件，那么将自动更新账户的日历中。默认情况下为所有账户禁用该选项。

自动拒绝与现有事件相冲突的请求
如果启用了自动处理会议请求和取消，默认情况下，在这些会议请求与现有事件相冲突时将自动拒绝这些请求。如果您允许创建相冲突的事件，请取消勾选此框。

自动拒绝循环会议请求
如果已启用了自动处理会议请求和取消，不过您又希望拒绝那些循环会议请求，请点击此框。

账户可以使用子寻址来将入站邮件路由到文件夹
如要允许对账户进行子寻址 640，可点击该选择框。

向来自这个账户的所有邮件应用域签名
存在受此模板控制的这些账户所属域的 "域签名 166 "时，此项允许您将这个签名添加到这些账户发送的所有电子邮件中。

账户免于 "身份验证凭证必须匹配这些电子邮件发件人"要求
如果您希望受此模板控制的这些账户免于 *"身份验证凭证必须匹配这些电子邮件发件人"*这个位于 SMTP 验证 438 "屏幕的全局选项，则使用此项。

需要应用程序密码才能登录 SMTP、IMAP、ActiveSync 等
如果您希望使用模板的账户必须使用邮件客户端中的应用程序密码 630 来登录 SMTP、IMAP、ActiveSync 或其他邮件服务协议，请勾选此框。不过，该账户的常规密码 717 必须仍被用来登 Webmail 或 Remote Admin。

"需要应用程序密码"有助于保护账户密码免受字典和通过 SMTP、IMAP 等进行的暴力攻击。这样更安全的原因是因为即使这种攻击是猜测账户的实际密码，它也不会不起作用，因为 MDaemon 只会接受正确的应用程序密码。此外，如果 MDaemon 中的账户正在使用 "活动目录"验证，"活动目录"又在达到失败的尝试次数后锁定了账户，该选项有助于防止账户被锁定，因为 MDaemon 只会检查应用程序密码，而不尝试对 "活动目录"进行身份验证。

还请参阅：

模板属性 667
群组属性 658
新建账户模板 667
账户编辑器 » 设置 639

5.3 账户设置

5.3.1 活动目录

使用位于 "账户» 账户设置» 活动目录"中的 "活动目录"选项，可将 MDaemon 配置为监控活动目录，并且当 MDaemon 的相关账户在活动目录中发生改变时，自动创建、编辑、删除和禁用 MDaemon 账户。此外，还能将其设置成使用存储在活动目录中的最新信息，使所有公共联系人记录保持在最新状态。将为常规字段 (例如账户的邮寄地址、电话号码、业务联系人信息等)填入其公共联系人记录，而且如果上述信息在 "活动目录"中发生变化，将随时更新这些数据。

创建账户

在设置监控 "活动目录"时，MDaemon 将按指定的时间间隔查询变更，然后每当它找到一个新添加的 "活动目录"账户就会创建一个新的 MDaemon 用户账户。将会使用全名、登录、邮箱、描述、以及启用/禁用在 "活动目录"中所找到的状态来创建一个新的 MDaemon 用户账户。

根据默认，由活动目录监控而创建的 MDaemon 新账户将添加到 MDaemon 的默认域。或者，您可以选择将这些帐户添加到在账户'"用户主要名称"的活动目录属性中所找到的域。当使用了此选项时，如果一个账户需要一个尚不存在于 MDaemon 的域，那么将自动创建一个新的域 149。

您还可以将*搜索过滤器* 692配置为监控 "活动目录"中的群组，因此将用户添加到组，或将组添加到用户，将导致在 MDaemon 中创建该用户，而从组中删除用户将导致该账户在 MDaemon 中被禁用 (而不是删除)。

删除账户

当从 "活动目录"中删除一个账户时，MDaemon 可配置成采取下列操作中的其中一种：无操作，删除相关的 MDaemon 账户，禁用相关的 MDaemon 账户，或者冻结相关的 MDaemon 账户 (例如：该账户仍可接收邮件但是用户无法收集或访问该邮件)。

更新账户

MDaemon 检测到活动目录账户有更改时，将自动更新对应 MDaemon 账户中的相关属性。

同步 MDaemon 与活动目录

"*即刻执行全面的 AD 扫描*"选项将使得 MDaemon 查询 "活动目录"数据库，若有需要，可创建或修改 MDaemon 用户账户。如果发现 "活动目录"账户与现有的 MDaemon 账户匹配，MDaemon 账户将链接到该账户。然后，对 "活动目录"账户所作出的任何进一步修改将自动套用到 MDaemon 账户。

活动目录验证

由 MDaemon 活动目录功能所创建的账户根据默认将设置为 "活动目录 (AD)验证"。凭借 AD 验证，MDaemon 无需在自身的用户数据库中存储账户的密码。取而代之的，账户持有人将使用他或她的 Windows 登录/密码凭证，并且 MDaemon 将会使这些通过 Windows 以验证相关账户。

要对 "活动目录"使用 "AD 验证"，一个 Windows 的域名必须出现在 "监控 694"上所提供的空间中。这是 MDaemon 尝试验证账户时将使用的 Windows 域。大多数情况下，MDaemon 会自动检测该 Windows 域名并完成填写。不过您也可以在此项中选择使用一个替代域；如果您希望在您所有的 Windows 域中允许验证而不是仅限于某个特定的域，您可以使用 "NT_ANY"。如果将此选项留空，创建新账户后 MDaemon 将不使用 "AD 验证"。而是会生成一个随机的密码，在用户可以访问他们的邮件账户之前，您必须手动编辑这些密码。

持续监控

即使当 MDaemon 关闭时，"活动目录"监控仍将继续运作。将会跟踪 "活动目录"的所有变更，一旦 MDaemon 重启后，会对这些变更进行处理。

活动目录文件安全

值得注意的是，MDaemon 的 "活动目录"功能不会以任何方式改变 "活动目录"方案文件——所有的监控都是单向的从 "活动目录"到 MDaemon。MDaemon 不会改变您的目录。

活动目录模板

每当 MDaemon 由于活动目录监控和扫描而向账户中添加或做出更改，将使用一个活动目录模板 ("MDaemon/app/ActiveDS.dat") 来将特定的活动目录属性名链接到 MDaemon 的账户字段。例如默认情况下，MDaemon 将活动目录属性 "cn"链接到 MDaemon的 "全称"字段。然而这些链接不是硬编码。如果需要您可以使用记事本轻松编辑该模板，并更改任何默认字段映射。例如，"FullName=%givenName% %sn%"可作为默认设置的备选项："FullName=%cn% "。请参阅 ActiveDS.dat 以获得更多信息。

更新公共地址簿

可以使用 "活动目录"监控来定期查询 "活动目录"，并使用最新信息将 MDaemon 中所有公共联系人的记录保持在最新状态。会为常规字段 (例如账户的邮寄地址、电话号码、业务联系人信息等)填入其公共联系人记录，而且如果上述信息在 "活动目录"中发生变化，将随时更新这些数据。要启用此功能，请使用 *"监控活动目录和更新公共地址簿"*选项，位于：活动目录» 监控 694。

大量联系人记录字段可以使用此功能进行监控。要获得可以映射到 "活动目录"属性的公共联系人记录字段的完整列表，请参阅 "ActiveDS.dat"文件。该文件拥有几个新的映射模板，允许您指定一个或多个 "活动目录"属性，并将其填入特定的联系人记录字段 (例如 %fullName% 用于全名字段、%streetAddress% 用于住址等)。

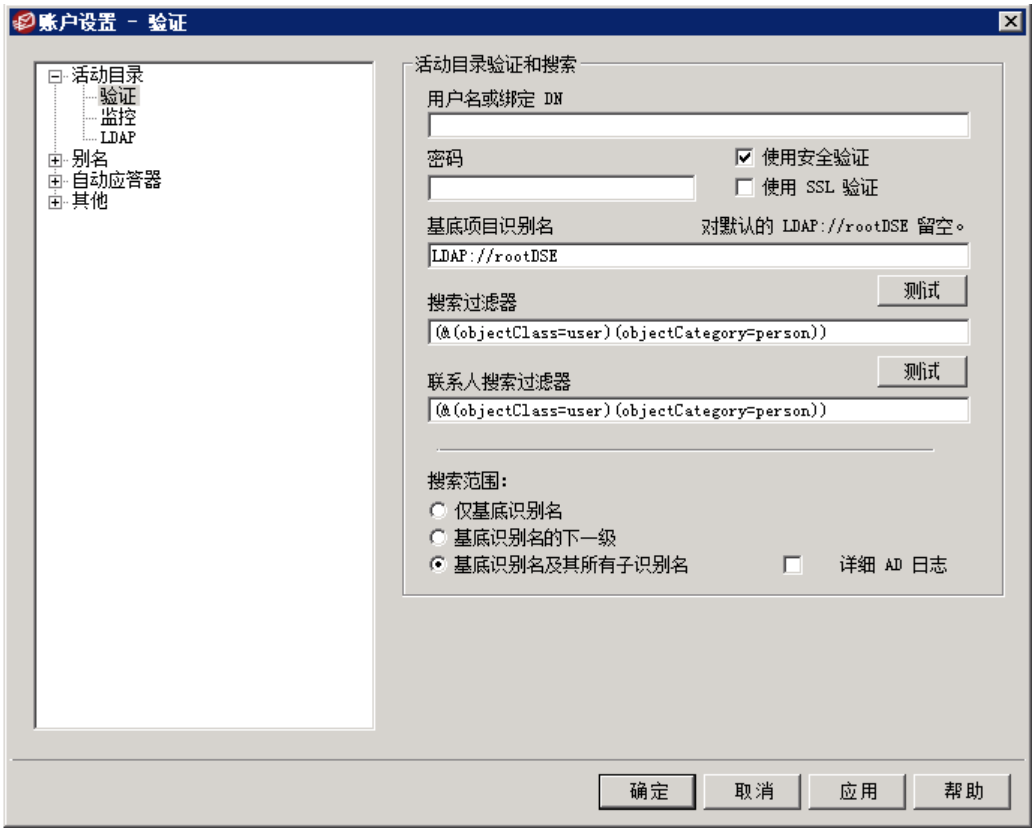
MDaemon 必须将账户的邮件地址与 "活动目录"内的一些属性进行匹配，以此来了解应该更新哪些联系人记录。如果未找到匹配则不执行任何操作。默认情况下，MDaemon 将尝试使用取自映射到 "邮箱"模板 (见 ActiveDS.dat)的数据来构建电子邮件地址，MDaemon 会有目的地将默认域 149名附加到这个模板，就像基于 "活动目录"数据实际创建和删除账户时会执行的操作一样。不过，您可以取消 ActiveDS.dat 内的 "abMappingEmail"模板，并将其与您需要的任何 "活动目录"属性相关联 (例如 %mail%)。值得注意的是，这个属性值必须包含将被识别为有效本地用户账户的电子邮件地址。

如果联系人记录不存在，该功能将创建这个联系人记录。如果联系人记录已存在，该功能将更新这个记录。此外，请注意该功能将覆盖您在 "活动目录"外做出的任何变更。未被映射的联系人记录字段将保持不变。因此，不受限于这个进程的现有数据既不会发生变化，也不会丢失。最后，被设置成 隐藏 639 的 MDaemon 账户不受到联系人记录的创建或更新的影响。

还请参阅：

活动目录 » 监控 694
活动目录 » 验证 692

5.3.1.1 验证



访问活动目录时可能需要设置特殊权限，才能正常使用全部功能。

活动目录 » 验证和搜索

用户名或绑定识别名
这是在通过 LDAP 绑定到 "活动目录"时 MDaemon 将使用的 Windows 账户登录或 DN。"活动目录"允许绑定时使用 Windows 账户或 UPN。

在此选项中使用识别名而不是 Windows 登录时，必须禁用或清除以下的 *"使用安全验证"*选项。

密码
这是在上述 *"绑定识别名"*选项中使用的识别名或 Windows 登录所对应的密码。

使用安全验证
执行活动目录搜索时如果要使用安全验证，请点击此复选框。当您在以上 *"绑定识别名"*选项中使用识别名而非 Windows 登录时，则无法使用本选项。

使用 SSL 验证
执行 "活动目录"搜索时如果要使用 SSL 验证，请点击此选择框。

使用该选项需要在您的 Windows 网络和 "活动目录"中存在 SSL 服务器和架构。如果不确定网络是否按此方式设置，请联系您的 IT 部门，并确定是否应启用该选项。

活动目录搜索

基底项目识别名
这是目录信息树 (DIT)中的标识名 (DN)或起点，MDaemon 将在此搜索活动目录以查找账户和变更。默认情况下，MDaemon 将从 RootDSE 开始搜索，这是您 "活动目录"分层的最顶层项目。指定更精确的起点，使其靠近您特定 "活动目录"树中的用户账户位置，可以减少搜索 DIT 的账户和账户更改所需的时间。留空该字段将存储 LDAP://rootDSE 的默认设置

搜索过滤器
当为账户及账户变更监控或搜索您的 "活动目录"时，这便是要使用的 LDAP 搜索过滤器。使用该过滤器精确地定位你想要包含在 "活动目录"监控中的用户账户。

您还可以将搜索过滤器配置为监控 "活动目录"中的群组，因此将用户添加到组，或将组添加到用户，将导致在 MDaemon 中创建该用户，而从组中删除用户将导致该账户在 MDaemon 中被禁用（而不是删除）。例如，正确的用于名为 "MyGroup"这个组的搜索过滤器可能如下所示：

```
(|(&(ObjectClass=group)(cn=MyGroup))(&(objectClass=user)
(objectCategory=person)
(memberof=cn=MyGroup,ou=me,dc=domain,dc=com)))
```

使用一些与您网络配置的值替换 "ou="和 "dc="。

联系人搜索过滤器
使用此选项可以为联系人搜索指定单独的搜索过滤器。如果您使用与上方 *"搜索过滤器"*选项中这个字段内相同的文本，只需使用一个查询即可更新所有数据。当搜索过滤器不同时，则需要两个单独的查询。

测试
使用 *"测试"*按钮来测试您的搜索过滤器设置。

搜索范围：
这是 "活动目录"的搜索范围或区域。

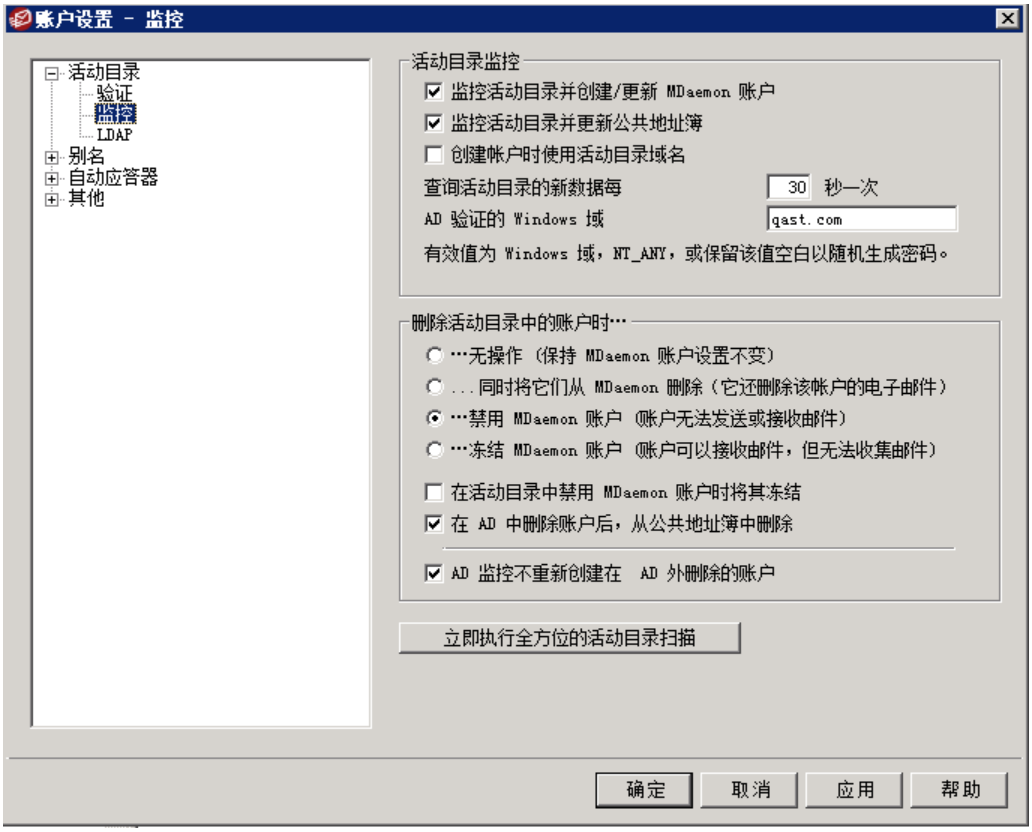
仅基底识别名
如果您搜索仅限制在如上所填的仅基底项目识别名的话，请选择该选项。搜索不会深入到目录信息树 (DIT)中该点的以下部分。

基底识别名的下一级
如果要将 "活动目录"搜索扩展到 DIT 中提供的基底识别名的下一级，则使用该选项。

基底识别名及其所有子识别名
该选项把搜索范围从所提供的 DN 扩展到其所有子项，直至 DIT 中的最低子条目。这是所选的默认选项，当其与下方默认的根 DSE 设置相结合时，就表示将搜索根 DSE 下的所有 DIT。

详细 AD 日志
根据默认，MDaemon 将为 "活动目录"使用详细日志。如果您希望所使用的 "活动目录"日志无需非常详细，请清除该选择框。

5.3.1.2 监控



活动目录监控

监控 "活动目录"并创建/更新 MDaemon 账户
点击此项来激活 "活动目录"监控，这将在 "活动目录"进行更新时创建并更新 MDaemon 账户。

监控活动目录并更新公共地址簿
如果您希望使用 "活动目录"来通过存储在其中的最新信息使所有公共联系人记录保持在最新状态，请启用此项。会为常规字段 (例如账户的邮寄地址、电话号码、业务联系人信息等)填入其公共联系人记录，而且如果上述信息在 "活动目录"中发生变化，将随时更新这些数据。大量联系人记录字段将以这种方式进行监控。要获得可以映射到 "活动目录"属性的公共联系人记录字段的完整列表，请参阅 "ActiveDS.dat"文件。还请参阅：更新公共地址簿 690 来获得更多信息。

创建账户时使用 "活动目录"域名
如果您希望将由 "活动目录"监控创建的新账户添加到在此账户的 "UserPrincipalName"活动目录属性下所找到的域，请使用此选项。当使用了此选项时，如果一个账户需要一个尚不存在于 MDaemon 的域，那么将自动创建一个新的域[149]。如果您希望将所有的新账户都添加到 MDaemon 的 "默认域[149]"，请清除/禁用此项。

每 [XX]秒为活动目录查询一次新数据
这是 MDaemon 用来监控 "活动目录"更改的时间间隔。

进行 AD 验证的 Windows 域
如果您希望对 "活动目录"监控创建的账户使用 "活动目录"身份验证，请在此处指定 Windows 域名。如果该字段留空，则将为新账户指定随机密码。然后，为了可以访问该账户，您必须手动地编辑这些密码。

账户从活动目录删除后...
下方所选择的选项决定了：当一个与 "活动目录"账户相关联的 MDaemon 账户被删除时，MDaemon 将采取何种措施。

...无操作
当 MDaemon 账户相关的账户已从 "活动目录"中删除时，如果不希望 MDaemon 对账户进行任何更改，请选择该选项。

...也从 MDaemon 中删除
选中此项，则 MDaemon 账户的相关账户从 "活动目录"中删除后将删除这个 MDaemon 账户。

这将导致相关的 MDaemon 账户被彻底删除。将删除该账户的所有邮件、邮件文件夹、地址簿和日历等。

...禁用 MDaemon 账户
当选中了此选项并且删除了一个 "活动目录"账户后，将禁用相应的 MDaemon 账户。这表示该 MDaemon 账户仍在服务器，但是无法再收发邮件或者无人能够访问。

...冻结 MDaemon 账户
选择了该选项后，MDaemon 仍会接收该账户的入站邮件，不过会有效地 "锁住"它使其无法被访问。换言之，指向该账户的入站邮件不会被 MDaemon 拒收或者删除，但是一旦冻结了该账户，那么账户持有人将无法收集或是访问此入站邮件。

在活动目录中禁用账户时冻结 MDaemon 账户
根据默认，当您禁用活动目录中的某个账户，MDaemon 也将禁用 MDaemon 中的相关账户。这会造成该账户无法访问且 MDaemon 无法接收或发送该账户的邮件。不过，如果要冻结而不是禁用相关联的 MDaemon 账户，可以启用此项。MDaemon 仍将为冻结的账户接收邮件，不过用户无法访问那些账户来收集或发送邮件。

在 AD 中删除账户时也从公共地址簿将其删除
默认情况下，每当从 "活动目录"中删除其关联账户时，都会删除公共文件夹联系人。不过，仅在联系人最初是由 "活动目录"集成功能创建[690]的情况下，将其删除。如果您不希望在 "活动目录"中删除关联账户时删除联系人，请禁用此选项。

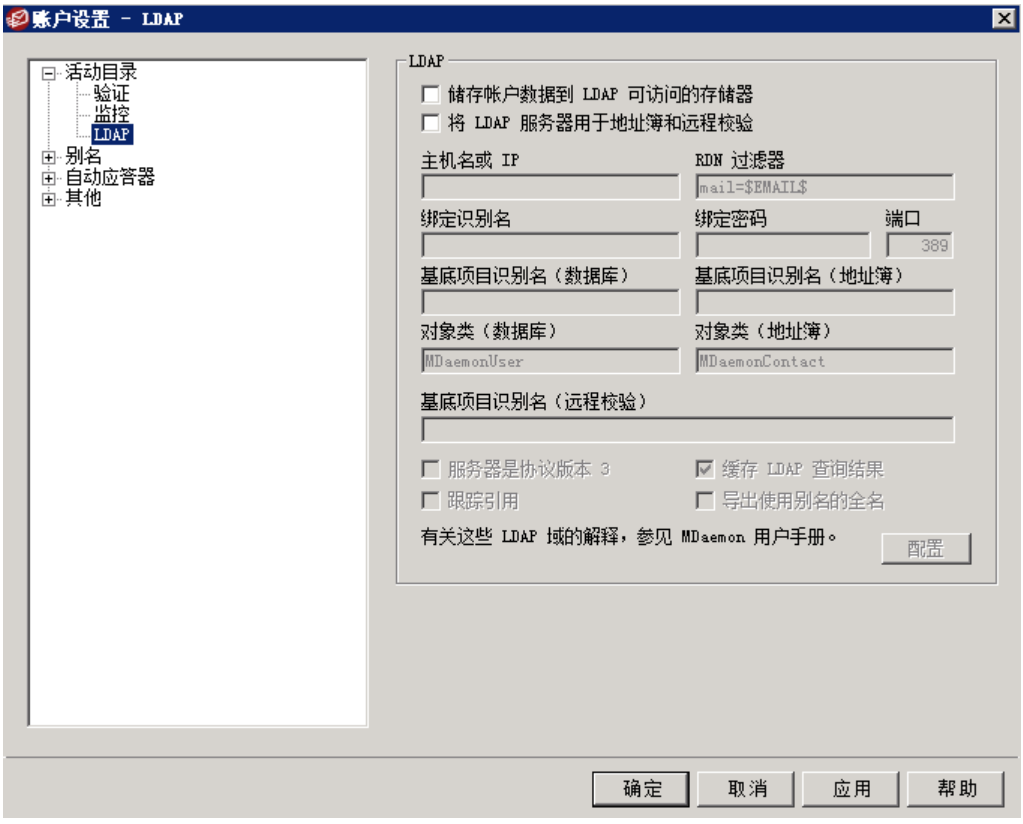
AD 监控不重新创建在 AD 外删除的账户
当您在 "活动目录"以外删除 MDaemon 账户时（例如，通过使用 MDaemon 界面手动将其删除），默认情况下 "活动目录监控"功能将不再重新创建该账户。如果您希望重新创建这些账户，请禁用此项。

立即执行全面的活动目录扫描
点击此按钮让 MDaemon 查询活动目录数据库，如有需要，对账户执行创建、编辑或者删除的操作。当找到一个与现有 MDaemon 账户相匹配的活动目录，那么该 MDaemon 账户将与其链接。

还请参阅：

活动目录 689
活动目录 » 验证 692

5.3.1.3 LDAP



MDaemon 支持轻量级目录访问协议（LDAP）功能。点击 "账户 » 账户设置 » LDAP"以抵达 LDAP 屏幕，用于配置 MDaemon 使您的 LDAP 服务器在其所有的用户账户上保持更新。每当 MDaemon 添加或删除其账户时都会同您的 LDAP 服务器通信，始终准确地更新用户的 LDAP 数据库。这帮助用户使用支持 LDAP 的邮件客户端 "共享"全局地址簿（将包含您的所有 MDaemon 用户条目以及您希望包含的其他联系人条目）。

您也可将 LDAP 服务器用作 MDaemon 用户数据库711，而不是其本地 USERLIST.DAT 系统或 ODBC 数据库。如果您有位于不同位置的多个 MDaemon 服务器，但希望它们共享一个用户数据库，您可能希望使用此方法来维护您的用户信息。每一个 MDaemon 服务器将被配置成连接相同的 LDAP 服务器，以便共享用户信息而不是在本地存储。

LDAP

储存账户数据到 LDAP 可访问的存储器
如果您希望 MDaemon 使用您的 LDaemon 服务器作为 MDaemon 用户数据库而不是 ODBC 或者它的本地 USERLIST.DAT 系统，请点击此选项。如果您有位于不同位置的多个 MDaemon 服务器，但希望它们共享一个用户数据库，您可能希望使用此方法来维护您的用户信息。每一个 MDaemon 服务器将被配置成连接相同的 LDAP 服务器，以便共享用户信息而不是在本地存储。

将 LDAP 服务器用于地址簿和远程验证
如果您使用 ODBC 或者默认的 USERLIST.DAT 方法来维护您的账户数据库而不是使用 LDAP 服务器方式，您可以点击该复选框以使 LDAP 服务器与您用户的名称，电子邮件地址，以及别名一起保持更新。因此，您可以使 LDAP 服务器为包含支持 LDAP 地址薄的电子邮件客户端的用户，使用全局地址薄以保持更新。

这将维护您邮箱，别名以及邮件列表的数据库，您的远程备份服务器可以查询这些邮件列表以进行远程的地址信息验证。要了解更多详情，请参阅以下的*基底项目识别名（远程认证）*。

LDAP 服务器属性

主机名或 IP
在此输入您 LDAP 服务器的主机名或者 IP 地址。

RDN 过滤器
此控件用来为每一个用户的 LDAP 条目生成 RDN。相关识别名 (RDN)在每一个条目识别名 (DN)的最左边。为了所有的对等条目，RDN 必须是独一无二的，因此我们建议使用每一个用户的电子邮件地址作为他们的 RDN，以免可能的冲突。在创建用户的 LDAP 条目时，使用 $EMAIL$ 宏作为在控制中的属性值 (比如 mail=$EMAIL$)将会使它被用户的电子邮件地址所替换。用户的识别名将会包括 RDN plus 和以下的*基底项目识别名*。

绑定识别名
向您的 LDAP 服务器输入您有权管理访问的条目的识别名，可以使 MDaemon 添加并修改您的 MDaemon 用户条目。这是绑定操作中用于身份验证的识别名。

绑定密码
该密码连同*绑定识别名*值将被传递到 LDAP 服务器用于身份验证。

端口
指定您 LDAP 服务器监视的端口。这是向 MDaemon 发送账户信息时它会使用的端口。

基底项目识别名 (数据库)
请输入基底项目 (根识别名)，当您使用 LDAP 服务器而并非使用 USERLIST.DAT 文件用作您的用户数据库的时候，您所有的 MDaemon 用户条目内都会使用这个基底项目。基底项目识别名与 RDN 结合在一起 (请参见以上的 *RDN 过滤器*)以将每个用户的识别名 (DN)补充完整。

基底项目识别名 (地址簿)
对 LDAP 数据库地址簿镜像账户信息时，请输入基底项目 (根识别名)，它将会被您所有的 MDaemon 用户地址簿条目所使用。基底项目识别名与 RDN 结合在一起 (请参见以上的 *RDN 过滤器*)以将每个用户的识别名 (DN)补充完整。

对象类 (数据库)
请指定每个 MDaemon 用户的用户数据库条目必须属于的对象类。每个条目都将包含 objectclass=属性，并将其作为自己的值。

对象类 (地址簿)
请指定每个 MDaemon 用户的 LDAP 地址簿条目必须属于的对象类。每个条目都将包含 objectclass=属性，并将其作为自己的值。

基底项目识别名 (远程验证)，
域网关与备份服务器通常会存在的一个问题就是它们并不总有办法能够确定接收邮件的收件人是否是有效。例如，一封发到 user1@example.com 的邮件进入 example.com 的备份服务器，但备份服务器无法识别该邮件是否来自真正的邮箱、别名或在 example.com 上“user1”的邮件列表。因此备份服务器无法进行选择只能接收所有邮件。MDaemon 可以提供一种方法以验证这些地址并解决这个问题。通过指定一个为所有邮箱，别名和邮件列表所使用的基底项目识别名，您的 LDAP 服务器可以保持所有这些信息的更新。之后，每次有邮件到达您的域，备份服务器会简单得询问 LDAP 服务器并且检验发件人的地址是否合法。如果为非法的，就会拒收该邮件。

服务器是协议版本 3
如果您希望 MDaemon 对您服务器使用 LDAP 协议版本 3，请点击此框。

跟踪引用
有时 LDAP 服务器没有请求的对象，不过可能交叉引用其位置，可以将客户端引用到这个位置。如果您希望 MDaemon 跟踪这些引用，请启用此项。默认情况下，禁用该选项。

缓存 LDAP 查询结果
默认情况下，MDaemon 将缓存 LDAP 查询结果。如果您不希望缓存这些结果，请禁用此项。

导出使用别名的全名
导出到 LDAP 地址簿的非别名会将账户的全名放置到 CN 字段。而别名在那里放置账户的实际 (非别名)邮件地址。如果您希望在那里放置账户的全名，请点击此框。默认情况下，禁用该选项。

