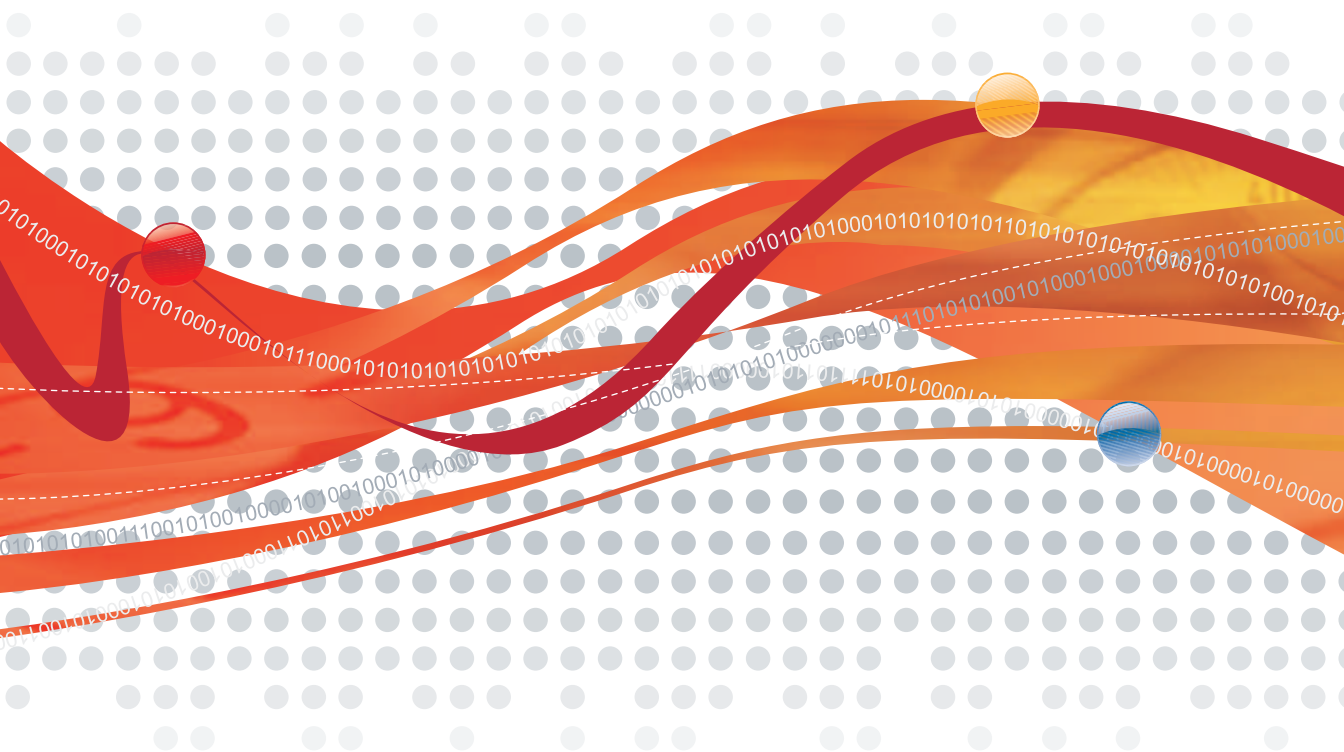
TREND MICRO™

Hosted Email Security

Hosted Service mit integriertem Schutz vor E-Mail-Bedrohungen

Web-Services-Handbuch



Messaging Security

Dokumenten-Nr. HSEM04284_91229

Veröffentlichungsdatum: 18.03.10

Geschützt durch die US-Patent-Nr. 5.623.600, 5.951.698, 5.983.348, 6.272.641

Im Benutzerhandbuch für Trend Micro™ Hosted Email Security sind die wesentlichen Funktionen der Software und Installationsanweisungen für Ihre Produktionsumgebung erläutert. Lesen Sie das Handbuch vor der Installation oder Verwendung der Software aufmerksam durch.

Ausführliche Informationen zur Verwendung bestimmter Funktionen der Software finden Sie in der Online-Hilfe und in der Knowledge Base auf der Trend Micro Website.

Das Trend Micro Team ist stets bemüht, die Dokumentation zu verbessern. Ihre Meinung ist uns wichtig. Bewerten Sie diese Dokumentation auf der folgenden Site:

http://www.trendmicro.com/download/documentation/rating.asp

Inhalt

Vorwort

Kapitel 1: Den Hosted Email Security Web-Services-Client installieren

Kapitel 2: Den Hosted Email Security Web-Services-Client verwenden

Kapitel 3: Fehlerbehebung

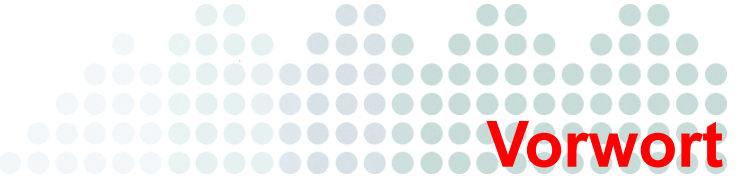
Anhang A: Hosted Email Security Web-Services-Anwendungen

Anhang B: Die Achitektur des ActiveDirectory Sync Clients

Anhang C: Installation und Konfiguration des ActiveDirectory Sync Clients

Anhang D: Hosted Email Security Web-Services Befehlszeilen-Referenz und -Programmierhandbuch

Abbildungsverzeichnis



Vorwort

Willkommen im *Trend Micro™ Hosted Email Security Web-Services-Handbuch*. Dieses Handbuch enthält Informationen zur Automatisierung administrativer Aufgaben in Hosted Email Security.

In diesem Vorwort werden die folgenden Themen erläutert:

Hosted Email SecurityDokumentation

Die Trend Micro™ Hosted Email Security Dokumentation umfasst die folgenden Komponenten:

Online-Hilfe – Hier finden Sie Informationen zur Konfiguration aller Funktionen über die Benutzeroberfläche. Der Zugriff auf die Online-Hilfe erfolgt über die Webkonsole durch Klicken auf das Hilfe-Symbol ().

Schnellstartanleitung – Damit können Sie Ihren Service schnell einrichten.

Administratorhandbuch – Hier finden Sie Informationen zur Verteilung und Konfiguration der Serviceeinstellungen.

Web-Services-Handbuch – Bietet Unterstützung bei der Automatisierung administrativer Aufgaben in Hosted Email Security.

Web EUQ Endbenutzerhandbuch – Bietet Unterstützung bei der Verwaltung von Spam-Mails in Quarantäne mit der Web End User Quarantine von Trend Micro.

Das ***Administratorhandbuch*** und das ***Web EUQ Endbenutzerhandbuch*** sind verfügbar unter:
http://de.trendmicro.com/de/products/enterprise/hosted-email-security

Zielgruppe

Die Hosted Email Security Dokumentation richtet sich an Hosted Email Security Administratoren, die Aufgaben ohne Zugriff auf die Webkonsole automatisieren möchten. Es werden umfangreiche Kenntnisse über die Verwendung von E-Mail-Messaging-Netzwerken einschließlich folgender Themen vorausgesetzt:

- SMTP-Protokoll
- Mail Transfer Agents (MTAs)

Kenntnisse über Antiviren- oder Anti-Spam-Technologie werden nicht vorausgesetzt.

Textkonventionen

Die Hosted Email Security Dokumentation verwendet die folgenden typografischen Konventionen, um dem Leser das Auffinden und Interpretieren von Informationen zu erleichtern.

KONVENTION	BESCHREIBUNG
NUR GROSSBUCHSTABEN	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs, Menübefehle, Befehlsschaltflächen, Registerkarten, Optionen und ScanMail Tasks
Kursivdruck	Verweise auf andere Dokumentation
`Schreibmaschinen-schrift`	Beispiele, Muster für Befehlszeilen, Programmcode, Internet-Adressen, Dateinamen und Programmanzeigen
Hinweis:	Konfigurationshinweise
Tipp:	Empfehlungen
ACHTUNG!	Hinweise auf Aktionen oder Konfigurationen, die vermieden werden sollten

Kapitel 1

Den Hosted Email Security Web-Services-Client installieren

Mit den Web-Services von Trend Micro™ Hosted Email Security können administrative Aufgaben, wie z. B. der Import gültiger E-Mail-Empfängeradressen, in Hosted Email Security automatisiert werden.

Dieses Dokument führt E-Mail-Administratoren durch die notwendigen Schritte zur Konfiguration eines Clients für die Kommunikation mit den Hosted Email Security Web-Services und erläutert die Anpassung der Automatisierung unterstützter administrativer Aufgaben in Hosted Email Security.

Unterstützte Hosted Email Security Web-Services-Anwendungen

Zu den größten Spam-Problemen zählen heute umgekehrte NDR- (Non-Delivery-Receipt) Angriffe – häufiger bekannt als Bounce-Nachrichten oder Backscatter-Spam. Mail-Server, die NDRs als Antworten versenden, werden von Spammern missbraucht, indem sie Spam-Nachrichten mit gespooften Sender- und Empfängerdaten senden. Der gespoofte Sender stellt das eigentliche Spam-Ziel dar. Mail-Server, die NDRs senden, werden unwissentlich zur Quelle solcher Backspatter-Spam-Mails.

Das Importieren von E-Mail-Adressen gültiger Empfänger in den Hosted Email Security Service bietet eine wirksame Möglichkeit, Angriffe dieser Art zu verhindern. Dies hat bedeutende Vorteile und reduziert das Risiko, in Datenbanken von Anti-Spam-Lösungen, wie z. B. die Trend Micro Email Reputation Services, gelistet zu werden. Darüber hinaus reduziert diese Vorgehensweise die Bandbreitenauslastung in Ihrer Betriebsumgebung ganz erheblich, da DHA-Angriffe (Directory Harvest Attacks) verhindert werden.

