



Installationsanleitung

MDaemon

Inhaltsverzeichnis

| | |
|-----------------------------------------------------------|----|
| Zielgruppe/Voraussetzungen | 3 |
| Grundinstallation des MDAemon Email Servers | 5 |
| Schritt 1: MDAemon installieren | 5 |
| Schritt 2: Angabe des Domänennamens | 6 |
| Schritt 3: Einrichtung des ersten Benutzerkontos | 6 |
| Schritt 4: Einrichtung des Windows-Dienstes | 6 |
| Schritt 5: Abschluss der Installation | 6 |
| Schritt 6: Aktivierung der Software | 7 |
| Schritt 7: Abschluss der Installation | 7 |
| Tipps aus unserem Support | 7 |
| Konfigurationseinstellungen in MDAemon | 11 |
| Posteingang und Postausgang | 11 |
| Zeitsteuerung | 16 |
| E-Mail-Adressen und Benutzer anlegen | 17 |
| Sicherheitseinstellungen | 18 |
| Grundinstallationen von MDAemon AntiVirus | 22 |
| Konfiguration der E-Mail-Anwendung auf der Arbeitsstation | 23 |
| Webmail-Zugriff über MDAemon Webmail | 24 |

| | |
|-----------------------------------------|----|
| MDaemon Instant Messenger | 25 |
| Administration mit der Remoteverwaltung | 26 |

| | |
|----------------------------|----|
| Einrichtung von ActiveSync | 27 |
|----------------------------|----|

| | |
|---------------------------------|----|
| Serviceleistungen | 28 |
| Support | 28 |
| Individuelle Schulungen vor Ort | 28 |
| Dienstleistungen | 29 |
| Consulting und Audits | 29 |

Zielgruppe/Voraussetzungen

MDaemon Server benötigt einen Rechner mit Microsoft Windows 7 / 8 / 10 / Windows Server 2008 / 2012 / 2016 / 2019 jeweils in 32-bit oder 64-bit. Alle weiteren Systemanforderungen können Sie unter www.mdaemon.com/Products/MDaemon-Email-Server-Windows/System-Requirements/ einsehen.

Der erforderliche Festplattenplatz richtet sich nach der Anzahl und Größe der einzelnen Postfächer. Da diese Größe sehr variiert, kann hierzu keine Empfehlung ausgesprochen werden. Sorgen Sie für ausreichend dimensionierten Festplattenplatz und verwenden Sie bitte schnelle Festplatten.

Für die SMTP-, POP-, IMAP- und vergleichbaren Dienste benötigen Sie das TCP/IP-Netzwerkprotokoll. Erforderlich ist zudem ein Internetzugang über einen Provider. Dieser kann entfallen, wenn der Postverkehr nur innerhalb des lokalen Netzwerks stattfinden soll und ein Post austausch mit externen Gegenstellen nicht gewünscht ist.

Der MDAemon Email Server richtet sich an Unternehmen aller Größen, die eine Vor-Ort-Installation im eigenen Haus realisieren möchten und eine einfache Administration und Wartung bei umfassenden Funktionen wünschen.

Diese Installationsanleitung wurde aus unseren Supporterfahrungen heraus entwickelt und stellt eine Standardinstallation für Firmen mit einer Domäne dar.

Was Sie benötigen, bevor Sie starten können:

- MDAemon als installierbare Datei für das entsprechende Betriebssystem, auf dem MDAemon als Server laufen soll. Diese erhalten Sie unter <https://www.mdaemon.de> und beinhaltet sowohl MDAemon AntiVirus, den MDAemon Connector und MDAemon ActiveSync. Die Module werden durch entsprechende Lizenzen freigeschaltet.
- Für den Virenschutz empfehlen wir Ihnen MDAemon AntiVirus, ein Zusatzprodukt für den MDAemon, das voll in diesen integriert und über dessen Oberfläche verwaltet und konfiguriert werden kann.
- Möchten Sie die Groupware-Funktionen von Outlook nutzen, lizenzieren Sie bitte auch den MDAemon Connector. Mit diesem greifen Sie gemeinsam mit Ihren Kollegen auf dieselben E-Mails, Kalender, Kontakte, Aufgaben oder Notizen zu.

- Um mit Ihren mobilen Endgeräten per ActiveSync auf E-Mails und persönliche Informationen wie Kontakte, Aufgaben und Kalender zugreifen zu können, empfehlen wir Ihnen MDAemon ActiveSync zu lizenzieren.
- Prüfen Sie eventuell Ihre Firewall auf die benötigten Ports. Weiterführende Informationen dazu erhalten Sie in unserer Knowledgebase unter <https://www.mdaemon.de/support-kb.cfm>

Grundinstallation des MDAemon Email Servers

Schritt 1: MDAemon installieren

- Laden Sie die Installationsdatei im Downloadbereich unter <https://www.mdaemon.de> herunter.
- Starten Sie den Installationsvorgang mit einem Doppelklick auf die Installationsdatei. Im darauf erscheinenden Willkommensfenster haben Sie die Möglichkeit, sich über die neuen Funktionen und Änderungen von dieser MDAemon-Version zu informieren. Wir empfehlen Ihnen hier insbesondere den Abschnitt "Zur besonderen Beachtung". Klicken Sie danach auf "Weiter".
- Lesen Sie bitte die Lizenzbestimmungen und klicken Sie danach auf "Weiter".
- Wählen Sie das Zielverzeichnis für die Installation aus und klicken Sie auf "Weiter". Tipp: Um die Schreib-/Lesezugriffe auf der Systemfestplatte, auf der das Betriebssystem installiert ist, zu minimieren, empfehlen wir Ihnen nach Möglichkeit die Installation auf D:\, E:\ bzw. einem anderen physikalischen Datenträger.
- Wählen Sie nun den gewünschten Installationstyp: A) Kostenlose Testversion oder B) Vollversion.
 - A) Wählen Sie die erste Option, um eine voll funktionsfähige 30-Tage-Testversion von MDAemon zu installieren.
 - B) Wählen Sie die untere Option, falls Sie einen Lizenzschlüssel käuflich erworben haben und tragen Sie den Lizenzschlüssel direkt ein.
- Geben Sie in dem Reiter „Kunden-Informationen“ den Namen, die Firma und das Land des Lizenznehmers ein. Im Falle einer Testinstallation geben Sie bitte auch eine E-Mail-Adresse ein, die zum Zeitpunkt der Installation abgerufen werden kann. Mit einem Klick auf „Weiter“ wird die Testlizenz per E-Mail angefordert. Bitte tragen Sie die Testlizenz in das entsprechende Feld ein.
- Nun wird die Lizenzdatei selbst angefordert. Hierzu ist eine ausgehende Verbindung über HTTPS notwendig. Stellen Sie daher sicher, dass weder ein Proxy noch eine Firewall ausgehenden Datenverkehr über HTTPS blockiert. Der Vorgang dauert nur wenige Sekunden.
- Im Fenster "Bereit zur Installation" klicken Sie auf "Weiter", um die eigentliche Installation zu starten. Die Dateien für MDAemon werden in das zuvor angegebene Zielverzeichnis kopiert.

Schritt 2: Angabe des Domänennamens

Geben Sie nun bitte den Domänenname Ihrer E-Mail-Adresse (z.B. company.test) und Ihren IMAP-/POP-Hostname (z.B. mail.company.test) ein.

Tipp: Sie können hier die tatsächliche Domäne eingeben, wie Sie auch aus dem Internet erreichbar ist. Sie müssen hier also nicht mit z.B. meinedomain.local arbeiten, wie es oft in privaten Netzwerken der Fall ist.

Schritt 3: Einrichtung des ersten Benutzerkontos

Geben Sie Vor- und Nachname sowie Postfachname und Kennwort ein. Lassen Sie das Kontrollkästchen aktiv, um diesem Benutzerkonto Administrationsrechte mit Vollzugriff über die webbasierte Remote-Verwaltung zu erteilen. Diesen administrativen Benutzer erkennen Sie später in dem Benutzerkonten-Manager an einem gelben Blitz-Symbol.

Schritt 4: Einrichtung des Windows-Dienstes

Lassen Sie das Kontrollkästchen aktiv, um MDAemon als automatisch startenden Windows-Dienst einzurichten und klicken Sie auf "Weiter".

Tipp: Per Standard wird der Dienst von MDAemon im Sicherheitskontext des Benutzerkontos SYSTEM ausgeführt. Dieses Benutzerkonto hat jedoch keine Berechtigungen für den Zugriff auf Netzwerkfreigaben. Sollte der Zugriff auf Ressourcen im Netzwerk gewünscht sein (in den meisten Fällen ist dies jedoch nicht notwendig), können Sie nach der Installation in MDAemon unter dem Menüpunkt „Einstellungen | Voreinstellungen | Windows-Dienst“ ein anderes Benutzerkonto angeben.