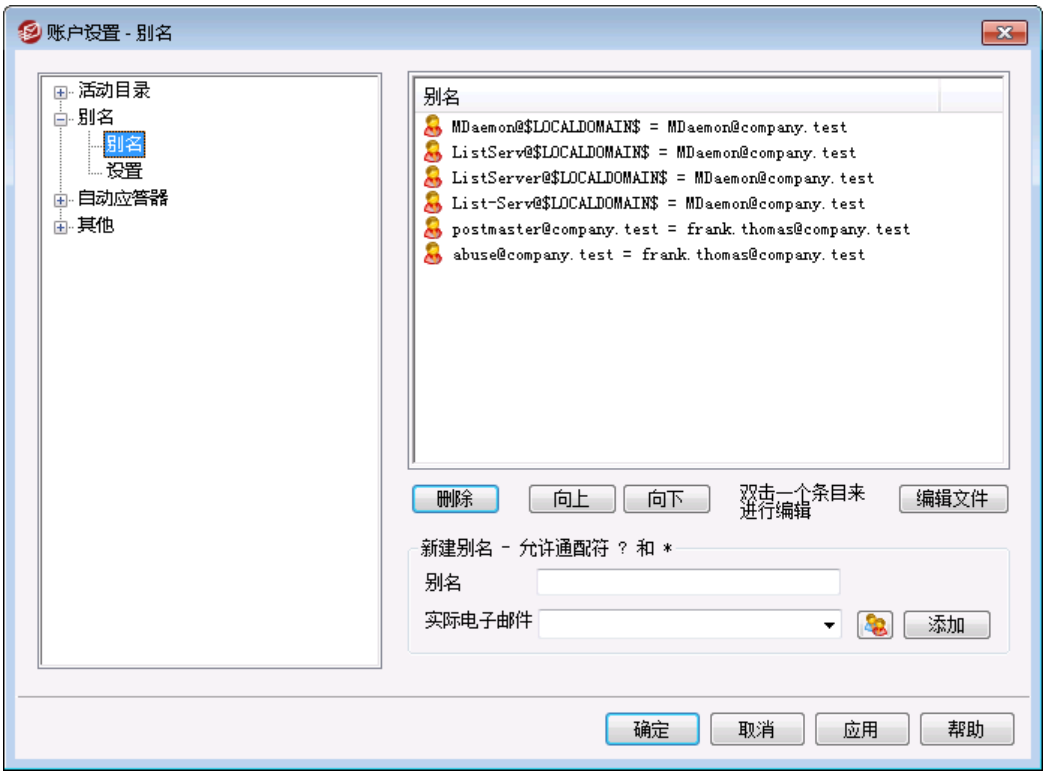
配置
点击此按钮以在文本编辑器中打开 LDAP.dat 配置文件。这在指定关联到每一个 MDaemon 账户字段的 LDAP 属性名称时，非常有用。

还请参阅：

账户数据库选项 711

5.3.2 别名

5.3.2.1 别名



"别名"功能帮助您为账户或邮件列表创建备用邮箱名，当您希望多个邮箱名解析成一个用户账户或列表时，这很有用。如果没有别名，那么您必须为每个地址创建单独的用户账户，然后转发邮件或使用繁琐的过滤器规则将其与其他账户相关联。

例如，如果 user1@example.com 解析了您域所有的账单查询，但您希望所有的人都发到 billing@example.com，那么您可以创建一个地址别名，所有发至 billing@example.com 的邮件实际上会发到 user1@example.com。或者，若您正托管着多个域，并且希望所有指向管理员（不分域）的邮件都发送到 user1@example.com，然后您可以使用一个通配符来关联别名 Postmaster@*，加上他的地址。

当前别名

该窗口包含您创建的所有现有别名。

删除

点击该按钮将删除*当前别名*列表中选定的条目。

正常运行

别名将会按照所列顺序来处理。通过选择和点击此该钮，您可以将别名移至较高的位置。

停机

别名将会按照所列顺序来处理。通过选择和点击此该钮，您可以将别名移至较低的位置。

编辑文件
如果您希望在文本编辑器中打开 Alias.dat 文件来进行手动搜索或编辑，请点击此按钮。完成所需更改后，退出文本编辑器，然后 MDaemon 将重新加载这个文件。

别名
输入您希望作为下方所列 *"实际电子邮件"*别名的邮件地址。您可以使用 "?"和 "*"通配符，也可以使用在别名中使用的 "@$LOCALDOMAIN$"作为通配符，它只匹配您的本地域。例如："user1@example.*"、"*@$LOCALDOMAIN$"和 "user1@$LOCALDOMAIN$"在别名中都可以有效使用。

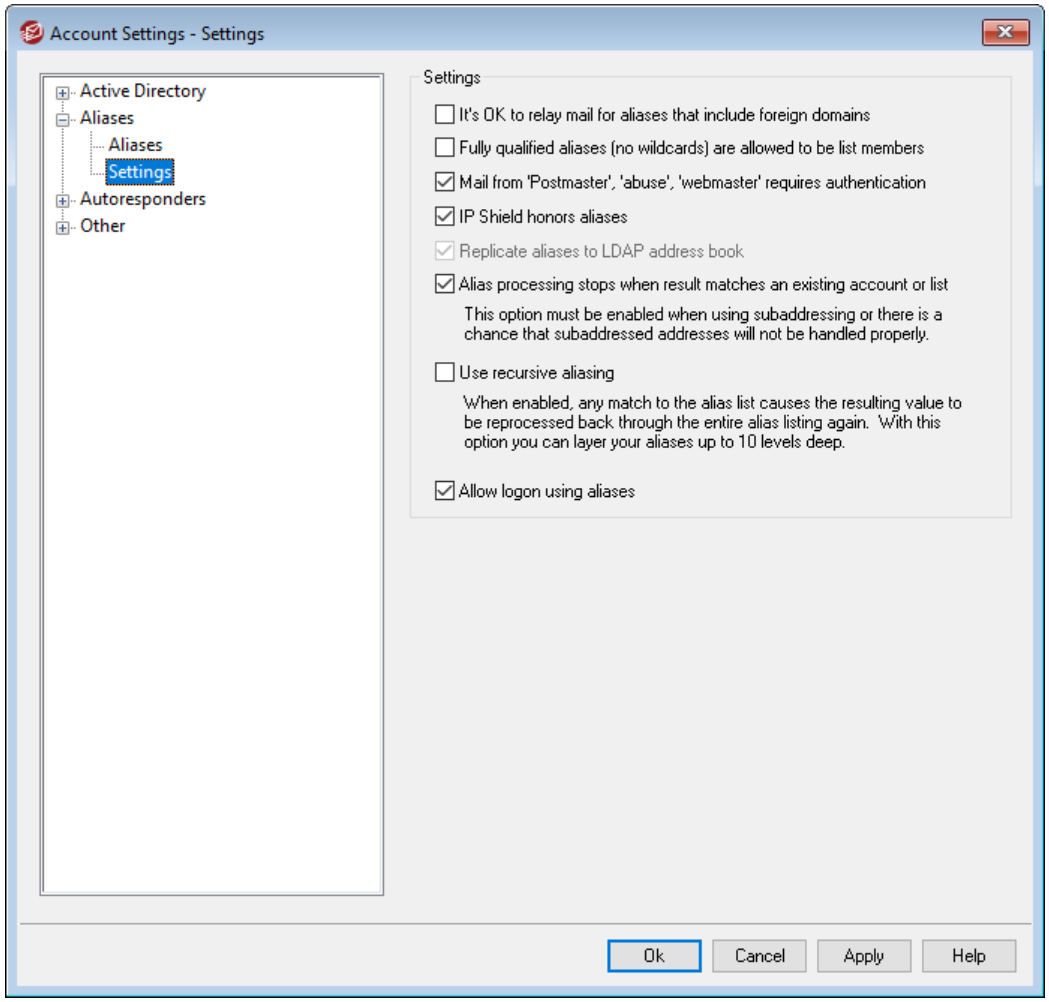
实际电子邮件
从下拉列表中选择一个账户，使用账户图标浏览账户，或者在此空白处输入一个新的电子邮件地址或邮件列表。这是发往相应别名时收件的实际电子邮件地址。

添加
点击 *添加*按钮将别名添加到列表中。将结合 *"别名"*和 *"实际电子邮件地址"*的值，并放置到 *"当前别名"*窗口。

还请参阅：

别名 » 设置 701
账户编辑器 » 别名 622

5.3.2.2 设置



设置

允许为包含外域的别名中继邮件
若您希望允许 MDaemon 为包含非本地域的别名中继邮件，请勾选此框。该选项为这些别名覆盖了*不允许邮件中继*选项（位于中继控制 428 中）。

完全资格的别名（不含通配符）允许为列表成员
如果你希望允许地址别名成为 MDaemon 的邮件列表成员，请选择该项。如果未启用此控件，那么只有实际账户可以成为列表成员。**请注意：**即使选择该选项，包含通配符的地址别名不允许成为列表成员。

发自"postmaster"、"abuse"和"webmaster"的邮件要求身份验证
启用此项时，MDaemon 在接收邮件之前，需要验证声称来自于"postmaster@ ..."、"abuse@ ..."或"webmaster@ ..."别名或账户的任何邮件。垃圾邮件制造者和黑客知道这些地址可能存在，因而会试图利用这些地址通过您的服务器发送给您。该选项将阻止他们和其他未经授权的用户，使其无法达到目的。出于便利，该选项同样可以在"SMTP 验证 438"屏幕上找到，位于："安全性» 安全设置"。在此改变设置将会在那里作出相同更改。

IP 防护接受别名
在默认情况下，当为有效域/IP 对检查入站邮件时，"IP 防护[436]"将准许别名。 "IP 防护"会将别名转换成其指向的实际账户，这样便能准许别名通过 "IP 防护"。如果您清除了此选框，那么 "IP 防护"会将各个别名视作一个与其所代表的账户无关的地址。因此，如果一个别名的 IP 地址违反 "IP 防护"规则，该邮件将被拒绝。该选项是映射在 IP 防护屏幕上的—在此更改设置也将在那里反映出来。

复制别名到 LDAP 地址簿
如果你想将别名复制到 LDAP 地址簿，请点击此复选框。别名的复制对 LDAP 远程验证功能的有效性至关重要，如果你不使用此功能，就不必将别名复制到 LDAP 地址簿。如果你不使用远程认证，您可以安全地禁用此功能来节约处理时间。有关远程 LDAP 验证的更多信息，请见 LDAP[696]。

结果与已有账户或列表匹配时停止别名处理
启用了该选项后，当入站邮件的收件人与现有账户或邮件列表相匹配时，别名处理将会停止。这尤其适用于包含通配符的别名。例如，如果您将一个别名设置成 "*@example.com=user1@example.com"，那么该选项将使得此别名只会适用于并非真实存在于您服务器上的地址中。所以，如果您也有账户 "user2@example.com"，那么指向 user2 的邮件仍将投递给他，因为该别名不适用于这些邮件。但是指向某些不存在的账户或列表的邮件将会发送到 "user1@example.com"，因为通配符别名将会应用于这些邮件。默认情况下启用此项。

当您正在使用子寻址[640]来避免处理这些邮件时所碰到的潜在问题，那么必须启用该选项。

使用递归别名
如果要处理递归别名请点击此选择框。任何别名匹配将使结果值通过整个别名列表进行二次处理——这可能内嵌别名深达十级。例如，你可以如下设置：

```
user2@example.com = user1@example.com
user1@example.com = user5@example.net
user5@example.net = user9@example.org
```

这在逻辑上等同与单别名：

```
user2@example.com = user9example.org
```

这也意味着：

```
user1@example.com = user9example.org
```

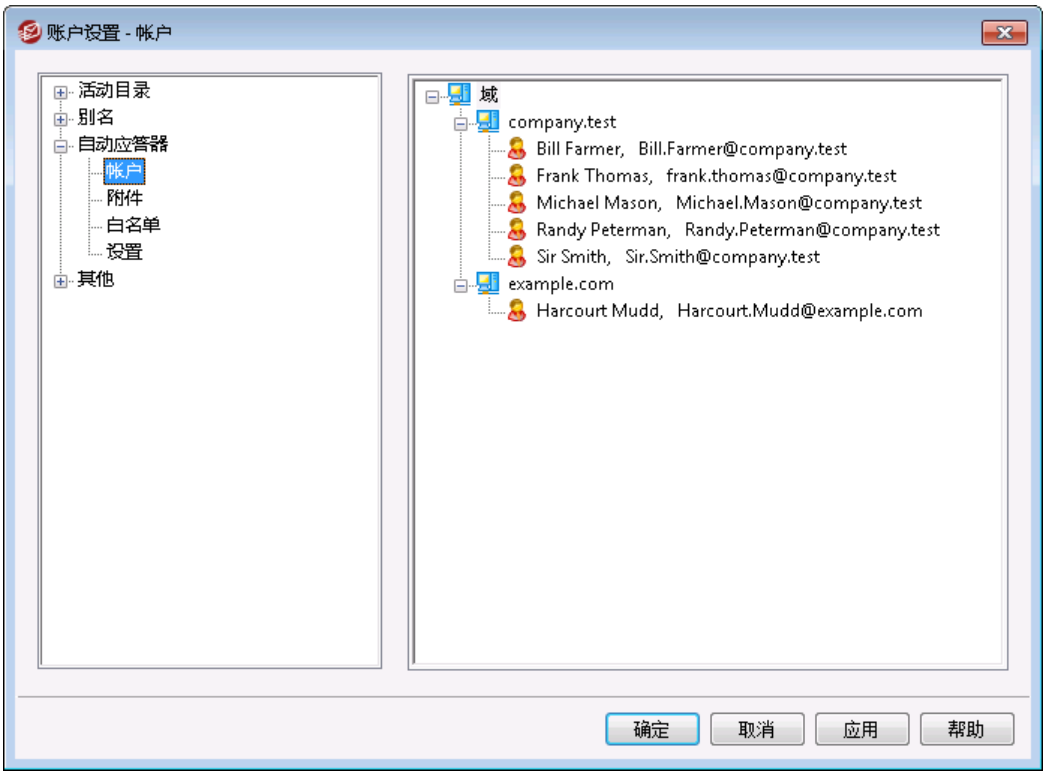
允许使用别名登录
默认情况下，允许用户使用其中一个账户别名[699]而不是其实际的邮箱名称来登录其账户。如果您不希望允许这样，请清除该复选框。

还请参阅：

别名[699]

5.3.3 自动应答器

5.3.3.1 账户



自动应答器是非常有用的工具，使得入站邮件自动触发某些特定事件，例如运行一个程序，添加发件人到邮件列表，以一封自动生成的邮件来应答等等。自动应答器最常见的用途就是以一封用户自定义邮件自动应答入站邮件，声称收件人正在休假目前无法回应，将尽快答复，诸如此类。使用 web 访问[603]和 Webmail[266] 或 Remote Administration[293] 的 MDaemon 用户可以使用所提供的选项来为自己编写自动应答邮件并且安排邮件将要使用的日期。最后，自动应答邮件基于 OOF.mrk 文件的内容，可以在每名用户的根 \data\ 文件夹中找到。此文件支持大量的宏，这些宏可用于引起动态生成邮件的许多内容，从而使自动应答器具有多种用途。

当触发一封来自远程来源的邮件时，总会准许自动应答事件。不过，对于来自用户相同域地邮件，只有在您启用了 *"自动应答器由域内邮件触发"*这个选项后（位于 "自动答器» 设置[706]"屏幕），才会触发自动应答器。您也可以使用该屏幕上的一个选项来限制每个发件人每天针对一个应答的自动应答邮件。

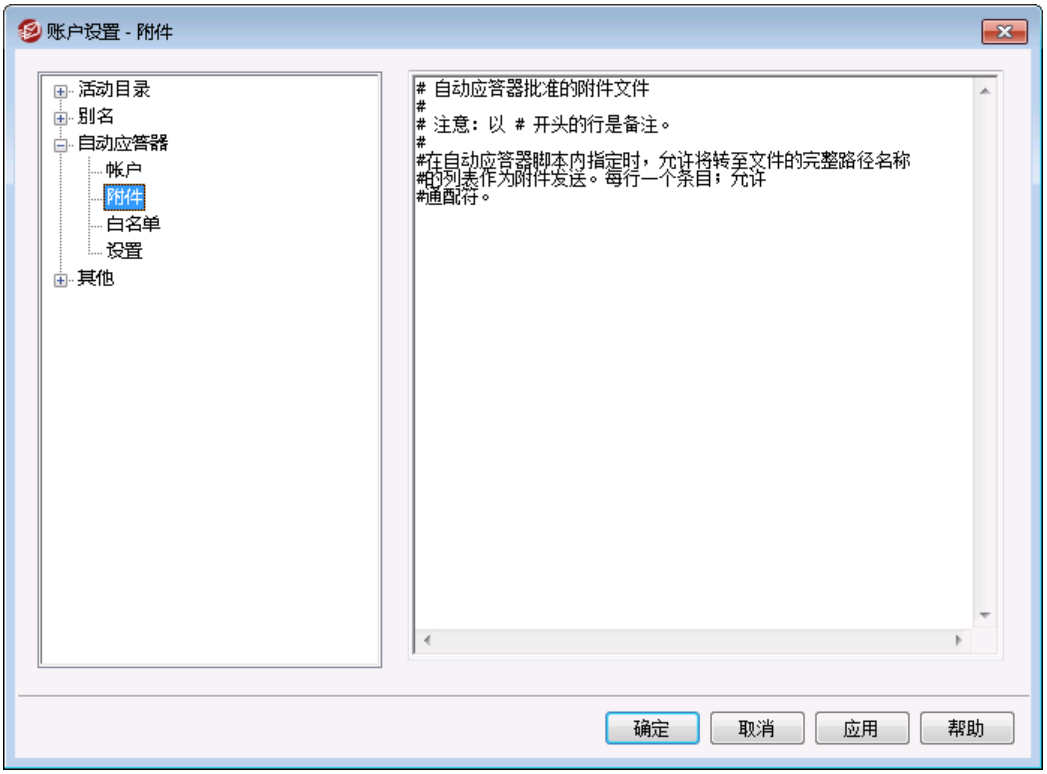
账户列表

此区域列出了允许自动回复的本地邮箱，双击列表里的名单可以打开相应的自动回复对话框。在该列表中双击一个账户来打开其相应的自动应答器[607]屏幕，用来配置该账户的自动应答器。

还请参阅：

自动应答器 » 豁免列表 705
自动应答器 » 设置 706
创建自动应答脚本 707
账户编辑器 » 自动应答器 607

5.3.3.2 附件

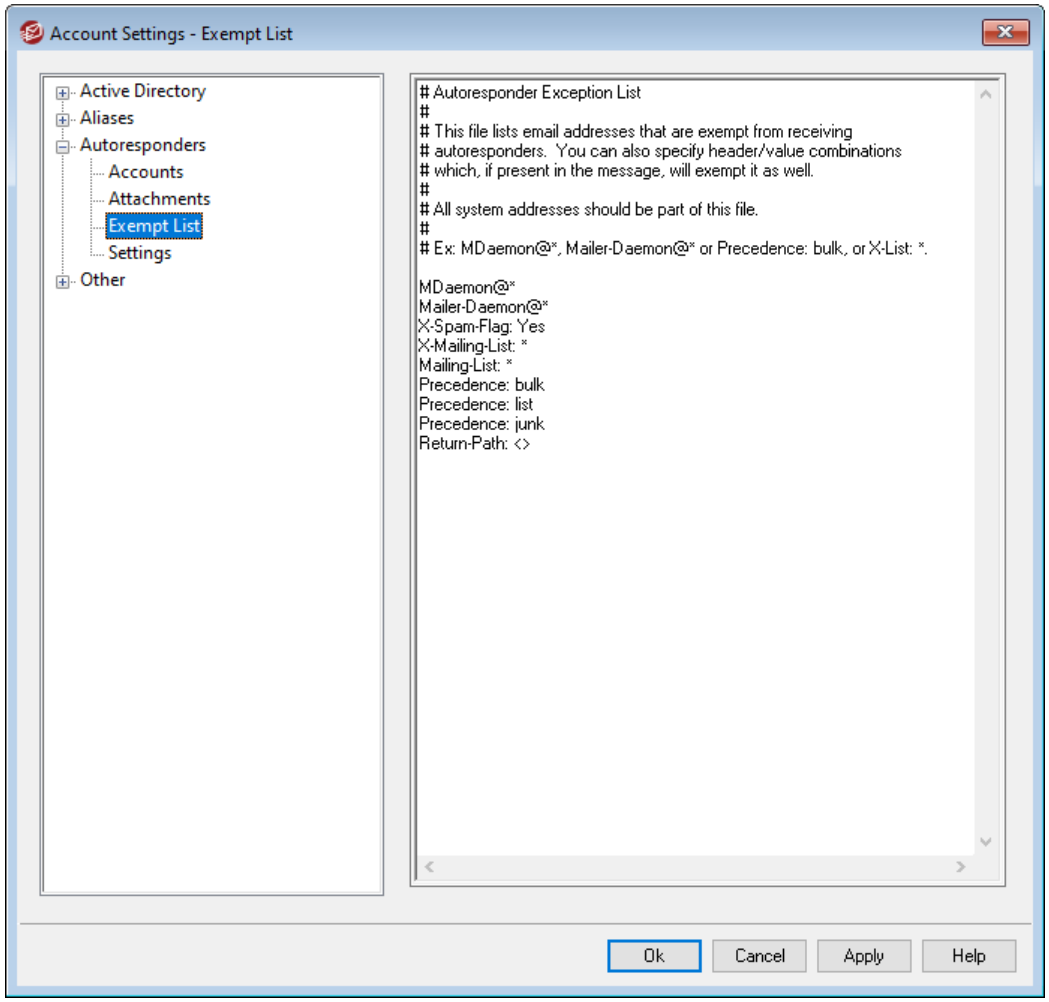


在此提供的转至任何文件的完整路径是您希望将其用作自动应答器脚本 707中的附件的文件。在自动应答器脚本中，请使用 **%SetAttachment%** 替换宏来附加文件。

还请参阅：

自动应答器 » 账户 703
自动应答器 » 豁免列表 705
自动应答器 » 设置 706
创建自动回复脚本 707
账户编辑器 » 自动应答器 607

5.3.3.3 豁免列表



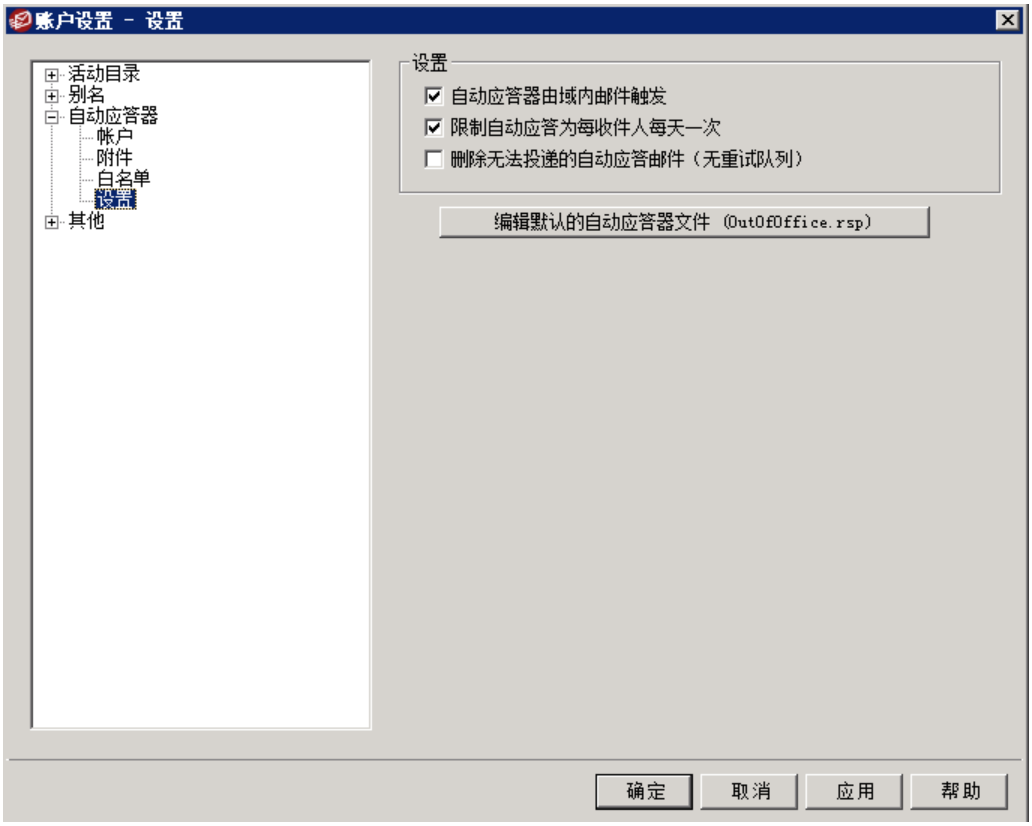
使用“自动应答器»豁免列表”来配置自动应答的全局例外。来自于此列表中条目的邮件将不会收到任何自动应答器。邮件地址和邮件头和值组合可以包含在列表。每一行输入一个地址，或邮件头和值。允许通配符。

所有的系统地址（如.mdaemon@*,mailer-daemon@*,等等）应该在此列出以避免邮件循环和其他问题。

还请参阅：

自动应答器 » 账户 703
自动应答器 » 设置 706
创建自动回复脚本 707
账户编辑器 » 自动应答器 607

5.3.3.4 设置



设置

自动应答器由域内邮件触发
默认情况下，本地和远程邮件都会触发自动应答器。如果您不希望在入站邮件与用户来自同一域时触发自动应答器，请清除此框。

限制每天给每个人只进行一次自动回复
默认情况下，自动应答器为任何给定的地址每天只会生成一封回复邮件。这样能防止从您这边在同一天里不断地，以及每次向您发送邮件时接收到相同的多余自动回复邮件。即使别人在一天内已收到了一封自动回复邮件，您还是希望每次别人发邮件给您时发送自动回复邮件，请清除此框。

该选项同样可以防止邮件循环，当您的自动回复邮件返回到一个同样启动了自动应答器的地址的情况下会产生邮件循环现象。该选项只允许每天向此地址发送一封邮件，而不是让两个地址给对方不断地发送自动回复邮件。

无法投递的自动应答电子邮件只需删除即可（无重试队列）
如果您希望在远程队列中无法投递的自动应答邮件过期时删除这些邮件，而不是将其移入重试队列[732]系统，请启用此项。

编辑默认的自动应答文件 (Out0ffice.rsp)
这是默认的自动应答邮件文件。如果文件缺失或为空，该文件的内容将被复制到账户的oof.mrk 文件[607]。

还请参阅：

自动应答器 » 账户[703]
自动应答器 » 豁免列表[705]
创建自动回复脚本[707]
账户编辑器 » 自动应答器[607]

5.3.3.5 创建自动应答脚本

OOF.mrk 文件是 ASCII 纯文本文件，位于每名用户的根 \data\ 文件夹，定义作为自动应答器结果返回的邮件。当自动应答器触发了一封自动应答邮件，将会处理脚本文件并扫描宏，然后会由触发该应答的入站邮件的真实数据来替代。忽略以 "#"字符开头的行，用作注释。下方列出了两封示例邮件[709]。

自动应答宏

$HEADERS$	该宏将被所有入站邮件的报头替换。该宏前面紧接的文本将在每个扩展的行首进行复制。
$HEADER:XX$	该宏可以使 "xx"所指定的报头值在邮件中扩展。例如：如果入站邮件有 "TO: joe@example.com"，那么 "$HEADER:TO$"宏将扩展为 "joe@example.com"。如果原始邮件拥有 "SUBJECT: 这是主题"，那么 $HEADER:SUBJECT$ 宏将被文本 "这是主题"替代。
$BODY$	该宏将被整个邮件正文替换。在尝试保留不同语言的字符集时，MDaemon 将使用二进制数据而非纯文本读取邮件，从而允许逐字节复制邮件正文。
$BODY-AS-TEXT$	与 $BODY$ 宏类似，该宏将用文本而非二进制的形式被整个邮件正文替代。该宏前面紧接的文本将在每个扩展的行首进行复制。所以，使用一个脚本中的 ">>$BODY-AS-TEXT$"会将原始邮件的每一行放到已生成的邮件中，但是每一行以 ">>"作为开头。文本也将添加到宏的右边。
$SENDER$	该宏解析成入站邮件中 "From: "报头中所包含的完整地址。报头中的地址。
$SENDERMAILBOX$	该宏解析成收件人的邮箱。邮箱是邮件地址中 "@ "符号左边的部分。

$SENDERDOMAIN$	该宏解析成收件人的域。域是邮件地址中 "@" 符号右边的部分。
$RECIPIENT$	此宏解析成邮件收件人的完整地址。
$RECIPIENTMAILBOX$	该宏解析成邮件收件人的邮箱。邮箱是邮件地址中 "@" 符号左边的部分。
$RECIPIENTDOMAIN$	该宏解析成邮件收件人的域。域是邮件地址中 "@" 符号右边的部分。
$SUBJECT$	该宏解析成 "Subject:" 报头的值。报头中的地址。
$MESSAGEID$	该宏解析成 "Message-ID" 报头的值。
$CONTENTTYPE$	该宏解析成 "Content-Type" 报头的值。
$PARTBOUNDARY$	该宏解析成多部件 (multipart) 邮件 "Content-Type" 报头中找到的 MIME "局部分界线" 的值。
$DATESTAMP$	该宏扩展为 RFC-2822 样式的日期时间戳行。
$ACTUALTO$	某些邮件包含 "ActualTo" 字段，一般表示由原来用户在任何格式重定或别名转换之前输入的目标邮箱和主机。该宏扩展为此值。
$ACTUALFROM$	某些邮件包含 "ActualFrom" 字段，一般表示任何格式重定或别名转换之前的原始邮箱和主机。该宏扩展为此值。
$REPLYTO$	该宏解析成 "ReplyTo" 报头的值。
$PRODUCTID$	该宏扩展为 MDaemon 版本信息字符串。
AR_START	返回自动应答器的开始日期/时间。
AR_END	返回自动应答器的结束日期/时间。

报头替换宏

下方列出的宏控制了自动应答邮件的报头。

%SetSender%
例如：%SetSender%=mailbox@example.com
为了达到自动回复邮件的目的，该宏在构建自动回复邮件报头之前重置了原始邮件的发件人。因此，该宏控制了自动回复邮件的 TO 报头。例如，如果原始邮件的发件人是 "user2@example.org"，那么收件人的自动应答器将使用 %SetSender% 宏来将其更

改成 "user1@example.com"，然后会将自动应答邮件的 "收件人"报头设置成 "user1@example.com"。

%SetRecipient%
例如：%SetRecipient%=mailbox@example.com
为了达到自动应答邮件的目的，该宏在构建自动应答邮件报头之前重置了原始邮件的收件人。因此，该宏控制了自动应答邮件的 "发件人"报头。例如，如果原始邮件的收件人是 "michael@example.com"，而且 Michael的账户有一个自动应答器，使用 %SetRecipient% 宏将其更改成 "michael.mason@example.com"，然后会将自动应答邮件的 "发件人"报头设置成 "michael.mason@example.com"。

