Securepoint GmbH
Salzstraße 1, 21335 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

Securepoint UMA Emailarchivierung

Best Practice Guide UMA2.0

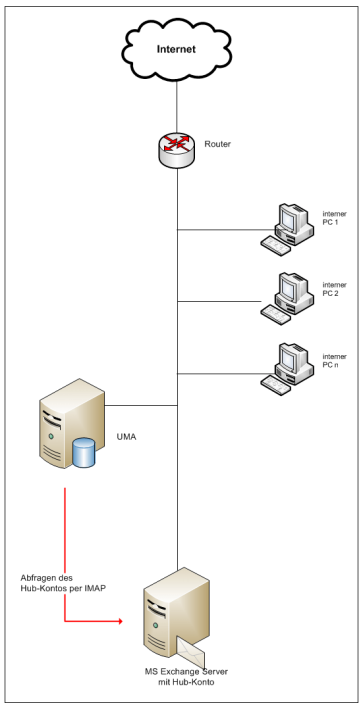
Stand: 12.08.2013

Inhalt

Positionierung des UMA im internen Netzwerk

Für die Einbindung der UMA Appliance in das bestehende Netzwerk gibt es verschiedene Möglichkeiten. Der Einsatz ist abhängig von der eingesetzten E-Mail Empfangs- und Versandtechnik.

Am häufigsten wird der sogenannte HUB-Modus verwendet, da hierfür die bestehende Netzwerkstruktur nicht verändert werden muss und dieser Modus als einziger in der Lage ist, auch E-Mails die andere Protokolle als POP3, IMAP oder SMTP nutzen (z.B. via Outlook über MAPI) zu archivieren.



Inbetriebnahme

Im Auslieferungszustand sind einige Einstellungen vorkonfiguriert. Dazu gehören z. B. die IP-Adresse und der Administrator Zugang.

Voreinstellungen:

IP-Adresse:	192.168.175.254
Subnetzmaske:	255.255.255.0
Benutzername:	admin
Passwort:	insecure

Verbinden Sie das UMA mit einem Stromanschluss und lassen Sie das Gerät hochfahren.

Anpassen der IP-Adresse

Um die Appliance in Ihrem bestehenden Netzwerk einzubinden, müssen Sie die IP-Adresse anpassen. Dazu haben Sie zwei Möglichkeiten: die „direkte Verbindung" und die „Netzwerkverbindung" über das Web-Interface.

Für die direkte Verbindung schließen Sie einen Monitor und eine Tastatur direkt an die Appliance an und konfigurieren diese, bevor Sie in das bestehende Netzwerk eingebunden wird.

Die direkte Verbindung mit Tastatur und Monitor dient nur dazu, die IP-Adresse temporär anzupassen und für den Netzwerk Einsatz vorzubereiten, ohne die IP-Adresse des Arbeitsplatz PCs zu wechseln.

Melden Sie sich mit dem vorkonfigurierten Administrator Account an:
login: admin
password: insecure

Sie sind jetzt als Benutzer mit eingeschränkten Superuser Rechten am System angemeldet.

In diesem Beispiel benutzen wir das Subnetz 192.168.100.0/24. Sinnvoll wäre, das Subnetz zu wählen, in dem sich auch der E-Mail-Server befindet.

Achten Sie darauf, dass die von Ihnen gewählte Netzwerk-IP für das UMA nicht schon von einem anderen Gerät ihres Netzwerkes genutzt wird.

Ändern Sie die IP-Adresse der UMA Appliance nun mit folgendem Befehl:

```
ip addr replace 192.168.100.254/24 dev bridge0
```

Achten Sie darauf, dass die so durchgeführte IP-Adressänderung nur temporär ist und nach einem Neustart wieder auf den Auslieferungszustand zurückgesetzt wird.
Zur permanenten Speicherung müssen Sie die IP-Adresse im Web-Interface ändern.

Anschließend verbinden Sie das UMA mit einem Netzwerk-Switch des Subnetzes.

Zugriff auf die Administrationsoberfläche

Die Konfiguration der UMA erfolgt über eine Weboberfläche, die mit einem Internetbrowser über eine Verschlüsselte Verbindung vorgenommen wird.

Nach dem Anschließen des UMA und der Anbindung an das Netzwerk über ein Patch-Kabel, öffnen Sie Ihren Internetbrowser (wir empfehlen Mozilla Firefox) und geben in das URL Eingabefeld die IP-Adresse inklusive Port des UMA ein:

```
https://192.168.100.254:11115
```

Da es sich um eine mit einem Zertifikat verschlüsselte Verbindung handelt, muss dieses mit „Ich kenne das Risiko", „Ausnahmen hinzufügen" und „Sicherheits-Ausnahmeregel bestätigen" bestätigt werden.

UMA-Administration-Center

Als nächstes sehen Sie das Login Fenster des UMA-Administration-Center. Benutzername und Passwort des UMA im Auslieferzustand ist:

Benutzername:	admin
Kennwort:	insecure

Nach einem Klick auf den Einloggen Button befinden sie sich im Status Fenster.

Lizenz importieren

Wechseln Sie in den Bereich Lizenz unter der Registerkarte Setup.

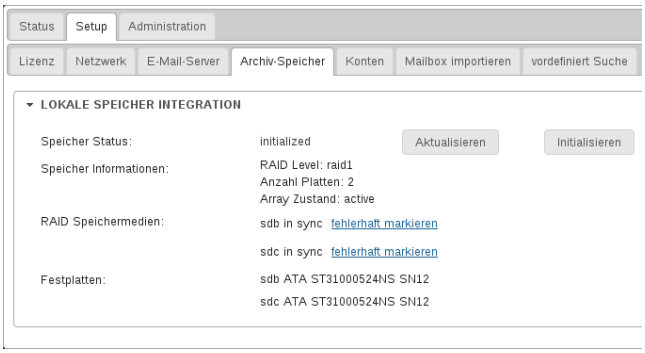
Klicken Sie auf Datei auswählen und wählen Sie im Dateifenster die Lizenzdatei vom Dateisystem Ihres Rechners.

Klicken Sie dann im Webinterface auf den Button Registrieren

Sollte Ihnen noch keine Lizenz-Datei vorliegen, erhalten Sie diese im Securepoint Registrierungsportal unter my.securepoint.de

Storage initialisieren

Wechseln Sie im Register „Setup" auf „Archiv-Speicher". Hier werden die Festplatten auf den weiteren Gebrauch vorbereitet.