Schritt 5: Abschluss der Installation

Lassen Sie das Kontrollkästchen aktiv, um MDAemon zu starten. Um die Versionsinformationen zu lesen, aktivieren Sie das untere Kontrollkästchen. Wir empfehlen Ihnen, immer die Versionsinformationen zu lesen – insbesondere die Hinweise zu den Änderungen und neuen

Funktionen bzw. zur besonderen Beachtung. Klicken Sie "Fertig stellen", um MDAemon nun zu starten.

Schritt 6: Aktivierung der Software

Zusätzlich zur eigentlichen Lizenzierung von MDAemon gibt es noch eine Aktivierung. Die Aktivierung erfolgt bei einer Neuinstallation in der Regel vollautomatisch im Hintergrund. Sollte es bei der Aktivierung wider Erwarten irgendwelche Probleme geben, erscheint nach dem ersten Start von MDAemon der Aktivierungsassistent. Klicken Sie in diesem Fall bitte einfach auf den Button "Weiter".

Tipp: Wird der Aktivierungsassistent nicht angezeigt, kann es an den erweiterten Sicherheitsfunktionen von z.B. Windows 7 oder Windows Server 2008 liegen. Beenden Sie in diesem Fall den Dienst von MDAemon über die Systemsteuerung und starten Sie MDAemon für den Zeitraum der Aktivierung mit der Datei \MDaemon\App\MDaemon.exe als Anwendung. Jetzt sollte der Aktivierungsassistent angezeigt werden und Sie können mit dem nächsten Schritt fortfahren.

Schritt 7: Abschluss der Installation

Klicken Sie auf "Fertig stellen", um die Aktivierung abzuschließen.

Herzlichen Glückwunsch, MDAemon wurde erfolgreich installiert.

Tipps aus unserem Support

An dieser Stelle haben wir für Sie noch ein paar Tipps aus unserem Support:

- Auslagern von Protokolldateien: Je nach Konfiguration der Protokollierung können die Protokolle über die Zeit hinweg einen gewissen Speicherplatz in Anspruch nehmen. Um die Systemfestplatte damit nicht unnötig zu belasten, empfiehlt es sich, die Protokolldateien auf einen anderen Datenträger aus zu lagern. Die Anpassungen dazu können Sie direkt in der Oberfläche von MDAemon unter dem Menüpunkt „Einstellungen | Server-Einstellungen | Protokollierung | Betriebsart des Protokolls...“ vornehmen. Geben Sie hier einfach den gewünschten Ordner an.

- Richtige Protokollierung: Protokollieren Sie bitte nur die Dienste, die Sie auch wirklich verwenden. Damit sparen Sie Speicherplatz. Außerdem können Sie veraltete Protokolldateien automatisch archivieren oder aber auch löschen. Die Konfiguration dazu finden Sie unter dem Menüpunkt „Einstellungen | Server-Einstellungen | Protokollierung | Einstellungen“ bzw. „Wartung“.
- Farblich getrennte Protokollierung: Um bei der Protokollanalyse einen besseren Überblick zu erhalten, empfehlen wir Ihnen die farblich getrennte Protokollierung zu aktivieren. Die Konfiguration dazu finden Sie unter dem Menüpunkt „Einstellungen | Voreinstellungen | Benutzeroberfläche“ und lautet „Protokolle auf der Benutzeroberfläche mehrfarbig darstellen“.
- Dienstzustand nach Neustart beibehalten: Wird z.B. weder MultiPOP noch DomainPOP verwendet, oder aber die Mitarbeiter greifen überhaupt nicht auf den POP-Server von MDAemon zu, können Sie diese Dienste deaktivieren. Damit diese aber auch nach einem Neustart deaktiviert bleiben, gibt es in MDAemon eine Einstellung dafür. Die Konfiguration dazu finden Sie unter dem Menüpunkt „Einstellungen | Voreinstellungen | Benutzeroberfläche“ und lautet „Dienstzustand aktiviert/deaktiviert nach Neustart beibehalten“.
- Backup der einzelnen Konfigurationsdateien: MDAemon bietet die Möglichkeit die Konfigurationsdateien immer um Mitternacht automatisch zu sichern. Im Ernstfall können Sie dann zumindest die Konfiguration des MDAemon wiederherstellen. Die Konfiguration dazu finden Sie unter dem Menüpunkt „Einstellungen | Voreinstellungen | Speicherplatz“ - „Konfigurationsdateien jeden Tag um Mitternacht sichern“. Wichtig: Diese Option ersetzt kein herkömmliches Backup der einzelnen Postfächer.
- Postfächer der Benutzer auslagern: Bevor die ersten Benutzer in MDAemon angelegt werden, empfiehlt es sich darüber nachzudenken, die Postfächer der Benutzer (MDaemon\Users\) auf einen anderen Datenträger aus zu lagern. Gerade in virtuellen Umgebungen können zukünftig Migrationen durch das "Aushängen" und "Einhängen" dieser virtuellen Festplatte, auf der sich dann lediglich die Postfächer befinden, wesentlich vereinfacht werden. Änderungen dazu nehmen Sie bitte in der Vorlage in MDAemon unter dem Menüpunkt „Benutzerkonten | Gruppen & Vorlagen | Vorlagen-Verwaltung | Neue Benutzerkonten...“ und dort in dem Abschnitt „Einstellungen für neue Benutzerkonten“ vor. Bitte verwenden Sie auch in dem neuen Pfad die Variablen \$DOMAIN\$ und \$MAILBOX\$.
- Vorhandenen Virens Scanner für die Verwendung von MDAemon AntiVirus konfigurieren: MDAemon AntiVirus selbst scannt jegliche ein- und ausgehende E-Mails, die von MDAemon verarbeitet werden. Wird zusätzlich ein weiterer Virens Scanner auf dem gleichen System einsetzt,

empfehlen wir Ihnen darin das Installationsverzeichnis von MDAemon (z.B. \MDaemon) als Ausnahme für den Echtzeitschutz bzw. für die geplanten Scanjobs zu konfigurieren.

- DNS-BL-Abfragen aktivieren: Per Standard sind die DNS-BL-Abfragen deaktiviert. Wir empfehlen Ihnen bei dem Direktempfang per SMTP in MDAemon unter dem Menü „Sicherheit | Spam-Filter | DNS-BL“ die Abfragen an einer DNS-Blacklist zu aktivieren. Bei einer Standardinstallation ist hier bereits der Host „zen.spamhaus.org“ eingetragen. Als weitere Host empfehlen wir Ihnen „ix.dnsbl.manitu.net“ einzutragen. Das Feld „Meldung“ können Sie bei Bedarf mit einem beliebigen Inhalt füllen. Weitere Informationen zu diesem Anbieter finden Sie auch online unter <http://www.dnsbl.manitu.net>.
- Spam automatisch in IMAP-Spam-Ordner der Benutzer verschieben: Diese Option bewirkt, dass MDAemon automatisch jede als Spam erkannte Nachricht in den IMAP-Ordner „Spam“ (oder auch Junk-E-Mail) des betreffenden Benutzers verschiebt, falls dieser Ordner besteht. So lange die Option aktiv ist, wird der Ordner für jedes neue Benutzerkonto automatisch angelegt. Beim Aktivieren dieser Option bietet MDAemon zudem an, diesen Ordner auch für alle bereits bestehenden Benutzerkonten automatisch anzulegen. Außerdem wird eine IMAP-Filterregel erstellt, welche dafür sorgt, dass die als Spam markierten Nachrichten in den Ordner verschoben werden. Die Option dazu finden Sie unter „Sicherheit | Spam-Filter | Einstellungen“.
- SSL-Zertifikate: Wir empfehlen Ihnen, entweder ein [kostenloses Let's Encrypt-Zertifikat in MDAemon zu erstellen](#) oder alternativ ein [Zertifikat einer öffentlichen Zertifizierungsstelle einzubinden](#).
- IMAP COMPRESS bei Bedarf deaktivieren: Bei IMAP COMPRESS handelt es sich um eine IMAP-Erweiterung, welche alle Daten zwischen Client und Server während der Übertragung komprimiert. Der MDAemon Outlook Connector unterstützt z.B. diese Erweiterung. Allerdings gibt es zahlreiche Virens Scanner, die diesen Datenstrom nicht scannen können. In diesem Fall empfehlen wir Ihnen die Funktion in MDAemon unter dem Menüpunkt „Einstellungen | Server-Einstellungen | Server...“ zu deaktivieren. Entfernen Sie dazu einfach den Haken bei der Option "IMAP-Server unterstützt den Befehl COMPRESS".
- Firewall konfigurieren: Prüfen Sie eventuell Ihre Firewall auf die benötigten Ports. Weiterführende Informationen dazu erhalten Sie in unserer Knowledgebase unter <https://www.mdaemon.de>

Konfigurationseinstellungen in MDAemon

Öffnen Sie die MDAemon-Administration unter Start | Programme | MDAemon oder per Doppelklick auf den weißen Briefumschlag in der Windows Taskleiste links neben der Systemuhr.