%SetReplyTo%
例如：%SetReplyTo%=mailbox@example.com
控制了自动应答邮件的 ReplyTo 报头的值。

%SetSubject%
例如：%SetSubject%=Subject Text
替换初始邮件的主题值。

%SetMessageId%
例如：%SetMessageId%=ID String
更改邮件的 ID 字符串。

%SetPartBoundary%
例如：%SetPartBoundary%=Boundary String
更改局部分界线。

%SetContentType%
例如：%SetContentType%=MIME type
将邮件的内容类型更改为声明的值。

%SetAttachment%
例如：%SetAttachment%=filespec
强制 Mdaemon 在新生成的自动回复邮件上附加一个指定文件为附件。只有在附件 704 屏幕可以被附加到自动应答器。

5.3.3.5.1 自动应答脚本示例

使用几个自动应答宏的简单的 oofmrk 自动应答邮件：

```
$SENDER$ 您好

我将不会读取与 $SUBJECT$ 相关的您的邮件，因为我正在放假。Hurray!!!
此致，

$RECIPIENT$
```

您同样可以使用一些报头替代宏来扩展脚本，并控制当自动回复邮件发回到 $SENDER$ 时将会生成的报头：

```
$SENDER$ 您好

我将不会读取与 $SUBJECT$ 相关的您的邮件，因为我正在放假。 Hurray!!!
此致，

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$
%SetAttachment%=c:\photos\me_on_vaction.jpg
```

使用了此脚本后，自动回复邮件会将 "RE: "添加到主题的开头并附有指定文件。

对 "%SetSubject%=RE: $SUBJECT$"行作如下处理：

1. $SUBJECT$ 部分将被原始邮件的主题文本扩展并替代。这将使该字符串等于：

   %SetSubject%=RE: 原始主题文本

2. MDaemon 以新计算的内容替代了原始主题，原始主题存储于内部缓存中。此后，对于脚本中 "$SUBJECT$"的任何使用都将返回一个新结果。

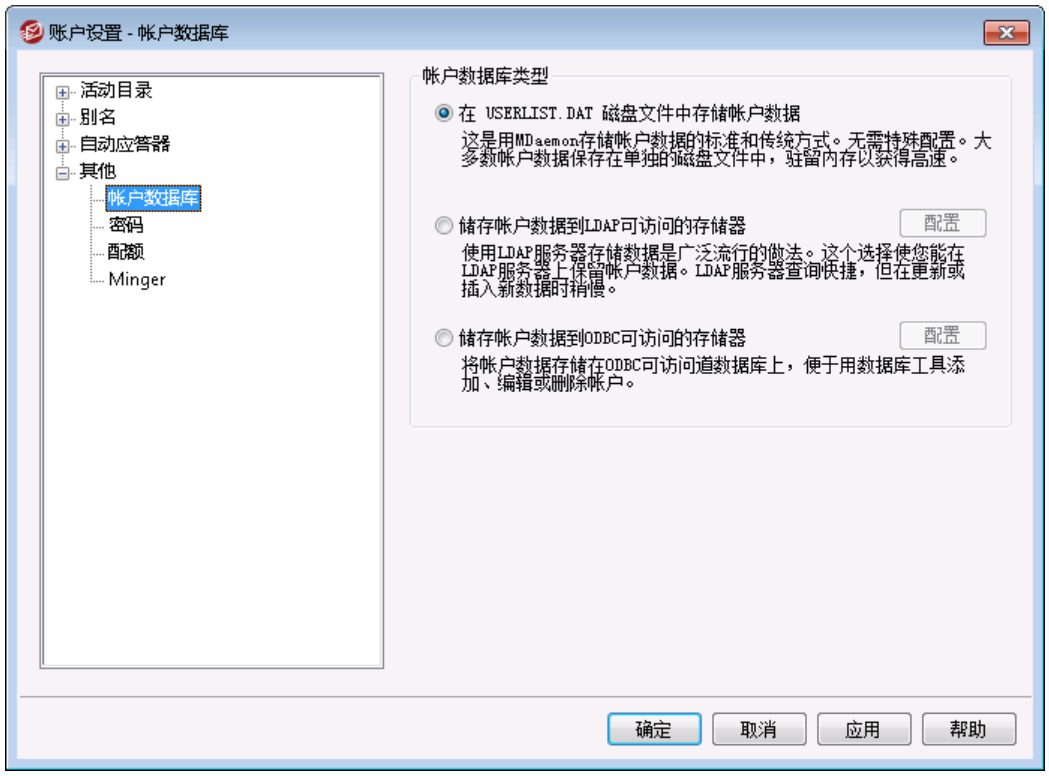
注意这些新宏的位置——它们列于回复脚本的底部。应注意避免副作用。例如，如果将 %SetSubject% 宏置于 $SUBJECT$ 宏之前（此宏位于回复脚本的第二行），那么在 $SUBJECT$ 宏扩展时，主题文本早已改变。因此，不以原始邮件的 "Subject:"报头内容来替代 $SUBJECT$，而以您设置的 %SetSubject% 值来替代。

还请参阅：

自动应答器 » 账户 703
自动应答器 » 豁免列表 705
自动应答器 » 设置 706
账户编辑器 » 自动应答器 607

5.3.4 其他

5.3.4.1 账户数据库



"账户数据库"对话框（位于"账户"»"账户设置"下方），用于指定使用 MDaemon 来维护您的用户账户的方式：ODBC、LDAP 或者本地的 USERLIST.DAT 系统。

账户数据库类型

在 USERLIST.DAT 磁盘文件中存储账户数据
如果您希望 MDaemon 使用其内部文件 USERLIST.DAT 作为账户数据库，请选择该选项。这是 MDaemon 的默认设置，并能使得所有的 MDaemon 用户账户信息都能存储于本地。大多数信息都存储于一个文件夹，通过内存驻留来提高效率与速率。

在 LDAP 存储账户数据
如果您希望 MDaemon 使用您的 LDAP 服务器作为 MDaemon 用户数据库，而不是使用 ODBC 或是其本地 USERLIST.DAT 系统，请选择此选项。如果您有多个 MDaemon 服务器在不同位置，但希望它们共享一个独立的用户数据库，您可能希望使用此方法维护您的用户账户数据。将每个 MDaemon 服务器件配置成连接相同的 LDAP 服务器，以便共享用户信息而不是在本地存储。LDAP 服务器对于查询的反应特别快，效率特别高，不过对于更新或是插入新数据速度相对较慢。

配置
当选中了 LDAP 账户数据选项时，点击此按钮来打开"LDAP 屏幕 696"以配置 LDAP 服务器设置。

储存账户数据到 ODBC 可访问的存储器
如果您希望使用 ODBC 适应数据库作为您的 MDaemon 账户数据库，点击此选项。

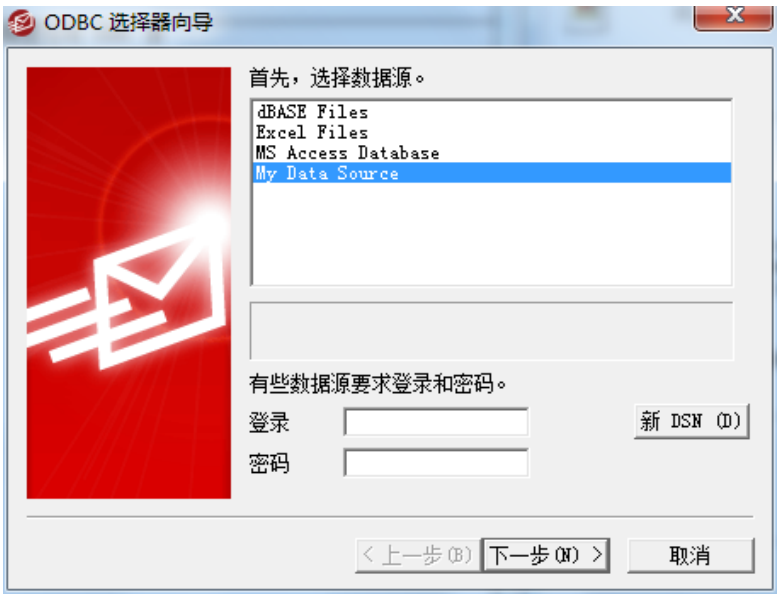
配置
当选中了 ODBC 账户数据选项，点击此选项来打开 "ODBC 选择器向导 712"以选择和配置您的 ODBC 兼容数据库。

5.3.4.1.1 ODBC 选择器向导

使用 "ODBC 选择器向导"来选择或配置一个符合 ODBC 的数据源用作您的 MDaemon 账户数据库。

迁移您的账户数据库到 ODBC 可访问的存储

1. 在 "账户数据库"对话框上 "账户» 账户设置» 账户数据库)，点击 **"存储账户数据到 ODBC 可访问的存储器"**，然后点击 **"配置"**来打开 "ODBC 选择器向导"。

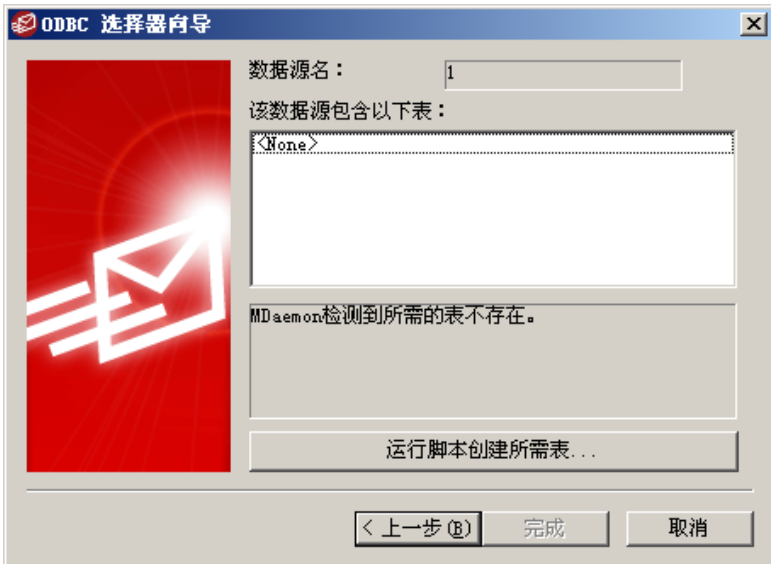


2. 选择**"您希望用于账户数据库的"**数据源。如果列表中没有兼容的数据源，请点击 **"新建 DSN"**并根据以下列出的指导说明，"创建新的 ODBC 数据源 713"。

3. 需要时，请输入数据源的 **"登录名"**和 **"密码"**。

4. 点击 **"下一步"**。

5. 如果数据源中已包含了 MDaemon 所需的表格，直接跳到 **"步骤 8"**。或者，点击 **"运行一个脚本来创建所需表格..."**



6. 在您希望用于数据库应用程序的脚本文件上键入文件路径，或者选择 "浏览")。"\MDaemon\app\"文件夹中包含了多个最流行的数据库应用程序脚本。

7. 点击 **"立即运行脚本并创建数据库表"**，然后点击 **"确定"**，再点击 **"关闭"**。

8. 点击 **"完成"**，然后点击 **"确定"**来关闭 "账户数据库"对话框。

9. 一个数据库迁移工具将迁移您所有的用户账户到 ODBC 数据源，然后关闭 MDaemon。点击 **"确定"**，然后重启 MDaemon，开始使用新的 ODBC 账户数据库。

还请参阅：

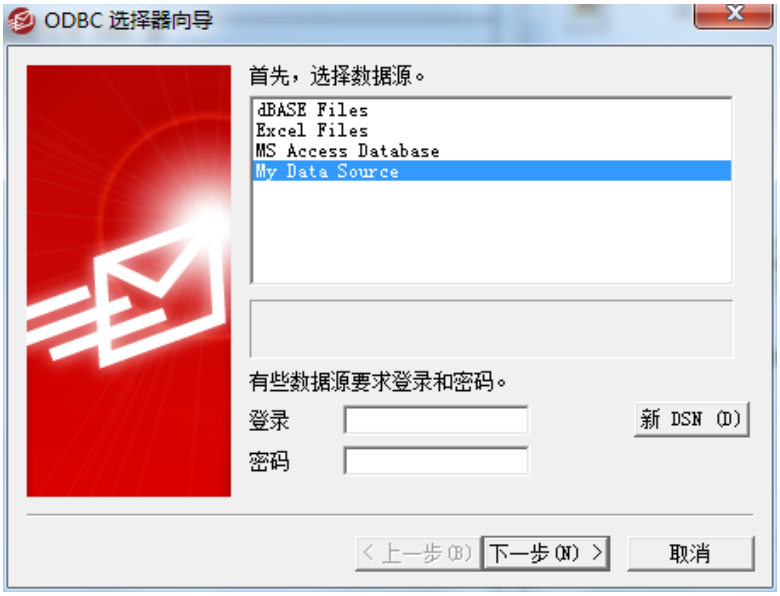
账户数据库 711
创建新的 ODBC 数据源 713

5.3.4.1.1.1 创建一个新的数据源

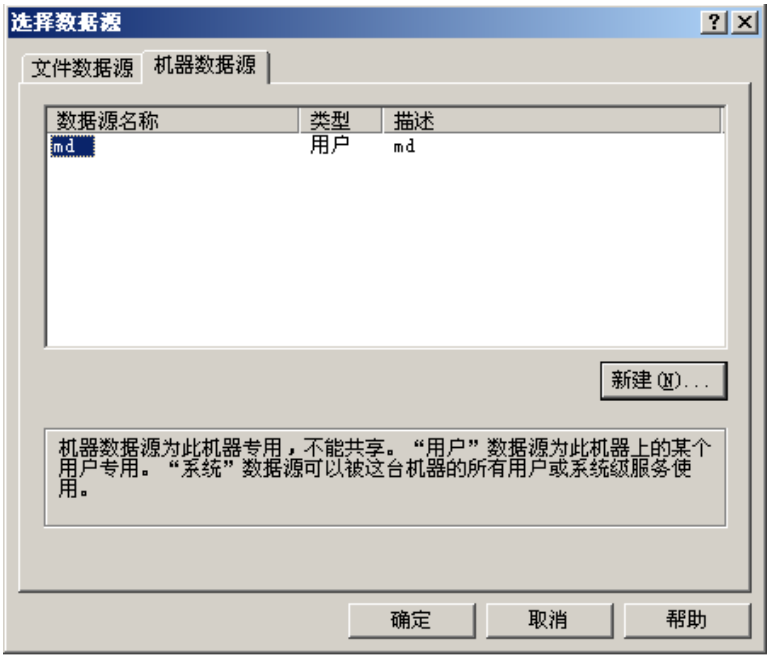
要创建一个新的 ODBC 数据源：

1. 在 "账户数据库"对话框上 "账户" » "账户设置" » "账户数据库"，点击 **"存储账户数据到 ODBC 可访问的存储器"**，然后点击 **"配置"**来打开 "ODBC 选择器向导"。

2. 点击 **新建 DSN**”以打开 选择数据源”对话框。



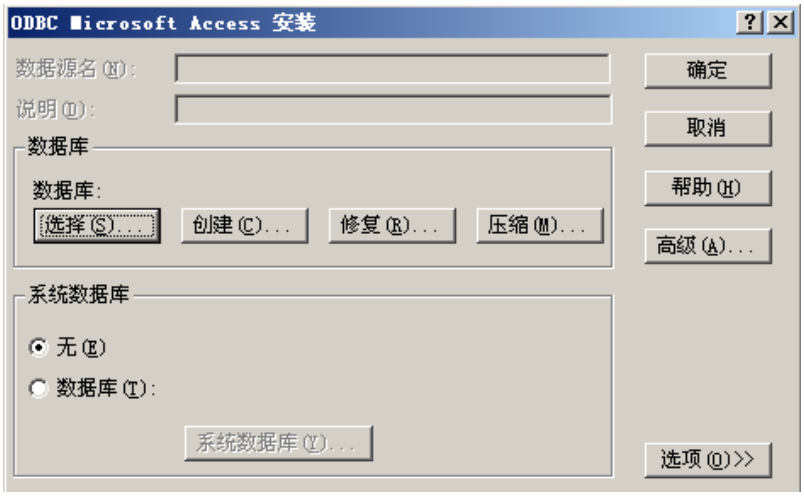
3. 切换到 **机器数据源**”选项卡并点击 **新建...**”以打开 创建新数据源”对话框。



4. 选择 **系统数据源**”并点击“**下一步**”。

5. 选择您想为其安装数据源的**数据**库驱动,**并点**击"**下一步**"。

6. 点击 **完成**"来显示指定驱动的安装对话框。此对话框的样式会根据您所选的不同驱动程序而改变 (以下为 "Microsoft Access 安装"对话框)。



7. 为您的新数据源指定一个 **数据源名称**"并填写指定驱动对话框所要求的任何其他信息(比如创建或指定一个数据库,请选择目录或服务器等)。

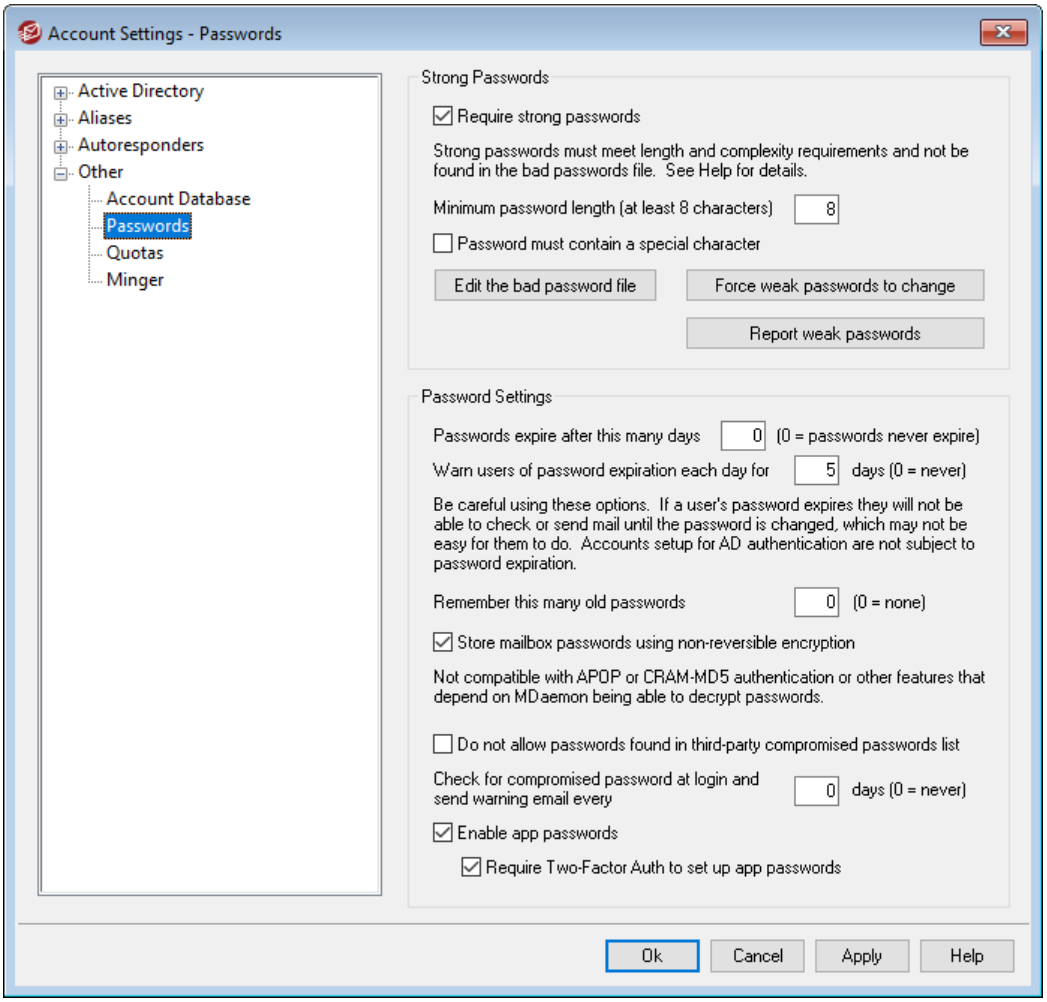
8. 点击 **确定**"以关闭特定的驱动对话框。

9. 点击 **确定**"以关闭 "选择数据源"对话框。

还请参阅:

账户数据库 711
ODBC 选择器向导 - 账户数据库 712

5.3.4.2 密码



强密码

需要强密码
默认情况下，MDaemon 在创建新账户或者更改现有密码时需要强密码。如果您希望禁用强密码要求，请清除此选择框。

强密码必须：
- 满足最小长度要求。
- 包含大小写字母。
- 包含字母和数字。
- 包含特殊字符（如果下方设置了特殊字符选项）
- 不包含用户的全名或邮箱名称。
- 不得在坏密码文件中找到。

密码长度最小值（至少 8 个字符）
使用此项来设置强密码需要的最小密码长度。这必须设置为至少 8 个字符，但建议使用更高的值。新的 MDaemon 安装的默认值为 10 个字符。更改这个设置不为密码长度短于新的最小值的密码自动触发密码变更要求，不过在这些用户下一次更改其密码时，将强制执行这个设置。

在设置了下方的*"使用不可逆加密存储邮箱密码"*选项时，无论最小值的设置如何，密码都可以超过 72 个字符。如果禁用该选项，密码不得超过 15 个字符。

密码必须包含一个特殊字符
默认情况下，对于新的 MDaemon 安装，强密码还必须包含至少以下一个特殊字符：!"#$% &'()*+,-./:;<=>?@ [\]^ _`{|}~. 如果您不希望在强密码中使用特殊字符，请禁用此选项。

编辑坏密码文件
点击此按钮来编辑坏密码文件。列在此文件中的条目区分大小写，而且无法用作密码。如果您希望创建更复杂更多变的条目，您可以使用正则表达式546来实现这一点。会将以 "!"开头的条目视作正则表达式。

强制更改弱密码
如果您希望强制使用弱密码的所有账户更改其密码，请点击此按钮。这将锁定每名使用弱密码的账户，直到他们更改了密码为止。管理员可以通过 MDaemon 界面更改这个密码，被锁定的用户也可以通过 Webmail 或 Remote Administration 界面来更改密码。在用户尝试使用旧密码登录时，将在继续前要求该用户创建一个新密码。**请注意：**在使用下方的*"使用不可逆加密存储邮箱密码"*选项时，此项不可用。

报告弱密码
点击此项来为使用弱密码的所有 MDaemon 账户生成一个报告。在您点击了"确定"之后会将该报告通过电子邮件发送至您指定的电子邮件。**请注意：**在使用下方的*"使用不可逆加密存储邮箱密码"*选项时，此项不可用。

密码设置

这些天后密码过期（0=密码永不过期）
如果您希望设置在需要更改账户密码前，可以访问这个账户的最大天数，请使用此项。此选项中的默认值是"0"，这就表示密码永不过期。不过如果您将其设置为一定数值，例如 30 天，那么**从上次账户的密码被更改那天起**，用户将有30天时间来更改其密码。因此，当您初次设置到期值时，任何具有在指定天数内未更改密码的账户，其密码将立即过期。如果用户的密码过期，那么他或她不能访问 POP、IMAP、SMTP、Webmail 或 Remote Administration。不过，用户仍然可以连接到 Webmail 或 Remote Administration，然后他或她会被要求只有更改密码后才能继续进行处理。无法使用电子邮件客户端（例如 Outlook 和 Thunderbird 等）来更改密码。此外，大量客户端甚至不会向用户显示有用的错误消息，因此他们可能需要管理员协助才能了解他们登录失败的原因。

为了让用户能够通过 Webmail 或 Remote Administration 更改其密码，他们必须先被授予在"Web 服务672屏幕上的"..编辑密

码”web 访问权限。此外，因为更改密码对某些用户而言可能不是易事，您应该慎用此项。

[xx]天来每天警告用户密码过期 (0 = 从不)
密码快要过期的账户可以接收需要更改其密码的每日提醒邮件。使用此项来指定在密码过期前，您希望 MDaemon 开始发送这些每日邮件的天数。

记住这么多旧密码 (0=无)
使用此项来指定您希望 MDaemon 为各名用户记住的旧密码数量。当用户更改了其密码，将不允许他们再次使用旧密码。默认情况下，将此项设置成 “0”(禁用)。

使用不可逆加密来保存邮箱密码
如果您希望 MDaemon 使用不可逆加密来保存密码，请选中此框。此项保护密码不被 MDaemon、管理员或可能存在的攻击者解密。要实现这点，MDaemon 使用 bcrypt 密码散列函数。它允许更长的密码 (长达 72 字符)，而且在导出和导入账户时将保留密码，并防止密码泄露。不兼容一些取决于 MDaemon 是否能够解密密码的功能 (例如弱密码检测和 APOP & CRAM-MD5[74] 验证)。默认情况下，启用不可逆密码。

已泄露密码

MDaemon 可以对照第三方服务中的泄露密码列表来检查用户密码。它能够执行此操作而无需将密码传输到服务，而且如果列表中存在用户的密码，并不表示该账户已被黑客入侵。这就意味着某人在某处使用了与他们的密码相同的字符，并且出现了数据泄露事件。黑客可能会在字典攻击中使用已泄露的密码，但是从未在其他任何位置使用过的唯一密码更加安全。请参阅Pwned Passwords (已泄露密码)获取更多信息。

不允许在第三方已泄露密码列表中找到的密码
如果您不希望将账户的密码被设置为已泄露的密码列表中的密码，请选中此框。

在登录时检查已泄露的密码，并每隔 [xx]天发送警告邮件 (0 = 从不)
使用此选项，您可以在每位用户登录时每隔指定的天数自动针对已泄露的密码列表检查每个用户的密码。如果发现他们正在使用泄露的密码，则会向该账户和邮件管理员发送警告电子邮件 。通过编辑 \MDaemon\App 文件夹中的邮件模板文件，可以定制警告邮件。由于有关如何更改用户密码的说明可能取决于该账户是使用 MDaemon 中存储的密码还是使用 “活动目录[689]”身份验证，因此有两个模板文件：CompromisedPasswordMD.dat 和 CompromisedPasswordAD.dat。宏可用于个性化邮件、更改主题和更改收件人等。

应用程序密码

应用程序密码[630]这个选项通过创建仅在电子邮件客户端和电子邮件应用程序中使用的随机生成的强密码，使账户更安全，因为这些应用程序无法受到双重验证[603] (2FA) 的保护。还请参阅：应用程序密码[630]。

启用应用程序密码
默认情况下，所有用户都可以在使用双重验证登录 Webmail时，为其账户创建应用程序密码。如果您希望为特定的用户禁用 “应用程序密码”支持，您可以使用*...编辑应用程序密码*[603]这个选项来实现这点，该选项位于用户的 “Web 服务”页面上。

要求双重验证来设置应用程序密码
默认情况下，用户必须使用双重验证[603] (2FA) 来创建一个新的 "应用程序密码"来登录 Webmail。不建议禁用上述要求。全局管理员[636]在 MDRA 中不受此要求的约束，但仍然建议他们在登录 MDRA 或 Webmail时始终使用 2FA。

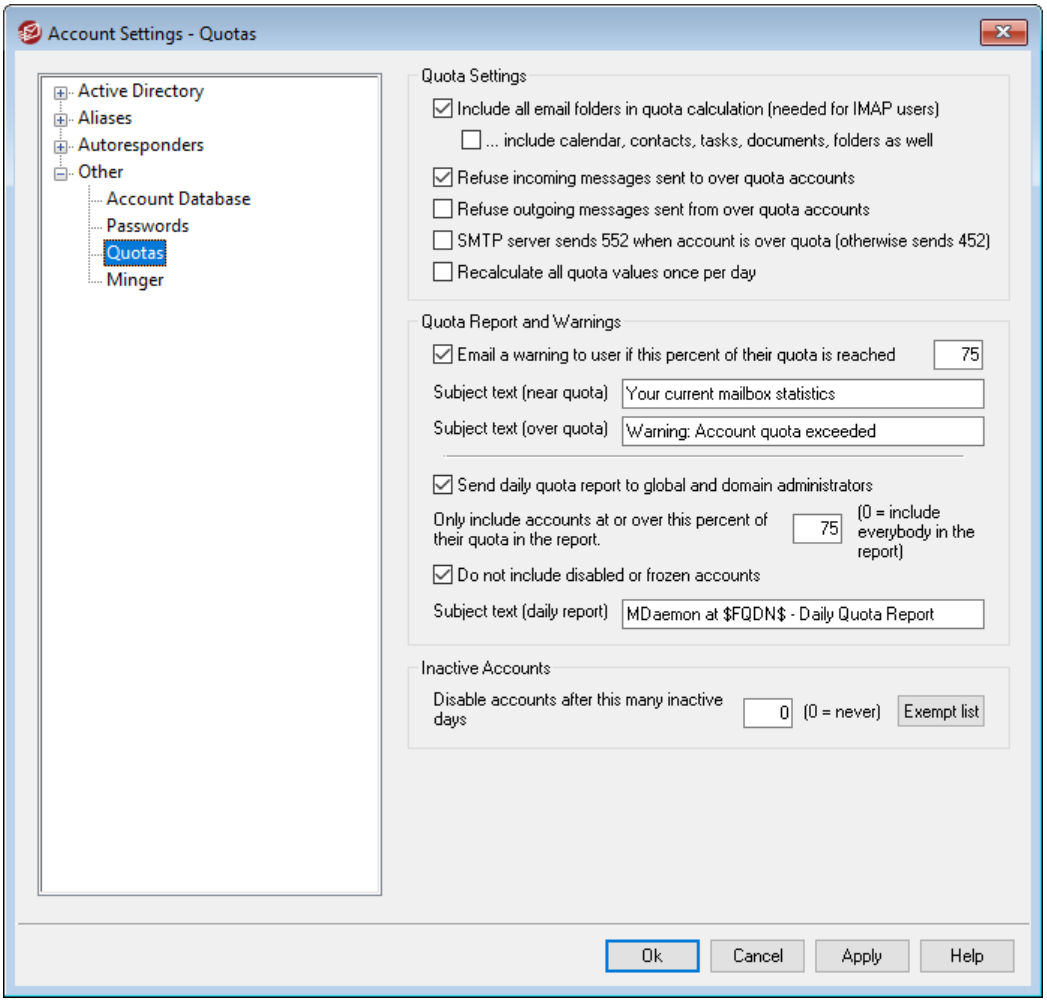
账户编辑器设置[639]页面上有一个账户选项，您可以使用它来要求 *"需要应用程序密码才能登录 SMTP、IMAP、ActiveSync 等。"*。