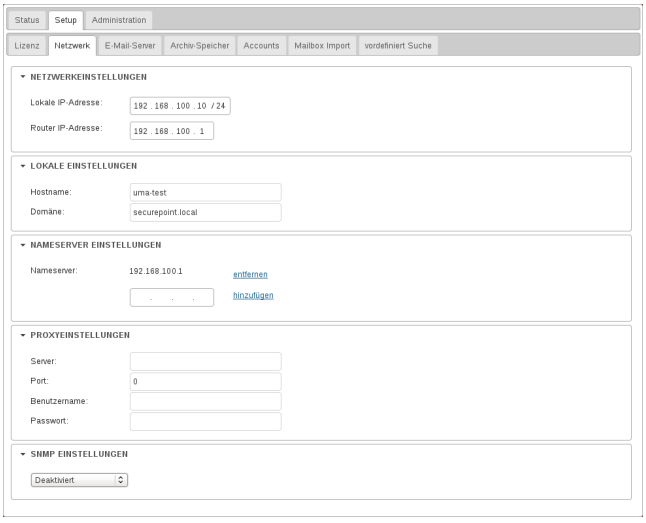


Sollte eine Initialisierung des Archiv Storage noch nicht stattgefunden haben, klicken Sie auf Initialisieren und warten Sie bis dieser Vorgang abgeschlossen ist.
Bei einer Appliance mit Software-RAID, wird das korrekte RAID-Level automatisch gewählt.

Bei vorhandenem Hardware RAID-Controller sind die Festplatten auf diesem schon konfiguriert und werden daher nur als eine Festplatte angezeigt.

IP-Adresse, Gateway, DNS und Domain anpassen

Um die IP-Adressen anzupassen, wechseln Sie unter „Setup" in den Bereich „Netzwerk".
Hier passen Sie die IP-Adresse des UMA an Ihr lokales Subnetz an und tragen die IP-Adresse der Firewall als Router IP-Adresse ein.



Im Anschluss wird das UMA neu gestartet und ist dann unter der neuen IP im Netz erreichbar.

Im Abschnitt „Lokale Einstellungen" tragen Sie den Hostnamen des UMA und die lokale Domain ein.

Sollte die Firewall in Ihrem Netzwerk auch als Nameserver dienen, tragen Sie diese IP in das entsprechende Feld im Bereich „Nameserver Einstellungen" ein. Ansonsten wählen Sie die IP des DNS-Servers ihres Netzwerkes.

Benutzer Konten

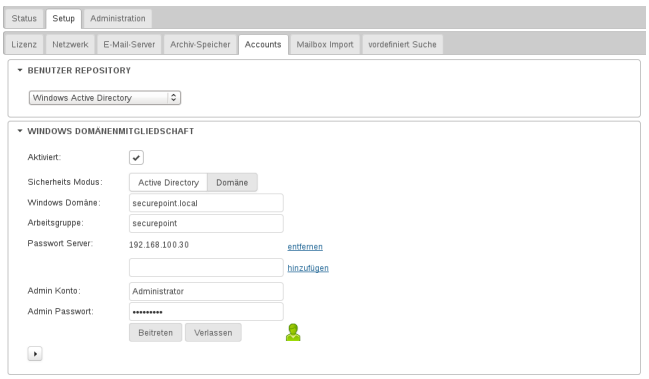
Als nächstes stellen Sie ein, welche E-Mail-Benutzerkonten von dem UMA System verwaltet werden und von welcher Quelle die Konteninformationen bezogen werden.

Als Quellen stehen zur Verfügung:

- Active Directory
- andere LDAP Server
- lokale Nutzer-Liste

ActiveDirectory Anbindung

Wechseln Sie unter „Setup" in den Bereich „Accounts" und wählen Sie im Abschnitt „Benutzer Repository" den Eintrag „Windows Active Directory" aus.
Setzen Sie im Abschnitt „Windows Domänenmitgliedschaft" den Haken auf „Aktiviert" und tragen Sie die lokale Windows Domäne, die Arbeitsgruppe, die Domänen-Server-IP ein. Geben Sie weiterhin den Namen des Administrator Kontos und das zugehörige Passwort an um die Appliance in die lokale Domäne einzubinden.

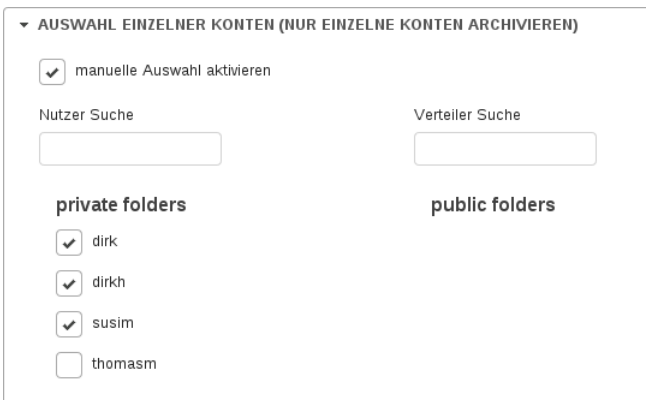


Nach dem Klick auf den Button Beitreten zeigt ein grünes Symbol das erfolgreiche Anmelden des UMA an der Domäne.

Auswahl einzelner Konten

Achten Sie bei Nutzung eines Authentifizierungs-Dienstes wie Active Directory darauf, welche E-Mail Konten wirklich archiviert werden müssen.

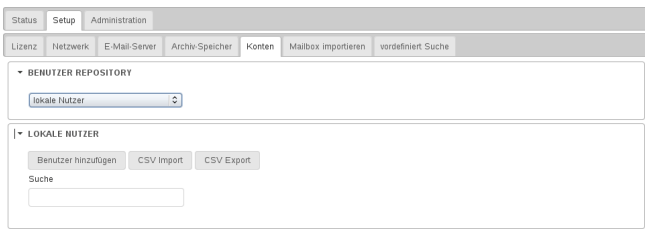
Im Abschnitt "Auswahl Einzelner Konten" haben Sie hierzu die Möglichkeit durch aktivieren des Feldes "manuelle Auswahl aktivieren" die zu archivierenden Konten genau zu selektieren und damit sehr viel "Lizenzschonender" zu arbeiten.



Lokale Nutzer-Liste

Sollten Sie keinen Authentifizierungs-Server betreiben, können Sie auch lokal eine Benutzerliste hinterlegen.

Hierzu haben sie entweder die Möglichkeit diese über den Button Benutzer hinzufügen einzeln anzulegen oder über den Button CSV Import eine Liste im CSV-Format zu importieren.