Tipp: Wird der weiße Briefumschlag nicht angezeigt, kann es unter Umständen an den erweiterten Sicherheitsfunktionen von z.B. Windows 7 oder Windows Server 2008 liegen. Der Dienst ist in der Regel trotzdem gestartet und MDAemon steht für die Benutzer ganz normal zur Verfügung. Starten Sie in diesem Fall die MDAemon-Administration wie oben angegeben über das Startmenü von Windows.

Shortcut oder Verknüpfung "MDAemon öffnen" im Startmenü ändern

Mit Version 19 des MDAemon Email Server verweisen der Desktop-Shortcut sowie die Verknüpfung "MDAemon öffnen" im Windows-Startmenü nicht mehr auf die traditionelle MDAemon-Benutzeroberfläche, sondern rufen die MDAemon-Remoteverwaltung in einem Browserfenster auf.

Um anstelle der MDAemon-Remoteverwaltung die klassische Benutzeroberfläche zu starten, können Sie die nachfolgende Datei editieren:

```
\MDaemon\App\MDaemon.ini
```

Innerhalb der MDAemon.ini finden Sie den Abschnitt „MDLaunch“:

```
[MDLaunch]
OpenConfigSession=No
OpenRemoteAdmin=Yes
```

Hier können Sie die Einträge OpenConfigSession und OpenRemoteAdmin mit den Einträgen Yes/No entsprechend ändern.

Weitere Informationen hierzu finden Sie in unserer [Knowledge Base](#).

Posteingang und Postausgang

Posteingang

Für den Empfang neuer Nachrichten bietet MDAemon unterschiedliche Optionen an. Unsere Empfehlung ist, den Direktempfang per SMTP zu verwenden. Alternativ dazu können Sie aber auch einzelne Postfächer bei Ihrem Provider per MultiPOP, oder aber ein Sammelpostfach per DomainPOP abrufen. Nachfolgend beschreiben wir Ihnen die notwendige Konfiguration.

Direktempfang per SMTP:

Der MDAemon benötigt in diesem Fall eine öffentliche IP-Adresse und der MX-Eintrag der Domäne im DNS muss auf den MDAemon Server zeigen. Vergessen Sie bitte außerdem nicht, einen PTR-Record (für Reverse DNS) auf die IP-Adresse des MDAemon Server zeigen zu lassen. Sprechen Sie hierzu bei Bedarf Ihren Provider an.

Aktivieren Sie in MDAemon unter „Einstellungen | Server-Einstellungen | Postausgang...“ die Option „Alle abgehenden Nachrichten direkt an den Mailserver des Empfängers senden“.

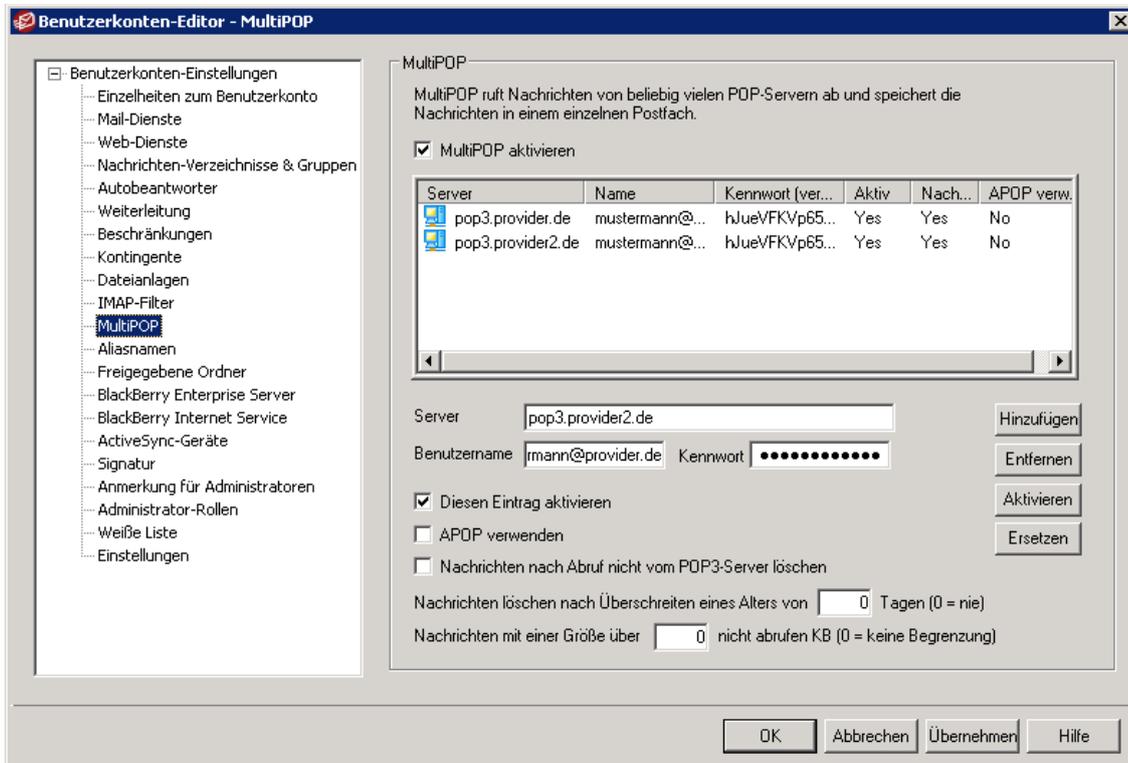
Vorteile:

- Volle Kontrolle über die Benutzerpostfächer und keine abhängig vom Provider.
- Zeitnahe Zustellung der E-Mails, da diese nicht per POP3 abgeholt werden.
- Weniger Spam, da alle Spam- und Sicherheitsfunktionen von MDAemon angewandt werden.
- Ausführliche SMTP-Protokollierung.

Empfang per MultiPOP:

Sie können für jeden Benutzer beliebig viele Postfächer, bei beliebigen Providern per MultiPOP abrufen. Die Konfiguration dafür erfolgt für jeden einzelnen Benutzer über den Menüpunkt „Benutzerkonten | Benutzerkonten-Manager“ und in dem Benutzerkonto unter dem Reiter „MultiPOP“. Bitte tragen Sie hier den POP-Server des Providers sowie die entsprechenden Zugangsdaten ein.

Tipp: Verlangt Ihr Provider den Abruf per SSL, tragen Sie einfach hinter dem Servernamen den Zusatz :995 ein. Aktivieren Sie zudem unter dem Menüpunkt „Sicherheit | Sicherheitseinstellungen | SSL & TLS | MDAemon“ die Optionen "SSL, STARTTLS und STLS", "Gesonderte SSL-Ports für SMTP-, IMAP- und POP3-Server aktivieren" sowie "DomainPOP-/MultiPOP-Server nutzen STLS, soweit möglich.



Aktivieren Sie abschließend noch den Dienst über den Menüpunkt „Datei | MultiPOP-Server“.

Empfang per DomainPOP:

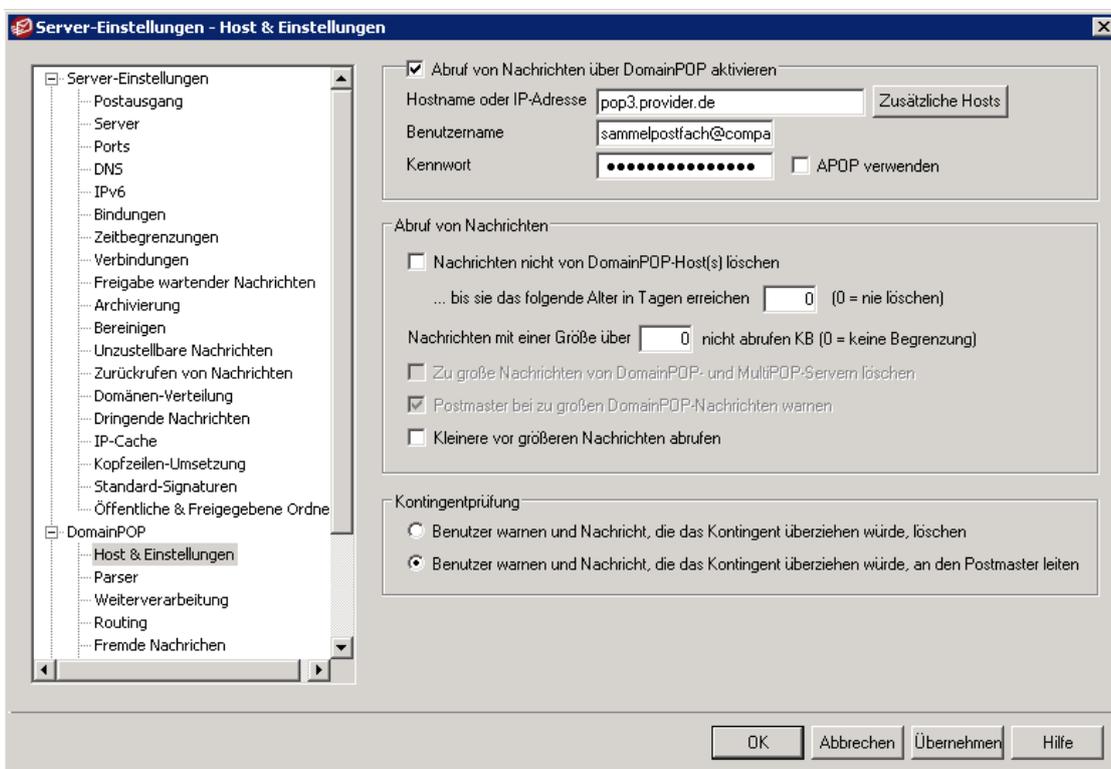
Mit dieser Option rufen Sie ein Sammelpostfach bei Ihrem Provider ab. Die Konfiguration dazu erfolgt in MDAemon unter Einstellungen | Server-Einstellungen | DomainPOP.