"需要应用程序密码"有助于保护账户密码免受字典和通过 SMTP、IMAP 等进行的暴力攻击。这样更安全的原因是因为即使这种攻击是猜测账户的实际密码，它也不会不起作用，因为 MDaemon 只会接受正确的应用程序密码。此外，如果 MDaemon 中的账户正在使用活动目录[689]验证，"活动目录"又在达到失败的尝试次数后锁定了账户，该选项有助于防止账户被锁定，因为 MDaemon 只会检查应用程序密码，而不尝试对 "活动目录"进行身份验证。

还请参阅：

账户编辑器 » 账户详细信息[598]
账户编辑器 » Web 服务[603]
账户编辑器 » 应用程序密码[630]
正则表达式[546]

5.3.4.3 配额



配额设置

在配额计算中包含了所有邮箱文件夹（IMAP 用户需要）
选中此框时，用户账户下所有邮件文件夹中的所有文件，将会受该账户上邮箱大小或邮件数量的限制。否则，只有收件箱中的邮件文件才会受到这种限制。通常情况下，只有 IMAP 用户才有此需要。

...同时包含日历、联系人、任务、文档和文件夹
如果您希望在配额计算中包括所有日历、联系人、任务和文档文件夹，请点击此勾选框。

拒收发送至超过配额账户的入站邮件
默认情况下，如果对一个账户设置了邮件配额限制，而且该账户已达到此配额限制，那么 MDaemon 将不再接收发送至此账户的任何入站邮件，直到账户持有人删除了一些他或她已存储的邮件。如果您不希望拒收这些邮件（发送至超出配额的账户），请清除该复选框。

拒收来自超过配额账户的出站邮件
如果出站邮件发自任何已抵达其配额限制的账户，而您希望拒收这些邮件，请勾选此框。超出配额限制的账户将不能再发送邮件，直到该账户持有人删除一些已存储的邮件。默认情况下，禁用该选项。

...在帐户超过配额时 SMTP 发送 552 (其他情况下则发送 452)
默认情况下，在 SMTP 进程中当某一账户超出配额[613]时，MDaemon 会发送 452 错误代码 (例如 "没有采取请求的操作：系统存储不足")。通常情况下，此代码表示该服务器应该稍后重试。如果您希望发送永久性失败 552 错误代码，请勾选此框 ("中止请求的邮件操作：超出存储分配")。

每天重新计算所有配额值一次
默认情况下，仅在启用了下方的 *"发送每日配额报告..."*这个选项并进行了发送时才会重置缓存的配额值。如果您希望将配额值作为日常维护例程的一部分重新计算，请点击此复选框。

配额报告和警告

如果达到这个配额百分比则通过电子邮件向用户发送警告
如果，在日常维护和清理事件[414]期间，MDaemon 确定了一个账户超过了在其 *"一次保存的邮件数量最大值"*或 *"允许的磁盘空间最大值"*配额限制的百分比值，(在账户编辑器[613]中指定)，会向该账户发送一封警告邮件。使用下方的 *"主题文本 (接近配额)"*选项来为邮件设置 "主题"。该邮件将列出此账户当前存储的邮件数量，其邮箱大小以及已经使用的百分比与剩余百分比。此外，如果在账户的邮箱里发现现有警告，会以更新过的邮件代替它。每当在用户的 "收件箱"中放置新的警告邮件时，系统日志中都会创建一个条目，让您知道它已完成。当邮件已经存在并且刚刚更新时，不会创建任何条目日志。如果一遍又一遍地添加日志条目，则表明用户正在从其 "收件箱"中删除邮件。如果您不希望向这些用户发送配额警告邮件，请禁用此项。

临近配额邮件模板 (位于：MDaemon\app\NearQuota.dat)，用来创建接近配额警告邮件。可以在模板中使用与用户账户相关的所有宏 (例如 $EMAIL$、$MAILBOX$、$DOMAIN$ 等)。

主题文本 (接近配额)
这是向超出配额百分比 (在上方指定)的任何用户发送的警告邮件的主题文本。这些邮件在日常维护和清理事件 (默认情况下在午夜发生)中每天发送。

主题文本 (超过配额)
类似 "接近配额"警告邮件，在用户的账户超过配额时，会向其发送另一封邮件。这是 "超过配额"警告邮件的主题文本。

向全局和域管理员发送每日配额报告
如果您希望向所有全局和域管理员发送每日配额报告，请勾选此框并指定值。该报告的内容包括到达或超过其指定配额限制一定百分比的所有账户的配额统计信息。如果您希望此报告包括所有人的配额统计，请使用 "0"值。

不包含禁用或冻结账户
默认情况下，配额报告不包括禁用或冻结的账户。如果您希望包含它们请取消勾选此框。

主题文本（每日报告）
如果您希望定制 MDaemon 发送给管理员的每日配额报告的主题文本，则使用此项。如果您希望亲自定制报告，请参阅 QuotaReport.dat 文件（位于 MDaemon\APP 文件夹中）。

闲置账户

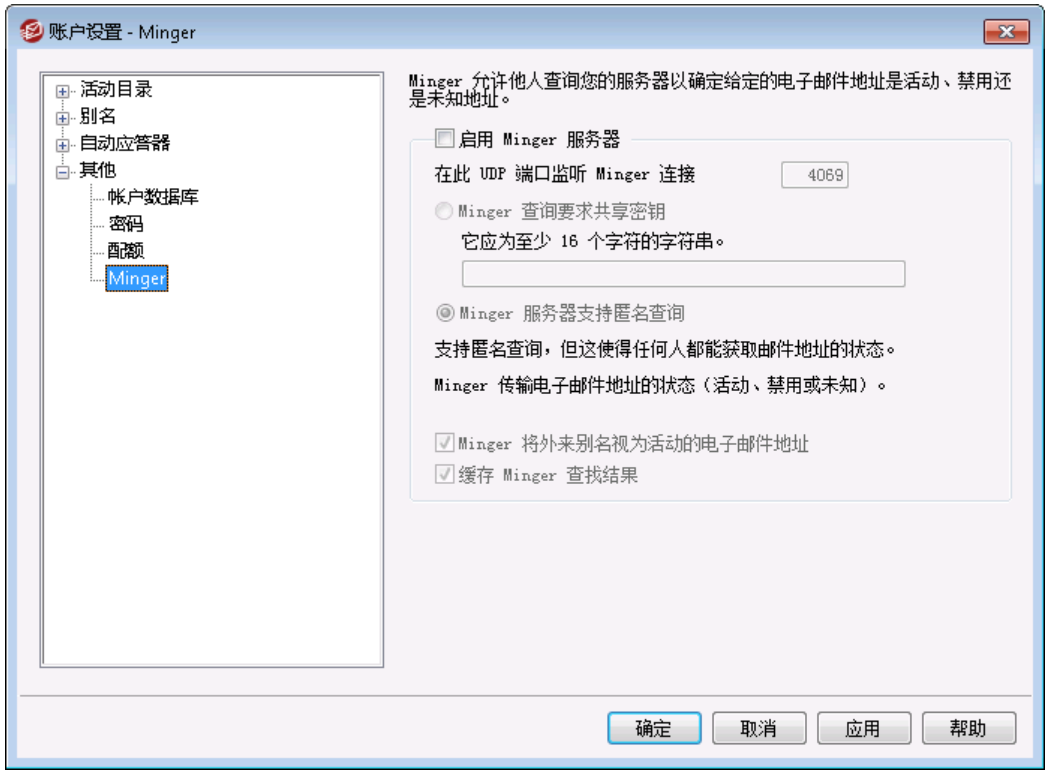
在闲置 XX 天后禁用账户（0=从不）
如果您希望在账户闲置时间超过指定天数时自动禁用该账户，请使用此项。一旦达到闲置天数的最大值，就会禁用该账户，并向邮件管理员发送一封邮件。回复这封邮件将重新启用该账户。该操作的处理将作为每晚夜间清理事件的一部分进行。默认值为 0（禁用）。

豁免列表
被添加到阻止列表的账户免于闲置账户禁用功能。

还请参阅：

账户编辑器 » 配额 613
模板管理器 » 配额 681

5.3.4.4 Minger



M i n g e r 位于 "账户» 账户设置", M i n g e r 是一个由 M D a e m o n T e c h n o l o g i e s 创建的邮件地址验证协议。原始 M i n g e r 松散地基于 F i n g e r 协议，主要用来提供一套简单高效的机制，使其他用户能够查询服务器以验证邮件地址是否有效。鉴于效率 M i n g e r 使用 U D P 而非 T C P，鉴于安全性可以要求验证——尽管也支持匿名查询。M i n g e r 对话框用于启用/禁用 M D a e m o n 的 M i n g e r 服务器、指定要使用的端口 (默认为 4069)和选择是通过共享秘钥系统要求验证还是允许匿名查询。

M D a e m o n 还包含 M i n g e r 客户端，该客户端内置在 "域网关"系统中 (请参阅验证 213)。可以配置由 M D a e m o n 作为网关或备份服务器的每个域使用 M i n g e r，这样 M D a e m o n 将连接到远程服务器并验证该域入站邮件的收件人是否有效。这可以阻止假设所有收件人都是有效的地址。

您可以在以下找到 M i n g e r 协议的最新草案：

http://tools.ietf.org/html/draft-hathcock-minger-06

M i n g e r 服务器

启用 M i n g e r 服务器
点击此选择框启用 M D a e m o n 的 M i n g e r 服务器。

监听此 U D P 端口上的 M i n g e r 连接
M i n g e r 服务器将监听此端口上的连接。Internet Assigned Numbers Authority (因特网号分配机构) (I A N A) 保留并指定 T C P 与 U D P 4069 端口用于 M i n g e r 客户 与服务器。不推荐更改此端口，因为已将它保留为专供 M i n g e r 使用。

Minger查询要求共享密钥
如果您希望通过共享密钥系统要求验证，请选择该选项并输入一个至少长达 16 个字符的文本字符串。选中该选项时，Minger服务器将拒绝未经验证的查询。

Minger服务器支持匿名查询
如果您希望支持匿名 Minger查询请选中该选项——在进行地址验证查询前，无需连接的客户端自我验证。这与现在通过使用 SMTP VRFY 命令或 SMTP "回呼"或"呼叫转移"同样可以实现这点的原始方案类似，但是它更有效并且不会导致许多通过 TCP 的 SMTP 会话停止，因为会话停止会造成 SMTP 日志紊乱，以及其他在那些方法中固有的类似问题。

Minger将外来别名视为活动的电子邮件地址
选中该框时，Minger会将外来别名（别名就是指向外部地址）视为活动的已知地址。此外，当查询是自 SecurityGateway 至 MDaemon 时，将不顾该选项的设置状态，强制执行这一行为。

缓存 Minger查找结果
默认情况下，MDaemon 将缓存 Minger查询结果。如果您不希望缓存它，请禁用此选项。

5.4 导入账户

5.4.1 从文本文件中导入账户

点击"账户» 导入... » 从逗号分隔的文本文件导入账户..."菜单选项来访问账户生成功能。点击"账户管理器"上的"导入"按钮也可访问此功能。这是导入账户和生成邮件账户的简单方法。Mdaemon 将读取文本文件然后生成仅使用用户姓名的新邮件账户。如果您谨慎设置账户模板字符串（请参阅 新账户默认值 667），您就可以仅使用姓名来创建唯一账户，不过您也可覆盖新账户默认值来为特定用户指定大量其他选项。所有字段必须以逗号分隔。

该逗号分隔的文本文件的每一行必须只包含一个条目。第一行必须为基行，包含名称和接下来几行的字段顺序。例子如下：

```
"Mailbox","FullName","MailDir","AllowAccess"
"arvel","Arvel Hathcock","C:\Mail\Arvel\", Y
"michael","Michael Mason","C:\Mail\Michael\", N
```

Mdaemon 使用基行中的字段名称确定数据顺序，因此可以是任意顺序。每一个字段值必须在引号之内。

所有的"字符串"值必须包含在引号内，将"bool"字段值视为 FALSE，除非第一个字符是：y、Y、1、t 或 T。

在每个全名字段中，你可以使用首名，中名及末名。之间可以不用逗号。

导入以后，Mdaemon 将创建 TXIMPORT.LOG，详述导入结果，列出哪些账户导入成功哪些账户导入失败。没有导入成功的普遍原因

> 是和现有账户的邮箱名、全名、目录信息、别名或邮件列表名称相冲突。
>
> 有关字段映射的更多详情，请参阅 MD_ImportUserInfo() 与 MD_ExportAllUsers() 描述，它们在 MD-API.HTML 文件中，位于您的 \API\ 目录。

使用基行中的以下值来映射到 Mdaemon 中的账户字段：

Field Name	Type
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

还请参阅：

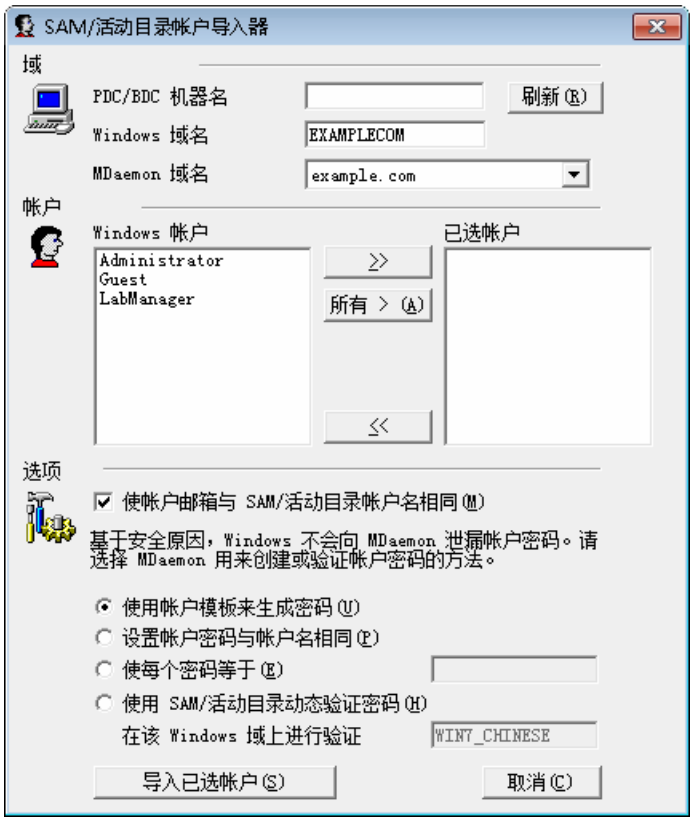
Windows 账户集成 727

5.4.2 Windows 账户集成

MDaemon 支持 Windows 账户集成。这种支持包括“SAM/活动目录”导入引擎，可以从 MDaemon 的“账户”菜单（“账户» 导入... » 从SAM/活动目录导入账户...）获得。此外，用户的活动目录（AD）认证支持被嵌入到 MDaemon 的用户管理代码中。可以在账户的密码字段指定一个 Windows 域，接着 MDaemon 将使用指定的 Windows 域的安全系统对这些账户进行动态的实时验证。在这种方案下，在 Windows 用户管理器中更改账户的密码将自动更新 MDaemon。因此，您的用户只需要记住一个验证凭证设置就可以了。对于初始安装来说，这使账户设置变得非常容易。

运行 MDaemon 的账户的安全相关信息必须具有 **SE_TCB_NAME** 权限（比如，“作为操作系统的一部分运行”）. 如果此进程是在“*本地系统*”账户中运行的服务，默认情况下它将具有这个权限。否则，它必须在 Windows 用户管理器中对运行 MDaemon 的帐户进行设置

SAM/活动目录账户导入器



域

PDC/BDC 机器名
该字段允许您指定 MDaemon 将用来从中读取 Windows 账户数据库信息的机器名。您可以指定 \\<DEFAULT> 并且 MDaemon 将从本地机器读取数据。

刷新
点击该按钮来刷新 Windows 账户列表。

Windows 域名
输入您想要从中导入账户的 Windows 域名。

MDaemon 域名
从下拉列表框中选择将导入账户的 MDaemon 域。

账户

Windows 账户
该窗口包含了一个从 Windows 账户数据库中收集的所有账户名称的列表。

已选账户
该窗口包含了您已选定并希望导入的所有账户名称。

>>
点击此按钮把选中的高亮账户名称从 "Windows 账户"移动到 "已选账户"窗口。

<<
点击此按钮把选中的高亮条目从 "已选账户"窗口中删除。

选项

使账户邮箱和 SAM/活动目录账户同名
单击此切换强制每个导入的用户的邮箱使用他们的 Windows 帐户名。通过这种方法，您不必担心是否正确地设置了新建账户模板[670]宏。

使用账户模板来生成密码
该选项使 MDaemon 使用账户模板设置来为导入的账户生成密码 (请参阅账户默认值[670])。

设置账户密码和账户同名
该选项使 MDaemon 使用账户名作为账户密码。

使每一个密码等于…
该切换允许您为所有导入的账户指定一个静态的密码值。

使用 SAM/活动目录动态验证密码
该参数为导入的账户启用 AD 验证。并非指定一个密码，而是 MDaemon 实时地使用 NT 数据库验证邮件客户端提供的用户名和密码值。

在该 Windows 域上进行验证
输入 MDaemon 对连接进行动态验证时将使用的 Windows 域名。**这不是域控制器的机器名。它是 Windows 域的实际名称。**

当账户被配置为用于 AD 验证，在账户的 密码字段中要使用以两个反斜杠字符打头的 Windows 域名，它没有加密，被储存在 USERLIST.DAT 文件内。例如，如果一个账户在一个叫做 ALTN 的 Windows 域上被配置为进行 AD 验证，则账户的密码字段要包含值 \\ALTN。域名前的两个反斜杠字符对 MDaemon 来说很重要，因为密码字段实际包含了 Windows 域名并且 MDaemon 要使用该域的帐户数据库来尝试验证由邮件客户端提供的用户名和密码值。 因此您一定不能在密码前加上两个反斜杠字符，除非该账户按照综上所述被配置成使用 AD 验证。换言之，您不能在常规密码中以两个反斜杠开头。以两个反斜杠开始的密码，总被认为是使用动态验证的 Windows 域名而非密码。

您可以在账户编辑器中 "账户详细信息[598]"屏幕上的账户密码字段内输入两个反斜杠和 Windows 域名。您不必限制您自己使用导入器以设置账户使用 AD 验证。

还请参阅：

从文本文件中导入账户 725
账户编辑器 » 账户 598

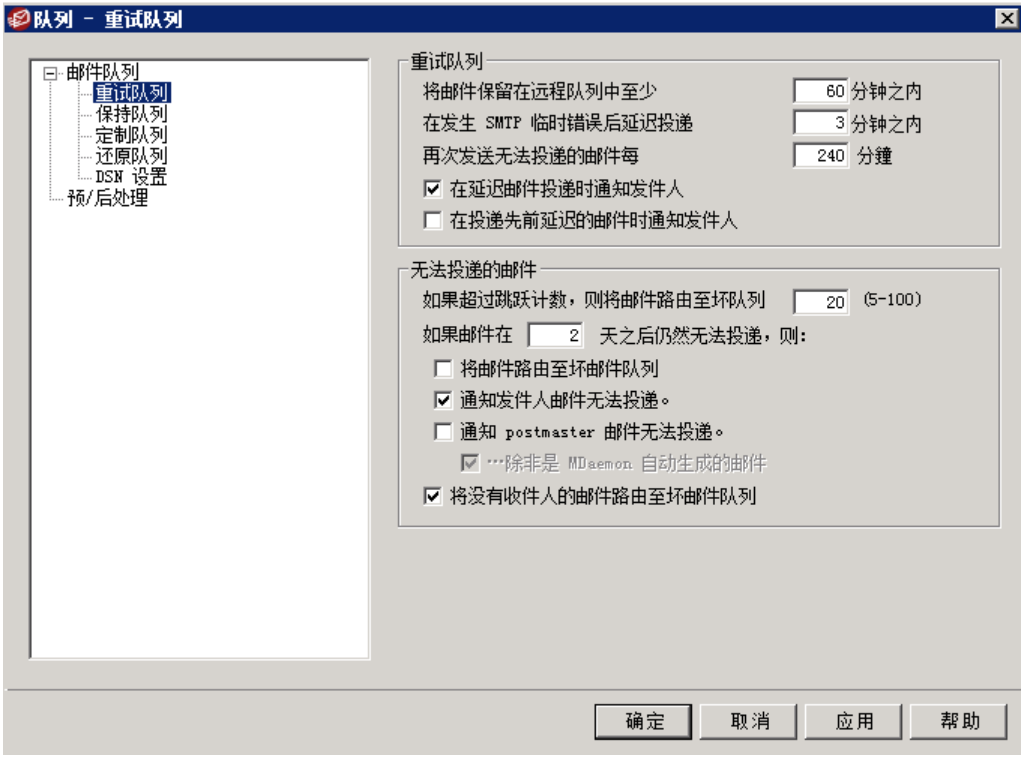
章节

6

6 队列菜单

6.1 邮件队列

6.1.1 重试队列



重试队列对话框，位于 "队列» 邮件队列" 之下，是用于决定 MDaemon 是否将处理那些因为某些非致命错误而无法进行投递的邮件，比如收件服务器暂时不可用。

重试队列

将邮件保留在远程队列中至少 XX 分钟之内
该设置控制邮件被删除或被置于重试队列之前在远程队列中保持的时间长短。远程队列和重试队列相比，通常会更频繁地进行尝试投递邮件。

SMTP 临时错误发生后延迟投递 xx 分钟
当 MDaemon 在尝试投递邮件时遇到 SMTP 临时 (4xx) 错误时，它将按这个分钟数延迟每个后续的投递尝试。这有助于防止 MDaemon 试图一次又一次地投递邮件。默认情况下将此延迟设置成 3 分钟。如果希望禁用延迟，则将该值设置为 "0"。

再次发送无法投递的邮件每 xx 分钟之内
该设置决定了在重试队列中邮件多久会被处理一次。

延迟邮件投递时通知发件人
默认情况下，MDaemon 将通知发件人，由于某些临时错误而无法投递的邮件，导致该邮件被放置在重试队列中。如果您不想通知发件人延迟事件，请取消选中此框。

投递先前延迟的邮件时通知发件人
如果您希望在被延迟发送的邮件在投递时通知发件人，请选中此框。默认情况下，禁用该选项。

无法投递的邮件

如果超过跳跃计数 (5-100)，则将邮件路由到坏队列
RFC 标准规定邮件服务器在处理邮件时，每次都必须盖印每封邮件。这些盖印可以累计，并作为一种权宜之计，来应对有时因错误配置而引起的循环邮件。如果未检测出，这些循环邮件投递会耗尽您的资源。通过计算邮件被处理的次数，可以检测这些邮件并放入坏邮件目录中。假设指定数量的邮件服务器处理了一封邮件后，这封邮件尚未抵达其收件人，那么在这个过程中就可能有一个邮件循环。通常此控件的默认设置能够绰绰有余地阻止邮件循环，无需做任何改动。

如果邮件在 xx 天之后仍然无法投递，则：
该设置确定了一封邮件在被删除前可以保留在重试对列中的天数。如果您在此选项中输入 "0"，那么邮件在第一次重试之后就会被退信。默认设置是 2 天。

将邮件路由到坏邮件队列
启用该选项时，一旦该邮件达到在 *"如果邮件在 xx 天之后仍然无法邮递，则："* 选项。

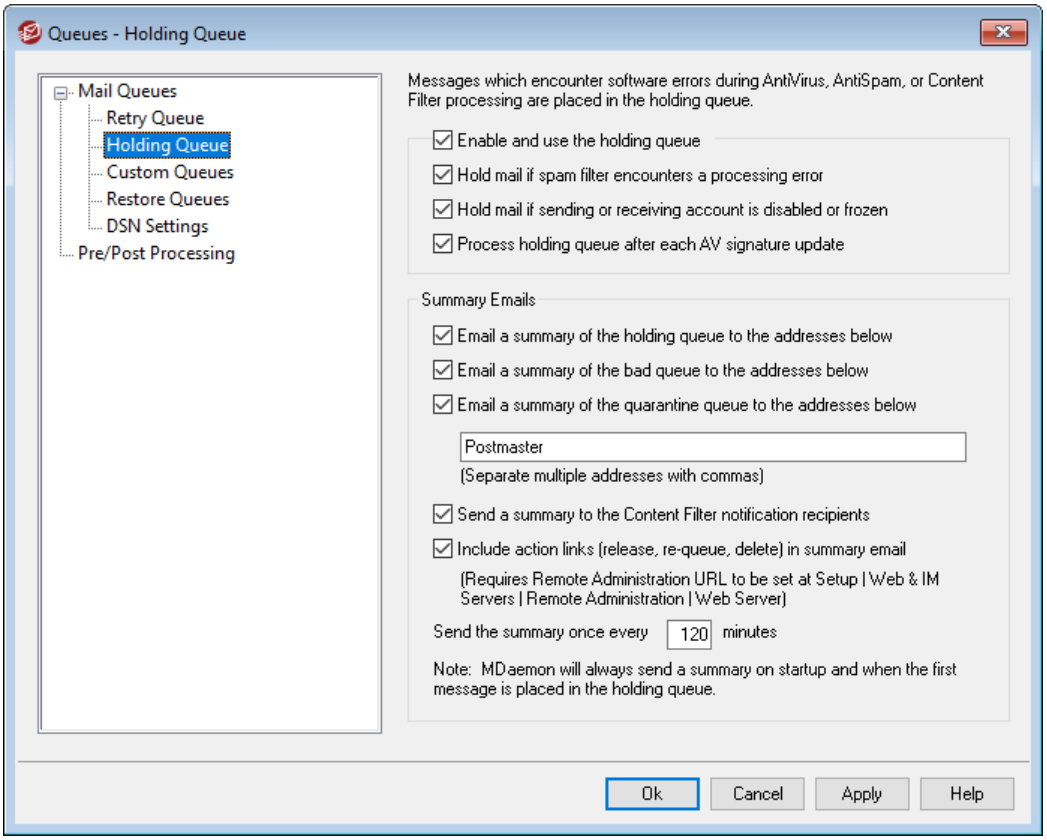
通知发件人邮件无法投递。
一旦邮件达到在 *"如果邮件在 xx 天之后仍然无法邮递，则："* 选项中设置的时间限制时，该切换将使 MDaemon 向发件人发送一封投递状态通知 738 邮件，通知他邮件被永久性从服务器删除。

通知邮件管理员邮件无法投递。
如果启用该选项，当邮件信息从重试系统中永久删除后，会通报 postmaster。

...除非是 MDaemon 自动生成的邮件
默认情况下，重试系统将不会通知 postmaster 无法投递由 MDaemon 自动生成的邮件。如果您希望也通知 postmaster 关于这些邮件投递失败的情况，请清除该选择框。自动生成的邮件是指回执通告，生成自动回复邮件，账户结果处理等。

将不含收件人的邮件路由到坏邮件队列中
启用此选项后，不含收件人数据的邮件将移动到坏邮件队列。禁用后，将删除这些邮件。默认情况下启用此项。

6.1.2 保持队列



位于 "队列» 邮件队列"之下的 "保持队列"可用来接受在反病毒、反垃圾邮件或 "内容过滤器"处理过程中导致软件异常的邮件。如果在处理邮件时软件出错，该邮件将被移入保持队列而不作投递。

放入保持队列中的邮件将留在其中直到管理员采取措施将其转移。在 MDaemon 的工具栏上有 *"处理保持队列"*按钮，在 "队列"菜单栏上也有相同选项。您也能通过在主界面上右键单击保持队列，然后从右键菜单中选择 "重新排队"来处理这些邮件。处理保持队列将把其所有邮件移入远程或本地队列以作正常邮件处理。如果导致邮件被放入保持队列的错误依然存在，则当该错误再次发生时邮件将被重新放回保持队列。如果您想尝试投递保持队列中的邮件而忽略任何可能发生的错误，那么您可以通过在主界面上右键单击保持队列然后从右键菜单中选择 "释放"来实现。当从保持队列中释放邮件时，将会打开一个确认框来提醒您这些邮件可能包含病毒或无法正确通过 "内容过滤器"、反垃圾邮件和/或反病毒引擎的过滤。

保持队列

启用并使用保持队列
点击该复选框可激活保持队列。每当错误发生时，会将在 "反病毒"和 "内容过滤器"处理过程中导致软件异常的邮件移到该队列。

如果垃圾邮件过滤器遇到处理错误则保留邮件
如果希望将在垃圾邮件过滤器处理过程中引发错误的邮件移动到保持队列中，请点击该选项。

如果禁用或冻结了发送或接收账户则保留邮件
启用此项时，在禁用或冻结了发送或接收账户时，MDaemon 将自动保留邮件。

每次 AV 定义更新后处理保持队列
启用该选项时，每次更新 AntiVirus 539 病毒定义后将自动处理保持队列。

摘要邮件

将保持队列的摘要发送到下方地址
如果您想定期发送保持队列中包含的邮件摘要到一个或多个电子邮件地址，请点击该选项并在下方提供的文本区域内列出地址。

将坏队列的摘要发送到下方地址
如果您想定期发送坏队列中包含的邮件摘要到一个或多个电子邮件地址，请点击该选项并在下方提供的文本区域内列出地址。

将隔离队列的摘要发送到下方地址
如果您希望以下方指定的间隔发送隔离队列的摘要，请启用此项。

摘要邮件收件人
使用这个文本框来指定您希望将前两个选项指定的队列内容摘要邮件发送到的邮件地址。当列出多个地址时，用逗号将其分隔开。

在启动 MDaemon 时、邮件首次放入保持队列时以及在下方的 *"每隔 XX 分钟发送摘要"*选项中指定的时间间隔发送通知邮件。

如果通知邮件导致软件出错，那么它可能无法投递到远程收件人。它将仍然被发送到本地收件人。

发送摘要到 "内容过滤器"通知收件人
如果希望将每封通知邮件的副本抄送 "内容过滤器"指定的通知 "收件人 555"，请点击该选项。

在摘要电子邮件中包含操作链接（释放、重新排队、删除）
默认情况下，用于保留、隔离和坏队列的 "摘要邮件"拥有一些链接来释放、重新排队或删除每封邮件。如果您不希望在摘要电子邮件中包含链接，请禁用此选项。

要生成这些链接，必须设置 Remote Administration URL 294。

每隔 XX 分钟发送摘要
使用该选项来指定 MDaemon 发送保持队列通知邮件到每个指定地址或内容过滤器收件人的时间间隔。

6.1.3 定制队列

请在队列» 邮件队列下使用 “定制队列”对话框来创建定制的本地和远程邮件队列。定制队列支持使您能利用 MDaemon 监控从中发送邮件的多个位置。您可创建新队列并将其指定为本地或远程队列，然后可使用 “内容过滤器”规则将邮件自动放入定制邮件队列，对于远程队列，可使用 “事件调度程序 318”创建定制调度以控制这些队列的处理频率。

定制队列

该区域针对每个定制队列显示一个条目，其中列出了文件路径及是否是本地或远程队列。

删除

如果要从列表中删除一个队列，请选择其条目，然后点击 *“删除”*按钮。

当你删除一个自定义队列时，任何和此队列关联的事件计划或内容过滤器都将被删除。

新建队列名称

请在此处输入新建邮件队列的名称。将在 MDaemon 的 \MDaemon\Queues\ 文件夹中创建这个队列

该队列包括...