Der Inhalt der .csv Datei muss folgendes Format haben:

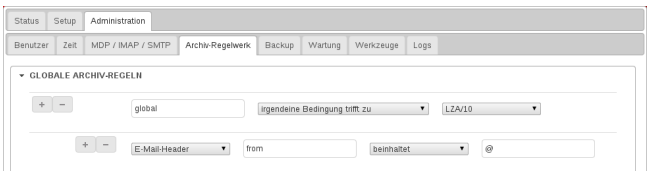
```
userid,password,firstname,lastname,email,optionalemail
```

Um diese zu importieren klicken Sie auf Durchsuchen... und, nachdem Sie eine entsprechende Datei ausgewählt haben, den Button Importieren

Anschließend werden die Nutzer im Abschnitt "Lokale Nutzer" angezeigt.

Globales Archivregelwerk

Um sicher zu gehen dass alle E-Mails archiviert werden ist es sinnvoll eine globale Archivregel zu erstellen.



Wechseln Sie dazu unter Administration in den Bereich Archiv-Regelwerk. Geben Sie in das erste Feld den Regel-Namen ein, wählen Sie „irgendeine Bedingung trifft zu" und das Langzeitarchiv für 10 Jahre „LZA/10„.

Als nächstes bestimmen Sie in der Regel, dass jede Quelladresse im E-Mail Header die ein @ beinhaltet Archiviert werden soll:

```
E-Mail-Header > from > beinhaltet > @
```

Einrichtung des Hub-Kontos

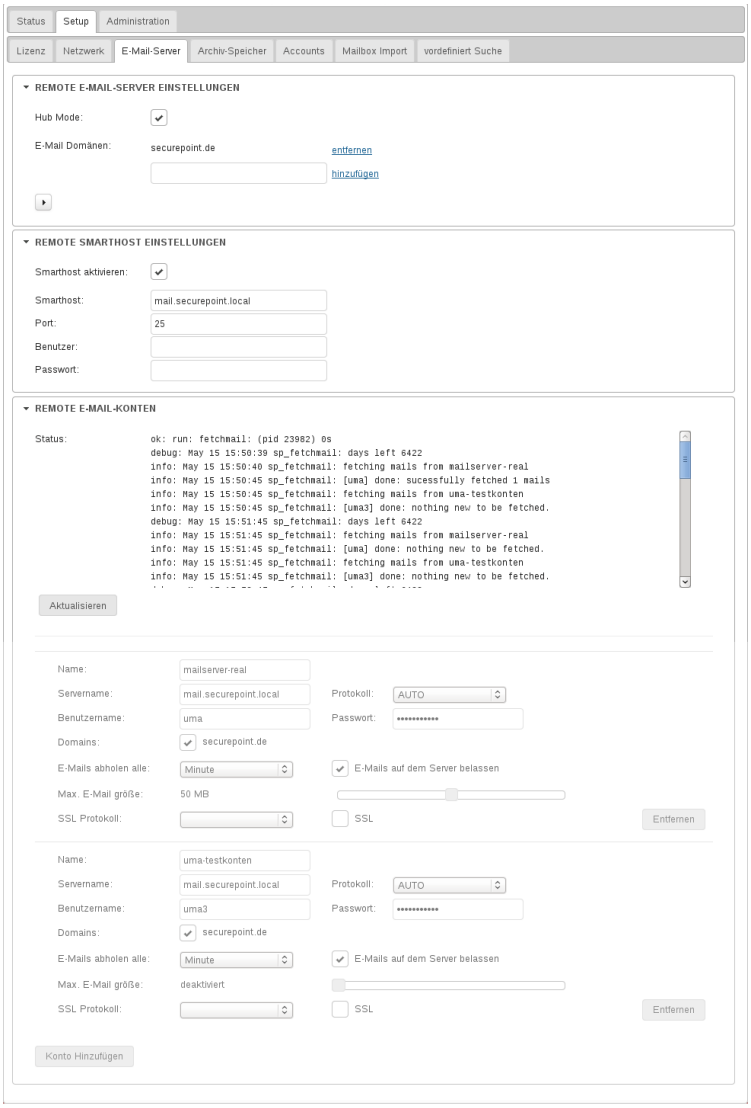
Einstellungen des UMA

Unter „Setup" im Bereich „E-Mail-Server" aktivieren Sie im Abschnitt „Remote E-Mailserver Einstellungen" den Hub Mode und tragen die E-Mail Domäne ein.

Nach einem Klick auf „Konto Hinzufügen" in dem Abschnitt „Remote E-Mail-Konten" öffnet sich eine Maske in der nun Angaben zum Mailserver erfolgen müssen.
Zu den Angaben der Mail-Server, Login des HUB-Kontos sowie das zu verwendende Protokoll (Automatische Auswahl, POP oder IMAP) müssen auch die Haken bei der zuvor angelegten Domain gesetzt werden.
Mit dieser Einstellung wird festgelegt welche Mails aus dem Konto des E-Mailservers abgeholt werden sollen.

Weiterhin können Sie festlegen, wie häufig der Abruf der Mails erfolgen soll und wie groß die E-Mail Maximal sein darf.

Nach dem Speichern der Einstellungen wird unter „Status" der interne Mailserver angezeigt.



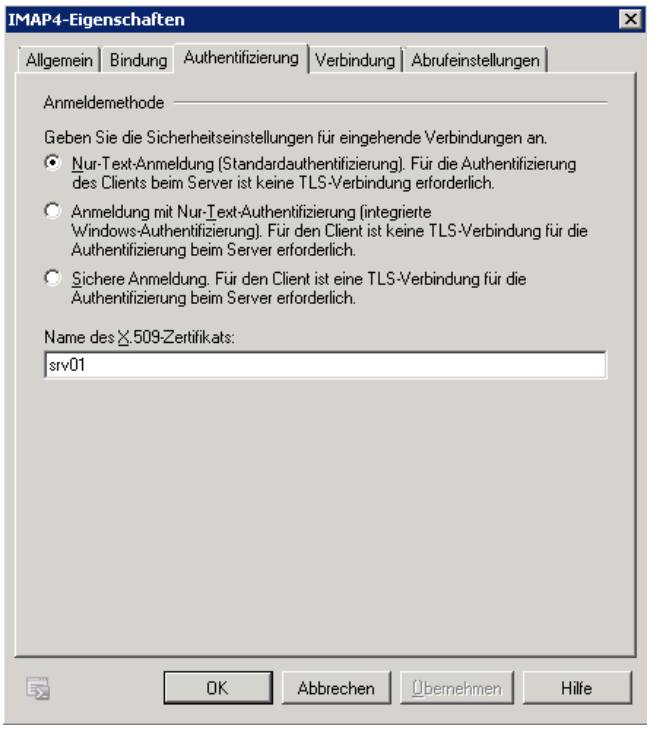
Anpassung des Exchange-Server für den HUB Modus des UMA

Für den HUB-Betrieb des UMA muss auf dem Exchange-Server ein dafür erforderliches HUB-Konto angelegt werden.
Alle Mails die den Mailserver passieren, eingehende sowie ausgehende, sollen so in das HUB-Konto kopiert werden damit das UMA diese dann von dem Konto via IMAP abholen und archivieren kann.