E-Mail-Administratoren können über die Importfunktion der Hosted Email Security Administrationskonsole gültige E-Mail-Empfängeradressen importieren und warten. Es werden Dateien im LDIF-Format (LDAP Data Interchange Format) oder kommaseparierte Textdateien (CSV) unterstützt. Statt der Administrationskonsole kann auch die Anwendung der Hosted Email Security Web-Services-Anwendung verwendet werden. Für Kunden mit ActiveDirectory steht zusätzlich ein ActiveDirectory Plug-in-Client (Hosted Email Security ActiveDirectory Sync Client) zur Verfügung.

Der E-Mail-Administrator wählt ein für die jeweilige Mail-Umgebung geeignetes Client-Programm aus, um mit den Hosted Email Security Web-Services zu kommunizieren. Das Client-Programm kann gültige E-Mail-Empfänger importieren oder die in Hosted Email Security aktuell gültigen E-Mail-Empfänger der Mail-Domain auflisten. Zurzeit sind die folgenden Hosted Email Security Web-Services-Clients zum Download verfügbar:

- Hosted Email Security ActiveDirectory Sync Client, ein Microsoft ActiveDirectory Client, ist für Windows Umgebungen mit ActiveDirectory verfügbar. Dieses Client-Programm dient ausschließlich zum Import gültiger E-Mail-Adressen in den Hosted Email Security Service.
- Der Hosted Email Security Web-Services-Client (imhs_web_svc_client) ist ein plattformunabhängiger Befehlszeilen-Client, der verschiedene Hosted Email Security Web-Services-Anwendungen unterstützt. Zurzeit unterstützt der Hosted Email Security Service-Client die Synchronisierung von Hosted Email Security E-Mail-Konten zum Import gültiger E-Mail-Empfängeradressen aus CSV-Dateien. Die Hosted Email Security Synchronisierung von E-Mail-Konten ist funktionell vergleichbar mit der Importfunktion für Benutzerverzeichnisse auf der Administrationskonsole.

Weitere Informationen zu Download und Installation eines Hosted Email Security Web-Services-Clients finden Sie unter *Den Web-Services-Client installieren* auf Seite 1-4.

Den Web-Services-Client installieren

Die Client-Programme der Hosted Email Security Web-Services sind Beispiel-Implementationen dafür, wie Sie über Ihre Betriebsumgebung mit den Hosted Email Security Web-Services-Anwendungen kommunizieren können.

Die Themen in diesem Kapitel führen Sie durch Auswahl, Installation, Konfiguration und Verwendung eines Client-Programms der Hosted Email Security Web-Services. Hierzu zählen die folgenden Aktionen:

- Ein Client-Programm der Hosted Email Security Web-Services auswählen
- Einen Hosted Email Security Web-Services-Client installieren
- Einen Hosted Email Security Web-Services-Client verwenden, um administrative Aufgaben in Hosted Email Security zu automatisieren

Ein Client- Programm der Hosted Email Security Web-Services auswählen

Es sind zwei Client-Programme der Hosted Email Security Web-Services verfügbar:

- Eine Beispiel-Implementation (imhs_web_svc_client: Hosted Email Security Web-Services-Client) für die Kommunikation mit den Hosted Email Security Web-Services-Anwendungen
- Ein ActiveDirectory-Plug-in (Hosted Email Security ActiveDirectory Sync Client) ausschließlich für Kunden, die gültige E-Mail-Empfänger mit Hilfe von ActiveDirectory in einer Windows Umgebung verwalten

Welches Client-Programm der Hosted Email Security Web-Services für Sie das richtige ist, hängt von Ihren Bedürfnissen ab.

Sollen weitere administrative Aufgaben in Hosted Email Security mit Hilfe der Hosted Email Security Web-Services automatisiert werden, empfiehlt sich die Installation des Client-Beispielprogramms (imhs_web_svc_client: Hosted Email Security Web-Services-Client).

Bei Verwendung von ActiveDirectory zur Verwaltung gültiger E-Mail-Empfänger können Sie den Importvorgang gültiger E-Mail-Adressen in den Hosted Email Security Service für die verwalteten Domains automatisieren, indem Sie den Hosted Email Security ActiveDirectory Plug-in-Client (Hosted Email Security ActiveDirectory Sync Client) installieren.

Während das ActiveDirectory Plug-in nur unter Windows ausgeführt werden kann, ist der Hosted Email Security Web-Services-Client vom Betriebssystem unabhängig.

Systemvoraussetzungen

Überprüfen Sie vor dem Download des ausgewählten Hosted Email Security Web-Services-Clients die unten stehenden Systemvoraussetzungen:

Microsoft ActiveDirectory Plug-in-Client

Beim Hosted Email Security ActiveDirectory Sync Client handelt es sich um den Microsoft Active Directory Plug-in-Client. Überprüfen Sie vor der Installation des Clients die Systemvoraussetzungen. Mindestvoraussetzungen für System und Installation:

- Windows 2003 Server oder Windows XP Professional SP2
- Mindestens 512 MB Arbeitsspeicher
- Mindestens 100 MB verfügbarer Festplattenspeicher
- Internet Explorer 6.0
- E-Mail-Adressen von Endbenutzern werden im ActiveDirectory gewartet
- Netzwerkzugriff auf:
  - `https://us.imhs-ws.trendmicro.com` (bei Hosted Email Security `https://us.emailsec.trendmicro.com` als Administrationskonsole)
  - `https://imhs-ws.trendmicro.eu` (bei Hosted Email Security `https://emailsec.trendmicro.eu` als Administrationskonsole)

Um den Hosted Email Security ActiveDirectory Sync Client (Microsoft Active Directory Plug-in-Client) zu installieren, führen Sie das heruntergeladene, selbstextrahierende Windows Installationsprogramm **`setup.exe`** aus. Folgen Sie den Hinweisen auf dem Bildschirm, um die Installation abzuschließen.

Weitere Installationshinweise finden Sie unter *ActiveDirectory Plug-in-Client zur Synchronisierung von ActiveDirectory E-Mail-Konten verwenden* auf Seite 2-4.

Plattformunabhängiger Hosted Email Security Web-Services-Client

Für Kunden steht eine Beispielimplementierung des Hosted Email Security Web-Services-Clients (imhs_web_svc_client) zur Verfügung. Der Client ist in der Skriptsprache Ruby geschrieben und wird von den meisten Betriebssystemen unterstützt.

Mindestvoraussetzungen für System und Installation:

Linux oder Unix

- Ruby Version 1.8.6 oder höher (falls Ruby bereits installiert ist, geben Sie **ruby -v** in eine Befehlszeile ein, um Versionsinformationen zu erhalten.) Ist Ruby noch nicht installiert ist, können Sie es unter `http://www.ruby-lang.org/en/downloads/` herunterladen. Ruby ist im Download-Paket des Linux/Unix Hosted Email Security Web-Services-Clients bereits enthalten.
- Folgen Sie den Hinweisen zur Installation.
- Ruby Gem (Ruby-Dienstprogramm zur Installation des zusätzlichen Pakets) für die Bibliothek rest-open-uri. Ruby rest-open-uri Gem ist ein erforderliches Open-Source-Dienstprogramm für Ruby. Sie können rest-open-uri Gem unter `http://rubyforge.org/frs/?group_id=2778&release_id=8581` herunterladen. Ruby ist im Download-Paket des Linux/Unix Hosted Email Security Web-Services-Clients bereits enthalten.
- Installieren Sie ***`rest-open-uri gem`***: Führen Sie **gem install rest-open-uri** über eine Befehlszeile aus.
- RPM-Umgebung für Linux oder ***`.deb`*** -Dateien für Debian, Ubuntu und andere.
- Der Hosted Email Security Web-Services-Client setzt als Standardinstallationspfad für Ruby den Pfad `/usr/bin/ruby` voraus.
- Netzwerkzugriff auf:
  - `https://us.imhs-ws.trendmicro.com` (bei Hosted Email Security `https://us.emailsec.trendmicro.com` als Administrationskonsole)
  - `https://imhs-ws.trendmicro.eu` (bei Hosted Email Security `https://emailsec.trendmicro.eu` als Administrationskonsole)

- Wenn die Ruby-Umgebung durch eine Firewall geschützt ist, führen Sie nach der Installation über eine Befehlszeile **gem install -p <URL Ihres Proxy-Servers> rest-open-uri** aus, wobei **<URL Ihres Proxy-Servers>** die Internet-Adresse Ihres Proxy-Servers ist, die in der Regel im Format ***http://proxy.ihredomain.de:proxy-port*** angegeben wird. Beispiel: ***http://proxy.beispiel.com:8080***. Die aktuelle Version von rest-open-uri ist die Version 1.0.0.

Windows

- Ruby Version 1.8.6 oder höher (falls Ruby bereits installiert ist, geben Sie **ruby -v** in eine Befehlszeile ein, um Versionsinformationen zu erhalten.) Ist Ruby noch nicht installiert ist, können Sie es unter `http://www.ruby-lang.org/en/downloads/` herunterladen. Ruby ist im Download-Paket des Windows Hosted Email Security Web-Services-Clients bereits enthalten.
- Folgen Sie den Hinweisen zur Installation.
- Ruby Gem (Ruby-Dienstprogramm zur Installation des zusätzlichen Pakets) für die Bibliothek rest-open-uri. Ruby rest-open-uri Gem ist ein erforderliches Open-Source-Dienstprogramm für Ruby. Sie können rest-open-uri Gem unter `http://rubyforge.org/frs/?group_id=2778&release_id=8581` herunterladen. Ruby ist im Download-Paket des Windows Hosted Email Security Web-Services-Clients bereits enthalten.
- Installieren Sie ***rest-open-uri gem***: Geben Sie **gem install rest-open-uri** in die DOS-Eingabeaufforderung ein.
- Netzwerkzugriff auf:
  - `https://us.imhs-ws.trendmicro.com` (bei Hosted Email Security `https://us.emailsec.trendmicro.com` als Administrationskonsole)
  - `https://imhs-ws.trendmicro.eu` (bei Hosted Email Security `https://emailsec.trendmicro.eu` als Administrationskonsole)
- Wenn die Ruby-Umgebung durch eine Firewall geschützt ist, führen Sie nach der Installation über die Eingabeaufforderung **gem install -p <URL Ihres Proxy-Servers> rest-open-uri** aus, wobei **<URL Ihres Proxy-Servers>** die Internet-Adresse Ihres Proxy-Servers ist, die in der Regel im Format `http://proxy.ihredomain.de:proxy-port` angegeben wird. Beispiel: `http://proxy.beispiel.com:8080`. Die aktuelle Version des Open-Source-Dienstprogramms rest-open-uri Gem für Ruby ist Version 1.0.0.