Aktivieren Sie die Option „Abruf von Nachrichten über DomainPOP aktivieren“.

Tragen Sie im Feld „Hostname oder IP“ den „POP3-Server“ Ihres Providers ein. Vergeben Sie den „Benutzernamen“ und das „Kennwort“.

Optional können Sie durch Klick auf den Button „Zusätzliche Hosts“ weitere Server zum Abholen der Post über DomainPOP definieren.

Klicken Sie dann auf „Übernehmen“.



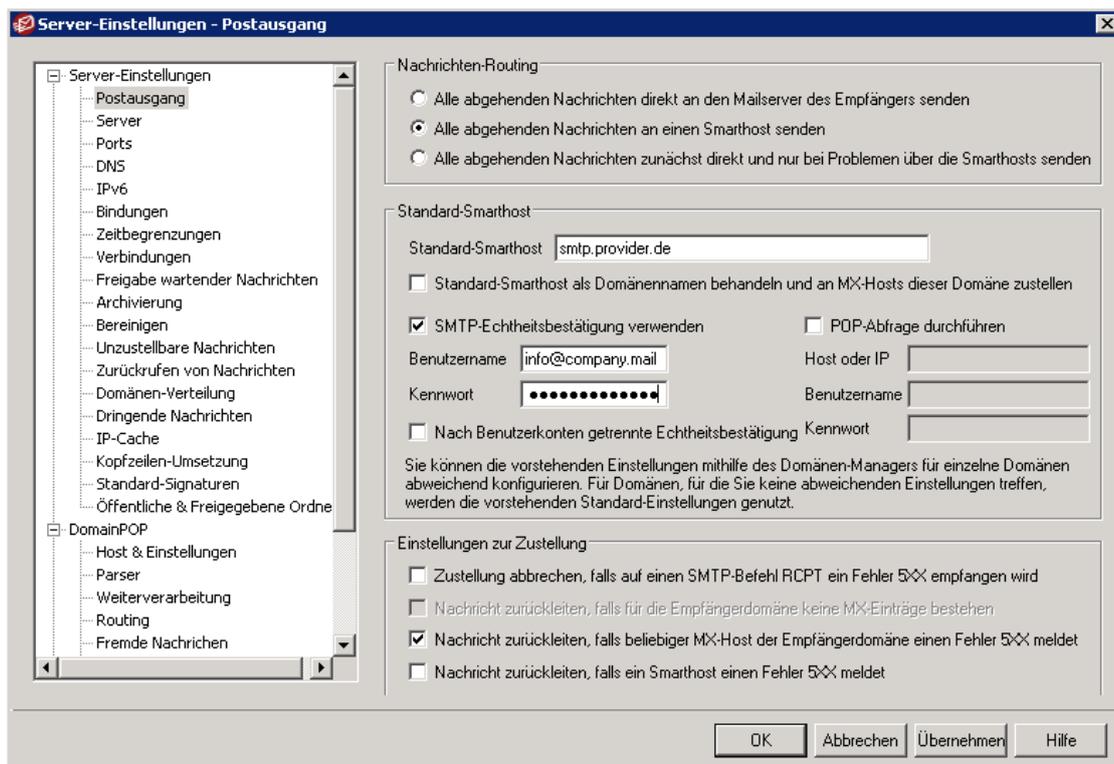
Aktivieren Sie abschließend noch den Dienst über den Menüpunkt „Datei | DomainPOP-Server“.

Postausgang

Wenn Sie sich für den direkten Empfang per SMTP entschieden haben, müssen Sie unter „Einstellungen | Server-Einstellungen | Postausgang...“ lediglich die Option „Alle abgehenden Nachrichten direkt an den Mailserver des Empfängers senden“ aktivieren.

Bei der Verwendung von MultiPOP bzw. DomainPOP passen Sie die Einstellungen noch wie folgt an: Klicken Sie auf „Einstellungen | Server-Einstellungen | Postausgang...“ und aktivieren Sie die Option „Alle abgehenden Nachrichten an einen Smarthost senden“.

Geben Sie nun im Feld „Standard-Smarthost“ den SMTP-Server Ihres Providers ein.

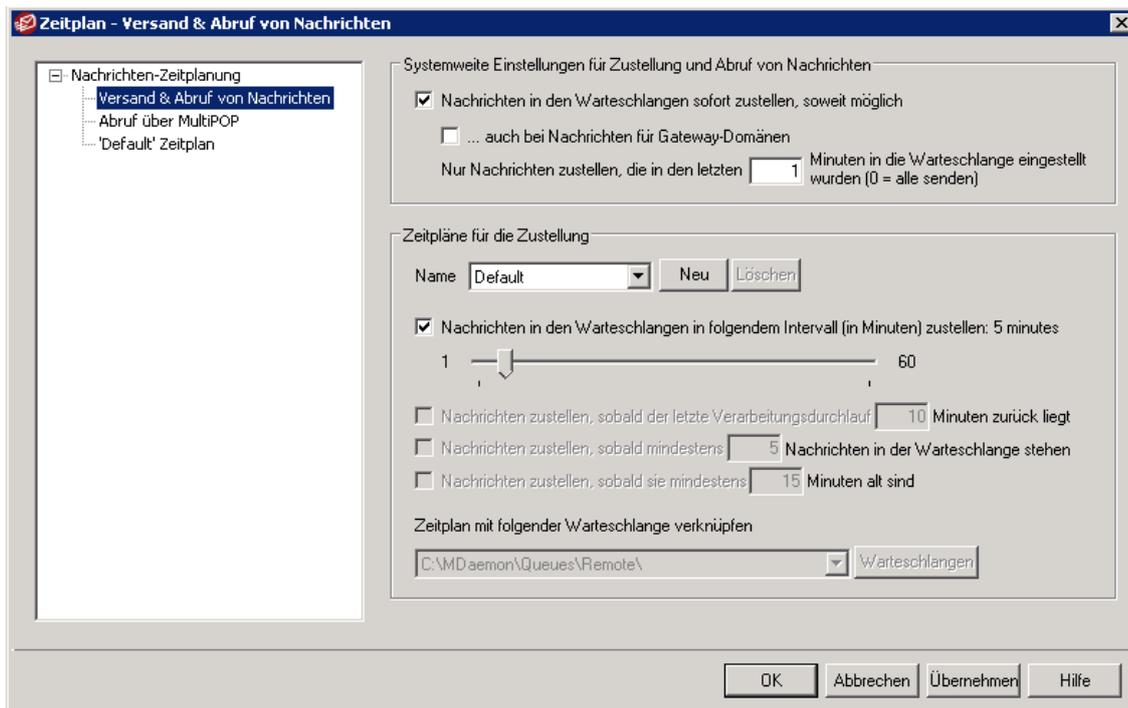


Erfordert der SMTP-Server eine Authentifizierung, aktivieren Sie „SMTP-Echtheitsbestätigung verwenden“ und geben Sie einen Benutzernamen und das dazugehörigen Kennwort ein. Hier reicht es in den meisten Fällen aus, sich mit einem Benutzer wie z.B. info@company.test zu authentifizieren. Hinweis: Sollte der Provider eine nach Benutzerkonten getrennte Echtheitsbestätigung verlangen, aktivieren Sie bitte noch die entsprechende Option und tragen Sie in jedem einzelnen Benutzerkonto unter dem Reiter „Mail-Dienste“ die Zugangsdaten ein.

Erfordert Ihr Provider eine POP-Abfrage vor dem eigentlichen Versand, aktivieren Sie bitte noch die Schaltfläche „POP-Abfrage durchführen“ und geben Sie die POP-Servereinstellungen für z.B. den Benutzer info@company.test ein.

Zeitsteuerung

Klicken Sie unter „Einstellungen“ den Punkt „Zeitplan...“.