Diese Konfigurationen werden direkt am Mailserver durchgeführt.
Dieser Abschnitt bietet nur einen kurzen Überblick. Für weitergehende Informationen lesen Sie die MS Exchange Dokumentation.
Die Bildschirmaufnahmen wurden in einem MS Small Business Server 2008 System angefertigt.

Authentifizierungsmethode des IMAP Servers einstellen

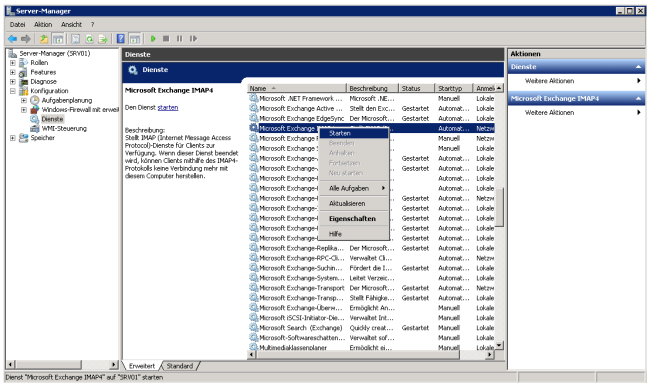
Zur Anmeldung muss die „Nur-Text-Anmeldung" ohne TLS Verbindung aktiviert werden. Standardmäßig ist die „Sichere Anmeldung" eingestellt.



Öffnen Sie die Exchange-Verwaltungskonsole.
Wählen Sie im Menüpunkt Serverkonfiguration den Eintrag Client Access.
Wählen Sie den Reiter POP3 und IMAP4.
Klicken Sie hier mit der rechten Maustaste auf IMAP4.
Wechseln Sie zur Registerkarte Authentifizierung und wählen Sie den obersten Eintrag aus. Nur-Text-Anmeldung (Standardauthentifizierung)

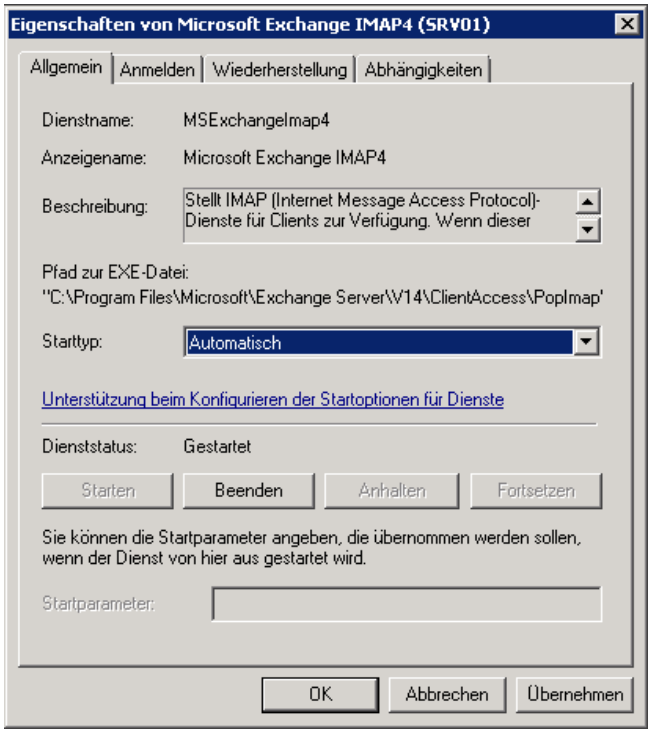
Starttyp des Dienst ändern

Der Dienst muss zur Übernahme der Änderung der Authentifizierungsmethode neu gestartet werden. Außerdem soll der Dienst automatisch gestartet werden.



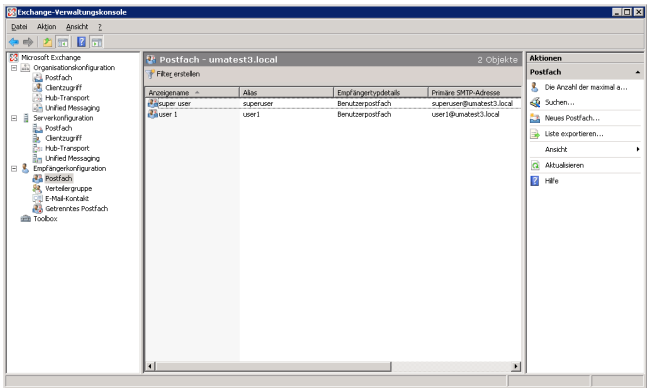
Öffnen Sie den Server-Manager.
Wählen Sie den Menüpunkt Konfiguration und hier den Untereintrag Dienste.
Wählen Sie aus der Liste den Eintrag Microsoft Exchange IMAP4. Öffnen Sie das Kontextmenü mit Klicken der rechten Maustaste auf diesen Eintrag.
Klicken Sie auf den Eintrag Starten, um den Dienst zu Starten.

Aktivieren Sie nochmals das Kontextmenü des Eintrags Microsoft Exchange IMAP4. Klicken Sie diesmal auf den Eintrag Eigenschaften.
Auf der Registerkarte Allgemein wählen sie im Dropdownmenü Starttyp den Eintrag Automatisch aus.
Klicken Sie auf OK.