Ein Client-Programm herunterladen

Das Client-Programm herunterladen:

1. Melden Sie sich an der Hosted Email Security Administrationskonsole unter einer der folgenden Adressen an:
   - **Europa:** https://emailsec.trendmicro.eu
   - **Andere Regionen:** https://us.emailsec.trendmicro.com

   Wählen Sie aus dem Hosted Email Security Menü **Administration** > **Web-Services** aus.

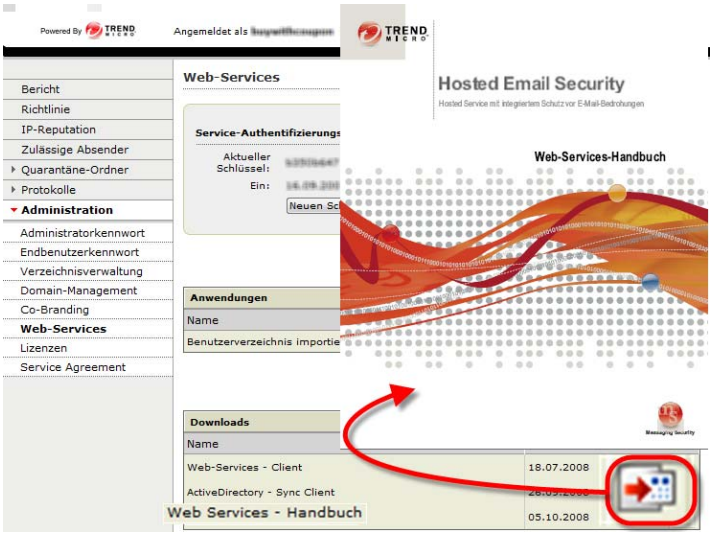


ABBILDUNG 1-1. Dieses Handbuch vom Hosted Email Security Web-Services-Fenster herunterladen

2. Wählen Sie den passenden Client für Ihr Betriebssystem aus.

Kapitel 2

Den Hosted Email Security Web-Services-Client verwenden

Mit Hilfe der Hosted Email Security Web-Services-Programme können einige administrative Aufgaben in Hosted Email Security automatisiert werden, wie z. B. der regelmäßige Import gültiger E-Mail-Adressen für Ihre Mail-Domains.

Vor der Konfiguration und Verwendung des Hosted Email Security Web-Services-Clients für die Kommunikation mit den Hosted Email Security Web-Services sind folgende Punkte zu beachten.

Hosted Email Security Web-Services aktivieren

Standardmäßig sind Web-Services-Programme in Hosted Email Security für Ihre Mail-Domains deaktiviert. Um dem Client die Kommunikation mit den Hosted Email Security Web-Services bezüglich Ihrer verwalteten Domains zu ermöglichen, melden Sie sich an der Hosted Email Security Administrationskonsole an, und aktivieren Sie die Hosted Email Security Web-Services. Der installierte Hosted Email Security Web-Services-Client kann mit den Hosted Email Security Web-Services erst nach deren Aktivierung kommunizieren.

Hosted Email Security Web-Services aktivieren:

1. Wählen Sie aus dem Hosted Email Security Menü die Optionen **Administration** > **Web-Services** aus.
2. Sind die Hosted Email Security Web-Services-Anwendungen noch deaktiviert (auf der Web-Services-Seite wird „Deaktiviert“ angezeigt), müssen sie zunächst aktiviert werden. Um die Web-Services-Anwendungen zu aktivieren, ist ein APIKEY erforderlich.

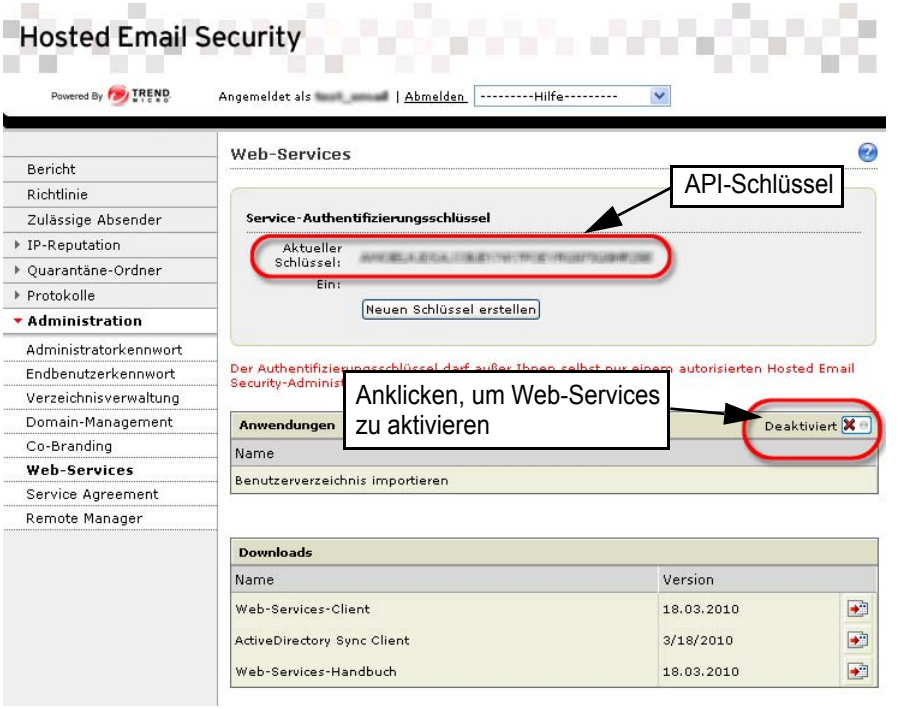


ABBILDUNG 2-1. Fenster „Hosted Email Security Web-Services“

3. Stellen Sie sicher, dass unter „Aktueller Schlüssel“ ein APIKEY angezeigt wird, und klicken Sie dann auf die Umschaltfläche **Deaktiviert**, um die Kommunikation zwischen dem Hosted Email Security Web-Services-Client und den Hosted Email Security Web-Services-Anwendungen zuzulassen.

Der Hosted Email Security Web-Services-Client verwendet den APIKEY, um die Kommunikation zu authentifizieren. Wenn bereits ein APIKEY auf der Administratorkonsole erstellt wurde, kopieren Sie diesen, und fügen Sie ihn in das Client-Programm der Hosted Email Security Web-Services ein. Ohne APIKEY kann der Web-Services-Client nicht mit den Hosted Email Security Web-Services-Anwendungen kommunizieren.

4. Klicken Sie auf **Neuen Schlüssel erstellen**, wenn bisher kein APIKEY generiert wurde.

Um die Sicherheit zu erhöhen, können Sie regelmäßig einen neuen APIKEY erstellen. Klicken Sie hierzu auf **Neuen Schlüssel erstellen**. Der Hosted Email Security Web-Services-Client wird dann für die Authentifizierung mit dem neuen APIKEY aktualisiert. Nach der Erstellung eines neuen Schlüssels ist der alte APIKEY ungültig.

Zugriffsbegrenzung für die Hosted Email Security Web-Services

Da der Web-Services-Client mit den Hosted Email Security Web-Services programmgesteuert und nicht über die Administrationskonsole in einem Internet-Browser kommuniziert, verhindert Hosted Email Security unbeabsichtigte Zugriffe durch eine Zugriffsbegrenzung. Hierzu zählen z. B. Denial-of-Service-Angriffe oder Programmierfehler (z. B. Endlosschleifen) in benutzerdefinierten Programmen des Hosted Email Security Web-Services-Clients. Eine solche Zugriffsbegrenzung stellt sicher, dass die Kommunikation Ihres Web-Service-Clients nicht durch andere Clients beeinträchtigt wird.

Jeder Kunde darf täglich pro Domain maximal 50 Synchronisierungsanfragen für E-Mail-Konten stellen.

ActiveDirectory Plug-in-Client zur Synchronisierung von ActiveDirectory E-Mail-Konten verwenden

Werden in Ihrem Unternehmen die E-Mail-Benutzerkonten mit ActiveDirectory verwaltet, können Sie den ActiveDirectory Plug-in-Client (Hosted Email Security ActiveDirectory Sync Client) auf einem Windows Computer installieren, um automatisch das Benutzerverzeichnis gültiger E-Mail-Empfänger in Hosted Email Security zu importieren. Dies bietet folgende Sicherheitsvorteile:

- Abwehr von DHA-Angriffen (Directory Harvest Attacks)
- Reduzierung von Backscatter-Spam (umgekehrte NDR-Angriffe)

Begrenzung der ActiveDirectory Größe

ACHTUNG! Beachten Sie vor der Konfiguration des Hosted Email Security ActiveDirectory Sync Clients die unten stehenden Einschränkungen:

Die Anzahl der im ActiveDirectory konfigurierten Benutzer überschreitet möglicherweise die zulässige Größe

Der Hosted Email Security ActiveDirectory Sync Client kann unter normalen Bedingungen bis zu 250.000 E-Mail-Adressen mit durchschnittlicher Adresslänge verarbeiten. Enthält das ActiveDirectory Verzeichnis sehr viele E-Mail-Adressen, überschreitet dies möglicherweise die Verarbeitungskapazität des Hosted Email Security ActiveDirectory Sync Clients.