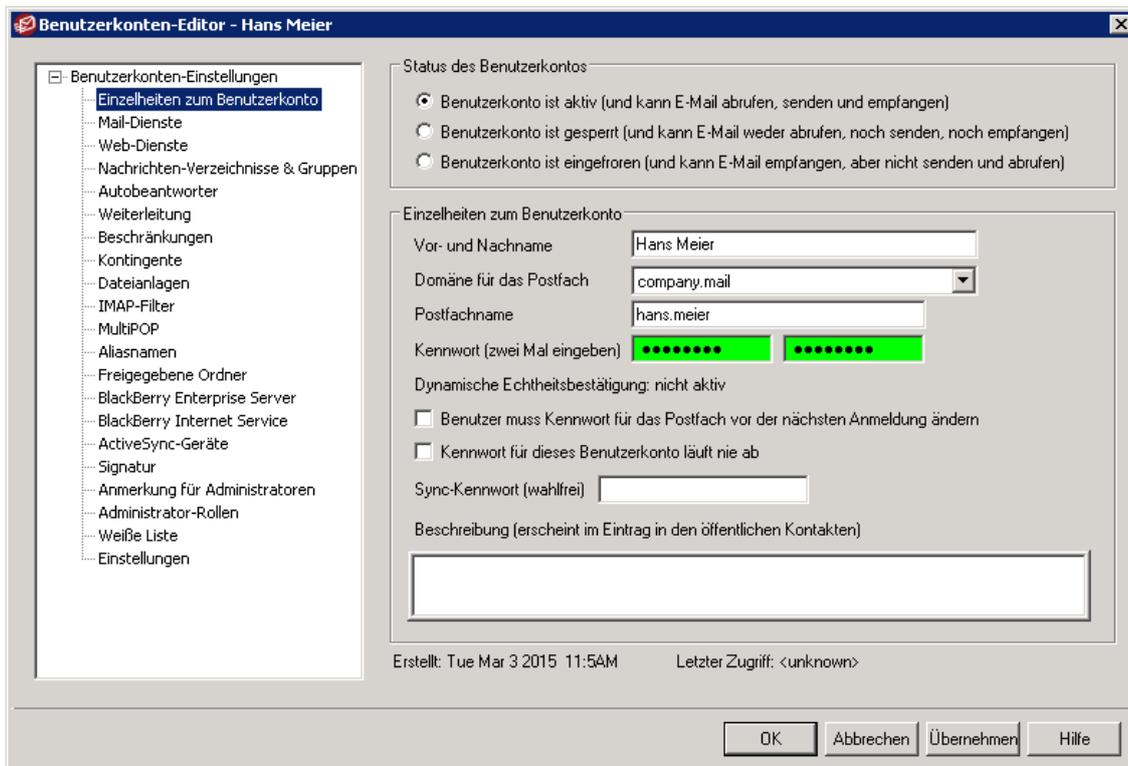
Die Standardeinstellung von MDAemon ist so konfiguriert, dass Post sofort zugestellt wird. Sie können dies durch Verstellen des Schiebereglers beliebig anpassen. Passen Sie die einzelnen Optionen je nach Bedarf an.

Hinweis: Per Standard wird alle 5 Minuten die Verarbeitung der Warteschlange gestartet. In diesem Intervall werden auch die Nachrichten per MultiPOP oder aber DomainPOP abgerufen. Möchten Sie dieses Intervall ändern, verwenden Sie bitte den Schieberegler. Beachten Sie jedoch, dass ein zu häufiger Abruf bei einem Provider eventuelle Sperren auslösen kann.

Unter dem Menüpunkt „Abruf über MultiPOP“, können Sie weitere Einstellungen treffen. Wir empfehlen Ihnen die Standardeinstellung „Nachrichten über MultiPOP bei jedem Verarbeitungsdurchlauf für externe Post abrufen“ beizubehalten. Hierzu wird das unter dem Schieberegler festgelegte Intervall verwendet.

E-Mail-Adressen und Benutzer anlegen

Klicken Sie unter „Benutzerkonten“ den ersten Punkt „Neues Benutzerkonto“.



In der ersten Schaltfläche „Benutzerkonto“ geben Sie bitte bei „Vor- und Nachname“ den Namen des Benutzers ein. Wählen Sie die gewünschte Domäne für das Postfach aus. Die vollständige E-Mail-Adresse besteht dann aus dem Feld „Postfachname“ und der Domäne. Diese Adresse ist zugleich der Benutzername zum Abholen der E-Mails von dem Client aus. Bei „Kennwort“ geben Sie bitte ein sicheres Kennwort ein und wiederholen die Eingabe. Klicken Sie auf „Übernehmen“.

Sofern für diesen Benutzer ein externes oder mehrere externe E-Mail-Konten abgefragt werden sollen, klicken Sie bitte im Menü auf „Datei | MultiPOP-Server“ aktivieren.

Öffnen Sie anschließend im Benutzerkonten-Manager den gewünschten Benutzer und tragen Sie unter „MultiPOP“ die Daten für den Abruf des externen Postfachs ein. Siehe hierzu auch den Abschnitt „Empfang über MultiPOP“.

Sicherheitseinstellungen

MDaemon enthält umfassende Sicherheitsfunktionen. Die Auswahl des Menüpunktes „Sicherheit“ eröffnet den Zugang zu folgenden Funktionen:

AntiVirus: MDAemon AntiVirus kann Viren filtern und stoppen, die über E-Mail verbreitet werden; dazu bietet diese Software den Benutzern eine vollständige und nahtlose Einbindung in MDAemon, wie sie keine andere Software erreicht. MDAemon AntiVirus erkennt, sperrt, repariert oder löscht alle E-Mail-Nachrichten, in denen ein Virus festgestellt wurde. Benutzern von MDAemon stellt das Modul unter anderem auch die Funktion Schutz gegen Massenangriffe zur Verfügung, mit deren Hilfe das System gegen bestimmte Spam-, Phishing- und Virenangriffe geschützt werden kann, die durch herkömmliche Schutzmechanismen auf Basis von Inhaltsauswertung und Signaturen vielleicht nicht entdeckt werden.

Inhaltsfilter: Ein höchst vielseitiges Inhaltsfilter-System mit uneingeschränkter Multithread-Unterstützung erlaubt es, das Verhalten des Servers vom Inhalt eingehender und abgehender Nachrichten abhängig zu machen. Kopfzeilen können in Nachrichten eingefügt und aus ihnen gelöscht werden, die Nachrichten können einen Fußtext erhalten, Dateianlagen können entfernt, Kopien können automatisch an andere Benutzer geleitet werden, Instant-Messages können ausgelöst, externe Programme ausgeführt werden und vieles mehr.

Spam-Filter: Die Technik des Spam-Filters prüft E-Mail-Nachrichten durch heuristische Verfahren, um eine Bewertung zu errechnen. Anhand dieser Bewertung stellt das System fest, wie wahrscheinlich es ist, dass es sich bei der Nachricht um Spam handelt. Aufgrund dieser Feststellung kann der Server dann bestimmte Aktionen auslösen, etwa die Nachricht abweisen oder kennzeichnen.

Schwarze Listen für DNS / DNS-BL: Mithilfe mehrerer Dienste, die schwarze Listen für DNS unterhalten und die der Benutzer auch selbst auswählen kann, wird bei jeder Übertragung einer Nachricht an den Server geprüft, ob sie von einer IP-Adresse ausgeht, die von einem solchen Dienst in einer Schwarzen Liste als gesperrt geführt wird. Trifft dies zu, wird die Nachricht abgewiesen oder entsprechend markiert.

Relaiskontrolle: Hiermit wird festgelegt, wie MDAemon mit Nachrichten verfahren soll, die weder von einer lokalen Adresse kommen noch an eine lokale Adresse gerichtet sind.

IP-Abschirmung: Wenn eine Verbindung von einem hier eingetragenen Domännennamen aus zum Server hergestellt wird, muss die IP-Adresse der Gegenstelle der hier erfassten entsprechen.

SMTP-Echtheitsbestätigung: Diese Einstellungen steuern das Verhalten von MDAemon, falls ein Nutzer eine Nachricht an MDAemon sendet, der nicht zuerst durch Anmeldenamen und Passwort identifiziert wurde.

Rückwärtssuche: MDAemon kann DNS-Server abfragen, um die Echtheit von Domännennamen und Adressen zu prüfen, die während der Anlieferung von Nachrichten übermittelt wurden. Diese Funktion kann dazu verdächtige Nachrichten abweisen oder ihnen eine besondere Kopfzeile hinzufügen. Ergebnisse der Rückwärtssuche werden auch in den Systemprotokollen vermerkt.

POP vor SMTP: Diese Einstellungen verlangen von den Benutzern, ihre Postfächer erst über POP abzufragen, bevor sie eine Nachricht über MDAemon versenden dürfen. Hierdurch wird sichergestellt, dass der Absender ein gültiges MDAemon-Benutzerkonto hat und den Mailserver verwenden darf.

Vertraute Hosts: Diese Domännennamen und IP-Adressen sind von den Relais-Einstellungen ausgenommen.

SPF/Sender-ID: Für alle Domänen sind MX-Einträge veröffentlicht, in denen die Rechner erfasst sind, die Post für die Domänen empfangen dürfen. Aus diesen Einträgen ergibt sich aber nicht, welche Rechner für diese Domänen Post versenden dürfen. Das Sender-Policy-Framework (SPF) ermöglicht es, für Domänen „umgekehrte MX-Einträge“ zu veröffentlichen, aus denen dann die Rechner ersichtlich sind, die für die Domäne Nachrichten versenden dürfen.