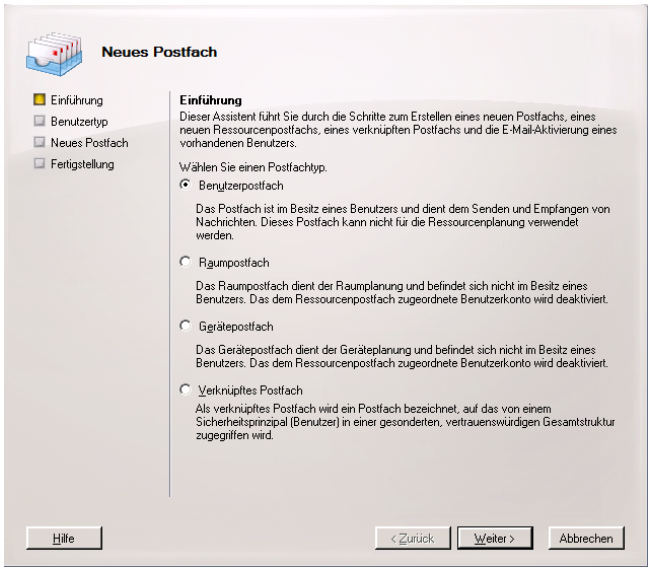


Anlegen des Postfaches
Als nächstes muss auf der Verwaltungskonsole des Exchange unter der Spalte „Aktion" ein neues Postfach hinzugefügt werden.

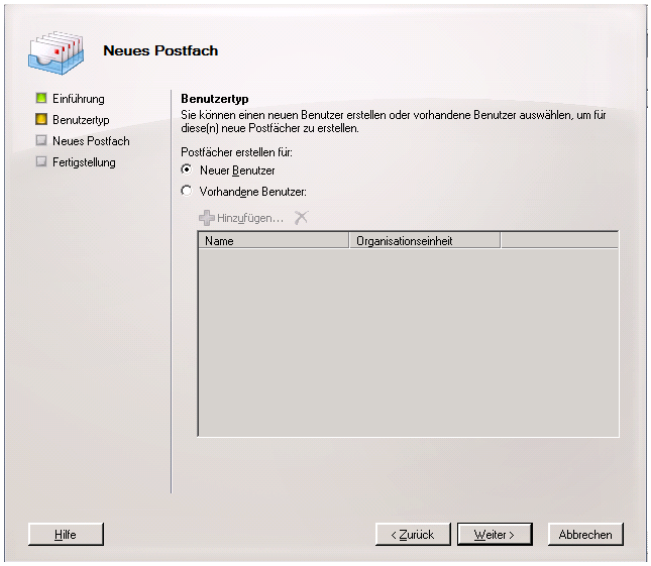
Dazu öffnen Sie in der Administrationsoberfläche Ihres Server Systems die Exchange Verwaltungskonsole. Klicken Sie im rechten Fensterbereich Aktionen auf den Eintrag Neues Postfach



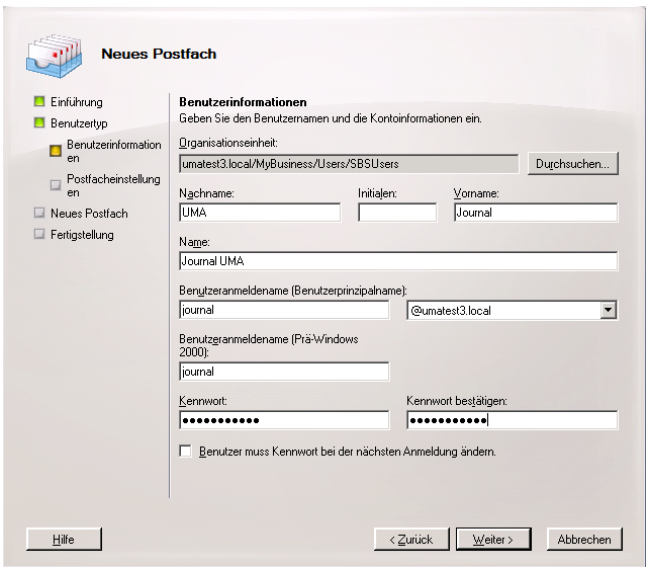
In dem folgenden Assistenten wählen Sie als Postfachtyp „Benutzerpostfach" und klicken auf Weiter.



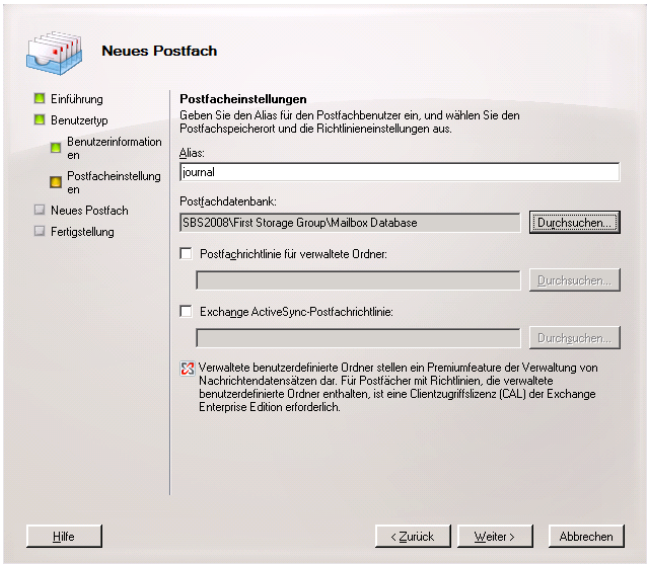
Als Benutzertyp wählen Sie "Neuer Benutzer" aus und klicken auf Weiter.



Nach Auswahl der Organisationseinheit für diesen Benutzer mit dem Button "Durchsuchen", werden die erforderlichen Werte „Nachname, Vorname, Name, Benutzeranmeldename sowie das Kennwort" eingetragen.

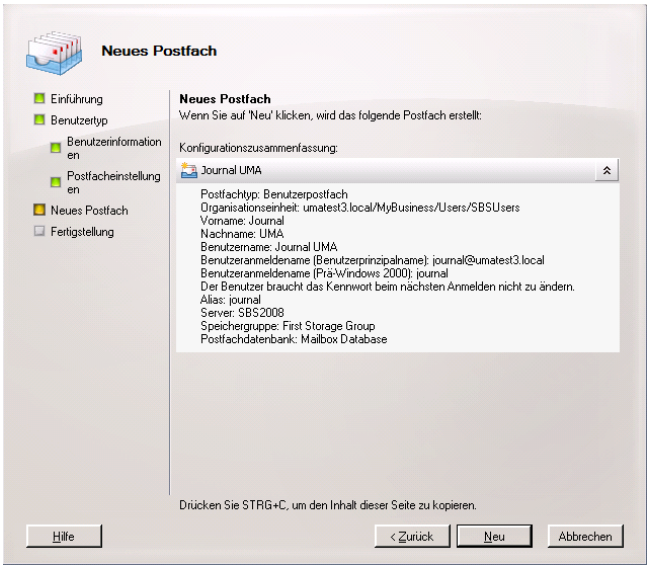


Wechseln sie zu dem Punkt Postfacheinstellungen, tragen sie noch einen Alias ein, wählen sie im Feld "Postfachdatenbank" den Speicherort des Postfachs und klicken sie auf Weiter.