Enthält ein einzelnes ActiveDirectory Verzeichnis sehr viele E-Mail-Adressen, sollten Sie die Benutzer über mehrere LDAP-Pfade auf kleinere ActiveDirectory Datenbanken aufteilen.

Verwendung mehrerer ActiveDirectory Sync Clients

Es sollte jeweils nur ein ActiveDirectory Verzeichnis synchronisiert werden, damit sich keine Synchronisierungsvorgänge überschneiden.

Bei Verwendung mehrerer Sync Clients sollten Sie sicherstellen, dass eine E-Mail-Domain nicht von zwei verschiedenen Sync Clients bearbeitet wird, da dies das Synchronisierungsergebnis verfälschen könnte.

Umgang mit mehreren ActiveDirectory Pfaden oder Servern

Bei Verwendung mehrerer ActiveDirectory Pfade oder Server für dieselbe zu synchronisierende E-Mail-Domain sollten Sie nur einen einzelnen Sync Client einsetzen und mehrere LDAP-Pfade konfigurieren (siehe *Abbildung C-15* auf Seite C-17).

Wenn Sie beispielsweise über zwei ActiveDirectory Pfade A und B verfügen, werden gemäß der ACL-Einstellung einige E-Mail-Adressen von ***abc.de***über Pfad A ermittelt. Auch Pfad B enthält E-Mail-Adressen der ***abc.de***-Domain. Erfolgt die Synchronisierung über die Pfade A und B getrennt mit Hilfe zweier Sync Clients (C1 und C2), aktualisiert C1 den Server und ersetzt alle dort vorhandenen Einträge durch die Daten aus Pfad A. Dadurch würden alle E-Mail-Adressen aus Pfad B überschrieben (und umgekehrt). In diesem Fall empfiehlt es sich, einen einzelnen Sync Client zu verwenden und die LDAP-Pfade A und B so zu konfigurieren, dass sie ihre Daten mit dem Server synchronisieren.

Zulässige E-Mail-Adresse

Als Mail-Attribut sind drei Typen von E-Mail-Adressen zulässig:

1. SMTP-Adresse mit dem Präfix „smtp:“. E-Mails mit anderen Präfixen (z. B. X500:) oder einer ungültigen SMTP-Adresse (z. B. person@domain) werden abgelehnt.

   Beispiel: ***smtp:person@domain.de***

2. SMTP-Adresse.

   Beispiel: ***person@domain.de***

3. Eine beliebige Kombination der oben beschriebenen Typen 1 und 2, durch Komma (,) oder Strichpunkt (;) getrennt.
   Beispiel: ***person@domain.de;smtp:Mitarbeiter_A@domain.de, SMTP:Mitarbeiter_B@domain.de***

   Im Beispiel oben ergeben sich aus dem einzelnen Eintrag drei verschiedene E-Mail-Adressen.

ACHTUNG! **Nahezu alle RFC 822 kompatiblen E-Mail-Adressen können vom ActiveDirectory Sync Client als zulässig eingestuft werden. Ausgenommen davon sind nur E-Mail-Adressen, die eines der folgenden Sonderzeichen links oder rechts vom @-Zeichen enthalten:**
`( ) < > @ , ; : \ " [ ]`

Adressen, die eines dieser Zeichen enthalten, werden zurückgewiesen. Weitere Informationen hierzu finden Sie in *Ungültige E-Mail-Adressen identifizieren* **auf Seite 3-2.**

Keine Teilsynchronisierung

Bei Konfigurierung mehrerer LDAP-Pfade wird die Synchronisierung über diese Pfade als „entweder-oder"-Transaktion durchgeführt, d. h., wenn die Synchronisierung von mindestens einem LDAP-Pfad fehlschlägt, schlägt die gesamte Synchronisierung fehl, und es werden keine Daten mit dem Server synchronisiert.

Aufgrund dieser Funktion muss bei der Konfiguration des ActiveDirectory Sync Clients im ActiveDirectory Server kein LDAP-Ausweichpfad festgelegt werden. Da bei der Konfiguration mehrerer Pfade die Wahrscheinlichkeit steigt, dass einer der Pfade fehlschlägt, ist diese Vorgehensweise ohnehin nicht empfehlenswert.

Hinweis: Schlägt die Synchronisierung fehl, bleiben die vorhandenen Daten auf dem Server bestehen.

Schlägt die ActiveDirectory Synchronisierung dauerhaft fehl, stellen Sie sicher, dass alle LDAP-Pfade gültig und erreichbar sind. Ist der Grund ein Netzwerk- oder ActiveDirectory Serverproblem (siehe die Verlaufsliste des AD Sync Clients), beheben Sie das Verbindungsproblem so schnell wie möglich, damit eine vollständige Synchronisierung durchgeführt werden kann.

Wenn Sie die Uhrzeit auf dem Computer ändern, muss der Service für den Hosted Email Security ActiveDirectory Sync Client neu gestartet werden.

Das Synchronisierungsintervall darf nicht kürzer als die erforderliche Zeit zum Synchronisieren der ActiveDirectory Benutzerverzeichnisse sein.
Enthält das ActiveDirectory sehr viele Benutzer, sollte das Synchronisierungsintervall auf mindestens 4 Stunden eingestellt werden, damit der Vorgang innerhalb des angegebenen Intervalls vollständig ausgeführt werden kann. Sich überschneidende Synchronisierungsvorgänge lösen Fehlerbedingungen aus und werden daher nicht unterstützt.

Zeitplan für den Import gültiger E-Mail-Adressen von E-Mail-Empfängern festlegen:

1. Starten Sie das Konfigurationsprogramm, und legen Sie im Dialogfeld „Hosted Email Security ActiveDirectory Sync Client“ den Zeitplan für den Import gültiger E-Mail-Empfängeradressen fest:

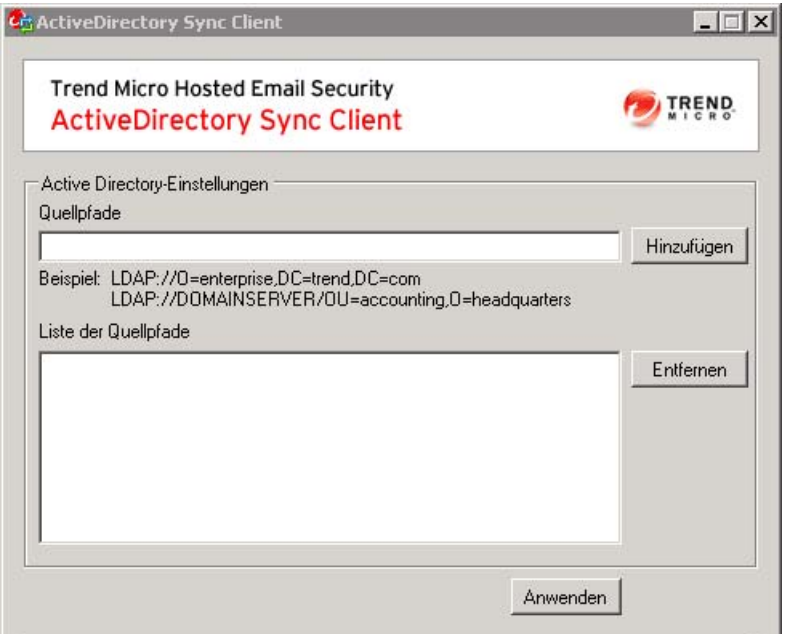


ABBILDUNG 2-2. Hosted Email Security ActiveDirectory Sync Client

2. Beachten Sie die Hinweise zur Installation und Erstkonfiguration des Hosted Email Security ActiveDirectory Sync Clients im Anhang C, Installation und Konfiguration des ActiveDirectory Sync Clients ab Seite C-1.

Beispiel für eine zeitgesteuerte Synchronisierung von E-Mail-Benutzeradressen

Im folgenden Beispiel werden mit Hilfe des ActiveDirectory Sync Clients E-Mail-Benutzeradressen aus einem ActiveDirectory Verzeichnis regelmäßig mit Hosted Email Security synchronisiert. Die Domain **test.de** verfügt in diesem Beispiel über zwei Benutzer: **abc** und **adam-paul**. Sie können überprüfen, ob die Daten im Hosted Email Security Service identisch sind.

Beispiel ausführen:

1. Geben Sie einen der folgenden Links in den Webbrowser ein:
   - Für Kunden in Europa:
     `https://imhs-ws.trendmicro.eu/imhs/v1.0/en/domains/test.com/users`
   - Für Kunden in anderen Regionen:
     `https://us.imhs-ws.trendmicro.com/imhs/v1.0/en/domains/test.com/users`

   Es erscheint ein Anmeldefenster.
2. Geben Sie den Namen des Hosted Email Security Administratorkontos und den APIKEY für das Kennwort ein.

3. Fügen Sie einen neuen Benutzer mit dem Namen „Engel“ und der E-Mail-Adresse **engel@test.de** hinzu. Weitere Informationen über das Einfügen eines neuen Benutzers in ein ActiveDirectory Verzeichnis erhalten Sie von Ihrem ActiveDirectory Administrator.