…远程邮件

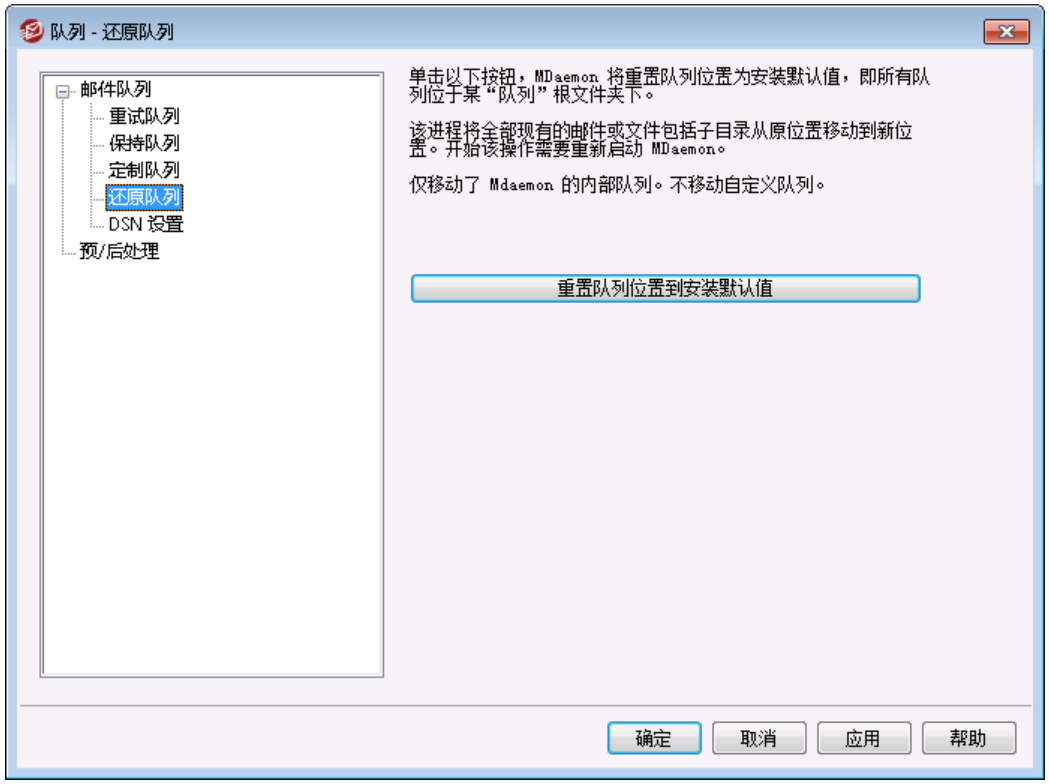
如果希望定制邮件队列用于远程邮件，请选择该选项。

队列凭证
您可以为任何远程队列指定一个*主机或 IP*、*验证登录/密码*、*SMTP MAIL"值*和*端口*。如果提供，则使用这些设置投递队列中的所有邮件。但是在某些情况下，队列中的单封邮件仍可能具有其自身唯一的投递数据，如果是这样，该数据将优先于这些设置。

…本地邮件
如果希望定制邮件队列用于本地邮件，请选择该选项。**请注意：**本地邮件队列不适用于定制的投递调度。

添加
在您为队列选择了名称和类型后，请点击*"添加"*按钮来将其添加到定制队列列表中。

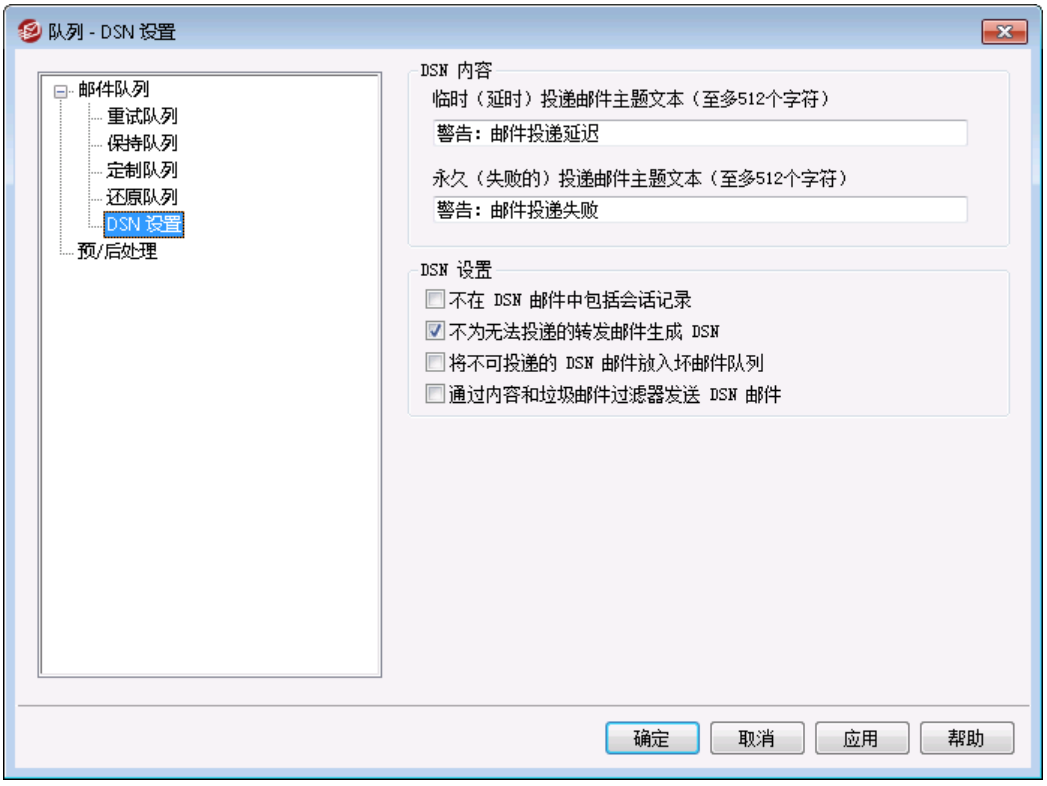
6.1.4 还原队列



重置队列位置到安装默认值
默认情况下，新安装的 MDaemon 把远程、本地、未处理等邮件队列保存在 \MDaemon\Queues\ 子目录下。先前版本的 MDaemon 将队列保存在其它地方。如果您安装的 MDaemon 使用原先的文件夹位置，而您想移动队列到此结构更为合理的目录中，请点击该按钮来转移所有队列及其包含的文件和邮件。点击该按钮之后，必须重启 MDaemon 以使更改生效

定制队列 736 不会被该功能移动。

6.1.5 DSN 设置



当 MDaemon 遇到邮件投递问题时，无论是临时性问题还是永久性投递错误，都会将一封 Delivery Status Notification (投递状态通知 DSN)邮件发送至邮件的发件人。该屏幕含有与这些 DSN 邮件有关的各种选项。其位于：*队列» 邮件队列 DSN... » DSN 设置*。

DSN 内容

临时性 (延迟的)投递邮件主题文本 (至多512字符)
这是作为 DSN 邮件标题的主题，当临时性问题延迟了邮件投递时，将发送该邮件。例如：当 MDaemon 尝试投递一封邮件时，如果收件人的邮件服务器不可用，MDaemon 将使用指定的时间间隔继续尝试投递该邮件，并发送这封 DSN 邮件，通知发件人出现了这个问题。还请参阅：定制 DSN 邮件 739。

永久性 (失败的)投递邮件主题文本 (至多512字符)
这是作为 DSN 邮件标题的主题，当出现一个问题使 MDaemon 无法投递邮件时，将发送该邮件。例如：如果收件服务器拒收邮件，指出收件人的电子邮件地址不存在，MDaemon 将停止尝试投递这封邮件，并发送 DSN 邮件，通知发件人无法投递此邮件。还请参阅：定制 DSN 邮件 739。

DSN 设置

在队列为空时不在 DSN 邮件中包含会话记录
如果您不希望在投递错误和警告邮件中包含 SMTP 会话记录，请点击此选项。默认情况下，禁用该选项。

在队列为空时不为无法投递的转发邮件生成 DSN
启用该选项时，会将遇到永久致命投递错误或从重试对列[732]过期的转发邮件移动到坏邮件队列，并且不会向原始发件人发送 DSN 邮件。默认情况下启用此项。

将无法投递的 DSN 邮件放到坏邮件队列
如果您希望将无法投递的"投递状态通知"邮件放到坏队列，而不是重新尝试发送这些邮件，请点击此选项。

此选项只对 MDaemon 产生的 DSN 邮件有效。

通过内容和垃圾邮件过滤器发送 DSN 邮件
如果您希望通过内容和垃圾邮件过滤器发送 DSN 邮件，请启用此项。默认情况下，禁用该选项。

定制 DSN 邮件

可以通过分别创建名为 DSNDelay.dat 或 DSNFail.dat 的文件（位于 \MDaemon\App\ 文件夹），来定制临时（延迟）和永久（失败）的 DSN 邮件的"人类可读（human-readable）"部分。使用像记事本这样的文件编辑器对其进行编辑并输入您希望使用的文本。可以在您的定制文本中使用以下宏：

$SESSIONID$ - 扩展成投递会话的 ID 字符串

$QUEUEID$ - 扩展成邮件的邮件队列 ID 字符串

$MESSAGEID$ - 扩展成 message-id 报头值

$RETRYDAYS$ - 队列中允许的时间长度（单位是天）

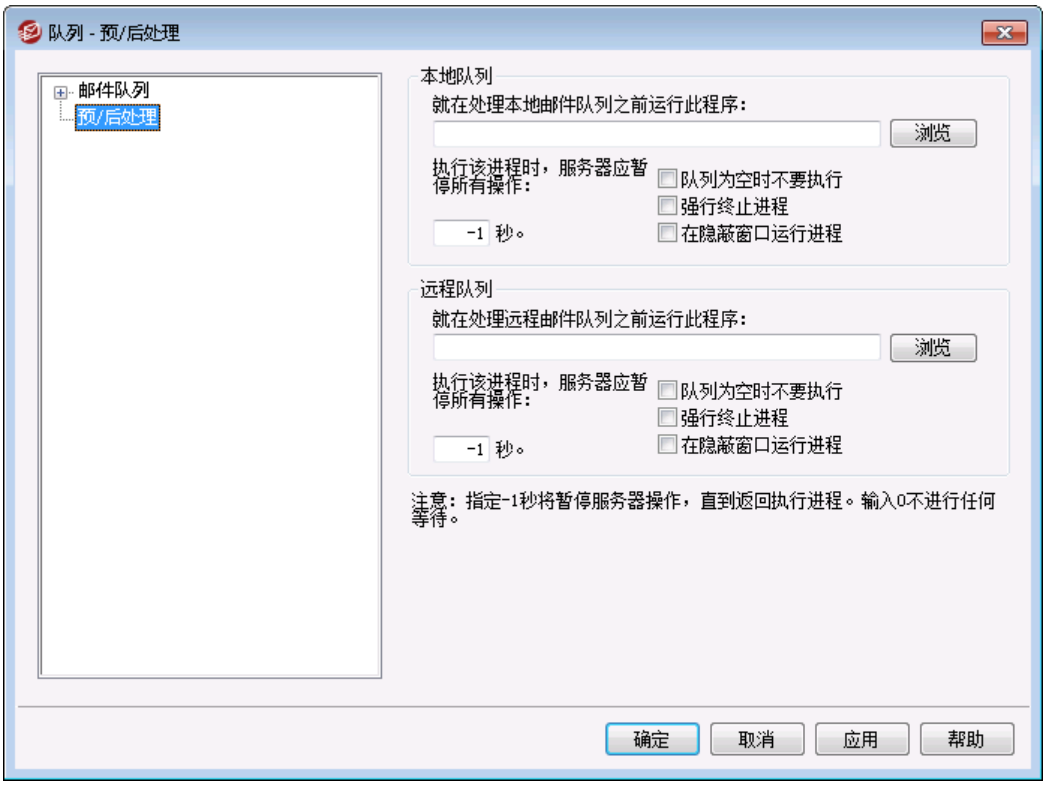
$RETRYHOURS$ - 队列中允许的时间长度（单位是小时）

必须重启 MDaemon 才能加载对这些文件做出的变更。

还请参阅：

重试队列[732]

6.2 预/后处理



本地与远程队列预/后处理

就在处理 (本地/远程)邮件队列处理之前运行此程序
该字段指定了在处理或投递任何可能在本地或者远程邮件队列中的 RFC-2822 邮件过程前，被执行的项目路径和名称。如果没有提供完整的路径信息，MDaemon 将会先在自己的目录里面搜索可执行的，然后到 Windows 系统目录中，再到 Windows 目录中，最后在列于路径环境变量中的目录里去寻找。

...执行该进程时，服务器应暂停所有操作 xx 秒
在此处输入的值决定了当指定项目进行中时，MDaemon 如何运行。 当等待运行线程返回时，MDaemon 可以被设置成在指定的时间暂停它的进程。如果在指定时间过去前，线程返回，MDaemon 将立即恢复它的执行线程。如果您在该选项中输入 "0"，MDaemon 将不会暂停操作。输入数字 "1"，将会使 MDaemon 一直等到处理返回，无论经过多长时间。

在队列为空时不执行
如果在队列为空时，您不希望运行指定的项目，请启用该选项。

强制终止进程
有时，您需要运行的进程自己不会停止。一旦过了在*暂停所有操作 XX 秒*指定的时间时，该选项会使 MDaemon 强行结束会话。如果过去的时间间隔被设置成 "1"，那么此选项不再工作。

在隐蔽窗口运行进程
如果您希望在隐蔽窗口中运行进程，请点击此复选框。

6.3 队列和统计管理器

MDaemon 的 "队列和统计管理器"可从 MDaemon 内的 "队列» 队列和统计管理器"菜单选项访问。"队列和统计管理器"由四页对话框组成。每一页的设计都有其独特的用途，同时保持了简单的格式，因而使用起来非常简便。

队列页面 742

默认选项卡是 *"队列页面"*。从该页面可轻松管理 MDadmon 的所有标准邮件队列以及 "用户账户"邮箱文件夹。只需点击所选队列或用户，即会显示该指定队列内包含的所有邮件文件的列表，以及与每个邮件相关的几条关键信息：发件人、收件人、"Deliver-To"报头的内容、邮件主题、大小及其在当前位置的保存时间。此外，还提供控件，使得在文件夹之间复制或移动邮件，或将其完全删除非常方便。

用户页面 744

"*用户页面*"显示了所有 MDaemon 用户的列表。该列表包含了他们的全名、邮箱名称、邮箱中的邮件数量、账户占用的磁盘空间容量，以及最近一次查看邮件的日期。该列表还可在磁盘上另存为文本文件，或以逗号分隔格式保存以供数据库使用。

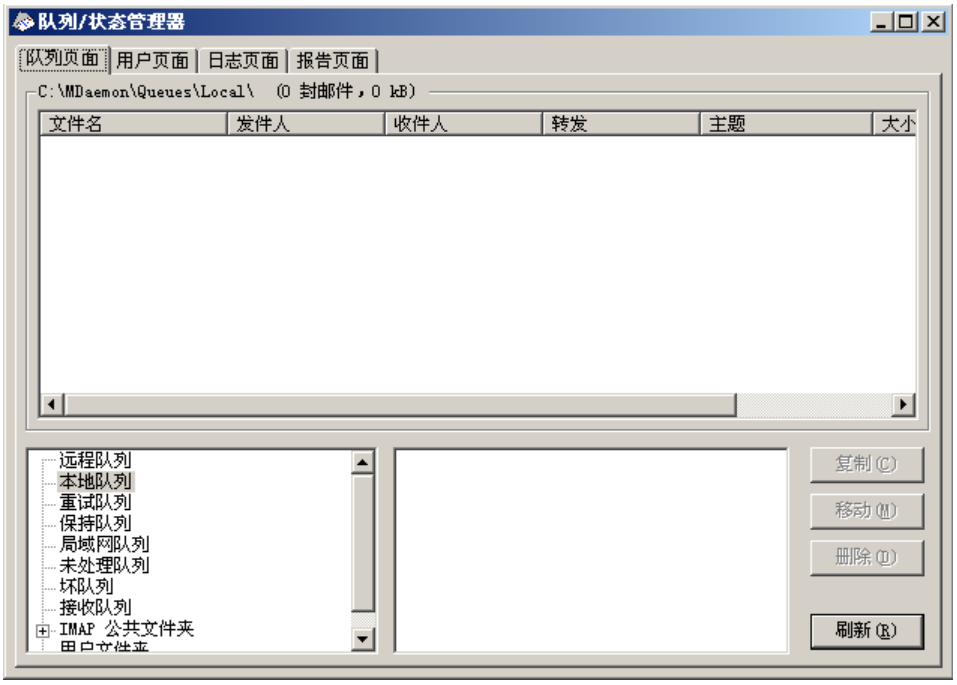
日志页面 746

使用该对话框，可用简单的列表格式显示 MDaemon 的 *"日志文件"*。该功能对于快速检查 MDaemon 的邮件传输历史记录非常有用，因为它将选定的 *"日志文件"*紧缩成纵栏式列表，其中包含：邮件类型 (POP 入站、DomainPOP、RFC822 等)传输过程 中 Mdaemon 所连接的主机，发件人，收件人，邮件大小，每封邮件的处理日期以及传输是否成功。您还可通过双击列表中的所需条目，进一步检查关于该条目的详细日志。这将显示出此传输发生时的那部分日志。*"日志页面"*上显示的日志可另存为文本文件，或以逗号分隔格式保存以供数据库使用。

报告页面 748

最后一个选项卡是 *"报告页面"*。利用该功能，能以纯文本可读格式编写报告，MDaemon 的所有配置设置。因为 MDaemon 里有大量的可选设置和配置，这会大幅度加快配置更改的管理过程，并有助于诊断可能的配置问题。而且，该报告以文本可编辑格式显示，因而能复制/粘贴其所包含的信息 (使用右键快捷菜单)，或在保存前向文件中添加注释或其他信息。

6.3.1 队列页面



队列页面列表框

当从*邮件队列*区域或边上的用户列表框中选择队列或用户时，在该页上的主列表框内将显示选定队列中包含的所有邮件文件列表。该列表包含每个邮件的文件名、发件人、收件人、"Deliver-To"报头的内容、邮件主题、大小以及在当前位置的保存期（显示为日期和时间）。

在该列表框上方给出了当前所显示目录的完整文件路径，以及显示的邮件数量和目录大小。

从该列表中选择一个或多个文件然后点击下方的相应按钮可以复制、移动或删除这些文件。

还可从*"队列页面"*列表框直接编辑这些文件的内容。只需双击想要编辑的文件（或从右键快捷菜单中选择"编辑"按钮），即会打开 Notepad 对该文件进行编辑。

如果希望"队列和统计管理器"默认打开记事本以外的编辑器，则必须编辑位于"MDaemon\app\"文件夹内的"mdstats.ini"文件。将位于"[QueueOptions]"节标下的"Editor="键值更改为"Editor=我的编辑器.exe"。如果 *.exe 文件不在当前路径中，则此处的文件名中必须包括文件路径。

使用垂直或水平滚动条，或点击列表框内的任意位置并使用方向键，可浏览列表框。按照您所选的任意列可对*"队列页面"*列表框中包含的信息进行排序。只要在所需列上点击一次即对该列按升序排序（a-z,1-2），或点击两次按降序排序（z-a,2-1）。通过把鼠标置于列标题之间的分隔线上直到它改变形状，然后拖动列到所需宽度，还可调整列大小。

选择文件

要逐个选择文件 点击所需文件。

要选择连续文件 点击想要选择的连续文件列表中的第一个文件，然后在按下 SHIFT 键的同时点击所需列表中的最后一个连续文件。

另外，可在按住 SHIFT 键的同时，使用方向键、HOME、END、PAGE UP 和 PAGE DOWN 键选择连续文件。

要选择非连续文件 在按住 CTRL 键的同时点击**文件名称**列中的所需文件。

邮件队列

点击左下方窗格中的一个队列，在 *"队列页面"*列表框中将显示该指定队列中包含的所有文件列表。 如果点击 *"用户文件夹"*选项，在 *"邮件队列"*部分右侧的 *"用户列表框"*中将显示所有 MDaemon 用户的列表。

用户列表框

当在 *"邮件队列"*部分 (左下窗格)中点击 *用户文件夹"*选项时，该列表框显示所有 MDaemon 用户的列表。点击用户名可显示在该用户的邮箱文件夹中当前包含的所有邮件文件的列表。

刷新

由于在 MDaemon 处于活动状态时邮件队列是动态变化的 - 从队列中不断收发邮件文件 - 所以因定期点击该按钮来刷新可能显示的任何文件列表。

可编辑 MDstats.ini 文件实现显示列表的自动刷新。为此，只需打开位于 MDaemon 的 \app\ 目录中的 MDstats.ini 文件，并根据两次刷新之间应间隔的秒数编辑 [QueueOptions] 标题下的 AutoRefresh 键值。赋 "0"值表示您不希望列表自动更新。示例：AutoRefresh=15 (列表每隔 15 秒刷新一次)。

复制

点击该按钮可以把选中的一个或多个文件复制到另一个队列或用户的邮箱文件夹中。点击该按钮后，会打开*复制邮件*对话框，从中可以为被选中的需要复制的文件确定目标位置。

移动

点击该按钮可以把选中的一个或多个文件移动到另一个队列或用户的邮箱文件夹中。点击该按钮后，会打开*移动邮件*对话框，从中可以为被选中的需要移动的文件确定目标位置。

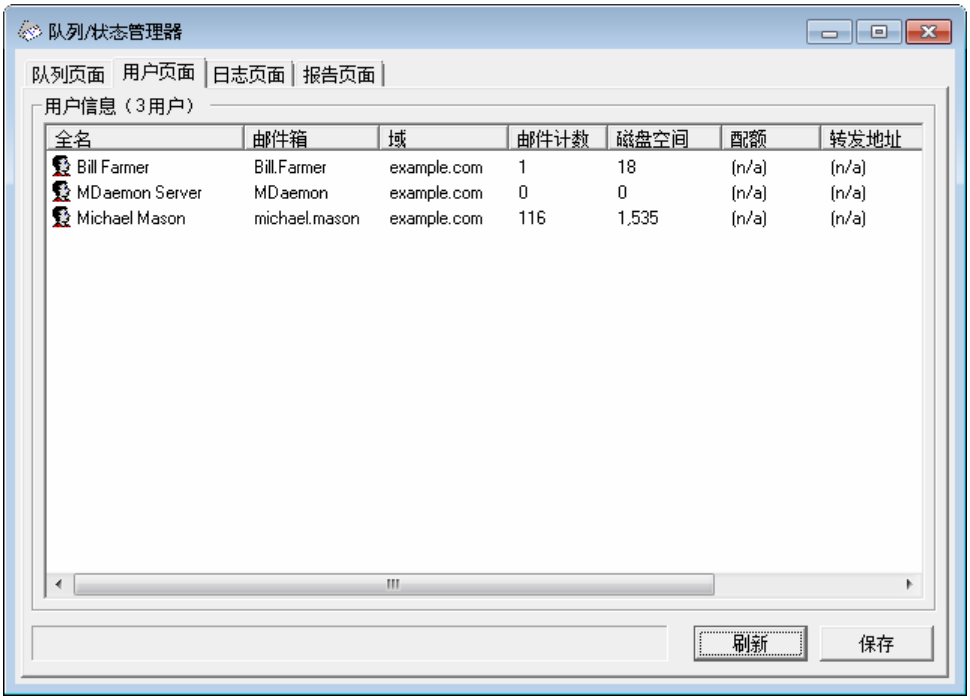
被复制或移动到其他队列的文件很少会保留原文件名。为了避免队列里同名文件被覆盖，MDaemon 始终基于目标文件夹中的 HIWATER.MRK 文件来计算下一目标文件名。

删除
点击该按钮可删除在*队列状态列表框*中选定的一个或多个文件。点击该按钮后会打开确认框，询问您是否确实询问删除选定文件。

在 MDaemon 处于活动状态时邮件队列是动态变化的 - 从队列中不断收发邮件文件。因此，应注意当您复制、移动或删除文件时，有时可能会遇到一则消息，声明您试图执行的操作无法完成。如果您尝试对邮件文件进行操作前，MDaemon 已经移除了该文件，就会收到这样的提示。点击*刷新*按钮，可更新列表框中显示的当前文件列表。

您可通过编辑 MDstats.ini 文件来防止邮件在编辑过程中被移出队列。为此，只需打开 MDaemon 的 \app\ 目录中的 MDstats.ini 文件，并将 [QueueOptions] 标题下的 LockOnEdit=No 键值更改为 LockOnEdit=Yes。这样，每当您编辑邮件时会创建 LCK 文件，从而防止该邮件在您结束编辑之前被移出队列。

6.3.2 用户页面



用户信息
选择*"用户页面"*时，所有 MDaemon 账户的列表将载入*"用户信息"*列表框。该列表包含了每个用户的全名、邮箱名、账户所属域、所含邮件数量、邮件格式、账户占用的磁盘空间容量 (以千字节为单位)、转发地址以及最后一次查看邮件的日期。如果该列表中包含的信息不断变化，可轻松地点击*刷新*按钮进行更新。

使用垂直和水平滚动条，或点击列表框内的任意位置并使用方向键，可浏览列表框。您可按照所选的任意列对 *"用户信息"*列表框中包含的信息进行排序。只要在所需列上点击一次即对该列按升序排序 (A-Z)，或点击两次按降序排序 (Z-A)。还可通过把鼠标置于列标题之间的分隔线上直到它改变形状，然后拖动列到所需宽度，来调整列大小。此外，双击任一条目，MDStats 将切换到 *"队列页面"*并显示相应邮件文件夹的内容。

默认情况下，该列表显示的是邮件数量而不是文件数量，以及邮件占用的 *"磁盘空间"*，而不是该目录中所有文件占用的空间。这即是 MDaemon 所报告的 *"配额"*信息。或者，您也可显示 *文件*计数和所有 *文件*，而不是邮件占用的磁盘空间。要更改该设置，只需打开 MDaemon 的 \app\ 目录中的 MDstats.ini 文件，并将 [UserOptions] 标题下的 ShowQuota=Yes 键值改为 ShowQuota=No。

用户文件夹包含 "hiwater.mrk"文件，用于确定某些用户信息。应避免无谓地删除该文件。否则，队列和统计管理器将无法获取 *"用户信息"*列表框中所列的某些信息。

刷新

诸如邮箱中包含的邮件数量、账户占用的磁盘空间容量这些用户统计信息是不断变化的。点击 *刷新*按钮可轻松更新 *用户信息*列表框中所含信息。这将立即使所有显示信息更新为当前状态。

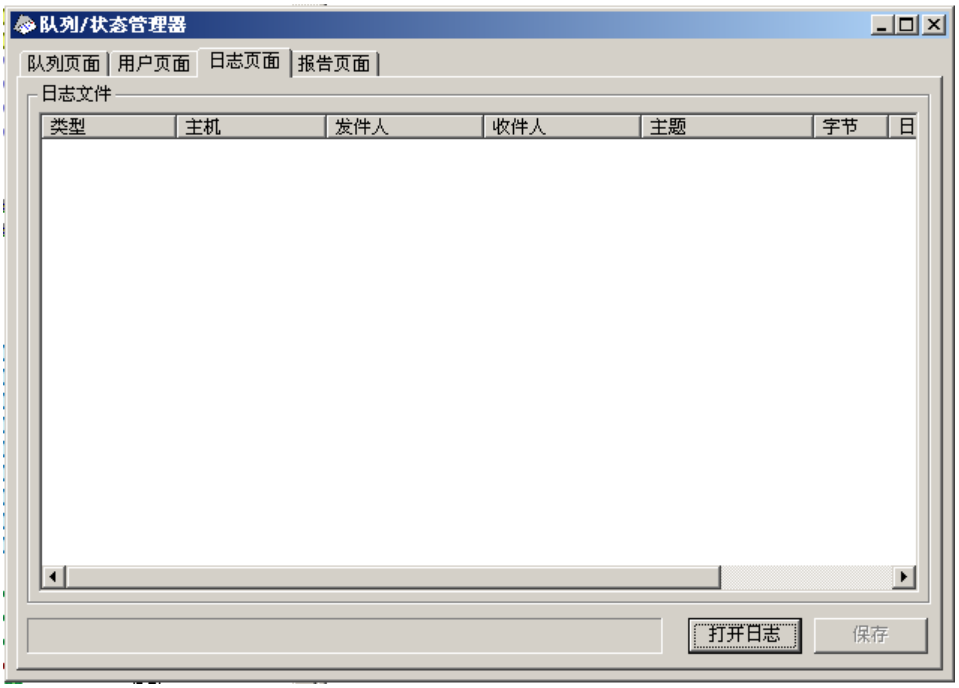
进度指示器

因为 *"用户信息"*列表有时可能非常庞大，*"用户信息"*列表框下面的进度指示条以直观的方式指明在加载或保存大型文件时程序仍在运行。

保存

点击 *保存*按钮，可将 *用户信息*列表框中包含的信息另存为逗号分隔格式以供数据库使用，或另存为纯 ASCII 文本文件。在 Windows 另存为对话框中选择了文件名和保存位置后，会询问您希望将文件另存为逗号分隔格式还是纯文本格式。

6.3.3 日志页面



日志报告

"*日志报告*"列表框中显示您通过 *"打开日志"*按钮和随后的 Windows 打开"对话框选择的 MDaemon 详细日志文件。*"日志报告"*显示提供了一种便捷的方式来检查 MDaemon 已处理的邮件传输历史记录，而无需翻看 MDaemon 日志文件有时可能包含的大量信息。当 *"日志报告"*显示在此列表框中时，"队列和统计管理器"将它分解成简单的格式，其中包含：邮件类型 (POP 入站、DomainPOP、RFC822 等)、传输过程中 Mdaemon 所连接的主机、发件人、收件人、邮件大小、每封邮件的处理日期以及传输是否成功。