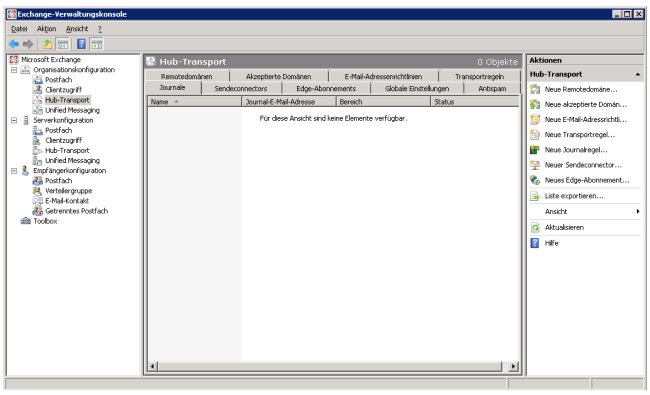


Der letzte Dialog fasst noch einmal die Eigenschaften des anzulegenden Postfaches zusammen.

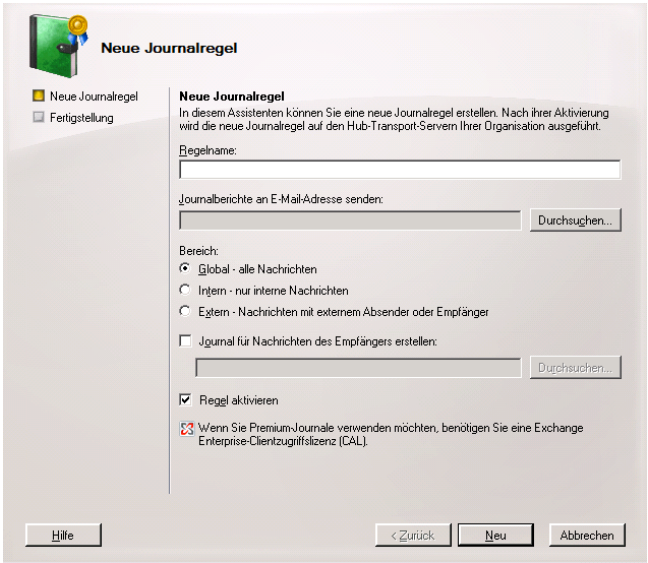
Nach Überprüfung der Eigenschaften und der Bestätigung mit einem Klick auf den Button „Neu“, ist das Anlegen des Postfaches abgeschlossen.

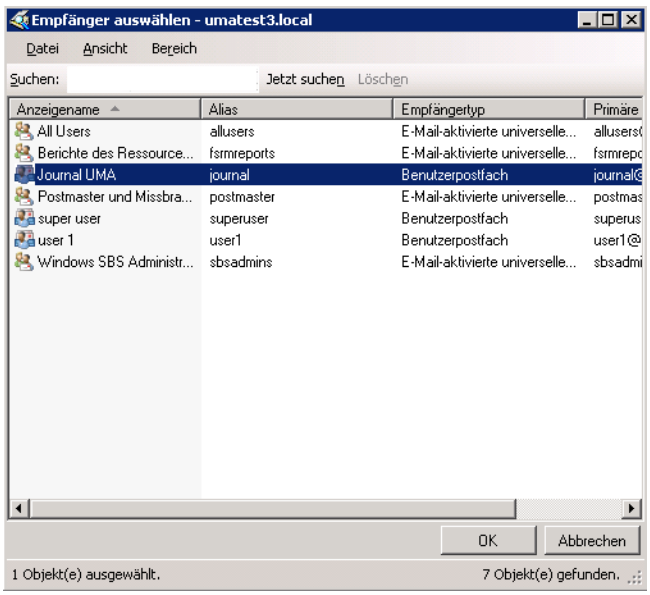


Hinzufügen einer neuen Journalregel
Wieder auf der Exchange Verwaltungskonsole, muss nach dem Anlegen des Postfaches eine neue Journalregel erstellt werden.
Dazu wählen Sie unter "Organisationskonfiguration" den Eintrag "Hub-Transport" und anschließen im Aktionsfenster auf der rechten Seite die Aktion "Neue Journalregel".

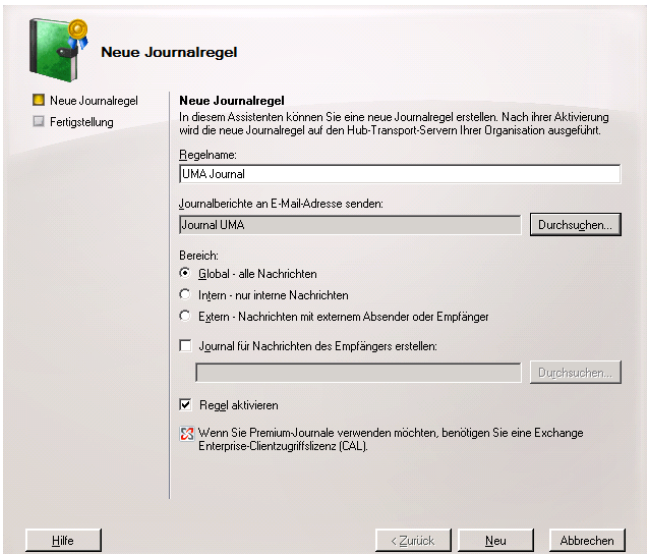


Im Dialog „Neue Journalregel" geben Sie zuerst einen Regelnamen an, anschließend wählen Sie im Feld „Journalberichte an E-Mail-Adresse senden", den zuvor neu angelegte Benutzer aus.