DomainKeys Identified Mail: Die Option DomainKeys Identified Mail (DKIM) prüft E-Mail-Nachrichten und kann die Nutzung gefälschter Absenderdaten (das "Spoofing") verhindern. Sie kann auch benutzt werden, um die Intaktheit eingehender Nachrichten zu prüfen und sicherzustellen, dass der Inhalt einer Nachricht nicht verändert wurde, nachdem sie den Mailserver des Absenders verlassen hat. Um diese Funktion bereitzustellen, kommen Schlüsselpaare aus je einem öffentlichen und einem geheimen Schlüssel zum Einsatz. Abgehende Nachrichten werden mithilfe eines geheimen Schlüssels signiert, eingehende signierte Nachrichten werden anhand des öffentlichen Schlüssels des Absenders geprüft, der über den DNS-Server des Absenders abrufbar sein muss.

Zertifizierung: Die Zertifizierung von Nachrichten ist ein Schutzmechanismus, in dessen Rahmen eine Stelle bestätigt oder dafür einsteht, dass eine andere Stelle gewisse ordnungsgemäße E-Mail-Praktiken anwendet. Die Zertifizierung ist vorteilhaft, da sie verhindern kann, dass Nachrichten eine unnötige Analyse durch den Spam-Filter durchlaufen. Sie kann auch helfen, die Ressourcen für die Verarbeitung einzelner Nachrichten zu verringern.

Schwarze Liste für Adressen: Liste der Adressen, die keine Nachrichten über das System versenden dürfen.

IP-Filter: Verbindungen von hier eingetragenen Adressen lässt der Server, je nach Einstellung, zu oder weist sie ab.

Host-Filter: Verbindungen von hier eingetragenen Hostnamen (Domännennamen) lässt der Server, je nach Einstellung, zu oder weist sie ab.

Dynamischer Filter: Mithilfe des dynamischen Filters kann MDAemon die Verhaltensweisen von Gegenstellen analysieren, die Nachrichten an das eigene System senden, und auf verdächtige Verhaltensweisen angemessen reagieren. IP-Adressen können beispielsweise vorübergehend gegen weiteren Verbindungsaufbau gesperrt werden, sobald eine bestimmte Zahl von Fehlern wegen „unbekannter Empfänger“ in einer Verbindung aufgetreten ist.

SSL & TLS: MDAemon unterstützt das Secure-Sockets-Layer-Protokoll (SSL) für SMTP, POP und IMAP sowie für den Webserver von WorldClient. SSL ist das Standardprotokoll für gesicherte Kommunikation zwischen Server und Client im Internet.

Schutz gegen Rückstreuung: Als "Rückstreuung" bezeichnet man Antworten auf E-Mail-Nachrichten, die bei Benutzern des lokalen Systems eingehen, obwohl diese Benutzer die Ursprungsnachrichten gar nicht versendet hatten. Rückstreuung tritt auf, wenn Spam oder durch Viren versandte Nachrichten einen Antwort-Pfad mit gefälschter Absenderadresse enthalten. Um die Rückstreuung zu bekämpfen, enthält MDAemon eine Funktion zum Schutz gegen Rückstreuung. Sie bewirkt, dass Statusnachrichten und Nachrichten von Autobeantwortern nur dann an die Benutzer weitergeleitet werden, wenn die Benutzer die Ursprungsnachrichten selbst versandt haben. Dazu dient ein Hash-Verfahren mit geheimem Schlüssel, das einen bestimmten uhrzeit abhängigen Code in den „Antwort-Pfad“ der abgehenden Nachrichten einfügt.

Bandbreitenbegrenzung: Die Bandbreitenbegrenzung gestattet die Überwachung und Steuerung der von MDAemon genutzten Übertragungsbandbreite durch Drosselung der Übertragungsgeschwindigkeit. Die gewünschte Geschwindigkeit für Verbindungen und die einzelnen Serverdienste lässt sich so beeinflussen; für alle wichtigen Serverdienste von MDAemon sind nach Domänen sowie Domänen-Gateways getrennte Einstellungen möglich.

Teergrube: Eine Technik, die Verbindungen mit Absicht verlangsamen und verzögern kann, sobald eine bestimmte Anzahl RCPT-Befehle vom Absender einer Nachricht übermittelt wurden. Die Funktion soll Spammer davon abhalten, über den Server unverlangte Massensendungen ("Spam") zu versenden. Die Methode fußt auf der Annahme, dass der Versuch, Massensendungen über den Server zu versenden, für Spammer unattraktiv wird, wenn der Versand jeder einzelnen Nachricht unverhältnismäßig lange Zeit in Anspruch nimmt, und dass Spammer solche Versuche aufgeben.

Graue Liste: Die Graue Liste ist eine Technik zur Bekämpfung von Spam. Sie nutzt die Tatsache, dass SMTP-Server die Zustellung von Nachrichten wiederholt, bei deren erstem Zustellversuch der Server des Empfängers den Fehlercode für einen vorübergehenden Fehler gemeldet hat (etwa „Bitte versuchen Sie es später erneut.“ oder „Please try again later.“). Wird diese Technik genutzt, und trifft eine Nachricht von einer Gegenstelle ein, die nicht bereits in einer Weißen Liste erfasst oder dem System bislang nicht bekannt war, so werden Absender und Empfänger der Nachricht und die IP-Adresse des zustellenden Servers protokolliert; danach wird die Nachricht während der SMTP-Übertragung unter Hinweis auf einen vorübergehenden Fehler abgewiesen. Versucht ein legitimer Absender etwas später die Zustellung erneut, so wird die Nachricht angenommen. Da Spamversender üblicherweise keine weiteren Zustellversuche unternehmen, kann die Graue Liste die Zahl der Spam-Nachrichten, die Ihre Benutzer erhalten, deutlich verringern.

HashCash: HashCash ist ein System zur Erstellung von "Arbeitsnachweisen", das zur Abwehr von Spam und von Denial-of-Service-Angriffen dient und in Form einer elektronischen Briefmarke verwirklicht ist. Mithilfe des HashCash-Systems kann MDAemon HashCash-Marken erstellen, die, bildlich gesprochen, mit Rechenzeit „bezahlt“ werden. HashCash-Marken werden in die Kopfzeilen abgehender Nachrichten eingefügt und sodann durch den E-Mail-Server des Empfängers geprüft, der sie anhand des Werts der Marken einstuft. Der Server des Empfängers geht dabei davon aus, dass mit Marken versehene Nachrichten wahrscheinlich seriös sind und daher nicht durch den Spam-Filter des Servers abgewiesen werden sollen.

LAN-IP-Adressen: In diesem Konfigurationsdialog tragen Sie die IP-Adressen ein, die über Ihr lokales Netzwerk (LAN) erreichbar sind. Datenverkehr mit den IP-Adressen wird wie lokaler Datenverkehr behandelt und von verschiedenen Sicherheitsmaßnahmen und Maßnahmen zur Spam-Abwehr ausgenommen.

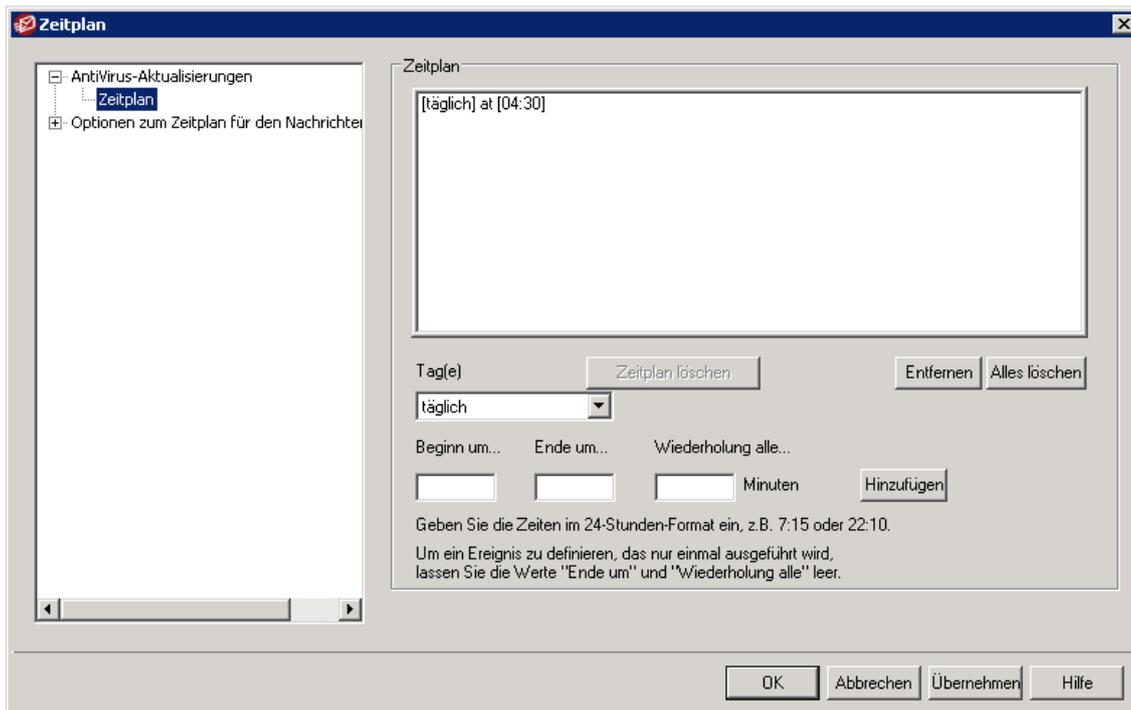
Nutzungsrichtlinien: Mit dieser Funktion werden Nutzungsbedingungen für das eigene System erstellt, die zu Beginn jeder SMTP-Verbindung an eine Gegenstelle übertragen werden, bevor diese mit der Postzustellung beginnt. Ein gängiges Beispiel für solche Nutzungsbedingungen ist der Hinweis „Relaisbetrieb ist auf diesem System gesperrt“.