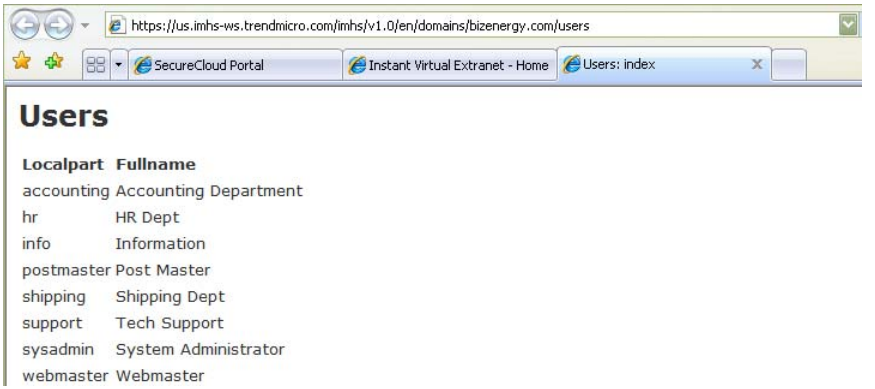


ABBILDUNG 2-3. E-Mail-Benutzer anzeigen

Möglicherweise aktualisieren Sie Ihr ActiveDirectory ähnlich wie in diesem Beispiel. Die folgende Beschreibung dient jedoch ausschließlich als Referenz.

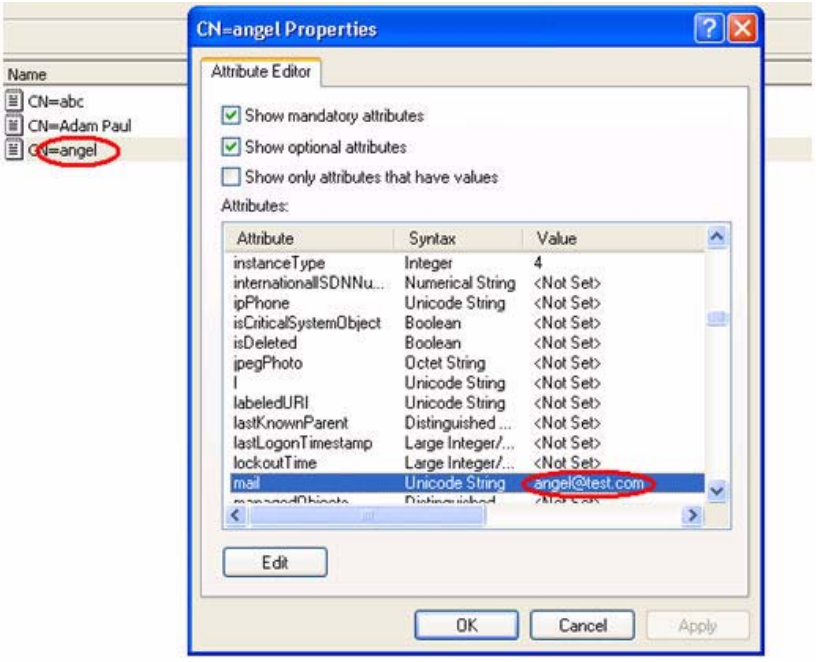


ABBILDUNG 2-4. Dialogfeld Eigenschaften (Beispiel)

Im nächsten Synchronisierungsintervall, z. B. in ungefähr einer Stunde, überprüft der Hosted Email Security ActiveDirectory Sync Client das ActiveDirectory Verzeichnis auf Änderungen, die nach dem letzten Update durchgeführt wurden. Der Client erkennt hierbei den hinzugefügten Benutzer mit der E-Mail-Adresse **engel@test.de**. Daraufhin kopiert der Client den Verzeichniseintrag **engel@test.de** über die Hosted Email Security Web-Services-Oberfläche in den Hosted Email Security Service.

4. Um das Ergebnis nach dem Synchronisierungsintervall zu überprüfen, geben Sie einen der folgenden Links in Ihren Webbrowser ein:
   - Für Kunden in Europa:
     `https://imhs-ws.trendmicro.eu/imhs/v1.0/en/domains/test.com/users`

- Für Kunden in anderen Regionen:
  `https://us.imhs-ws.trendmicro.com/imhs/v1.0/en/domains/test.com/users`

Es erscheint ein Anmeldefenster.

5. Geben Sie den Namen des Hosted Email Security Administratorkontos und den APIKEY für das Kennwort ein.

   Die E-Mail-Adresse wird wie folgt angezeigt.

ABBILDUNG 2-5. Ergebnis nach der Synchronisierung

Befehlszeilen-Client der Hosted Email Security Web-Services zum Synchronisieren gültiger E-Mail-Empfängeradressen verwenden

Werden die E-Mail-Benutzerkonten in Ihrem Unternehmen nicht mit ActiveDirectory verwaltet, können gültige E-Mail-Empfänger als kommagetrennte Textdatei (CSV) importiert werden. Die meisten LDAP-Server verfügen über ein Dienstprogramm, um die Inhalte der LDAP-Datenbank in eine CSV-Datei zu exportieren.

Im folgenden Beispiel werden E-Mail-Benutzeradressen regelmäßig aus einer CSV-Datei in Hosted Email Security unter Verwendung des vom Betriebssystem unabhängigen Hosted Email Security Web-Services-Clients ***`imhs_web_svc_client`*** importiert.

ABBILDUNG 2-6. CSV-Import durch Client

Übersicht

Der folgende Abschnitt gibt eine kurze Übersicht über die Verwendung von Hosted Email Security Web-Services.

1. Melden Sie sich an der Hosted Email Security Administrationskonsole im Fenster **Administration > Web-Services** an. Notieren Sie sich den aktuellen APIKEY in diesem Fenster. Wenn es sich um ein neues Administratorkonto handelt, ist noch kein APIKEY vorhanden.
2. Klicken Sie auf **Neuen Schlüssel erstellen**, um einen APIKEY zu generieren.
3. Überprüfen Sie, ob ein APIKEY verfügbar ist, und stellen Sie sicher, dass die Web-Services-Anwendungen aktiviert sind.
4. Laden Sie das Client-Programm der Hosted Email Security Web-Services herunter.
5. Folgen Sie den Installationshinweisen für den Hosted Email Security Web-Services-Client, um das Client-Programm zu installieren. Für die Installation benötigen Sie den gültigen APIKEY.
6. Konfigurieren Sie das Client-Programm gemäß den Erfordernissen im Unternehmen.

Kapitel 3

Fehlerbehebung

Dieses Kapitel beschreibt mögliche Probleme bei der Verwendung von Hosted Email Security Web-Services und die jeweiligen Lösungen.

Das Kapitel enthält die folgenden Themen:

Das Fehlerbehebungsprotokoll des AD Sync Client verwenden

Der Active Directory Sync Client bewahrt Fehlerbehebungsprotokolle für die Fehlerbehebung auf. Protokolldateien zur Fehlerbehebung befinden sich im folgenden Verzeichnis: `[Your_AD_Client_InstallFolder]\log`

Es gibt drei Typen von Fehlerbehebungsprotokollen:

1. Verlaufsprotokoll (unter `\log\PluginHistory`)
2. Überwachungsprotokoll (unter `\log\PluginMonitor`)
3. Plug-in-Serviceprotokoll (unter `\log\PluginService`)

Standardmäßig werden alle drei Protokolltypen 7 Tage lang gespeichert.

Die Fehlerbehebungsprotokolle entsprechend den folgenden Konventionen benannt:

{Protokolltyp}-{Jahr}-{Monat}-{Tag}.log

Beispiel:

```
IhreADSyncClientInstallation\log\PluginHistory\
PluginHistory-2008-5-9.log
IhreADSyncClientInstallation\log\PluginService\
PluginService-2008-10-24.log
```

Tipp: Senden Sie sie die entsprechenden Protokolldateien, wenn Sie Kontakt mit dem Trend Micro Support aufnehmen; dadurch helfen Sie Trend Micro, das Problem zu beheben.

Ungültige E-Mail-Adressen identifizieren

Bei jeder Synchronisierung Ihres AD Servers über den AD Sync Client protokolliert der Client alle E-Mail-Adressen auf Ihrem AD Server, die von Mail-Servern für eingehende oder ausgehende E-Mails nicht zugelassen sind. (Weitere Hinweise zur Einstufung von E-Mail-Adressen finden Sie unter *Zulässige E-Mail-Adresse* auf Seite 2-5.)

Der AD Sync Client erstellt eine Datei mit dem Namen `InvalidUsers.txt`, die in Ihrem AD Sync Client Installationsverzeichnis gespeichert wird un Ihnen bei der Identifizierung ungültiger Adressen hilft.

Diese Datei wird während der Synchronisation erstellt und ersetzt jedesmal vorherige, entsprechende Datei. Sollte es bei der Synchronisation keine ungültigen Adressen geben, wird eine leere Datei erstellt. E-Mail-Adressen werden nach Domain sortiert.

Häufig gestellte Fragen

Wie kann ich feststellen, ob das Programm zur Synchronisierung der Clients ordnungsgemäß ausgeführt wird?

Als erstes können Sie die Benutzer mithilfe eines Webbrowsers ermitteln. Dies zeigt das Beispiel in Abschnitt *Beispiel für eine zeitgesteuerte Synchronisierung von E-Mail-Benutzeradressen* auf Seite 2-8.

Sie können auch die Verlaufsinformationen überprüfen. Bei erfolgreicher Datensynchronisierung wird der Vorgang als Erfolg im Protokoll verzeichnet. Ist der Vorgang fehlgeschlagen, finden Sie eine entsprechende Fehlermeldung im Protokoll. Verwenden Sie die Protokolloption „Gründe“, um Diagnose-Hinweise zum vorliegenden Problem zu erhalten. Wenn keine Informationen im Protokoll gespeichert sind, wurden keine Benutzerdaten aktualisiert. Es wurde also keine Synchronisierung durchgeführt.

Was tun, wenn die Synchronisierung fehlgeschlagen ist?

Überprüfen Sie zunächst die Verlaufsinformationen, um die Fehlerursache zu ermitteln. Wenn Hosted Email Security keine ActiveDirectory Daten ermitteln konnte, überprüfen Sie, ob der LDAP-Pfad noch gültig ist.