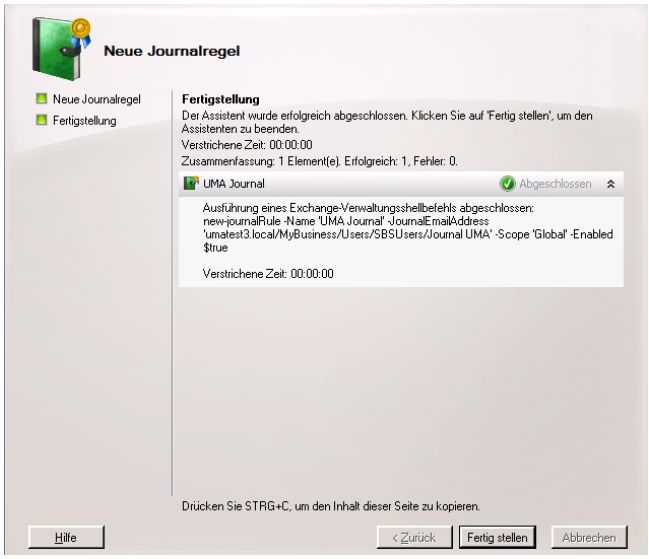




Unter „Bereich" wird der Punkt „Global – alle Nachrichten" ausgewählt und der Haken bei „Regel aktivieren" gesetzt.



Im letzten Fenster werden noch einmal alle Einstellungen zusammengefasst.



Nach dem Kontrollieren und dem Klick auf Fertigstellen ist das Hinzufügen der Journalregel abgeschlossen.

Diese Regel besagt, dass alle Nachrichten/Mails in das neu angelegte Postfach kopiert werden, wo sie nun von dem UMA via IMAP abgeholt werden können.

Abschließend kopieren Sie alle bisher auf dem Mailserver gespeicherten Mails in das HUB-Konto, damit diese im Anschluss an die UMA-Anbindung von dem UMA abgeholt und archiviert werden können.

Einrichtung des Backup

Sie können das gesamte System entweder auf einem Netzwerkspeicher oder auf ein externes Speichermedium sichern. Externe Speichermedien werden über einen USB Anschluss an die Appliance angeschlossen. Es werden externe Festplatten und Flash Speichermedien unterstützt.

Backup Device

Zunächst definieren Sie im Abschnitt „Backup Devices" das oder die Geräte auf denen die Backups gesichert werden sollen.

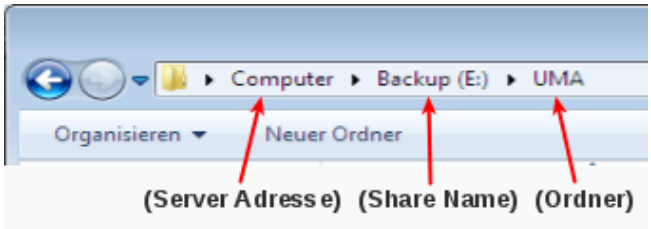
Tragen Sie einen Namen für das Gerät ein und wählen Sie den Typ Ihres Netzwerkspeichers aus. Zur Verfügung stehen:

- Windows-Share
- FTP
- SSH
- iSCSI
- USB

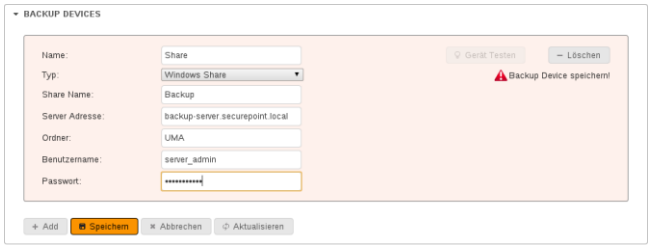
In Abhängigkeit des gewählten Typs ändern sich die Eingabefelder der Maske.

Windows Share

Sehr häufig wird Windows Share verwendet. Achten Sie dabei darauf den korrekten Share Name einzutragen. Dieses soll die nebenstehende Abbildung verdeutlichen.



Sollten Sie keinen Ordner auf dem Laufwerk eingerichtet haben, tragen Sie im Eingabefeld Ordner folgendes ein:



Wichtig ist weiterhin die Eingabe des Benutzernamens und Passwort des Backup Server.

Nachdem alle benötigten Daten eingetragen sind klicken Sie auf Speichern und zum Testen der Speicherverbindung auf Gerät Testen

Wenn alles funktioniert, legen Sie mit + Add einen weiteren Backup-Speicher an oder wechseln in den Abschnitt „Backup Jobs".

iSCSI
Sehr interessant ist die Kombination von iSCSI mit dem Sicherungsformat Time Machine.

Bei Time Machine" handelt es sich um inkrementelle Backups, welche weniger Speicherplatz benötigen.

Wählen Sie als Typ einfach „iSCSI" aus, tragen Sie die Server Adresse ein und klicken Sie auf Registrieren

Nach erfolgreicher Registrierung wir Ihnen die UUID des Laufwerkes und das aktuelle Speicher-Ziel angezeigt.

Um ein anderes Ziel auszuwählen, wählen Sie aus der Drop Down Liste unter „iSCSI Ziel" ein Ziel aus und klicken auf Ziel ändern

Abschließend klicken Sie auf Speichern

Backup Job
Im Abschnitt „Backup Jobs" werden regelmäßige Sicherungsläufe erstellt, die automatisch ausgeführt werden.

Backup Job mit Windows Share und tar
Auch hier tragen Sie zuerst den Namen des Jobs ein und wählen dann eines der von Ihnen angelegten Speicher aus.
Anschließend definieren Sie den Zeitplan dieses Jobs und die Anzahl der Backups.

Die Anzahl der Backups legt fest wie viele Backups vorgehalten werden.

Wenn Sie Null wählen, ist die Anzahl der vorgehaltenen Backups unbegrenzt.

Als Sicherungsformat steht ihnen bei Windows Share nur „tar" zur Verfügung.

Backup Job mit Time Machine
Achten Sie darauf, dass das Sicherungsformat Time-Machine aufgrund der verwendeten Hardlinks nur in Verbindung mit iSCSI und USB einsetzbar ist.

Manuelles Backup erstellen
Neben den automatisierten Backups, gibt es natürlich auch die Möglichkeit ein Backup "per Knopfdruck" zu erstellen. Dazu wechseln Sie einfach in den entsprechenden Backup Job und klicken auf Backup erstellen

Backup wiederherstellen

Das wiederherstellen eines Backup ist ausschließlich mit der Konfiguration möglich, die während des Backup-Laufes aktiv war, da das Backup von der Konfigurations-ID abhängig ist.

Konfiguration Exportieren
Wechseln Sie unter Administration in den Bereich Wartung und klicken sie im Abschnitt "Konfiguration Import/Export" auf Exportieren . Dieser wechselt daraufhin auf Download und nach einem wiederholten Klick auf diesen Button, öffnet sich das Browser Downloadfenster und Sie können die Datei auf ihrem PC abspeichern.