Für nähere Informationen zur Konfiguration empfehlen wir das Handbuch, unsere Knowledge Base im Supportbereich unter <https://www.mdaemon.de>.

Grundinstallation von MDAemon AntiVirus

Die Installationsroutine von MDAemon installiert das Modul MDAemon AntiVirus automatisch mit, welches dann über die entsprechende Lizenz freigeschaltet werden kann.

Öffnen Sie MDAemon und wählen Sie im Menü „Sicherheit“ den Punkt „AntiVirus“. Wählen Sie im Reiter „AV-Aktualisierung“ den Button „Zeitplan“. Richten Sie hier einen Zeitplan zum Aktualisieren der Virendefinitionen ein. Wir empfehlen die Signaturen alle vier Stunden aktualisieren zu lassen.



Weitere Optionen und Ausnahmen im Virenschanner können bei Bedarf vorgenommen werden. Mit den Standard-Einstellungen werden sofort alle ein- und ausgehenden E-Mails, als auch die lokal versandten E-Mails überprüft.

Konfiguration der E-Mail-Anwendung auf der Arbeitsstation am Beispiel von Outlook

E-Mail-Konto mit MDAemon Connector

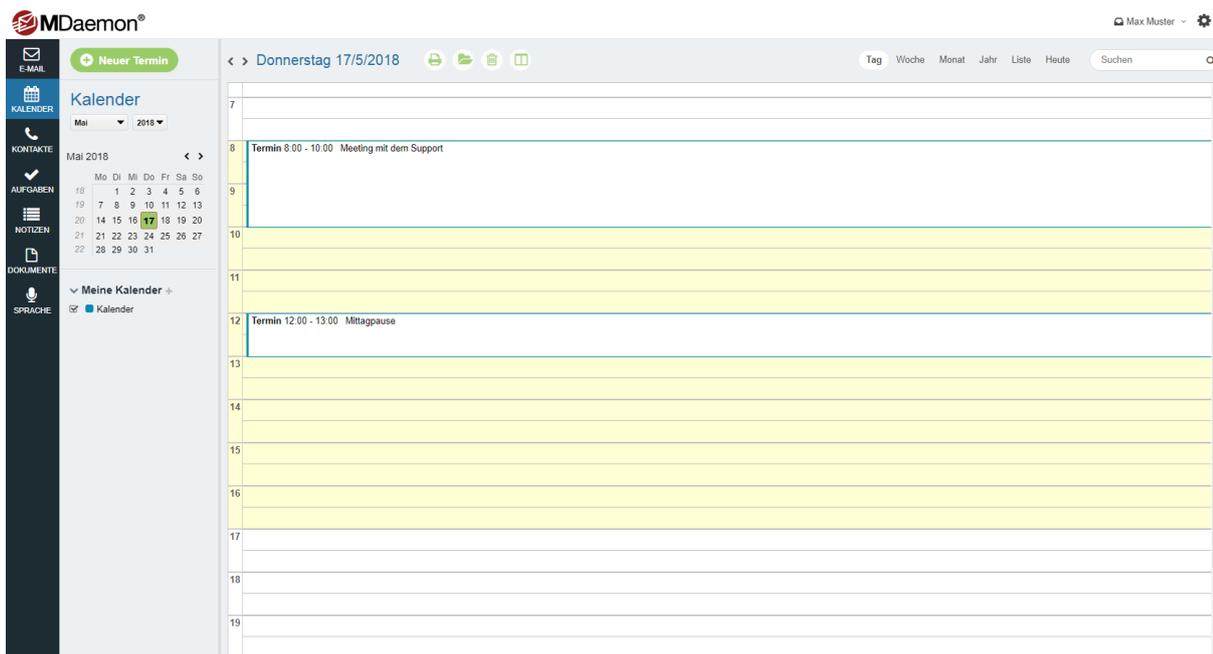
Mit der Installation des Add-ons MDAemon Connector erhalten Sie Zugriff auf nahezu alle Leistungsmerkmale im Bereich Groupware von Microsoft Outlook. Öffentliche Ordner, Kalender, Kontakte, Aufgaben und viele weitere Funktionen stehen Ihnen so zur Verfügung.

Eine umfassende Installationsanleitung für den MDAemon Connector finden Sie in unserem Downloadbereich unter <https://www.mdaemon.de/download.cfm>.

Webmail-Zugriff über MDAemon Webmail

MDaemon Webmail ist eine webgestützte Oberfläche, die den Benutzern alle E-Mail-Funktionen innerhalb ihres bevorzugten Web-Browsers bietet. Alle durch die Benutzer angelegten E-Mail-Ordner und gespeicherten Informationen liegen zentral auf dem Server.

MDaemon Webmail kann es dank seiner Benutzerfreundlichkeit leicht mit vielen bekannten E-Mail-Programmen aufnehmen und bietet zusätzlich den Vorteil, dass die Benutzer jederzeit und überall auf ihre gesamte E-Mail zugreifen können.



MDaemon Webmail kann über die Eingabe der IP-Adresse oder des Hostnamens des Mailervers und dem Port 3000 in Ihrem Webbrowser aufgerufen werden. Beispiel: <http://192.168.0.1:3000>. Sie können sich nun mit der eingerichteten E-Mail-Adresse und dem dazugehörigen Kennwort in dem Webmailer einloggen.

Tipp: Für einen sicheren Zugriff per HTTPS empfehlen wir Ihnen den Webserver von MDAemon unter HTTPS laufen zu lassen. Die Konfiguration dazu finden Sie unter „Einstellungen | Web- & IM-Dienste | Webmail | SSL & HTTPS“.

MDaemon Instant Messenger

Der MDAemon Instant Messenger ist ein sicheres Instant-Messaging-System, ein Adressbuch-Client und eine Anwendung für den Systray, die schnellen Zugriff auf die wichtigsten E-Mail-Funktionen von MDAemon Webmail bietet. Jeder Benutzer von MDAemon Webmail kann den MDAemon Instant Messenger selbst laden und auf dem lokalen Rechner installieren.

Key Features des MDAemon Instant Messenger

- installiert und konfiguriert sich selbst
- überwacht Ihr E-Mail-Konto auf eingehende Nachrichten
- hält Ihr lokales Windows-Adressbuch auf dem aktuellen Stand
- benachrichtigt Sie, sobald neue Nachrichten eingehen
- meldet Sie automatisch an und ruft Ihre E-Mails ab
- zeigt Ihnen auf einen Blick die Anzahl der Nachrichten je Ordner
- hilft Ihnen beim Verfassen neuer Nachrichten
- und vieles mehr...

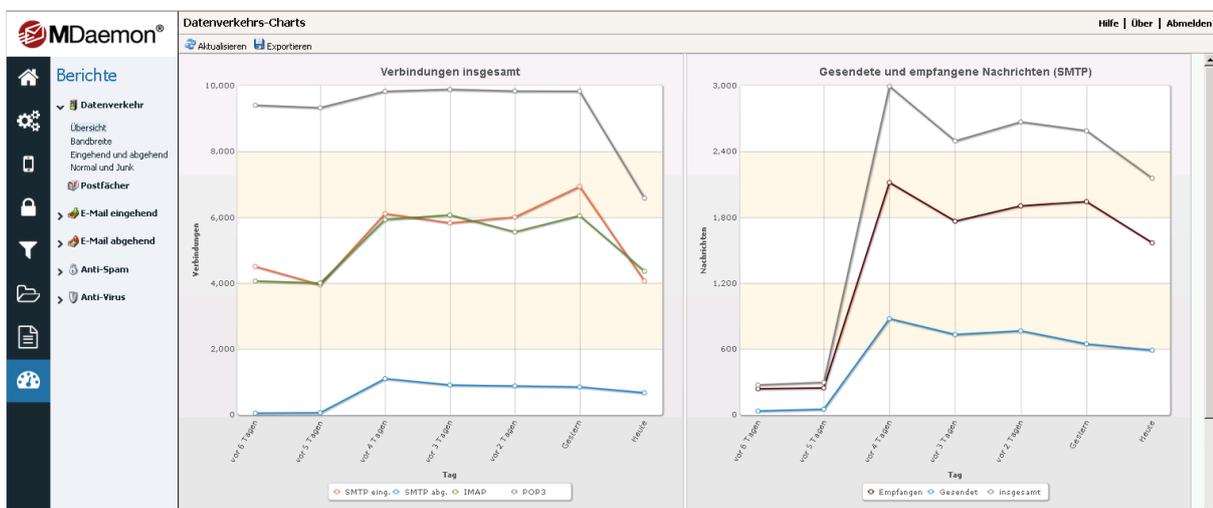
Und das alles über das Symbol in Ihrer Taskleiste. Loggen Sie sich in MDAemon Webmail ein und klicken Sie auf Optionen | MDAemon Instant Messenger, um das Tool auf der Arbeitsstation zu installieren.