Wenn der Fehler durch den Web-Service verursacht wird, überprüfen Sie die Proxy-Einstellungen, den Benutzernamen und den Schlüssel. Wenn der Schlüssel ungültig ist, ermitteln Sie den gültigen Schlüssel über die Hosted Email Security Administrationskonsole, oder generieren Sie einen neuen Schlüssel.

Welches Synchronisierungsintervall ist empfehlenswert?

Der Standardwert (1 Stunde) eignet sich in den meisten Fällen. Es ist in der Regel nicht erforderlich, diesen Wert zu ändern. Wenn die ActiveDirectory Daten jedoch sehr umfangreich sind (über 250.000 E-Mail-Empfänger-Nachrichten), sollte der Intervallwert erhöht werden.

Tipp: Trend Micro empfiehlt, das Synchronisierungsintervall in solchen Fällen auf 4 Stunden einzustellen.

Kann ein Verzeichnis über die Administrationskonsole importiert werden, wenn gleichzeitig ein Web-Service-Client ausgeführt wird?

Während des aktiven Synchronisierungsvorgangs sperrt der Web-Service die Ziel-Domain und verhindert dadurch einen Verzeichnisimport über die Administrationskonsole. Schlägt die Synchronisierung während des Vorgangs fehl und kann der Web-Service die Synchronisierung nicht schließen/rückgängig machen, wartet der Web-Service-Server zwei Stunden. Dann läuft die zulässige Zeit für die Synchronisierung ab, und die Sperrung der zu synchronisierenden Domain wird aufgehoben.

Warum kann der Synchronisierungsservice nicht gestartet werden, und warum wird die Fehlermeldung „Fehler 1069: Der Service konnte aufgrund eines Anmeldefehlers nicht gestartet werden“ ausgegeben?

Überprüfen Sie, ob das Kennwort für das Domain-Konto geändert wurde. Wurde das Kennwort geändert, müssen auch die Anmeldeinformationen für den Service wie folgt geändert werden:

1. Öffnen Sie die **Systemsteuerung**, und wählen Sie **Verwaltung** > **Dienste** aus.
2. Suchen Sie im Fenster „Dienste“ den Dienst **Hosted Email Security ActiveDirectory Sync Service**.
3. Klicken Sie mit der rechten Maustaste auf den Dienst, und klicken Sie dann auf **Eigenschaften**.
4. Stellen Sie sicher, dass im Anmeldefenster die Option **Als dieses Konto anmelden** aktiviert ist, und geben Sie die gültigen Anmeldeinformationen (Domain, Benutzername und Kennwort) ein.

Anhang A

Hosted Email Security Web-Services-Anwendungen

Die Informationen in diesem Anhang richten sich an Value Added Reseller, professionelle Service Provider und Softwareentwicklungspartner von Trend Micro. Andere Kunden der Hosted Email Security Services gehören nicht zur Zielgruppe dieser Dokumentation.

Dieser Anhang enthält zusätzliche Informationen über die Anpassung und Programmierung des Hosted Email Security Web-Services-Clients zur Kommunikation mit Anwendungen der Hosted Email Security Web-Services. Die Themen dienen als Referenz zu dem von Trend Micro bereitgestellten Beispiel-Client.

Hinweis: Zur Erstellungszeit dieses Anhangs lagen nicht alle APIs vor.

Sicherheit der Web-Services

Die Verbindung zu den Hosted Email Security Web-Services wird durch den Client unter Verwendung von SSL gestartet. Zur HTTP-Authentifizierung wird außerdem der Aktivierungscode des Kunden, der Name des Administratorkontos und ein durch Hosted Email Security erstellter APIKEY für das Kennwort verwendet. Unter der Voraussetzung, dass die Client-Programmkonfiguration mit dem aktuellen APIKEY aktualisiert wird, kann der APIKEY immer wieder neu erstellt werden.

Web-Services-Anwendungen

Die Hosted Email Security Web-Services bieten eine Reihe von APIs (Application Programming Interfaces) mit einer RESTful-Webanwendungsarchitektur. Die APIs dienen überwiegend zur Automatisierung administrativer Routineaufgaben in Hosted Email Security.

Bereitstellung

Zu den Routineaufgaben zählt z. B. das Verwalten von E-Mail-Benutzerkonten. Diese müssen auf den verschiedenen Mail-Servern des Unternehmens und in Hosted Email Security konsistent gehalten werden. Die Hosted Email Security Web-Services bieten APIs zur Verwaltung von Benutzerverzeichnissen, um folgende oder andere Aufgaben zu automatisieren:

- E-Mail-Benutzeradresse zu einer verwalteten Domain des Hosted Email Security Services hinzufügen
- E-Mail-Benutzeradressen aus einer verwalteten Domain der Hosted Email Security Services löschen
- E-Mail-Adressen einer verwalteten Domain der Hosted Email Security Services anzeigen
- Große Mengen von E-Mail-Adressen zu einem Hosted Email Security Administratorkonto hinzufügen
- Domain-Namen anzeigen, die durch ein Hosted Email Security Administratorkonto verwaltet werden
- E-Mail-Benutzeradressen anzeigen, die von einem Hosted Email Security Administratorkonto verwaltet werden

Web-Services-Clients

Hosted Email Security ActiveDirectory Sync Client

Für Benutzer mit Active Directory (AD) Installationen bietet Trend Micro den unter .NET entwickelten Hosted Email Security ActiveDirectory Sync Client. Hierbei handelt es sich entweder um ein Microsoft Active Directory Plug-in oder einen AD Connector. Der Client dient als direktionale Pipe zwischen dem Active Directory des Benutzers und den Hosted Email Security Web-Services zur Übermittlung von Bereitstellungsdaten (z. B. beschränkt auf aktualisierte gültige Benutzer für die Web-Services Version 1.0). Der Hosted Email Security ActiveDirectory Sync Client fragt in konfigurierbaren Abständen die AD Server des Kunden nach gelöschten oder hinzugefügten gültigen Benutzern ab. Der AD Connector synchronisiert dann die Hosted Email Security Benutzerdaten des entsprechenden Benutzerkontos durch Aufruf einer Web-Service-API.

Hosted Email Security Web-Services-Clients

Für die allgemeine Kommunikation mit den Hosted Email Security Web-Services bietet Trend Micro eine plattformunabhängige Beispielimplementation des Web-Services-Clients: **imhs_web_svc_client**.

Der Hosted Email Security Web-Services-Client (**imhs_web_svc_client**) ist in der plattformunabhängigen Skriptsprache Ruby geschrieben. Der Ruby-Client ist ein vollständiger Web-Services-Client mit Zugriff auf die Berichterstellungs- und Bereitstellungsressourcen der Hosted Email Security Web-Services. Als solcher kann er zu Bereitstellungszwecken als Upload-Komponente dienen und eine CSV-Datei mit gültigen E-Mail-Adressen hochladen oder einen Aufruf des Web-Services beim Hinzufügen oder Löschen eines Benutzers ausführen.

Zum Extrahieren von Berichten kann der Ruby-Client mit den entsprechenden Parametern aufgerufen werden, um den erforderlichen Bericht entweder im XML- oder CSV-Format als lokale Datei zu speichern. Die unterstützte Bibliothek des Ruby-Clients kann auch direkt aufgerufen werden, um eine benutzerdefinierte clientbasierte Anwendung herzustellen. Ruby-Ports stehen zur Ausführung auf .nix- oder Windows Plattformen zur Verfügung.

Anhang B

Die Achitektur des ActiveDirectory Sync Clients

Dieser Anhang beschreibt die Software-Architektur des Hosted Email Security ActiveDirectory Sync Clients. Er soll weitere Informationen zum besseren Verständnis des Client-Designs bieten.

Übersicht

Der Hosted Email Security ActiveDirectory Sync Client ist ein Plug-in für Microsoft Active Directory. Der Client wird in der Betriebsumgebung installiert und hat Zugriff zum Active Directory. Er fragt in regelmäßigen Abständen die E-Mail-Benutzerkonten aus den Active Directory Datenquellen ab und gibt Änderungen an den Hosted Email Security Service weiter. Die komplexe Architektur ist folgendermaßen aufgebaut:

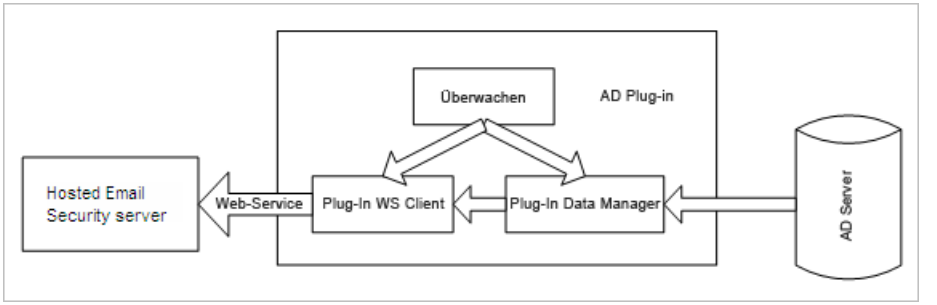


ABBILDUNG B-1. Architektur des Hosted Email Security ActiveDirectory Sync Clients

Hosted Email Security umfasst die folgenden drei Hauptkomponenten:

- *Plug-In Data Manager*
- *Plug-In WS Client*
- *Monitor*

Diese werden in den nächsten Abschnitten einzeln beschrieben.

Plug-In Data Manager

Der Plug-In Data Manager ruft Daten aus dem Active Directory ab. Zurzeit werden nur E-Mail-Benutzeradressen abgefragt. Der Plug-In Data Manager wird als Windows Dienst unter der Bezeichnung Hosted Email Security ActiveDirectory Sync Dienst ausgeführt.