您还可通过双击列表中的所需条目，进一步检查关于该条目的详细日志。这将显示出此传输发生时的那部分日志。如有必要，可使用右键快捷菜单将详细日志部分复制/粘贴到文本编辑器供保存或编辑。

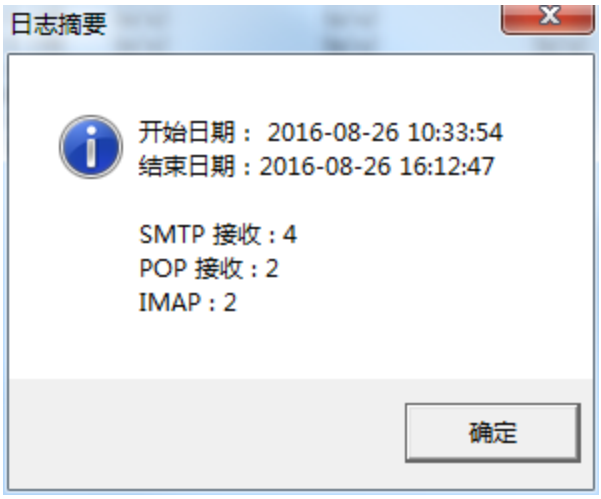
使用垂直和水平滚动条，或点击列表框内的任意位置并使用方向键，可浏览列表框。通过把鼠标置于列标题之间的分隔线上直到它改变形状，然后拖动列到所需宽度，可以调整列表框中的列大小。

"*日志页面*"将显示已使用 *"记录详细邮件会话日志"*或 *"记录摘要邮件会话日志"*选项编译过的日志文件，这两个选项位于日志记录» 日志模式"之下。不过我们强烈推荐您使用 *"记录详细邮件会话日志"*选项。使用 *"记录摘要邮件会话日志"*格式时，您将发现 *"日志报告"*中显示的信息非常少。因为 *"日志页面"*本身会把详细日志精简成 MDaemon 的活动摘要，同时在必要时 (通过双击一个条目)仍能查看每个传输的详细记录，因此无需使 MDaemon 在编译日志文件的同时进行摘要汇总。

打开日志

点击该按钮打开 Windows 打开对话框以选择希望查看的日志文件。如果在*日志报告*列表框中已显示有*日志文件*时点击该按钮，则可选择将新文件追加到已显示文件之后。

日志显示之后，会打开一个消息框，其中包含选定日志的摘要。当把 "日志报告"另存为文本文件时，该日志摘要会附加在后面。



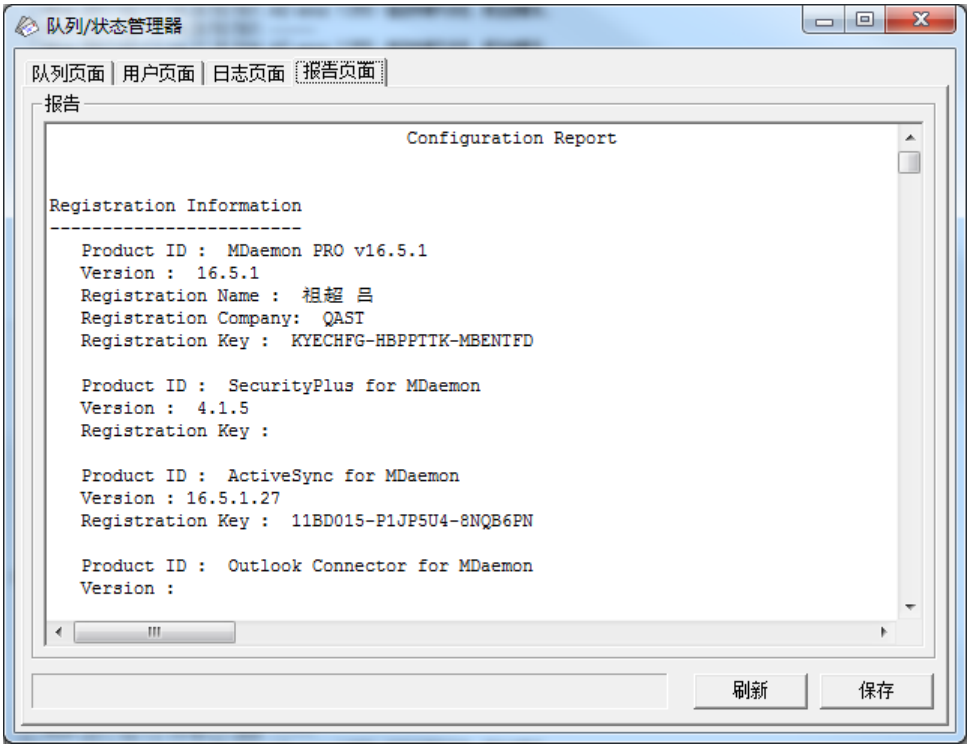
进度指示器

因为 *"日志文件"*可能非常庞大，*"日志报告"*列表框下面的进度指示条以直观的方式指明在加载或保存大型文件时程序仍在运行。

保存

点击*保存*按钮，可将*日志报告*列表框中包含的信息另存为逗号分隔格式以供数据库使用，或另存为纯 ASCII 文本文件。在 Windows 另存为对话框中选择了文件名和保存位置后，会询问您希望将文件另存为逗号分隔格式还是纯文本格式。

6.3.4 报告页面



报告
点击*报告页面*时，会生成一份综合性报告，它以便于阅读的文本格式列出了 MDaemon 内的每项设置。该功能大大缩减了管理员检查 MDaemon 的许多配置设置所需花费的时间，并有助于快速解决可能的配置问题。

您可使用滚动条或方向键浏览该报告，且*"报告"*的显示器也是一个文本编辑器 - 因而在将报告保存为文件之前可插入有关该报告的注释或其他希望包含的信息。此外，可单击鼠标右键利用弹出的快捷菜单对报告进行剪切、复制、粘贴操作。

刷新
点击该按钮可更新当前显示的 MDaemon 设置*报告*。

进度指示器
类似于"队列和统计管理器"中的其他选项卡，*"报告页面"*包含的进度指示条以直观的方式指明在加载或保存大型文件时程序仍在运行。

保存
点击该按钮保存当前显示的*报告*。点击该按钮后，会弹出标准的另存为对话框，在此可指定文件名和想要保存的位置。

6.3.5 定制队列与统计管理器

6.3.5.1 MDstats.ini 文件

定制队列/统计管理器

以下是在 MDstats.ini 文件中可修改的设置列表 (该文件位于MDaemon 的 \app\ 目录中):

[MDaemon]

AppDir=C:\mdaemon\app\	MDaemon 的 \app\ 目录位置。

[QueueOptions]

Editor=NOTEPAD.EXE	双击邮件或右键单击邮件然后选择 "编辑"时使用的编辑器。
LockOnEdit=No	编辑邮件时是否创建 LCK 文件。这将防止邮件在编辑过程中被移出队列。
AutoRefresh=Yes	邮件列表自动刷新之间的时间间隔 (以秒为单位)。0 表示不自动刷新。
ShowDirectories=Yes	除了邮件之外,显示列表框中队列的子目录。目录将显示为 <目录名>。

[UserOptions]

ShowQuota=Yes	确定用户列表是否显示配额信息 (正如 MDaemon 计算所得的邮件数目和磁盘空间)或文件信息 (文件数目和总磁盘空间)。

[LogOptions]

ShowUnknown=Yes	显示 MDStats 无法确定是入站还是出站、SMTP 还是 POP 的会话。
ShowSmtpInbound=Yes	显示 SMTP 入站会话。
ShowPopInbound=Yes	显示 POP 入站会话 (邮件检查)。
ShowSmtpOutbound=Yes	显示 SMTP 出站会话。
ShowPopOutbound=Yes	显示 POP 出站会话 (MultiPOP,DomainPOP)。
ShowRFC822=Yes	显示 RFC822 本地邮件投递。
ShowSmtpHelo=Yes	对于 SMTP 入站会话,在 "主机"列显示 HELO 域。

IgnoreEmptyPop=Yes	未投递邮件时忽略邮件检查。
ShowImap=Yes	显示 IMAP 会话。
[Remap]	驱动器盘符重新映射;针对运行 MDStats 的计算机不同于 MDaemon 所在计算机的情况。
C:=\\server\c	读取 MDaemon.ini时，用 "\server\c"替换 "C:"。
[Special]	
OnlyOneInstance=No	只允许运行一例 MDStats。试图再次打开它将激活已经运行的实例。

还请参阅：

MDStats 命令行参数 750

6.3.5.2 MDStats 命令行参数

请注意：所有的命令行参数都不区分大小写。

数字 1 到 8	在队列页面中显示指定队列。 = 远程队列 = 本地队列 = 重试队列 = 局域网队列 = 未处理队列 = 坏队列 = Smtp 入站队列 = 保存队列
/L[N] [InputFile] [OutputFile]	生成日志文件报告。在 "L"后指定 "N"表示不要保存为逗号分隔文件。
/A	生成日志文件报告时，将新信息附加到输出文件后面而不是覆盖它。

章节

7 MDaemon 附加功能

7.1 MDaemon 与文本文件

MDaemon 使用若干纯文本文件来储存它的一些数据，由系统产生的邮件模板以及配置设置，提供了大量的灵活性。您可以使用 "文件» 新建" 菜单选项，自 MDaemon 内部创建新的文本文件。这有助于为自动恢复和各种其它 MDaemon 功能快速创建数据文档，如 RAW 文档。

编辑 MDaemon 文件

MDaemon 的各种数据文件都是纯文本文件并且可以在记事本中编辑。您可以使用 "文件» 打开» 空文本文件" 菜单选项方便地自 MDaemon 内部打开这些文件。默认情况下，这会查找 MDaemon 的 \app\ 文件夹中的 *.txt 文件。切换 *文件类型：* 从下拉列表选择 "所有文件" 以查看该文件夹中的其余文件。

7.2 通过电子邮件远程控制服务器

可以使用邮件传输系统，通过将专用格式的电子邮件发送至 MDaemon 的系统账户 "MDaemon@<MDaemon's Domain>" 来远程访问 MDaemon 的大量功能。发送到服务器的邮件储存在服务器邮件目录中。

某些控制邮件需要服务器上存在有效账户。对于这些需要有效账户的命令，邮件必须在 SMTP 进程期间使用 AUTH 进行验证。

邮件中可使用的命令有两大类：邮件列表 752 和常规电子邮件 754。

还请参阅：

邮件列表控制 752
常规邮件控制 754

7.2.1 邮件列表和编录控制

这些命令不需要服务器上的账户。[方括号] 中的参数是可选的。例如："姓名 [地址]" 可以仅仅是 "Michael" 或使用可选参数："Michaeluser1@example.com"。应该在邮件正文的各行内包含一个命令和相关联的参数，将这些邮件发送至 "mdaemon@[MDaemon domain]"。

COMMANDS	PARMS	DESCRIPTIONS
订阅	列表名 [地址] [{实名}] [(密码)]	将发件人添加到指定列表的成员名单中，前提为该列表存在并允许远程订阅。若在列表名称后指定了可选地址，则将该地址而不是订阅邮件 FROM: 字段中的地址添加到该列表的成员名单中。要添加订阅者的真实姓名，必需将其用小括号括起来 (例如 {Bill F})。如果该命令后接列表密码 (必需用小括号括起

		来），那么即使关闭了此列表的订阅功能，该命令仍有效。 示例： SUBSCRIBE list@example.com SUBSCRIBE list@example.com me@example.com {Bill F} SUBSCRIBE list@example.com you@example.org (PASS)
UNSUBSCRIBE 或 SIGNOFF	列表名 [地址][(密码)]	从指定列表成员名单中删除发件人，前提为该列表存在且发件人为其当前成员。若在列表名称后指定了可选地址，则从该列表名单中删除这一地址而不是 退订邮件 FROM：字段中的地址。如果该命令后接列表密码 (必需用小括号括起来)，那么即使关闭了此列表的退订功能，该命令仍有效。 示例： UNSUBSCRIBE list@example.com (listPASS) SIGNOFF list@example.com me@example.com
DIGEST	列表名 [地址]	发件人设置为以摘要格式从列表中接收邮件。如果在列表名之后指定了可选地址，则将该地址设为摘要模式。 示例： DIGEST list@example.com DIGEST list@example.com user1@example.com
NORMAL	列表名 [地址]	发件人设置为以普通 (非摘要)格式从 "列表"中接收邮件。如果在列表名之后指定了可选地址，则将该地址而不是发件人设为接收普通格式。 示例： NORMAL list@example.com NORMAL list@example.com user1@altn.com
NOMAIL	列表名 [地址]	该命令设置 "地址"为无邮件 (nomail)模式。该账户将进入挂起状态，并不再接收列表数据流。若未指定地址，则将使用该邮件的发件人地址。 示例： NOMAIL list@example.com me@example.com
MAIL	列表名 [地址]	该命令使 "地址"从无邮件 (nomail)模式返回到普通模式。若未指定地址，则将使用该邮件的发件人地址。 示例： MAIL list@example.com MAIL list@example.com me@example.com

REALNAME	列表名 [地址] {实名}	该命令将 "地址"(它是 "列表名"的成员)的实际姓名设为给定值。真实姓名必须用 { 和 } 字符括起来。 示例： REALNAME list@example.com {Bill Farmer}
LIST	[列表名] [列表密码]	提供有关邮件列表的信息。如果没有提供列表名称，则将返回所有列表的摘要。如果已提供列表密码，那么将返回有关该列表的更高级别信息。 示例： LIST list@example.com Lz$12

还请参阅：

通过电子邮件远程控制服务器 752
常规邮件控制 754

7.2.2 常规邮件控制

这些是可通过电子邮件发送到系统账户的常规邮件命令。应该在邮件正文的各行内包含一个命令和相关联的参数，将这些邮件发送至 "daemon@ [MDaemon domain]"。

COMMANDS	PARMS	DESCRIPTIONS
HELP	none	处理并传回 NEW USERHELP.DAT 文件副本到邮件发件人。
STATUS	none	将有关服务器操作和当前情况的状态报告传回邮件发件人。由于此状态报告中含有的信息被视为私人信息，必须将请求此报告的用户验证为管理员。 例如：STATUS

还请参阅：

通过电子邮件远程控制服务器 752
邮件列表控制 752

7.3 RAW 邮件规范

7.3.1 RAW 邮件规范

MDaemon 内在支持一个简单而强大的邮件格式，即所谓的 RAW 邮件。RAW 邮件系统的目的在于提供一个简单、标准的格式供 MDaemon 之类的软件系统用来创建远为复杂的 RFC-2822 兼容邮件。使用 RAW 之类邮件传输代理允许客户端软件把保持遵守互联网邮件标准这一复杂的工作推卸给服务器。

RAW 邮件由一系列必需的和可选的文本报头后接邮件正文组成。大多数报头包括一个标记，后接用 <> 符号括起来的值。每一报头行以 <CRLF> 字符组合结尾。报头用空行与邮件正文分隔开，而且区分大小写，*"发件人"*和 *"收件人"*是唯一必需的报头。所有的文本、报头和正文都是纯 ASCII 文本，并且必须包括在一个扩展名为 ".raw"的文件中 (例如 "my-message.raw")。然后，为了将邮件放入队列以等候投递，请把 "*.raw"文件放入 MDaemon 的 RAW 队列 (通常位于 "C:\MDaemon\Queues\Raw")。

绕过内容过滤器

默认情况下，RAW 邮件就像普通邮件一样穿过内容过滤器。如果希望给定的 RAW 邮件绕过过滤器，则将文件名以 "p"或 "P"开头。例如 "P_my-message.raw"将绕过内容过滤器，但 "my-message.raw"将照常经由过滤器处理。

绕过内容过滤器将阻止邮件被 DKIM 签名。如果已配置 MDaemon 对所有邮件进行签名，这可能会引发某些邮件投递问题。如果希望 MDaemon 对配置为绕过内容过滤器的 RAW 邮件进行签名，则可使用下述的 x-flag=sign 选项达到这一目的。

RAW 报头

From <mailbox@example.com>	该字段为发件人的电子邮件地址。
To <mailbox@example.com [, mailbox@example.com]>	该字段为收件人的电子邮件地址。可指定多个收件人，互相之间用逗号隔开。
ReplyTo <mailbox@example.com>	可选的电子邮件地址，邮件回复将导向该地址。
CC <maibox@example.com[, mailbox@example.com]>	可选的邮件抄送人列表。可指定多个抄送人，互相之间用逗号隔开。
Subject <text>	邮件的可选主题。
Header <Header: Value>	允许您直接将报头:/值组合放入邮件。这使您得以在 *.raw 邮件中插入定制或非标准报头。

RAW 支持的特殊字段

附件和编码

x-flag=attach <filepath, method> [-x]

例如：x-flag=attach <c:\utils\pkzip.exe, MIME> -x

该 X-FLAG 选项指定了值 "ATTACH"及 <> 符号中的两个参数。第一个参数是邮件附件的完整文件路径。第二个参数与第一个参数用逗号隔开，它指定了插入附件时要使用的编码方式。MDaemon 支持该参数有两种取值。MIME 方式指示服务器使用互联网标准的 Base64 邮件编码方式。ASCII 方式指示服务器简单地把文件导入到邮件中。字符串末尾的可选 -X 参数指示服务器一旦附加了文件后即将其从磁盘上删去。

投递状态通知

x-flag=confirm_delivery

当把包含该标志的 RAW 邮件转换成 RFC-2822 邮件时，该字符串将转化为 "Return-Receipt-To: <sender@example.com>"结构。

将特定的报头/值组合插入 RFC-2822 邮件

header <header: value>

如果希望把特定的报头/值组合插入从 RAW 文件生成的 RFC-2822 邮件，则需要使用上述 RAW 报头部分中所列的 HEADER 宏。例如，如果希望将报头 "Delivered-By: mail-machine@example.com"插入 RFC-2822 邮件，则应在 RAW 邮件中插入："header<Delivered-By: mail-machine@example.com>"。请注意："header"宏需要字段和值。您可按需在 RAW 邮件中插入多个 "header"宏。

DKIM 签名 RAW 邮件

x-flag=sign

*.raw 文件中包含此特殊命令将使 RAW 邮件接受 DKIM 签名。只应在配置为绕过内容过滤器（通过以 "p"或 "P"作为文件名开头来实现）的 RAW 邮件中使用该命令。不应在经由过滤器处理的普通 RAW 邮件中使用该命令。这些邮件将被照常签名。

由内容过滤器生成的所有 RAW 邮件将自动使用 x-flag=sign 命令。

RAW 邮件示例

示例 1：

```
from <mdaemon@altn.com>
to <user01@example.com>

你好，John！
```

示例 2：

```
from <user01@example.com>
to <user09@example.net>
主题 <Requested Files>
X-FLAG=CONFIRM_DELIVERY
X-FLAG=ATTACH <c:\docs\files\data01.zip, MIME> -X
```

这些是您需要的所有文件。

7.4 信号文件

MDaemon 支持“信号文件”，可用于各种目的，包括触发 MDaemon 执行特定操作。MDaemon 会定期扫描 \APP\ 子文件夹以查找是否存在这些文件。如果存在，则会触发关联行为并删除该信号文件。这为管理员和开发人员提供了一种简单的机制，使他们无需使用真正的界面即可操纵 MDaemon。以下为信号文件列表及其功能：

FILENAME	ACTION
ACLFIX.SEM	运行 ACL 文件清理例程。
ADDUSER.SEM	该信号文件创建新账户。它用于强制 MDaemon 将新记录追加到 USERLIST.DAT 文件末尾，而无需完全重建用户数据库（这可能很费时）。该文件中每一行必须是完整的账户记录，并采用在 MDaemon API（参见 MDaemon \docs\API\ 子目录中的 MD-API.html 文件）的账户管理功能部分中指定的格式。可以指定多个新账户——每行一条账户记录。MDaemon 一次处理一行，并添加新账户。您可以创建 ADDUSER.LCK 在更新文件时将其锁定，MDaemon 不会访问 ADDUSER.SEM 直到 ADDUSER.LCK 被删除。要查看 ADDUSER.SEM 文件示例，请用文本编辑器打开 APP 目录中的 ADDUSER.SMP。
ALERT.SEM	向创建该信号文件时登录的所有 Webmail 用户在弹出式窗口中显示该文件的内容。然而，它并非立即显示给所有用户—而是下一次当每个用户的浏览器向 Webmail 服务器发出请求时逐一显示。 **请注意：**不同于其他信号文件，该文件针对 Webmail。它必须放在 \MDaemon\WorldClient\ 目录中，而不是 \app\ 目录中。
ALIAS.SEM	重新加载别名数据文件。
AUTORESPEXCEPT.SEM	重新加载自动应答例外文件。
BATV.SEM	重新加载反向散射保护（BATV）数据文件。
BAYESLEARN.SEM	该信号文件手动启动贝叶斯学习进程。这类似于在垃圾邮件管理器的贝叶斯选项卡上点击“学习”按钮。请注意：

即使禁用了“贝叶斯”学习，这仍将启动“贝叶斯”学习进程。

BLACKLIST.SEM　重新加载黑名单数据文件。

CFILTER.SEM　重新加载内容过滤器规则、清除内容过滤器缓存数据、重新加载垃圾邮件过滤器的允许列表（无过滤）[578]文件。

CLEARQUOTACOUNTS.SEM　用户配额检查结果保留在 quotacounts.dat 文件中。如果您要清除缓存中某用户的配额值，请将该用户的邮件地址添加到此信号文件中，然后将其置于 \app\ 文件夹。如果星号（*）单独一行，则将删除整个文件，使得缓存中的所有配额计数都作废。

DELUSER.SEM　使用该信号文件可删除一个或多个用户账户。创建一个文本文件包含要删除的账户地址（每行一条地址），将该文件命名为 DELUSER.SEM，然后移入 MDaemon 的 \app\ 目录。MDaemon 将删除账户，然后删除 DELUSER.SEM 文件。如果您希望删除账户但不删除其邮件文件夹，请为该地址附加“ ”（例如 frank@example.com^）。

DNS.SEM　重新加载 Windows DNS 服务器[85]和“垃圾邮件过滤器”的 DNS 设置。

DOMAINSHARING.SEM　重新加载域共享数据文件。

EDITUSER.SEM　该信号文件用于更新 USERLIST.DAT 文件内的特定记录，而无需可能很费时的完全重建。要在 USERLIST.DAT 内更新任何特定的用户记录，请创建一个名为 EDITUSER.SEM 的文件，并在其中包含完整的替换记录，每行一个记录，用于您想要编辑的任何用户记录。必须根据 USERLIST.DAT 格式（在用户列表文件格式知识库文章中有所概述）构建每个记录，但必须以原始记录的电子邮件地址开头，后接逗号。MDaemon 每次处理一行 EDITUSER.SEM 文件。可创建 EDITUSER.LCK 在更新文件时将其锁定，MDaemon 不会访问 EDITUSER.SEM 直到 EDITUSER.LCK 被删除。要查看 EDITUSER.SEM 文件示例，请用文本编辑器打开 \APP\ 目录中的 EDITUSER.SMP。

EXITNOW.SEM　关闭 MDaemon

GATEWAYS.SEM	为了获得最佳性能，MDaemon 在内存中保留网关列表。在 MDaemon 的 APP 目录中创建 GATEWAYS.SEM 将重新加载 gateways.dat 文件。
GREYLIST.SEM	重新加载灰名单数据文件。
GROUPS.SEM	重新加载账户分组数据文件。
GRPLIST.SEM	重新加载内部缓存的邮件列表名称
HANGUPG.SEM	强制有条件地挂断 RAS 设备。MDaemon 将等待所有未决邮件会话结束然后挂断 RAS 会话。
HANGUPR.SEM	强制无条件地挂断 RAS 设备。这是立即且无条件的挂断，而不考虑连接中可能正在进行的邮件会话。
HOSTSCREEN.SEM	重新加载主机屏蔽数据文件。
IPSCREEN.SEM	重新加载 IP 屏蔽数据文件。
IPSHIELD.SEM	现在，已将 IPShield.dat 文件缓存在内存中，以便加快访问速度。使用 IPSHIELD.SEM 来将此文件重新加载回内存中。
LDAPCACHE.SEM	重新加载 LDAP 和网关用户数据文件。
LOCKSEMS.SEM	禁止处理所有信号文件，直到删除了该文件。
LOGSETTINGS.SEM	重新加载文件设置。
MDSPAMD.SEM	重新加载垃圾邮件过滤器允许列表和 MDSPAMD，这将强制它重新初始化其所有配置数据。
MINGER.SEM	停止并重启 Minger 724 服务器。
MXCACHE.SEM	重新加载 MX 缓存数据文件。
NODNSBL.SEM	重新加载 DNSBL 允许列表文件。

NOPRIORITY.SEM	强制 MDaemon 重新加载 NoPriority.dat 文件。
ONLINE.SEM	MDaemon 一旦使用 RAS 成功连接到 ISP 后，将创建该信号文件。一旦连接终止，MD 将删除该信号文件。这有助于了解 MD 何时使用 RAS 子系统。
POSTDIAL.SEM	当 MDaemon 建立的连接被取消后，MDaemon 将立即创建该文件。
PREDIAL.SEM	MDaemon 将在试图使用 RAS/DUN 前创建该文件。这使得其他软件能检测何时应释放拨号端口以便 MDaemon 能加利用。
PRIORITY.SEM	重新加载优先级邮件数据文件。
PROCBAD.SEM	启动投递坏队列内容。
PROCDIG.SEM	启动构建并投递邮件列表摘要。
PROCHOLDING.SEM	启动投递保持队列内容。
PROCNOW.SEM	启动检查远程邮件并投递队列中的远程邮件。
PROCREM.SEM	MDaemon 将立即进入邮件处理模式并处理所有远程邮件。
PROCRETR.SEM	启动投递重试队列内容。
PRUNE.SEM	重新加载自动清理设置。
PUBLICSUFFIX.SEM	重新加载 “公共后缀 459”文件。
QUEUE.SEM	信号文件用来启用/禁用邮件队列。该文件可以包含任何行数，不过每行只能含有以下一个字符串 (每行一个)：ENABLE INBOUND、ENABLE REMOTE、ENABLE LOCAL 或 DISABLE INBOUND、DISABLE REMOTE、DISABLE LOCAL。
RESTART.SEM	停止然后启动 MDaemon。
RESTARTCF.SEM	停止并重启 CFEngine.exe (内容过滤器可执行文件)。

RESTARTWC.SEM	停止和重启 MDaemon Webmail。此项仅在 Webmail 使用其自身内置的 web 服务器 270 运行时才有效。
RELOADCACHE.SEM	重新加载缓存中的所有数据设置和文件，内容过滤器设置和文件除外。
REVERSEEXCEPT.SEM	重新加载反向查询例外文件。
SCHEDULE.SEM	重新加载调度数据文件。
SPAMHONEYPOTS.SEM	重新加载垃圾邮件蜜罐数据文件
SPF.SEM	重新加载 SPF、DKIM 和 VBR 数据文件。
SUPPRESS.SEM	重新加载阻止列表设置，并清除缓存的域设置。
TARPIT.SEM	重新加载缓送和动态屏蔽数据文件。
TRANSLAT.SEM	重新加载报头转换数据文件。
TRAY.SEM	重绘任务栏中的 MDaemon 图标。
TRUST.SEM	可信域和 IP 地址驻留在内存中以获得最佳性能。如果需要手动重新加载这些设置，可通过创建 TRUST.SEM 来实现。
UPDATEAV.SEM	启动反病毒定义更新。
UPDATESA.SEM	启动垃圾邮件过滤器更新。
USERLIST.SEM	重新加载 USERLIST.DAT 文件。当修改了 USERLIST.DAT 并需要 MDaemon 重新加载时，可使用该文件。
WATCHDOG.SEM	MDaemon 每隔大约 10 到 20 秒在 APP 目录中查找并删除该信号文件。外部应用程序可利用该文件来检测 MDaemon 是否在运行。如果该文件在 APP 目录中保留时间超过 20 秒，则足以表明 MDaemon 不再运行。

7.5 路由名单

在队列中等候的邮件文件通常在其报头中包含了将该邮件投递到正确位置所需的所有信息。保存在文件中的某些报头（例如 X-MDaemon-Deliver-To）指示 MDaemon 应将该邮件投递到哪个地址和哪个收件人。然而，有时覆盖该信息并为邮件发送的目的地址和收件人提供特定的替代方案十分必要或有用。路由名单正是提供了这样一种机制。路由名单这一文件就邮件发送的目的地址和收件人为 MDaemon 提供了非常明确的指示。如果对于特定邮件文件存在路由名单，那么该路由名单中的设置而不是 .MSG 文件自身包含的设置将控制邮件发送的目的地址和收件人。

路由名单扩展名为 .RTE。例如：如果等待发送的邮件文件称为 "MD0000.MSG"，那么该邮件相应的路由名单文件将称为 MD0000.RTE 且必需与邮件文件处在相同的文件夹（邮件队列）内。

路由名单的格式如下：

```
[RemoteHost]
DeliverTo=example.net
```

该部分路由名单指示 MDaemon 应将相应的 .MSG 文件发往哪台服务器。MDaemon 将始终尝试与该主机建立直接连接，以试图在尽可能短的时间内路由该邮件。只可指定一台主机。

```
[Port]
Port=xxx
```

该参数指定应在哪个端口上建立 TCP/IP 连接并尝试投递。SMTP 邮件默认使用 25 端口。

```
[LocalRcpts]
Rcpt0=address@example.com
Rcpt1=other-address@example.com
Rcpt2=yet-another-address@example.com

[RemoteRcpts]
Rcpt0=address@example.net
Rcpt1=other-address@example.net
Rcpt2=yet-another-address@example.net
```

该部分路由名单允许您指定任意数量的本地和远程收件人，他们应接收相关 .MSG 文件的副本。本地和远程收件人地址必须分隔开来，分别置于相应的 [LocalRcpts] 和 [RemoteRcpts] 部分内。

路由名单提供了良好的机制用于投递或重定向邮件，但它们通常并不是必不可少的。在"路由"邮件列表邮件时，MDaemon 会用到路由名单。如果邮件列表设置为将该列表邮件的单个副本路由到某台远程主机，则将使用路由名单来完成该操作。当您要将邮件群发到多个地址时，这是一种非常有效的邮件投递方式，因为只需要该邮件的单个副本并可指定任意数量的邮件收件人。然而，并非所有远程主机都支持该类路由方式。因为最终必须由这些主机将邮件文件的副本投递到每个地址，因此某些主机对您能指定的收件人数量设置了上限。