Administration mit der Remoteverwaltung

Die Remoteverwaltung ist im Lieferumfang von MDAemon bereits enthalten und gestattet die webbasierte Fernwartung von MDAemon und dem integrierten webgestützten E-Mail-Client MDAemon Webmail.

Der Zugriff auf die Remoteverwaltung ist durch einen Webbrowser möglich, indem dort URL und Portnummer eingegeben werden, die der Remoteverwaltung zugewiesen sind (per Standard auf Port 1000). Gerade für den Zugriff aus dem Internet empfehlen wir Ihnen, parallel zur Konfiguration von MDAemon Webmail auch hier HTTPS zu verwenden.

Beispiel: <http://192.168.0.1:1000> oder <https://192.168.0.1:444>



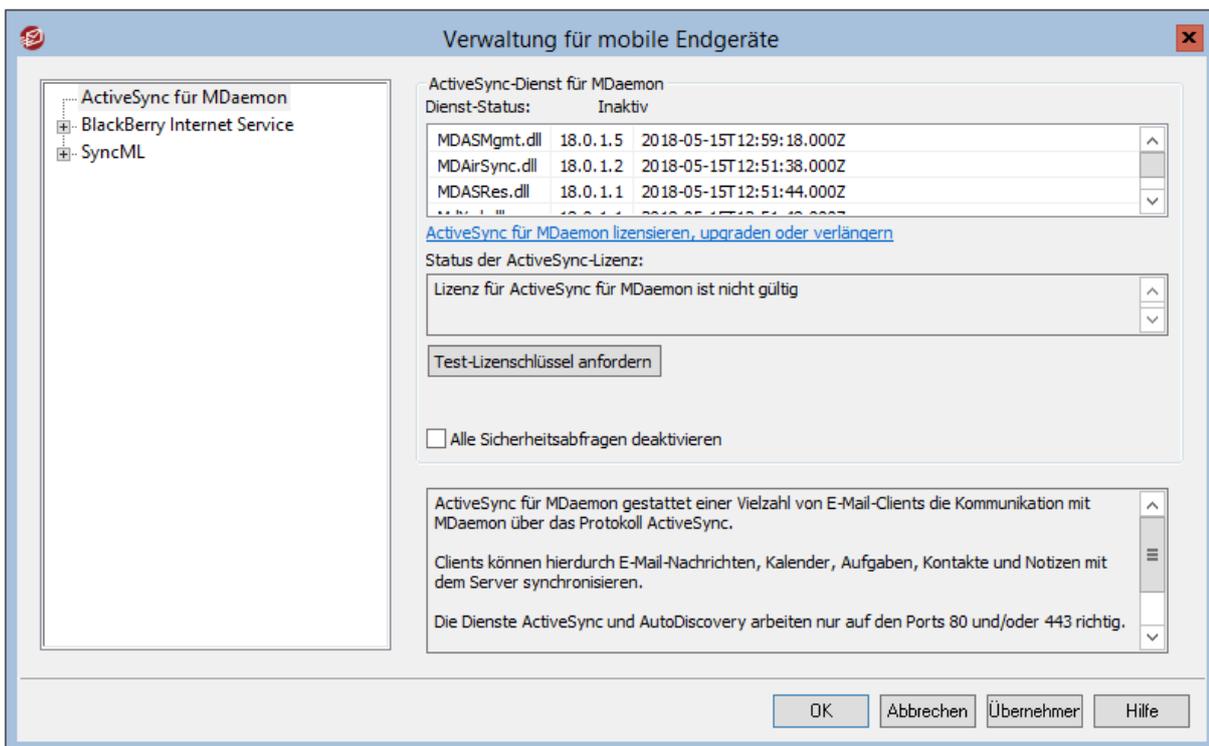
Nach der Benutzeranmeldung erhält der Benutzer Zugriff auf die verschiedenen Einstellungen von MDAemon. Art und Umfang der Einstellungen, auf die der Benutzer Zugriff erhält, richten sich nach seiner Zugriffsberechtigung. Es sind drei Zugriffsberechtigungen zu unterscheiden, die einem Benutzer zugewiesen werden können: Global, Domäne und Benutzer.

Weitere Informationen hierzu erhalten Sie im Handbuch.

Einrichtung von ActiveSync

Um ActiveSync nutzen zu können, müssen Sie erst den ActiveSync-Server aktivieren bzw. den Test-Lizenzschlüssel anfordern.

Diese Aktivierung können Sie im Menü unter „Einstellungen | Verwaltung für mobile Endgeräte | ActiveSync für MDAemon“ vornehmen. Bei der erstmaligen Aktivierung wird nach einem Klick auf „Test-Lizenzschlüssel anfordern“ die Testphase gestartet. Eine bereits gekaufte Lizenz kann auch über das Menü „Hilfe | MDAemon-Produkte registrieren“ eingetragen werden.



Der ActiveSync-Server in MDAemon (ab v13.x.x) synchronisiert Kalender und Kontakteinträge. Um die Aktivierung auf einem Smartphone vorzunehmen, nutzen Sie einfach das Setup für die Einrichtung eines Exchange-Kontos, das auf vielen Smartphones vorinstalliert ist. Whitepaper zu diesem Thema finden Sie in unserem Downloadbereich auf <https://www.mdaemon.de>.

Serviceleistungen

Ob Support, Consultings oder Vor-Ort-Installationen – wir sind für Sie da und stehen Ihnen mit unseren [Serviceleistungen](#) jederzeit zur Seite.

Support

Den Support für den deutschsprachigen europäischen Raum leistet die EBERTLANG Distribution GmbH, Garbenheimer Str. 36, 35578 Wetzlar.

Wir bieten:

- Ein deutsches Support-Team
- Kostenlosen Support per E-Mail (support@ebertlang.com)
- Attraktive Premium-Supportverträge mit
- flexiblen Laufzeiten
- telefonischer Unterstützung
- Fernwartung (z.B. per Teamviewer)
- garantierten Reaktionszeiten

Individuelle Schulung vor Ort

Gerne weisen wir Sie bei Ihnen vor Ort ein und erläutern Ihnen Ihr neues System in der Live-Umgebung. Im Rahmen einer Tagesschulung (zusätzliche Tage bei Bedarf beliebig zubuchbar) beantworten wir alle aufkommenden Fragen und gehen speziell auf Ihr individuelles Anwendungsszenario und Ihre Wünsche ein. Am Ende dieser Schulung ist Ihr System ideal eingerichtet und Sie administrieren dieses sicher im Tagesbetrieb.

Dienstleistungen

Sie wünschen eine Installation und Konfiguration durch einen Spezialisten unseres Hauses per Remote-Verbindung? Mit diesem Service-Produkt unterstützen wir Sie zwei Stunden lang bei der Einrichtung Ihres Systems. Eine Erläuterung und Demonstration des Systems rundet die Sitzung ab. Diese Einführung lässt sich individuell auf Ihre Anforderungen zuschneiden und kann beliebig verlängert werden.

Consulting und Audits

Im Rahmen eines Audits prüfen unsere Spezialisten Ihr System auf Herz und Nieren. Einer Live-Analyse per Fernwartung über 1 bis 1,5 Stunden schließt sich eine umfangreiche Auswertung Ihrer Installation und Konfiguration an, bei der wir neben der Analyse des Ist-Zustands auch detaillierte Empfehlungen aussprechen und einen individuell ausgearbeiteten Bericht zur Verfügung stellen.

Sie haben Interesse oder Fragen zu unseren Serviceleistungen? Informationen erhalten Sie auf unserer [Webseite](#), per E-Mail an sales@ebertlang.com oder telefonisch: +49 (0)6441 67118-0.

EBERTLANG Distribution GmbH
Garbenheimer Straße 36
D-35578 Wetzlar

 Tel.: +496441 67 11 80
Fax: +496441 67 11 8222

 Tel.: +43820 00 10 36

 Tel.: +4144 58 65 910

Allgemeine Informationen zu MDaemon finden Sie unter www.mdaemon.de.