Plug-In WS Client

Der Plug-In WS Client ist eine statuslose Bibliothek, die mit dem Web-Service-Server kommuniziert. Der Client sendet Webabfragen an den Server und empfängt die entsprechenden Antworten.

Monitor

Der Monitor überwacht die Ausführung des Hosted Email Security ActiveDirectory Sync Dienstes, insbesondere des Plug-In Data Manager Dienstes und des Plug-In WS Client Dienstes. Der Monitor selbst wird als Windows Dienst unter der Bezeichnung Hosted Email Security ActiveDirectory Sync Agent ausgeführt.

Betriebsumgebung

Hosted Email Security ActiveDirectory Sync wird unter Windows XP und Windows Server 2003 ordnungsgemäß ausgeführt und kann auf verschiedene AD Server unter Windows Server 2003 zugreifen. Auf dem Client-Computer ist die Installation von .NET Framework 2.0 erforderlich. Ohne eine ordnungsgemäße Installation von .NET Framework 2.0 können verschiedene Installations- und Laufzeitprobleme auftreten.

Tipp: Trend Micro empfiehlt mindestens 512 MB Arbeitsspeicher und 100 MB freien Festplattenspeicher für Hosted Email Security ActiveDirectory Sync.

Der Hosted Email Security ActiveDirectory Sync Client wurde unter Verwendung der Entwicklungsplattform und -sprache .NET C# geschrieben.

Anhang C

Installation und Konfiguration des ActiveDirectory Sync Clients

Dieser Anhang bietet eine Übersicht über die Installation, Konfiguration und Anpassung des Hosted Email Security ActiveDirectory Sync Clients.

Den Hosted Email Security ActiveDirectory Sync Client installieren

Wenn Sie den aktuellen Hosted Email Security ActiveDirectory Sync Client nicht bereits installiert haben, melden Sie sich an der Hosted Email Security Administrationskonsole an, klicken auf **Administration > Web-Services** und laden den neuesten Client herunter.

Damit Hosted Email Security ActiveDirectory Sync ordnungsgemäß installiert und ausgeführt werden kann, ist Microsoft .NET Framework 2.0 erforderlich. Während des Installationsprozesses werden Sie deshalb eventuell aufgefordert, .NET Framework 2.0 zu installieren.

Hosted Email Security ActiveDirectory Sync Client installieren:

1. Klicken Sie auf **Akzeptieren**, um .NET Framework von der Microsoft Website herunterzuladen. Dieser Vorgang kann je nach Geschwindigkeit der Internet-Verbindung einige Minuten dauern. (Überspringen Sie diesen Schritt, und fahren Sie mit Schritt 2 fort, wenn .NET Framework 2.0 bereits installiert ist.)

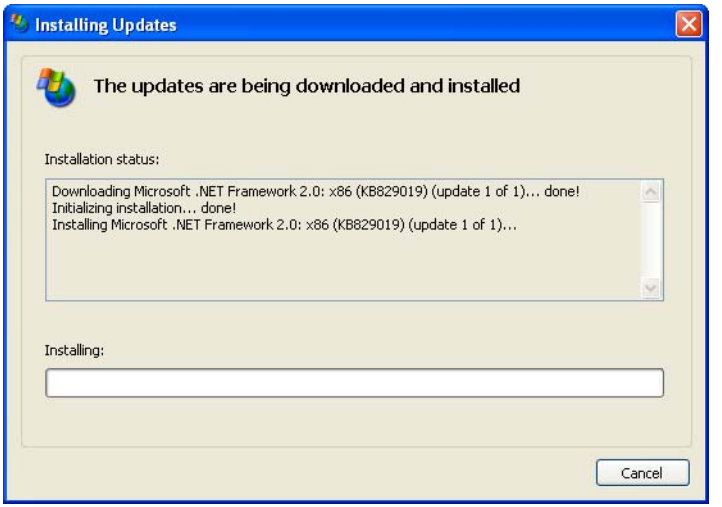


ABBILDUNG C-1. Microsoft .NET 2.0 herunterladen und installieren

Die Installation von .NET Framework 2.0 startet nach Abschluss des Downloads automatisch. Dieser Installationsschritt dauert etwa zehn Minuten.

Nach der erfolgreichen Installation von .NET Framework 2.0 beginnt der Installationsprozess des Hosted Email Security ActiveDirectory Sync Clients. Das folgende Fenster wird angezeigt:

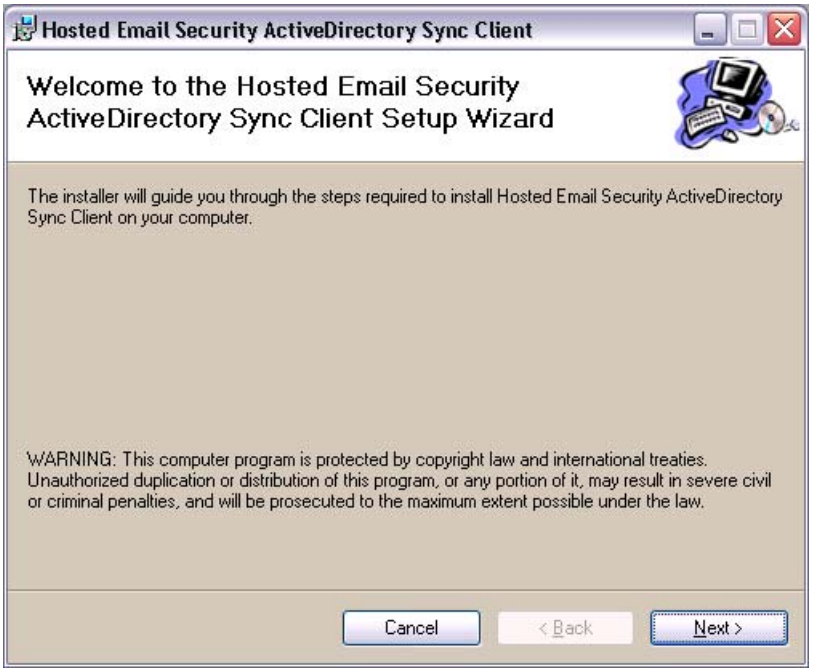


ABBILDUNG C-2. Begrüßungsfenster

2. Klicken Sie auf **Weiter**, um die Lizenzvereinbarung zu lesen.
   Das Fenster „Lizenzvereinbarung“ wird angezeigt:

ABBILDUNG C-3. Das Fenster „Lizenzvereinbarung“

3. Wählen Sie die Option **Ich stimme zu**, und klicken Sie auf **Weiter**, um den Vorgang fortzusetzen.

Das Fenster zur Eingabe des Domain-Kontos wird angezeigt:

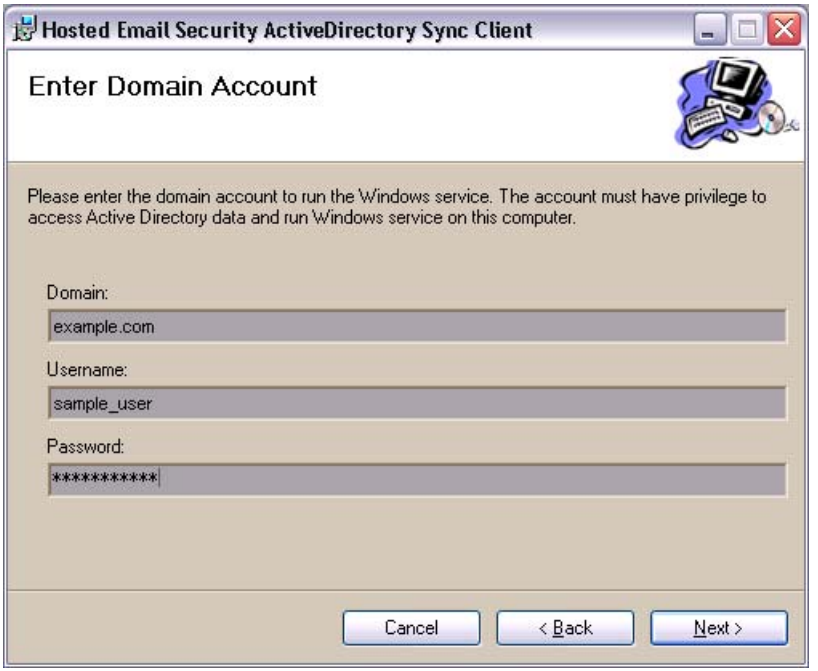


ABBILDUNG C-4. Das Fenster „Domain-Konto eingeben“

4. Geben Sie das Domain-Konto ein, das berechtigt ist, auf den Active Directory Server zuzugreifen und Windows Dienste auf dem Computer auszuführen. Klicken Sie auf **Weiter**.

Hinweis: Die Angabe des korrekten Kontos ist besonders wichtig. Bei Eingabe eines Kontos ohne Zugriffsberechtigung für einen der beiden aufgeführten Punkte wird der Hosted Email Security ActiveDirectory Sync Client nicht ordnungsgemäß ausgeführt.