Wiederherstellen eines Backup
Da die Backup Jobs verschiedene Formate und /oder verschiedene Speicherorte haben, ist die Wiederherstellungsfunktion bei den einzelnen Jobs eingefügt.

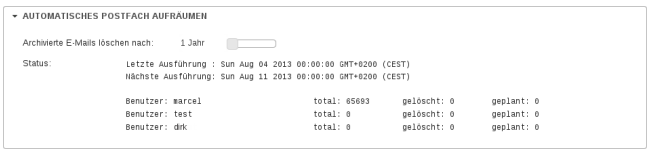
Zur Wiederherstellung der Daten aus einem Backup wählen Sie aus der Dropdownmenü ein Backup aus. Die Bezeichnung der Backups setzt sich wie folgt zusammen:
uma-backup-JJJJ-MM-TTTSS-MM-ssZ+ZZV.tar.gz

JJJJ Jahr vierstellig
MM Monat zweistellig
TT Tag zweistellig
Das hierauf folgende **T** steht für Tag.
SS Stunde zweistellig
MM Minute zweistellig
ss Sekunden zweistellig
Das hierauf folgende **Z** steht für Zeit.
ZZV Zeitzonenverschiebung vierstellig
Das Vorzeichen (+/-) zeigt an, ob die angezeigten Stunden zur Koordinierten Weltzeit (UTC) addiert werden oder von dieser subtrahiert werden.

Die Schaltfläche Aktualisieren aktualisiert die Auflistung der Backups und mit einem Klick auf wiederherstellen wird die Wiederherstellung gestartet.

Wartung

Automatisches Postfach Aufräumen



Im Bereich Wartung finden Sie ebenfalls die Möglichkeit einzustellen, wann die Mails aus den Inboxen der Benutzerkonten gelöscht werden sollen.

Alle bis dahin nicht in die Langzeitarchive kopierten E-Mails die sich auf dem UMA befinden, werden ebenfalls gelöscht.

Unter Status wird das Datum der Letzten und der Nächsten Ausführung angezeigt, sowie die Mailboxen die bereinigt wurden.

Langzeitarchiv und nicht Archivierte E-Mails

Im Abschnitt Langzeitarchiv der Wartung wir ein Status ausgegeben, dass demnächst eine Löschung von E-Mails aus den Langzeitarchiven bevor steht und wie viele E-Mails davon betroffen sind.
Es werden nur die E-Mails gelöscht, die eine gewisse Vorhaltezeit überschritten haben.

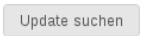
Ist die Langzeitarchivierung überschritten, werden die E-Mails noch vorgehalten, bevor sie endgültig gelöscht werden. Die Vorhaltezeit kann über einen dann eingeblendeten Schieberegler von 180 bis 365 Tagen gewählt werden.

Im Abschnitt "Aufgrund von Fehlern nicht archivierte E-Mails" können Sie bei E-Mails die als fehlerhaft markiert sind, die Signaturen und Dateianhänge prüfen lassen und die Archivierung mit einem Klick auf den Button 

wiederholen.

Firmware Version

Um den Firmware Version einzusehen, schauen Sie unter Wartung einfach in den Abschnitt "Firmware Version". Hier werden Ihnen die aktive und gegebenenfalls die vorher installierte Version als "Verfügbare Version" angezeigt.

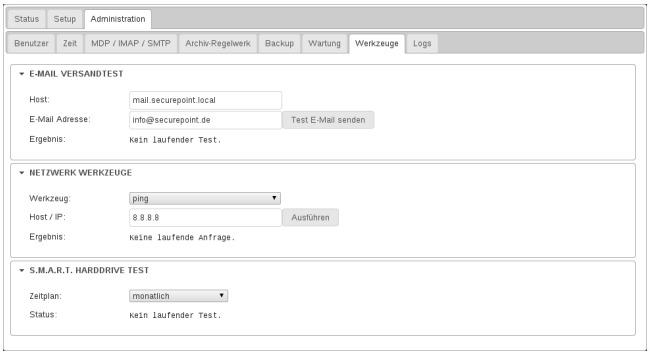
Um zu überprüfen, ob einen neue Version des UMA vorhanden ist, klicken Sie einfach auf 

Weiterhin ist es möglich, nach einem Firmware-Update wieder auf die vorher auf dieser Maschine installierte Version zu wechseln. Diese Version wird Ihnen als "Verfügbare Version" angezeigt und mit einem Klick auf 

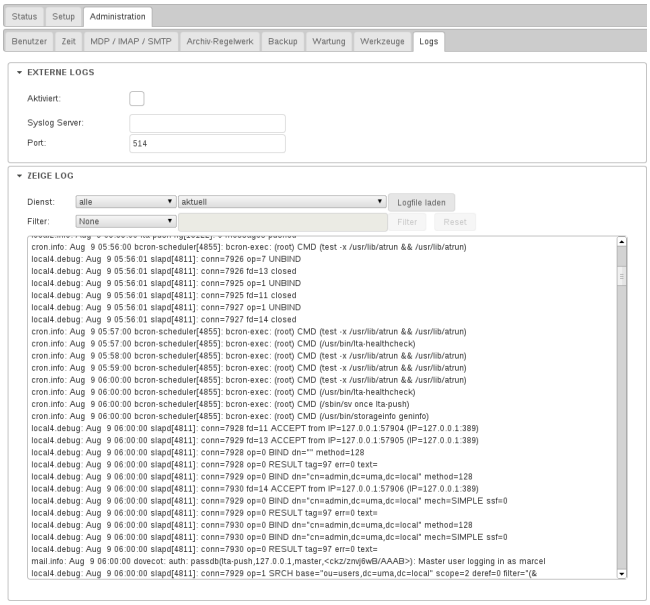
wieder aktiviert.

Und wenn es mal klemmt ...

Natürlich bietet das UMA im Bereich Werkzeuge auch einen kleinen "Werkzeugkasten", um zu überprüfen ob E-Mails Versendet werden, das Netzwerk erreichbar ist oder die Festplatten zu testen.



Weiterhin bringt ein Blick in die Log-Dateien häufig den Ansatz, an welcher Stelle zu suchen ist, wenn nicht alles so läuft, wie gewünscht.



Weitere Informationen und Hilfe zum UMA und anderen Produkten der Securepoint GmbH finden Sie unter http://wiki.securepoint.de