章节

8

8 创建和使用 SSL 证书

当使用 SSL 和 TLS 对话框创建证书时，MDaemon 会生成自签名的证书。换句话说，证书的颁发者，或认证机构 (CA)，即为证书的拥有者。这是完全有效和合法的，但是由于该 CA 尚未列入用户的可靠 CA 列表中，因此每当他们连接到 Webmail 或者 Remote Administration 的 HTTPS URL 时，将接受询问是否要进入该站点并/或安装证书。一旦他们同意安装证书并且信任 Webmail 域为合法 CA，则在连接 Webmail 或 Remote Administration 时将不再看到此安全警告消息。

但是，当通过邮件客户端 (例如 Microsoft Outlook)连接 MDaemon 时，他们无法选择是否安装证书。他们可选择是否希望继续使用临时证书，即使它尚未经过验证。每当他们启动邮件客户端并连接服务器时，将不得不选择继续使用未经验证的证书。T为了避免这种情况，您可以从证书颁发机构获取证书，例如 Let's Encrypt 496，或者您可以导出证书，并通过电子邮件或者其他方法分发给用户。然后，他们可以手动安装并且信任您的证书，从而避免今后再此出现警告消息。

创建一个证书

要从 MDaemon 内创建一个证书：

1. 转到 MDaemon 内的 SSL 和 TLS 对话框 (点击**安全 » 安全设置 » SSL 和 TLS » MDaemon**)。
2. 选中标注为 "**启用 SSL, STARTTLS 和 STLS**"的复选框。
3. 点击 "**创建证书**"。
4. 在标注为 "**主机名**"的文本框内，输入证书所属的域 (例如 "*mail.example.com*")。
5. 在标注为 "*机构/公司名称*"的文本框内输入拥有证书的机构或公司名称。
6. 在 "*备选主机名...*"中，输入用户会使用以访问服务器的所有其他域名 (例如 *.example.com", "example.com", "mail.altn.com" 等)。
7. 从下拉列表框中，选择密匙长度。
8. 选择你服务器所在的国家/地区。
9. 点击 "**确定**"。

使用第三方 CA 颁发的证书

如果您从 MDaemon 以外的其他渠道购买或者生成了证书，则通过使用 Microsoft 管理控制台将其导入 MDaemon 所用证书库，您仍可使用该证书。为此，在 Windows XP 中：

1. 在 Windows 工具栏上，点击**开始» 运行...**，然后在文本框中输入 "**mmc /a**"。
2. 点击**确定**。
3. 在 Microsoft 管理控制台中，点击菜单栏上的**文件» 添加/删除管理单元...**，(或在键盘上按下 **Ctrl+M**)。
4. 在独立选项卡上，点击**添加...**
5. 在*添加独立管理单元*对话框上，点击**证书**，然后点击**添加**。

6. 在*证书管理单元*对话框上，选择**计算机账户**，然后点击**下一步**。
7. 在*选择计算机*对话框上，选择**本地计算机**，然后点击**下一步**。
8. 点击**关闭**，然后点击**确定**。
9. 在左窗格中的*证书（本地计算机）*下，如果您导入的证书是自签名的，则点击**可信根证书颁发机构**，然后点击**证书**。如果不是自签名的，则点击**个人**。
10. 在菜单栏上，点击**操作» 所有任务» 导入...**，然后点击**下一步**。
11. 输入要导入证书的文件路径（必要时请使用浏览按钮），然后点击**下一步**。
12. 点击**下一步**，然后点击**完成**。

MDaemon 将只显示具私人密钥且该密钥使用个人信息交换格式（PKCS #12）的证书。如果导入的证书未出现在列表中，则可能需要导入既包含证书密钥又包含私人密钥的 *.PEM 文件。使用与上述相同的处理步骤导入此文件，可将其转换成 PKCS #12 格式。

使用 Let's Encrypt 来管理您的证书

Let's Encrypt 是一个证书颁发机构（CA），通过专门设计的自动化流程来为"传输安全层（TLS）"加密提供免费的证书，该流程使您可以免于现在复杂的手动创建、验证、签名、安装、以及续订证书这些用来保护网站安全的环节。

要支持使用 Let's Encrypt 的自动化流程来管理证书，提供 Let's Encrypt 496 屏幕来帮助您轻松简便地配置和运行 PowerShell 脚本，位于"MDaemon\LetsEncrypt"文件夹。运行该脚本将使一切为 LetsEncrypt 准备就绪，包括将一些必要的文件放置在 WebmailHTTP 的目录中来完成 http-01 挑战。它将 SMTP 主机名 151（属于默认域 149）用作证书域，包含您已指定的任何*备选主机名称*，检索证书，将其导入 Windows，并配置 MDaemon 如何使用针对 MDaemon、Webmail 和 Remote Administration 的证书。此外，该脚本将在名为 LetsEncrypt.log 的"MDaemon\Logs\"目录中创建一个日志文件 LetsEncrypt.log。每次运行脚本时，都会删除并重新创建该日志文件，并且包含脚本的开始日期和时间。此外，如果您指定了*通知的管理员邮件*，将在出错时发送通知邮件。请参阅 Let's Encrypt 496 主题了解更多信息。

还请参阅：

SSL 和 TLS 479

章节

9 术语表

ACL——表示访问控制列表 (Access Control Lists)。ACL 是 Internet 邮件访问协议 (IMAP4)的扩展，它可以使您为您的每一个 IMAP 邮件文件夹创建一个访问列表，这样在您邮件服务器上具有帐户的其他用户，也能在您授权之下访问您的文件夹。此外，您还可以设置权限以管理每位用户对那些文件夹的控制程度。比如，您可以指定用户是否可以删除邮件，将邮件标记为只读或未读，将邮件复制到文件夹，创建新的子文件夹等等。只有支持 ACL 的邮件客户端可以用来共享这个访问与权限设置。但是，如果您的邮件客户端不支持 ACL，您仍可以从 MDaemon 界面设置这些权限。

ACL 在 RFC 2086 中有完整的讨论，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc2086.txt

ASCII——ASCII 的发音是 as-key，是如下短语的首字母缩写词 "American Standard Code for Information Interchange"(美国标准信息交换代码)。这是一个国际标准代码，以七位二进制数表示所有的大写与小写拉丁字母，数字及标点符号，每个字符都被指定一个从 0 到 127 之内的阿拉伯数字。(比如，0000000 到 1111111) 比如，表示大写字母 M 的 ASCII 代码为 77。大部分计算机使用 ASCII 代码表示文本，以便它们将数据传输给其他的计算机。大多数文本编辑器与文字处理器能够以 ASCII 格式贮存文件 (有时叫做 ASCII 文件)。然而，大多数数据文件——尤其是那些包含数字数据的文件，不以 ASCII 格式贮存。

一些较大的字符集由另外 128 个字符表示，因为它们使用 8 位而不是 7 位二进制数。这些额外的字符用来表示符号与非英语字符。DOS 操作系统使用 ASCII 扩展集，叫做扩展型 ASCII 或高级 ASCII。不过，ISO Latin 1 也是一个普遍的标准，被许多操作系统与网络浏览器使用。

ATRN——请参见以下的 ETRN 与 ODMR。

附件——附加在邮件中的文件。大多数邮件系统只支持发送格式为文本文件的邮件，所以当附件是一个二进制文件或格式化文本文件的时候 (比如，文字处理器文档)，在发送前它必须先被编码为文本，一经接收再进行解码。有许多编码方案——其中最为普遍的两个是多用途互联网邮件扩展 Multipurpose Internet Mail Extensions (MIME)与 Unix-to-Unix encode (Uuencode)。对于接收的邮件，可以将 MDaemon 服务器配置为将解码过程留给收件人的邮件客户端或在将邮件投递给本地用户前自动解码附件并将它们贮存在一个指定的位置。

骨干——一条或多条自网络内主要路径的连接。该术语是相对而言的，因为大型网络的非骨干线路可能比较小型网络内的骨干大。

带宽——在固定的时间内通过网络或调制解调器连接传输的数据量，通常以 bps (比特/秒)计算 (bits-per-second)。全页的英文文本大约为 16000 比特，高速的调制解调器可在 1 至 2 秒内传完。全动态全屏影像可能需要大约 10,000,000 bps，取决于其压缩率。

可以将带宽形象地比作高速公路。高速公路表示连接，而来往急驶的车辆表示计算机数据。道路越宽，(带宽越大)就可以让更多的车辆在上面行驶。

波特——波特率测量载波信号在电话线上更改值的频率。它可以作为调制解调器传输数据的速度参考。通常，较慢的调制解调器会以波特率来描述，而较高速的调制解调器会以 bps 来描述。"波特率"与 "bps"并非同义术语，因为每个信号在高速连接中都能进行大于 1 比特的编码。

比特——一个二进制数（Binary digit）。它是计算机数据的最小单位；其中的数字只有两种（比如 0 或 1）。Bit 一般缩写为小写字母 "b"，比如在 "bps"中（bits per second）。全页文本大概为 16,000 比特。

位图——您在计算机中看到的大多数图片，包括因特网中的所有图片，都是位图。位图实际上就是就是由点（或比特）组成的图，只要您不凑近屏幕或将位图放得太大以观看那些点（或比特）组成的形状，它们看上去就是一张图片。常见的位图文件类型有 BMP, JPEG, GIF, PICT, PCX, 与 TIFF。因为位图图象是由无数的点组成的，所以当您放大一张位图时，它看上去就不再平滑，会呈班驳状。矢量图（通常由 CorelDraw，PostScript 或 CAD 格式创建）的放大效果就好很多，因为它们是精确产生的几何图形，不是简单地由似乎很"随意"的点组成的。

Bps——比特/秒（"Bits Per Second"）测量计算机数据从一处移动到另一处的速度。比如，一个 33.6 kbps 的调制解调齐每秒可以传输 33,600 比特。Kilobits (1000 比特) /秒与 megabits (1,000,000 比特)/秒，分别缩写为 "Kbps"与 "Mbps"。

浏览器—— "网络浏览器"（"Web browser"）的缩写，用于显示网页。它解释 HTML 代码，文本，超文本链接，图像，JavaScript 等等。分布范围最广的浏览器是 Internet Explorer 与 Netscape Communicator。

字节——一组比特（通常八位），代表一个字符。一字节有 8 位，有时更多，由度量单位决定。"字节"缩写为大写字母 "B"。

缓存——发音与 "cash"一样。有各种类型的缓存，但是全部都用来贮存最近使用的信息，以便可以在稍后快速访问它们。比如，网络浏览器使用缓存来贮存您近来访问过的网页，图像，URL 与网站上的其他元素。当您返回到"缓存"页面，浏览器就不必再次下载这些元素。因为访问您硬盘上的缓存远比访问因特网来的快，这极大地加快了浏览。

MDaemon 的 IP 缓存贮存您近来投递邮件至一些域的 IP 地址。这使得 MDaemon 在向相同的域投递其他邮件的时候不必再次查找这些地址。这极大地加快了投递过程。

CGI——公共网关接口（Common Gateway Interface）是一套规则，描述 Web 服务器如何与在同一台机器上的其他软件进行交流，这些软件（"CGI 程序"）又如何与 Web 服务器会话。只要按照 CGI 标准处理输入与输出，任何一款软件都能够成为 CGI 程序。但是，CGI 程序通常只是一个小程序，从 Web 服务器上取一些数据作一些处理，比如将表格内容放入邮件，或对此数据作一些其他处理。CGI 程序一般贮存在网站的 "cgi-bin"目录里，因此出现在可以访问它们的 URL 中，但并不总是如此。

cgi-bin——贮存 CGI 程序的 web 服务器上最常见的目录名。"cgi-bin"的 "bin"部分是 "binary"的缩写，因为大多数程序都被习惯性认为是 "二进制"的。事实上，大多数 cgi-bin 程序都是文本文件；由程序执行的脚本位于其他位置。

CIDR—— "无类别域间路由"（Classless Inter-Domain Routing）是一种新的 IP 地址分配方法，替代了基于 A 类 B 类与 C 类地址的旧系统。CIDR IP 地址看上去就像一般的 IP 地址后面跟着斜线号与数字，斜线号与数字称作 IP 前缀。例如：

123.123.0.0/12

IP 前缀定义 CIDR 地址所包含的地址数量，数字越小包含的地址就越多。在上述例子中，"12"为 IP 前缀，可以用来分配 4096 条从前的 C 类地址。

CIDR 地址缩小了路由表，并增加了企业内可用的 IP 地址。

RFCs 1517-1519 中有 CIDR 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

客户端——一个软件程序，用于连接服务器，自或向*服务器*软件程序获取或发送数据。服务器一般位于另一台计算机，可以在您的本地网络也可以在其他的位置。每个*客户端*程序都被指定与一个或多个特定类型的*服务器*程序一起作业，每个服务器也需要一个特定类型的客户端。web *浏览器*是一个特定类型的客户端，与 web *服务器*通信。

公共网关接口——参见以上的 CGI。

Cookie——在计算机术语中，*cookie* 是由 web 服务器发送至您 web 浏览器的数据，会保存它并在以后当您返回至相同的站点或访问站点的其他地方时出于各种目的而使用它。当 web 服务器收到包含 cookie 的 web 浏览器的请求时，它就能使用 cookie 所包含的信息完成其被指定的目的，比如定制发送回用户的信息，或保持一份记录着用户请求的日志。通常，cookie 用于贮存密码，用户名，首选项，购物车信息以及一些与它们对应的站点相关的小事件，这样站点就似乎可以 "记住"您是谁以及您在这里做了什么。

取决于您服务器的设置，您可以接收或不接收 cookies，或花些时间保存它们。通常，将 cookie 设置为在一段预先决定的时间过后就过期，并将其保存在内存里直到 web 浏览器关闭，此时它们会被保存在硬盘里。

Cookies 不能读取您的硬盘驱动器。但是它们可以用来收集关于您的信息，相关您对它们的特定网站的使用，少了它们便无法进行这些操作。

拨号上网——Windows 中的一个部件帮助您通过调制解调器将您的计算机连接到网络。除非您的计算机连接到可以访问因特网的局域网 (LAN)，不然您将需要配置拨号上网 (DUN)以拨号一个接入服务提供点 (POP)并在您可以访问因特网前登陆到您的互联网服务提供商 (ISP)。您的 ISP 可能需要提供某些信息，比如网关地址与您计算机的 IP 地址。

DUN 可以通过我的电脑图标访问。可以配置不同的拨号配置文件，用于每一个您使用的在线服务。一旦完成配置，您可以将配置文件的快捷方式复制到桌面，这样您只需双击连接图标就可以创建连接。

默认——该术语被习惯性认为是计算机程序中的选项当前值。默认设置就是那些用户没有指定特定设置时会被使用的设置。比如，Netscape Communicator 中设置的默认字体是 "Times"。该设置将一直保持为 "Times"，除非您将其改作其他。默认设置通常是大多数人会选择的值。

*默认*术语还被频繁地作为动词使用。如果无法进行自定义操作或程序缺少必需的数据而无法完成任务的时候，通常会 "默认"一项特定的设置或操作。

DHCP——动态主机分配协议（"Dynamic Host Control Protocol")的首字母缩写。网络服务器使用该协议动态地向连网的计算机分配 IP 地址。DHCP 服务器等候计算机与它连接，然后从存储的列表中分配一个 IP 地址给该计算机。

RFC-2131 中有 DHCP 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc2131.txt

域网关——参见以下的网关。

域名——识别因特网网站的唯一名称。例如，“daemon.com”是 MDaemon Technologies 的域名。每个域名包含两个或更多部分，分别用点隔开；最左边的部分最独特而最右边的部分最普遍。每个域名还指向一个服务器的 IP 地址，但是一个服务器所具有的域名可能不止一个。比如，“mail.mdaemon.com”，“smtp.mdaemon.com”以及“example.com”可以全部指向同一个服务器作为“daemon.com”，但是“daemon.com”不能指向两个不同的服务器。但是如果主服务器停止工作，就可以指定客户端将指向的备用服务器，否则网站将不可用。

通常会注册域名而并非连接到实际的机器上。多数情况是因为域名的所有者还没有创建网站，那么注册域名就可以使他们不必维护网站也能够在某个域上具有邮件地址。若要连接到实际的计算机上，就必须有一个真正的因特网机器来处理列出域名的邮件。

最后要注意的是，常常看到“域名”这个术语被缩写或被认为是“域”。“域”有另外的意义而且表示其他事件，比如 Windows NT 域或一类值，所以您应该注意区分两者以免混淆。

RFCs 1034-1035 中有域名地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc1034.txt

http://www.rfc-editor.org/rfc/rfc1035.txt

DomainPOP——由 MDaemon Technologies 将其发展为 MDaemon 服务器的一部分，DomainPOP 自一个 ISP POP 邮箱为整个局域网或工作组提供邮件服务。过去，向工作组提供因特网邮件服务的唯一方法是，公司的邮件服务器必须无间断地与因特网保持“活动”连接状态，每个人必须在公司的 ISP 上拥有他们自己的邮箱，他们可以从那里收集自己的邮件。DomainPOP 只需要一个邮箱就可以全部搞定。ISP 将所有具有公司域名的邮件集中到该信箱，DomainPOP 会定时从中收集邮件。接着，DomainPOP 会分析邮件以决定每个目标收件人并将邮件分发到每个正确的本地用户邮箱。这样从一个拨号 ISP 帐户就能为整个网络提供邮件了。

下载——您的计算机从其他计算机找回或获取数据的过程。比如，从因特网上获取的是信息是通过从其他计算机上*下载*得到的。下载的反向操作是*上传*。如果您希望将信息发送到其他计算机，那么您要将信息*上传*到该计算机。

驱动——与某个硬件设备通信的小程序。计算机与其他控制与识别设备的程序都需要包含信息的驱动。基于 Windows 的计算机经常具有作为动态链接库 (DLL)文件的驱动包。Macs (苹果)系统使用的大多数硬件设备不需要驱动，需要驱动时，会进入系统扩展模式。

DUN——请参见以上的拨号上网。

电子邮件——表示**电子邮件**（“Electronic mail”）。该术语还有以下几种形式：“E-mail”，“e-mail”，以及“email”；意义完全相同。电子邮件是通过通信网络的文本信息的传输。大多数计算机网络具有某种形式的电子邮件系统。一些邮件系统局限于一个计算机网络，另外一些与其他网络间有网关 (使他们能够与多个位置通信)，或与因特网间有网关 (使他们能够在世界任何一处发送邮件)。

大多数电子邮件系统包括某种形式的*电子邮件客户端* (也被称作*邮件客户端*或只是*客户端*)，它包含文本编辑器，其他用于编写邮件的工具，以及一个或多个*服务器*，这些服务器从客户端接收邮件并将邮件路由到其正确的目的地。通常，使用客户端编写邮件，将邮件传到服务器并将其投递至在信中指定的*邮件地址* (或地址)，然后由服务器路由至另外一个服务器，该服务器用于存储发往那个地址的邮件。如果邮件的目的地是原始服务器管辖的本地地址，那么该邮件就会存储在原始服务器上而不会被路由至其他服务器。最后，

邮件收件人将连接他们的服务器并使用他们的邮件客户端取回邮件。将邮件从您的客户端传输到其目标服务器的整个过程只需花几秒或几分钟时间。

除了包含简单的文本，电子邮件信息还可以包括*附件*文件。这些附件可以是您想要的任何类型的文件。图片，文本文件，程序文件以及其他的电子邮件信息等等。但是，因为大多数邮件系统只支持发送文本文件，在发送附件前，它们必须先进行编码（转换成文本格式），然后在它们抵达其最终目的地时再进行解码。该过程通常会由发件与收件的邮件客户端自动实行。

所有的因特网服务提供商（ISP）都提供电子邮件服务。大多数还支持网关，这样您就可以同其他邮件系统的用户进行邮件交流了。虽然许多不同的邮件系统会使用各种各样的协议来处理邮件，事实上一些公共的标准帮助用户可以在所有的系统上进行邮件交流。

邮件地址——识别在网络中特定的电子邮箱的名称或字符串，邮件可以被发送至该邮箱。邮件地址就是一个位置，可以将电子邮件发送至这个位置，也可以从这个位置发送邮件。邮件服务器需要邮件地址，这样它们才能将邮件路由至其正确的目的地。不同类型的网络，其邮件地址的格式也各不相同，但是在因特网上所有的邮件地址都具有以下格式：“mailbox@example.com”。

例如：

Michael.Mason@altn.com

电子邮件客户端——也叫做*邮件客户端*（或只是*客户端*），*电子邮件客户端*是一个软件应用程序，使您能够发送，接收以及编写邮件。之所以被称为客户端是因为邮件系统基于客户端服务器架构；客户端用于编写邮件并将其发送至服务器，服务器再将邮件路由至收件人的服务器，收件人的客户端就会从这个服务器取回邮件。通常，邮件客户端是安装在用户机器上的独立的软件应用程序，但有些产品比如MDaemon会包含一个内置的客户端，作用于用户的 web 浏览器。这样，他们的浏览器就能作为客户端使用，而无需在他们的机器上安装客户端了。这极大地加强了邮件的移动性与便利性。

加密——一项安全措施，*加密*就是将文件中的信息进行编码或者打乱，这样只有经过解码或解密，才能读懂文件。邮件中会频繁地使用加密，这样如果第三方截取了邮件，他们也无法读懂。发送邮件时会对它进行加密，当它抵达其最终目的地时再进行解密。

以太网——局域网（LAN）内使用最普遍的连接类型。最广泛使用的两种以太网形式是 10BaseT 与 100BaseT。10BaseT 以太网可以以快至 10 mbps（兆/每秒）的速度通过数据线或无线连接传输数据。100BaseT 以太网可以以快至 100 mbps 的速度传输数据。吉比特以太网可以以快至 1000 mbps 的速度传输数据，某些苹果计算机会使用它。

ETRN——“Extended TURN”的首字母缩写。它是 SMTP 的扩展功能，可以使 SMTP 服务器发送请求至另外一个 SMTP 服务器，以让其发送队列中等候发送的邮件或为该邮件“消除队列”。因为 SMTP 本身不能对邮件提出请求（通常通过 POP 或 IMAP 协议对邮件提出请求），这就可以使 SMTP 服务器提出 ETRN 请求让远程的服务器启动 SMTP 对话并开始向请求中指定的主机发送被存储的邮件。

用于该目的的 TURN 命令存在安全风险，因为它会使 SMTP 会话反向并立即开始发送被储存的邮件，不会验证请求中的服务器的实际身份。ETRN 会启动一个新的 SMTP 会话，而不是反向操作。因此如果提出请求的是一个“作骗”主机，发件服务器将仍旧尝试将邮件投递至真正的主机。现在已建议引入的标准是 Authenticated TURN（ATRN），同 TURN 一样，使 SMTP 会话的方向相反，但在此操作前会要求验证。这个新标准是 On-Demand 邮件投递（ODMR）。MDaemon 支持 ETRN 和 ODMR 的 ATRN。

RFC 1985 中有 ETRN 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc1985.txt

RFC 2645 中有 ODMR 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc2645.txt

FAQ——连在一起读的发音和 "fack"一样或将字母分开来读作 "F-A-Q"，FAQ 表示常见问题解答（"Frequently Asked Questions"）。FAQs 是一些文档，提供关于一个指定主题的常见问题的解答。它们通常以格式列表的形式表现，每一个列出的问题后都有其解答。较大的常见问题解答中，通常会在文档的开头列出所有的问题以及一些引用（或超级链接，在线常见问题解答），带您进入文档中关于问题与解答的位置。常见问题解答常被用作技术支持与说明书的起始点——如果您能够使用常见问题解答来解决您的问题而不是集中注意力联系技术支持，将节省您大量的时间与精力。

文件传输协议——请参见以下的 FTP。

防火墙——在计算机术语中，当您采取安全措施时，就会有*防火墙*存在，可以通过软件方法，也可以通过硬件方法，将计算机网络分成两个或多个部分，再不然就限制某些用户的访问。比如，您想要让每个人都能看到主机架设在您网络上的网站主页，但只允许您的员工进入"仅员工"区域。不考虑您为达成这一点而使用的方法——要求输入密码，只允许来自某些 IP 地址的连接，或类似的——将员工区域置于防火墙后。

FTP——文件传输协议，"File Transfer Protocol"的缩写。是通过因特网将文件从一台计算机传输到另一台计算机最普遍而有效的方法。专门为该目的设计了一些特定的客户端/服务器应用程序，叫做"FTP 服务器"与"FTP 客户端"——例如 FileZilla 是最常用的客户端之一。通常 FTP 客户端除了简单地传输文件外还可以执行许多其他功能，因此是非常有用的产品。一些 web 浏览器也支持文件传输协议，虽然有时只是为了下载需要。此外，大多数 FTP 服务器是"匿名 FTP"，这就表示任何人都可以登陆进去下载文件——通常指定"匿名"作为用户名，将您的邮件地址作为密码。通常您根本不用登陆就可以从匿名 FTP 站点下载文件——只要单击链接就可以获得文件。对于支持 FTP 的浏览器而言，一般只需要在其 URL 中使用"ftp://…"而不是"http://…"以连接到 FTP 站点即可。

RFC-959 中有 FTP 址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc959.txt

网关——在两个应用程序或网络间使用不同的协议传输数据的计算机硬件或软件。"网关"还是一种可以自一个系统访问另一个系统的方法。比如，您的 ISP 就是您连接到因特网的网关。

MDaemon Messaging Server 通过使用其域网关功能就能作为其他域的邮件网关运行。它运作起来就相当于是一个中间人或网关，收集域的邮件并将邮件保留到域收集它们为止。这有两点好处，不但可以使域不必持续地连接到因特网，还向域提供了一个备份服务器以防它们发生故障。

GIF——图像互换格式（"Graphics Interchange Format"）是一种普遍的的图像文件格式，也是因特网上最常用的图像格式。GIF 使用索引色（Indexed colors）或有若干颜色的色板，极大地缩小了文件——尤其当图像包含大量相同色域时更是如此。规格缩小的文件便于图像在系统间快速传输，这也就是为什么它们在因特网上那么流行的原因。GIF 压缩格式最初是由 CompuServe 开发的，因此您常常可以看见 GIF 也被称为 CompuServe GIF。

图形用户界面——请参见以下的 GUI。

GUI——发音为 "gooey"，图形用户界面，"Graphical User Interface"的首字母缩写。GUI 通过使用定点设备点击屏幕上的图形元素，而不是在命令行里输入文本，让您与您的计算机或应用程序互动。Microsoft Windows 与 Apple Mac 操作系统都是基于 GUI 的，虽然首先引入这个的是 Apple——但实际上图形用户界面这个概念最早是由 Xerox 提出来的。

主机——网络上任何一台计算机，在相同的网络中作为其他计算机的服务器。主机机器可能运行网络服务器，邮件服务器或其他服务器，通常会一次提供几种服务。主机（Host）还常被用作动词形式托管（"to host"）。比如，运行邮件服务器的机器将"托管"邮件。

在点对点网络，计算机在同一时间既作为主机又作为客户端是很普遍的。比如，您的计算机可以托管您网络的打印机，但同时也被您用作从其他主机收集邮件与下载文件的客户端。

HTML——超文本标记语言，"Hypertext Markup Language"的首字母缩写。它是一种代码语言，用于创建在万维网上使用的超文本文件。简单来说，HTML 文件是一个包含格式化代码与标签的纯文本文件，用户的 web 浏览器会解释它并显示为包含格式化文本与颜色的网页。比如，当浏览器接收到一个包含"<B>Text</B>"文本的 HTML 文件时，会以粗体显示文字"Text"。因为纯文本文件非常小，这就使得它们能够迅速地在因特网进行传输。

HTTP——超文本传输协议（Hypertext Transfer Protocol）是一项用于通过因特网在计算机间传输*超文本*文件的协议。HTTP 要求在一个终端有一个客户端程序（通常是 web 浏览器）而在另一个终端有一个 HTTP 服务器。

RFC-2616 中有 HTTP 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc2616.txt

超文本——任何文本，只要包含一条超链接通往在同一文档内的其他文件或位置，就叫做超文本。有时该文本也被叫做超文本链接或只是链接。超文本可以是一个内嵌链接的单词或短语，这样当您单击它的时候就会将您带往"指定"的位置或显示被链接的文件。通常超文本链接非常明显，因为文本会以下滑线或不同颜色表示，但这个并不作要求。有时超文本看上去与一般文本无异，但是当您的鼠标指针移至上面的时候，您的指针会产生某种图形变化为您作出指示。

超文本标记语言——请参见以上的 HTML。

IMAP——由斯坦福大学开发，因特网邮件获取协议（Internet Message Access Protocol）是一项用于管理与取回邮件信息的协议。最新的版本是 IMAP4，与 POP3 类似但它有若干附加功能。IMAP4 作为一项协议用来管理服务器上的而不是用户本地计算机上的邮件，是非常有名的——可以用关键字搜索邮件，可以将邮件组织到文件夹中，可以选择指定的邮件进行下载，还有其他一些功能，邮件被用于上述各种操作时，它们仍旧在服务器上。因此 IMAP 对用户的机器配置要求不高，并会将邮件集中起来，这样就能从多种位置访问它了。

RFC-2060 中有 IMAP 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc2060.txt

IMAP4 ACL 扩展——请参见以上的 ACL。

因特网——因特网于 1969 年由美国军事学院创建，最初只是一个在核战中不能被摧毁的通信网络。现在因特网由成百万的计算机组成并遍布全世界。根据设计，因特网是分散的——它无法被任何一个公司，企业或国家所控制。每台因特网上的主机（或计算机）是独立于其他计算机的，并且能够提供其操作者希望的任何可行的信息或服务。不过，大多数在某些点通过因特网传输的数据都要经过“骨干”，它其实就是由最大的因特网服务提供商或企业控制的高带宽高速度的连接。大多数人访问因特网是通过在线服务比如 AOL，或通过因特网服务提供商（ISP），他们维护或连接到某一骨干。

许多人认为*万维网*（WWW）与因特网是相同的，但事实上并非如此。WWW 只是因特网的一部分而并非因特网本身。它是最可见与最普遍的部分，很大程度上由商业驱动，但仍然仅是一部分。

Intranet——简单来说，intranet 是一个小型的或私人的因特网，在公司或企业的网络内部严格地进行使用。即使企业间的 intranet 各不相同，它们可以包含因特网上任何可用的功能。它们可以具有它们自己的邮件系统，文件目录，要浏览的网页，要阅读的文章等等。intranet 与因特网的主要不同之处在于 intranet 相对来说比较小，并且局限于一个企业或小组。

IP——因特网协议“Internet Protocol”的首字母缩写（比如在 TCP/IP 中的 IP）。因特网协议使得数据能够通过因特网在系统间传输。不考虑每台计算机的平台与操作系统，如果每台计算机使用相同的因特网协议，它们就能够互相传输数据。术语“IP”还常常被用作另一个术语“IP 地址（IP Address）”的缩写。目前标准的因特网协议是 IP 版本 4（IPv4）。

RFC-791 中有因特网协议地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc791.txt

IP 地址——偶尔也会被叫做 IP 号码，IP 地址表示因特网协议地址（Internet Protocol Address）用于识别特定的 TCP/IP 网络以及该网络上的主机或计算机。它是一个 32 位数字地址包含 4 个 0 至 255 之间的数字，分别由点隔开。（比如“127.0.0.1”）。在一个单独的网络中，每台计算机必须有一个唯一的 IP 地址，可以随意指定。但是，每台因特网上的计算机必须有一个注册过的 IP 地址，以免重复。每个因特网 IP 地址可以是静态的也可以是动态的。静态地址不会变化并且只表示因特网上的相同位置或计算机。动态 IP 地址会变化并且通常由 ISP 将它指向只是临时连在因特网上的计算机——比如在用户通过拨号帐户访问因特网的时候。但是，拨号帐户仍旧可以有一个指向因特网的静态 IP 地址。

ISP 与大型企业通常会尝试从 InterNIC 注册服务（InterNIC Registration Service）那获取一系列或一套 IP 地址，因此所有在它们网络的或使用它们服务的客户端可能会具有类似的地址。这一系列的 IP 地址会被分成以下几类：A 类 B 类与 C 类。A 类与 B 类 IP 地址用于规模庞大的企业并分别支持 16,000,000 与 65,000 台主机。C 类 IP 地址用于小型网络并支持 255 台主机。因为缺少可用的地址，很难获取 A 类与 B 类 IP 地址；因此大多数公司不得不退而求其次使用 C 类 IP 地址。因为缺少这种 IP 地址，现在有一种新的 IP 地址协议叫做无类别域间路由（CIDR）逐渐地替代了比较旧的系统。

RFC-791 中有目前的因特网协议标准 IPv4 的地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc791.txt

RFC-2460 中有 IP 版本 6（IPv6）的地址，位于：

http://www.rfc-editor.org/rfc/rfc2460.txt

RFCs 1517-1519 中有 CIDR 的地址，位于：

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 号码——请参见以上的 *IP 地址*。

ISP——因特网服务提供商 (Internet Service Provider)是向终端用户提供因特网访问与服务的公司。大多数 ISP 向它们的客户提供多种因特网服务，比如：WWW 访问，邮件，新闻组或新闻服务器访问等等。通常，用户通过拨号或其他连接形式连接到他们的 ISP，接着 ISP 会将他们连接到一台路由器，该路由器将轮流将他们路由到因特网骨干。

Java——由 Sun Microsystems 开发，Java 是一个具网络导向的使用句法的计算机编程语言，与 C/C++ 语言非常相似，但是它是围绕类而不是特性构建的。在因特网应用中，它常被用于编程 applet，applet 是内嵌在网页中的小程序。用户的浏览器可以自动地下载与执行这些程序，以提供大量仅靠 HTML 与其他脚本语言可能无法产生的功能，而且不必担心病毒入侵或对您计算机造成损害。因为 Java 语言既有效又简单易用，在许多软件与硬件开发者间越来越流行。

JavaScript——不要与 Java 混淆，JavaScript 由 Netscape 开发，作为脚本语言专为扩展 HTML 的性能与创建互动性网页而设计。它是一个高度精简使用方便的编程语言，使用起来远比 Java 或其他语言方便，但也有一定的局限性。且不论它的局限性，它非常有助于向网站添加一系列互动性元素。比如，当您希望在把数据提交到服务器之前预处理数据，或在您希望您的页面通过链接或形状要素与用户产生响应互动时，JavaScript 是很有用的。它还可以根据用户的选择，用于控制插件与 Java 程序 (applet)，并能实现大量的其他功能。JavaScript 包含在 HTML 文件的文本内，由 Web 浏览器对它进行解释以执行各种功能。

JPEG——一种图像格式，能够非常有效地压缩高质量色彩与照片图像——压缩比率远比 GIF 格式大。对于包含规则形状与大块区域为重复色彩的图像来说 GIF 是最好的选择，而 JEPG 更适合不规则图案与大量色彩的图像。JEPG 是因特网上那些高质量色彩与照片图像最常用的格式。JPEG 是 "Joint Photographic Experts Group"（联合摄影专家组）的首字母缩写——该小组开发了这种格式。

Kbps——常用于表示调制解调器的速度 (比如 56 Kbps)，它是 "Kilobits Per Second"（千比特/秒）的首字母缩写。它表示每秒会移动或处理 1000 比特量的数据。注意它是千*比特*而不是千*字节*———一个千字节的数据量是一个千比特的 8 倍。

千字节——一个千字节 (K 或 KB)是一个一千字节的计算机数据。通常它等于 1024 个字节 (2^10 = 1024)但为了简单方便通常就用作 1000。

LAN——局域网 (Local Area Network)是一个局限于一幢楼或一块区域的计算机网络，通常所有的节点 (计算机或工作站)会使用某些数据线或电缆或其他形式媒介的配置连接在一起。大多数大型公司都有局域网，这极大地简化了员工与办公室间的信息管理与共享。大多数局域网使用某些形式的邮件或聊天系统，并共享设备比如打印机以免必须为每个岗位配置一台独立的设备。当网络的节点通过电话线，无线电波或卫星通信线路连接在一起时，它不再是局域网 (LAN)而被称作广域网 (Wide Area Network)。

延时——数据包通过网络连接所用的时间。当发送一个数据包时，发送的计算机在等待数据包已被接收的确认期间有一个 "延时"。除了带宽以外，延时也是您网络连接速度的一个决定要素。

LDAP——轻量级目录访问协议（Lightweight Directory Access Protocol）是一个在线目录服务协议，简称为目录访问协议（Directory Access Protocol）。目录系统是一个分等级的结构，由以下几个级别组成：一个 LADP 目录中有"根"目录或开始目录，国家，企业，企业单位以及个人。每个 LDAP 条目是具有唯一标识符的属性集合，该标识符叫做区别名（Distinguished Name）。因为它是一个开放的协议，所以非常有效并且能够跨多个服务器进行分布，LDAP 最终可以使任何平台上的任何应用程序都能够访问目录信息以定位全球的邮件地址，企业，以及文件等等。

RFC-2251 中有 LDAP 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc2251.txt

链接——请参见以上的*超级链接*。

列表服务器——一个服务器应用程序，用于只要在邮件中写下一个地址，就能将邮件发送给多个收件人。简单来说，当邮件是发往由列表服务器维护的*邮件列表*时，邮件就会被自动地分发给列表中的成员。邮件列表通常有一个常规的邮件地址（比如，listname@example.com），但是该地址却表示列有收件人的整张列表而不是一个指定人或特定的邮箱。当某一个人*订阅*邮件列表时，列表服务器会自动地将其邮件地址加入列表，并将以后指向该列表的邮件分发到那个地址或成员以及所有列表中的其他成员。如果有人希望取消订阅，列表服务器就会删除其地址那么他不会再收到列表邮件。

通常术语 listserv 更常用，表示所有的邮件列表服务器。但是，Listserv® 是 L-Soft international, Inc. 的注册商标，且是 BITNET 的 Eric Thomas 于 1986 开发的一种特定程序。除了其他的列表服务器之外，MDaemon 还配备了一整套列表服务器，或邮件列表，功能及特性。

登陆——一个唯一的代码或一系列字符用于获得准许进入服务器或计算机，或用于向服务器或计算机证明自己的身份。多数情况下，登陆时必须有一个密码以获得准许。

"登陆（logon）"有许多同义的术语，比如*login（登陆）*，*username（用户名）*，*user name（用户名）*，*user ID（用户 ID）*，*sign-in（登陆）*等等。通常，"登陆（logon）"还被用作动词。比如，"我将*登陆（logon）*到邮件服务器"。但是在那句话中，比较常用的（也许更加适合）还是"我将*登陆（log on）*到邮件服务器"。

邮箱——内存或存储设备上的一个区域，它被指定到一个用来存储邮件信息的特定邮件地址。任何的邮件系统里，每个用户都有一个私人邮箱，当用户的邮件服务器收到邮件后会将它们存储在那个邮箱中。术语"邮箱"常用来表示邮件地址的最左边部分。例如"user01@example.com"中的"user01"是邮箱，而"example.com"是域名。

邮件列表——也叫做邮件组，邮件列表是一列或一组邮件地址，由一个邮件地址表示。比如，"listname@example.com"。通常当列表服务器收到一封邮件是发往其某一邮件列表时，该邮件就会被自动地分发给列表中所有的成员。（比如，列表中包括的那些地址）。MDaemon 配备了一套丰富的邮件列表功能，可以使列表是公共的或者私人的（任何人都可以发件或加入，或只有成员可以发件或加入），适度的（每封邮件在发往列表前必须经过某人允许），以摘要格式或作为个人邮件发送，并有大量的其他用法。

Megabyte——虽然从技术上来说是 1,048,576 字节（或 1024 千字节），但 Megabyte 更通用，它用于表示一个百万字节。Megabyte 缩写为："MB"，比如在"20 MB"中。

MIME——由因特网工程任务组（Internet Engineering Task Force）于 1992 年定义，多功能因特网邮件扩展（Multipurpose Internet Mail Extensions）是标准的将非文本文件附加到标准因特网邮件信息的编码方法。因为通常只有纯文本文件才能通过邮件进行传输，非文本文件必须先被编码为纯文本文件格式并在它们抵达其目的地后再进行解码。因

此如果邮件程序可以使用 MIME 标准收发文件，它就被称为 MIME Compliant。发送一个 MIME 编码的邮件附件时，通常被发送的文件类型与用来将附件转换为其原始形式的方法都被指定为邮件的一部分。有许多预定义的 MIME 内容类型，比如 "Image/jpeg"与 "text/plain"。不过，它也可以定义您自己的 MIME 类型。

web 服务器也会使用 MIME 标准以识别它们发送至 web 浏览器的文件。因为 web 浏览器支持各种 MIME 类型，这使得浏览器可以显示或输出非 HTML 格式的文件。此外，通过更新浏览器的 MIME 类型列表与用于处理每一种类型的软件，可以很轻松地支持新的文件格式。

RFCs 2045-2049 中有 MIME 地址，可以在以下地址中查看到：

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

镜像——一台服务器 (通常是 FTP 服务器)，它有另一台服务器上相同文件的副本。其目的在于当原服务器发生故障或过载的时候，可以提供一个备用位置下载镜像文件。术语 "镜像"还表示将信息同时写入多个硬盘的配置。它被作为一种沉余方法使用，这样如果一个硬盘坏了，计算机也能不丢失任何重要数据继续运行。

调制解调器——调节器解调器（modulator-demodulator)的首字母缩写。调制解调器是连接到计算机的设备，可以使数据通过电话线传输到其他计算机。调制解调器将计算机的数字数据转换为模拟信号 (调制)接着将数据传输到另一个调制解调器，那里的处理过程是相反的 (解调)。简单来说，调制解调器就是一个模拟信号到数字信号再由数字信号到模拟信号的转换器。数据传输的速度可以用波特率来表示 (比如 9600 波特)或千比特/秒 (比如 28.8 kbps)。

MultiPOP——MDaemon 的组件，可以将其配置为通过 POP3 协议，同时从各种代表 MDaemon 用户的邮件服务器收集邮件。这就使得在其他邮件服务器上也有邮件帐户的 MDaemon 帐户持有者可以将他们 MDaemon 帐户的邮件同所有邮件一起收集与共享。如此也能在一个邮箱内贮存他们所有的邮件。

NAT——请参见以下的网络地址转换 (Network Address Translation)。

网络——以某种方式将两台或多台计算机连接在一起。网络的目的就是实现多系统间的资源与信息共享。一些常见的例子如下：多台计算机共享打印机，DVD-ROM 驱动，硬盘，个人文件等等。

有多种类型的网络，但是最广泛定义的类型是局域网 (LAN)与广域网 (WAN)。在局域网中，每台计算机 (或节点)在地理位置上都靠得很近——通常在同一幢大楼里。它们通常通过电缆直接连在一起，尽管无线连接正在普及。广域网中的节点通常分散得更开，(在另一幢楼或城市中)，它们通过电话线，卫星连接或其他连接形式连在一起。

因特网本身就是一个网络。常将它描述为由许多网络组成的网络。

网络地址转换——网络地址转换 (NAT)是由一个网络使用两组因特网协议地址 (IP 地址)的系统——一个 IP 地址用于外部通讯，另一个用于内部通讯。这主要被用来作为防火墙有助于确保网络安全。您的计算机对您局域网外部的计算机而言看起来是有个确定

的 IP 地址，但您实际的 IP 地址是完全不同的。您的网络与因特网 "之间"放置着硬 ◆◆◆ 或软件，执行两个地址的转换。局域网中的多台计算机常用这种方法来 "共享"一个公司 IP 地址。这样您网络外部的人只要没有在转换期间先通过验证，就无法知道您实际的 IP 地址也无法直接连接到您的计算机。

网卡——网卡 (NIC)是一块计算机电路板，以让计算机连接到网络。NIC 提供全天候的网络连接，而调制解调器 (由大多数家庭计算机使用以通过电话线拨号上网)通常只提供临时的连接。大多数 NIC 被专门设计成用于特定类型的网络与协议，比如以太网或令牌环网与 TCP/IP。

网络新闻传输协议——请参见以下的 NNTP。

NIC——请参见以上的网卡 (Network Interface Card)。

NNTP——**网络新闻传输协议**（Network News Transfer Protocol)是一项用于在 USENET 新闻组上传输与分发邮件的协议。现在最普遍与最流行的浏览器与邮件客户端都有内置的 NNTP 客户端。

RFC-977 中有 NNTP 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc977.txt

节点——连接到网络上的任何一台计算机。

ODMR—**按需邮件转发**（On-Demand Mail Relay)是一项新的协议，它被设计为可以将邮件服务器间歇性地连接到服务提供商，而且没有静态 IP 地址就可以接收邮件，类似于那些有静态 IP 地址且使用 ETRN 命令的邮件服务器。如果系统有静态 IP 地址，就可以使用 ESMTP ETRN 命令。但是，动态 IP 地址的系统没有广泛配置的解决方案。ODMR 解决了这一问题。此外，ODMR 引进了经验证的 TURN 命令 (ATRN)使得 SMTP 的会话流反向 (就像比较旧的 TURN 命令)，但要求请求中的服务器进行验证从而加强了安全性。这就使得具有动态 IP 地址的 SMTP 服务器可以连接到它的 ISP，并通过 SMTP 将一个或多个主机的邮件投递到服务器，而不是通过 POP 或 IMAP 来收集邮件。这对那些需要他们自己的邮件服务器又无法担负起静态 IP 地址或专门从事在线业务的公司来说，是满足他们广泛的低成本需求的完美解决方案。

RFC 2645 中有 ODMR 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc2645.txt

OEM——**原厂设备制造商**（Original Equipment Manufacturer)是一个非常容易混淆与引起误解的术语。OEM 是一个公司，它在自己的产品中使用其他公司的设备或产品，该产品是以不同的品牌或公司名称进行包装与出售的。比如，HyperMegaGlobalCom, Inc. 就是一个 OEM，因为它从一个或多个不同的公司购买计算机部件，将它们全部放入一个定制的产品，再印上 "HyperMegaGlobalCom"品牌将该产品卖出去。如果将部件卖给 HyperMegaGlobalCom 的公司也从其他公司得到他们所需的部件，亦可将它们称为 OEM。 "OEM"是一个不走运的不恰当用词，因为 OEM 实际上不是原制造商；它们只是 "包装商"或 "定制商"。尽管如此，许多人仍旧使用术语 "OEM"来表示实际的硬件制造商而非那些重新包装产品的公司——这是可以理解的。

On the fly——术语 "On the fly"有两种不同用法。首先，在执行一些任务 "期间"，它常被用来表示一些做起来 "迅速"或简单的事情。比如，簿记产品在输入销售数字中途能支持 "On the fly"地创建账户—— "只要停止输入数字，单击 X 按钮，输入一个名字即可，然后再继续输入更多的数字。" "On the fly"的第二种用法表示可以动态地或自动产生的事物而不用进行手动操作或是静态地产生。比如，当用户返回网站，通过使用贮存

在 "cookie"中的信息，定制的网页就能够 "on the fly"地产生。并非要求某人去手动创建一张根据用户口味定制的网页，它只是根据那人在浏览时的操作动态地产生。

原厂设备制造商——请参见以上的 OEM。

数据包——通过网络传输计算机数据的单位。无论何时，您从您局域网上的其他计算机或通过因特网收到的数据，它都是以 "数据包"的形式进入您的计算机的。原始文件或信息先被分成这些数据包，通过传输，最后在目的地进行重组。每个数据包都包含一个包括其来源与目的地的报头，一大块数据内容以及错误检查代码。它还可以进行 "计算"，这样就能把它同相关被发送的数据包连接起来了。发送与接收数据包的过程被称作 "数据包-交换"。数据包通常还被称为 "datagrams (数据报)"。

数据包交换——通过网络或因特网发送与接收数据包的过程。与电路交换相反，(比如在模拟信号电话中)，数据包交换是通过一条单一路径或电路以连续数据流的方式传输数据，而且这些数据会被分成 "包"，这样就没有必要从相同的路线到达它们的目的地。此外，因为数据是分别独立的单位，多个用户可以同时在同一条路径上发送不同的文件。

参数——参数是一种特性或值。在计算机中，它是被用户或一个程序传递到另一个程序的任何值。您的名字和密码，首选项设置，字体大小等都是参数。在编程中，参数是用于处理被传递到一个子程序或函数的值。

PDF——便携文档格式（Portable Document Format (PDF))是一种高压缩多平台文件，由 Adobe Systems Incorporated 开发，它可以从各种应用程序中捕获文档格式，文本以及图像。这使得文档可以在多个计算机和平台上无差别显示并进行准确地打印 (不像许多文字编辑器无法做到这一点)。查看 PDF 文件需要安装 Adobe Acrobat Reade 程序，它是由 Adobe Systems 免费发行的应用程序。还有使用您的 web 浏览器查看 PDF 文件的插件。这就可以直接查看网站上的 PDF 文件，而不用先下载它们再使用独立的程序进行查看。

解析——在语言学中，解析就是把语言分成可以进行分析的语法成分。比如，将一句句子分成动词，形容词，名词等等。

在计算机中，解析是将计算机语言内容分成可以对计算机有用的部分。编译器中的解析程序会将每个开发者编写的程序内容分成几部分，这些部分可以用于发展进一步行为或创建指令，以形成一个可执行程序。

MDaemon 和其他产品通常会分析邮件信息，以决定它们的目的地或通过过滤器与其他工具处理它们。

Ping——因特网包探索器，Packet Internet Groper 的首字母缩写。它是基本的因特网程序，用于确定一个特定的 IP 地址是否可以获得以及接收请求。它通过发送因特网控制消息协议 (ICMP)回声请求并等待回应做到这一点。 "Ping"常被用作动词表示这一过程。比如，"我要 ping 这台服务器以查看它是否在线。" "Pinging"一个 IP 地址通常只要在 DOS 提示符里输入 "ping"，接着输入 IP 地址或域即可。例如 "Ping 192.0.2.0."。

RFC-792 里有 ICMP 地址，RFC-862 里有回声协议 (Echo protocol)。这些都可以在以下查看：

http://www.rfc-editor.org/rfc/rfc792.txt

http://www.rfc-editor.org/rfc/rfc862.txt

POP——表示邮局协议 (Post Office Protocol)。POP (通常会以 POP3 形式出现)是最常用的邮件协议，用于从邮件服务器上接收邮件。大多数邮件客户端使用 POP 协议，虽然

有一些还支持新的 IMAP 协议。POP2 在 20 世纪 80 年代中期成为标准并需要 SMTP 来发送邮件。新版本 POP 3 取代了 POP 2，有没有 SMTP 都可以使用它。可将 POP 用作动词表示从服务器收集您的邮件。比如，“我要POP我的邮箱以获得我的邮件。”

RFC-1939 中有 POP3 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc1939.txt

端口——在 TCP/IP 与 UDP 网络与因特网中，端口是本地连接的终端，由 0 至 65536 之间的数字识别。保留端口 0 至 1024 用于某些特许的协议与服务。比如，典型的 web 浏览器的端口是 80，SMTP 服务器的通信端口是 25，POP 服务器发送与接收邮件的端口是 25。通常，一次只有一个程序可以使用或“无视”每台计算机上的任何指定端口。浏览因特网时，某些服务器常常会在非默认的端口上运行，这就需要您在 URL 的冒号后指定端口。比如，“www.example.com:3000”。

端口还被用于表示计算机上使用的套接字 (socket)以连接外部设备与硬件。比如，串行端口，平行端口，USB 端口等等。

最后，端口 (port)还常用于描述一个编程过程以让指定平台或计算机在另一个平台上运行的。比如，“port 一个 Windows 应用程序到 UNIX”或“为一个应用程序创建一个 UNIX 端口。”

Post——在因特网通讯中，就像邮件或新闻组那样，它是种输入网络通信系统以让其他人看见的单一信息。比如，新闻组，邮件发送列表或讨论板上显示的一条信息，都是一个 Post。它还可被用作动词，比如“将邮件投递 (Post)到邮件列表或新闻组。”

PPP——表示“点对点协议”(“Point to Point Protocol”)。这是拨号连接的因特网标准。PPP 是一套规则，定义您的调制解调器连接如何与因特网上的其他系统交换数据包。

RFC-1661 中有 PPP 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc1661.txt

协议——在计算机中，协议是一套方针或标准，服务器与应用程序据此通信。有多种多样用于各种不同目的的协议，比如，TCP/IP, SLIP, HTTP, POP3, SMTP, IMAP, FTP 等等。

注册表——Microsoft Windows 使用的数据库，用来存储关于安装在计算机上的软件的配置信息。这些配置信息例如用户设置，文件扩展关联，桌面背景，颜色方案等等。它有以下六个部分：

HKEY_User——为系统的每个用户存储用户信息。

HKEY_Current_User——当前用户的首选项。

HKEY_Current_Configuration——为显示器与打印机存储设置。

HKEY_Classes_Root——文件关联与 OLE 信息。

HKEY_Local_Machine——硬件，操作系统与已安装的应用程序设置。

HKEY_Dyn_Data——执行数据。

当在您的计算机上安装程序时，安装程序总会自动地向注册表写入一些信息。但是您可以使用 Windows 内置的 regedit.exe 程序手动编辑注册表。不过您应该小心谨慎地编辑注册表，因为◆◆改后的错误设置将导致您的计算机运行紊乱或无法运行。

RFC——请求评议（Request For Comments）用于在因特网上创建标准的过程与结果名。每个新的标准和协议都作为"请求评议"（"Request For Comments"）在因特网上提出与发表。因特网工程任务组（The Internet Engineering Task Force）推动了关于新标准的讨论并最终创建了它。尽管建立好的标准无需进一步的"请求""评议"，但是该标准仍将保持"请求评议"（"Request for Comment"）的首字母缩写与其识别号码。比如 RFC-822（目前由 RFC-2822 替代）或"RFC"是一个邮件的官方标准。但是，这些被官方采用作为"标准"的协议确实具有一个与它们关联的官方标准号码，这些号码被列在因特网官方协议标准（Internet Official Protocol Standards）文档中。（其本身是 STD-1 当前是 RFC-3700）。您可以在因特网的许多地方找到 RFC，但是最具权威性的来源是 The RFC Editor，位于http://www.rfc-editor.org/。

因特网官方协议标准（Internet Official Protocol Standards）文挡位于：

http://www.rfc-editor.org/rfc/std/std1.txt

RTF——富文本格式（Rich Text Format）是一个通用的文件格式，由 Microsoft 开发，几乎所有的文字处理器都支持它。与纯文本格式相反，RTF 可以让您保留格式，字体信息，文本颜色等等。与其他文件格式相比（例如 Microsoft Word 格式 *.doc 和 *.docx 以及 Adobe PDF），RTF 文件非常大。

服务器——一个计算机或者程序，它向运行在其他计算机上的客户端软件提供特定类型的服务。该术语可以表示特定的软件，比如 SMTP 服务器，或是装了该软件的计算机。单一的服务器*机器*可以同时具有许多不同的服务器*程序*在其上运行。比如，您的网络服务器可以同时运行 web 服务器，邮件服务器，FTP 服务器，传真服务器等等。

SMTP——简单邮件传输协议，Simple Mail Transfer Protocol 的首字母缩写。这是一个用于在因特网上从一个服务器向另一个服务器或从一个客户端向一个服务器发送邮件的主要协议。SMTP 由一套规则组成，该规则规定发送邮件的程序应该如何与接收邮件的程序相互作用。一旦服务器通过 SMTP 接收了邮件，邮件通常会被储存在那里，接着由客户端通过 POP，IMAP 或其他协议取回邮件。

RFC-2821 中有 SMTP 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc2821.txt

垃圾邮件——因特网上的垃圾邮件。"垃圾邮件"最常用于表示未经请求的群发邮件，尽管一般而言，它常被用于表示任何不需要的邮件。"垃圾邮件发送者"将包含几百，几千甚至几百万条来自各种来源的邮件地址，接着向该地址列表发送垃圾邮件或欺诈信息。"垃圾邮件"也可用于表示新闻组或讨论板的垃圾帖，这些帖子通常是关于一个产品或网站的不需要或不相关的广告。

垃圾邮件迅速成为因特网上一个严重的问题，浪费了大量的时间与服务器资源。因为垃圾邮件发送者通常会使用各种技术试图掩饰邮件的发源处——比如将它们的地址"伪造"成其他人或尝试偷偷地通过多个邮件服务器转发垃圾邮件——防范这些垃圾邮件是很有挑战性的。MDaemon Technologies 的 MDaemon 服务器配备了一系列特别为打击垃圾邮件而设计的功能，例如：DNS 阻止列表（DNS-BL），IP 防护，IP 屏蔽，中继控制等等。

将术语"Spam"表示为垃圾邮件的起源颇具争议，但逐渐被接受的一个说法是它来自（1970 年）流行的 Monty Python 剧团里一幕短小的系列喜剧（Sketch），其中北欧海盗（Vikings）的歌谣中周而复始地重复着单词"Spam"，"Spam spam spam spam，spam spam spam spam……"。但是，它也可以是具有相同名称的 Hormel 肉制品的诋毁性比喻——每个人都有一次或几次机会得到它，但是人们真的希望得到它或喜欢它吗？

TCP/IP——传输控制协议/因特网协议（Transmission Control Protocol/Internet Protocol(TCP/IP)）是因特网的基础。它是一套基本的通信协议，用于在因特网上连接主机。它也是局域网上最常用的协议。它是双层系统，最顶层是 TCP，它管理将文件分解并集合成数据包以便在网络上传输。IP 是较低的那层，处理数据包的地址以便让它们抵达正确的目的地。RFC-793 中有 TCP 地址。RFC-791 中有 IP 地址。这些 RFC 都可以在如下找到：

TCP ——http://www.rfc-editor.org/rfc/rfc793.txt

IP ——http://www.rfc-editor.org/rfc/rfc791.txt

Telnet——一个命令与程序，用于登陆到支持 Telnet 访问的因特网站。Telnet 命令将您带到 Telnet 服务器的登陆提示。如果您在那台服务器上拥有帐户，您就可以获得允许您访问的资源，比如您的文件，邮件等等。Telnet 的底侧有一个使用 Unix 命令的命令行程序。

RFCs 854-855 中有 TELNET 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc854.txt

http://www.rfc-editor.org/rfc/rfc855.txt

终端——一个设备，允许您向远程的计算机发送命令。终端可以是一个键盘，显示屏以及其他一些简单电路。但通常将个人计算机用作“仿效”终端。

Tiff——标签图像文件格式，Tagged Image File Format 的首字母缩写。它是一个图像文件格式，被创建为跨多个计算机平台的通用图像翻译器。TIFF 可以处理颜色深度从 1 位至 24 位 的图像。

UDP——用户数据报协议（User Datagram Protocol)是弥补用于数据传输的 TCP/IP 协议族的一个协议。UDP 是一种无状态连接，因为它不会告知发送出去的数据包是否已被接收。

RFC-768 中有 UDP 地址，可以在以下地址中查看到：

http://www.rfc-editor.org/rfc/rfc768.txt

Unix——Unix 或 UNIX，是由 BellLabs 于 20 世纪 60 年代创建的操作系统。其设计可以让多用户在同一时间使用，它是因特网上用于服务器的最流行的操作系统。现在有许多不同的基于 UNIX 的操作系统，比如 Linux，GNU，Ultrix，XENIX 等等。

URL——每个因特网上的文件或服务器都有一个统一资源定位符 (Uniform Resource Locator)。它是您输入 web 浏览器并能抵达该服务器或文件的地址。URL 不能有空格，通常使用分隔符。它们有两部分，用“//”分隔。第一部分是要使用的协议或需要写明地址的资源 (比如，http，telnet，ftp 等等)，第二部分是文件或服务器的因特网地址 (比如，www.altn.com 或 127.0.0.1)。

Uuencode——一套运算法则，为了通过因特网进行传输将文件转换成一系列 7 位的 ASCII 字符。尽管它表示 Unix-to-Unix 编码，它不再属 UNIX 专有。它已成为不同平台间传输文件的通用协议。它是邮件中常用的编码方式。

WAN——WAN，或广域网 (Wide Area Network)，与局域网 (LAN)类似，但是通常跨多城市甚至国家。WAN 有时也由互相连接的较小型 LAN 组成。可以将因特网描述成世界上最大的广域网 (WAM)。

Zip——指的是一个经压缩的或"zip"过的文件，常跟".zip"文件扩展名。"Zipping"就是将一个或多个文件压缩成一个存档文件以为存贮节省空间或加快文件传输到另一台计算机的过程。但若要使用 zip 文件，您首先需要使用正确的程序，比如 PKZIP 或 WinZip 对它进行解压缩。有多种可用的压缩/解压缩工具——既有共享软件也有免费软件——可以从因特网上的许多站点获得。希望您在安装该工具前，不必先对其进行解压。

索引

- 2 -

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- J -

- L -

- M -

- O -

- P -

- Q -

- R -

- S -

- T -

- U -

- V -

- W -

- X -

- Z -