Das Fenster zur Auswahl des Zieldatenträgers wird angezeigt:

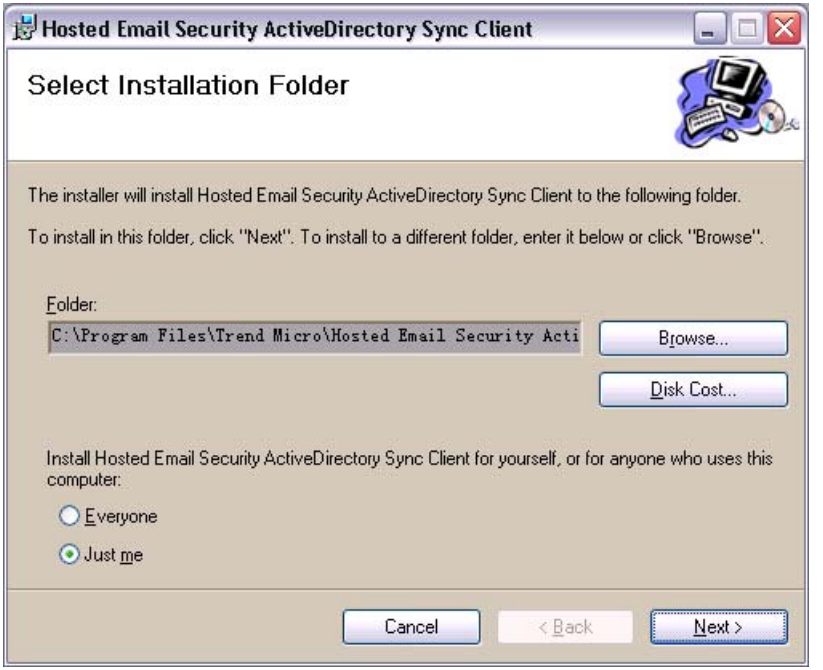


ABBILDUNG C-5. ActiveDirectory Sync Client-Fenster „Installationsordner auswählen“

5. Wählen Sie den Installationsordner und den Zielbenutzer aus. Die Eingabe von „Jeder“ oder „Nur aktueller Benutzer“ bedeutet für die Verwendung des Hosted Email Security ActiveDirectory Sync Clients keinen wesentlichen Unterschied. In beiden Fällen kann der aktuell angemeldete Benutzer den Web-Service-Client verwenden. Bei der Angabe von „Nur aktueller Benutzer“ wird die Menügruppe des Client-Programms jedoch nur für den aktuellen Benutzer erstellt. Andernfalls wird diese für alle Benutzer erstellt.

6. Klicken Sie auf **Weiter**. Das Fenster zum Bestätigen der Installation wird angezeigt:

ABBILDUNG C-6. Das Fenster „Installation bestätigen“

7. Klicken Sie auf **Weiter**, um den Vorgang fortzusetzen.

   Die Installation wird gestartet. Das Installationsprogramm zeigt das folgende Fenster an:

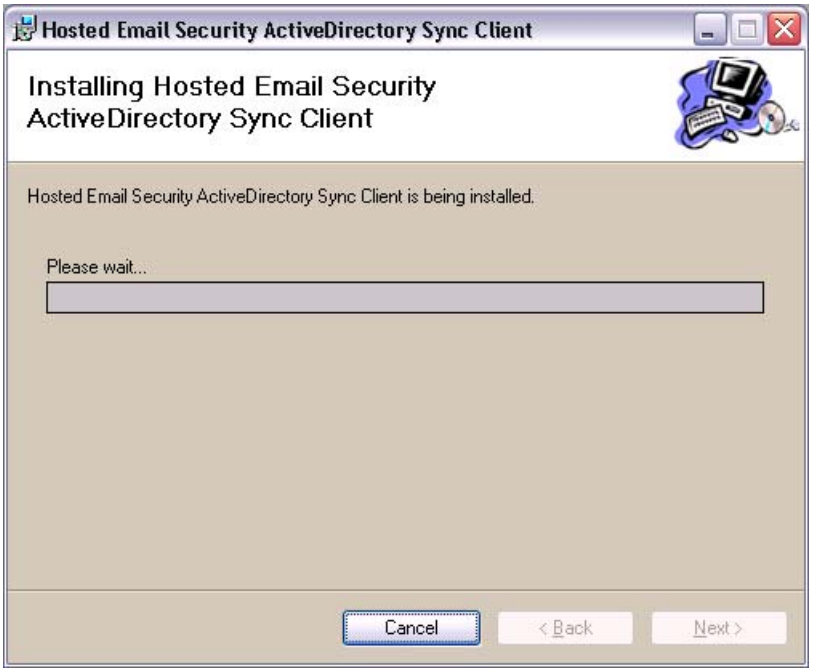


ABBILDUNG C-7. Das Fenster „Installieren“

Nach erfolgreichem Abschluss der Installation zeigt das Installationsprogramm das folgende Fenster an.

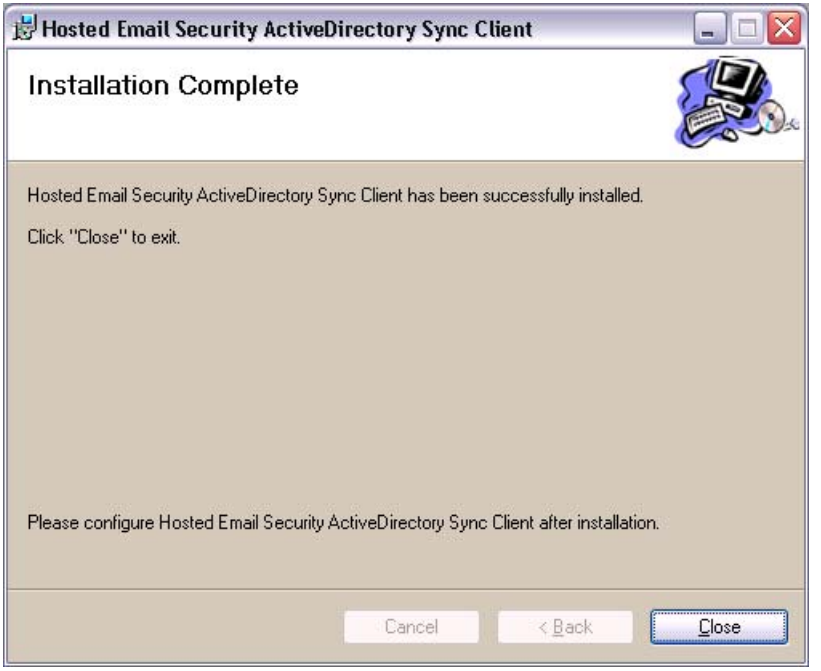


ABBILDUNG C-8. Das Fenster „Installation abgeschlossen“

8. Klicken Sie auf **Schließen**, um die Installation zu beenden. Geben Sie ein, dass es sich um eine Erstkonfiguration des Hosted Email Security ActiveDirectory Sync Clients handelt.

Den ActiveDirectory Sync Client konfigurieren

Nach der Installation des Hosted Email Security ActiveDirectory Sync Clients müssen zunächst einige Parameter konfiguriert werden. Erst dann können mit Hilfe des Clients E-Mail-Adressen aus dem Active Directory mit dem Hosted Email Security Service synchronisiert werden.

Der Hosted Email Security ActiveDirectory Sync Client wird nach Abschluss der Installation automatisch gestartet. Es sind drei Konfigurationsschritte erforderlich:

- *LDAP-Pfad (ActiveDirectory) einstellen* auf Seite C-11
- *Die Netzwerkeinstellungen konfigurieren* auf Seite C-12
- *Suchkriterien ändern* auf Seite C-15
- *Verlaufsprotokoll anzeigen* auf Seite C-20

LDAP-Pfad (ActiveDirectory) einstellen

Der LDAP-Pfad wird im Hauptfenster eingestellt. Geben Sie den LDAP-Pfad (ActiveDirectory) ein, über den der Client die E-Mail-Adressdaten abrufen kann.

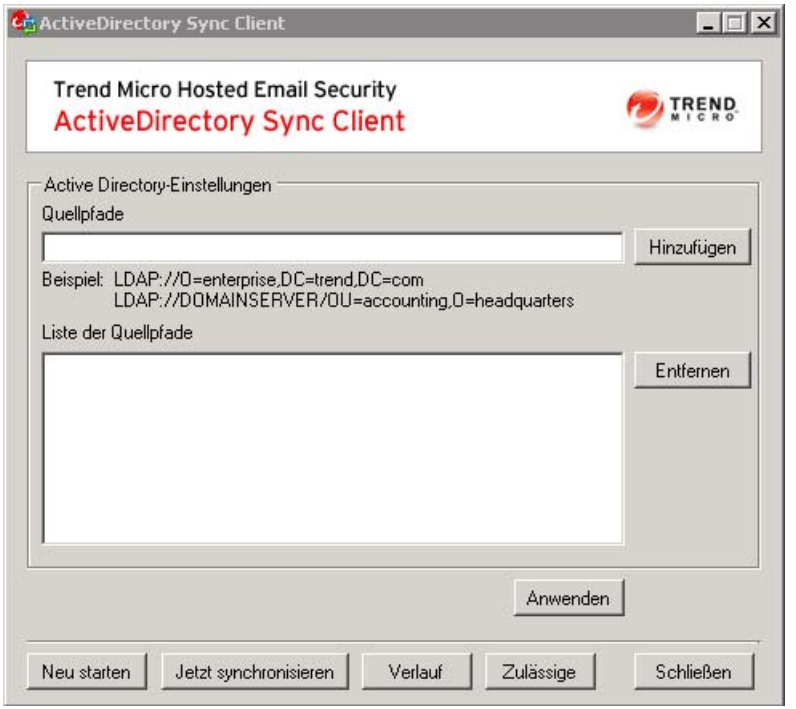


ABBILDUNG C-9. Den Hosted Email Security ActiveDirectory Pfad einstellen

Sie können einen oder mehrere LDAP-Pfade eingeben, über die der Synchronisierungsclient die E-Mail-Adressdaten von Benutzern abrufen kann.

Die Netzwerkeinstellungen konfigurieren

Die Konfiguration des Netzwerks umfasst die folgenden Einstellungen:

Zugriffsauthentifizierung

Um auf die Hosted Email Security Web-Services-Anwendungen zuzugreifen, sind bestimmte Netzwerkparameter erforderlich. Klicken Sie unten im Hauptfenster auf **Konfigurieren**, um die Netzwerkeinstellungen zu konfigurieren. Das Dialogfenster „Netzwerkeinstellungen“ wird angezeigt.

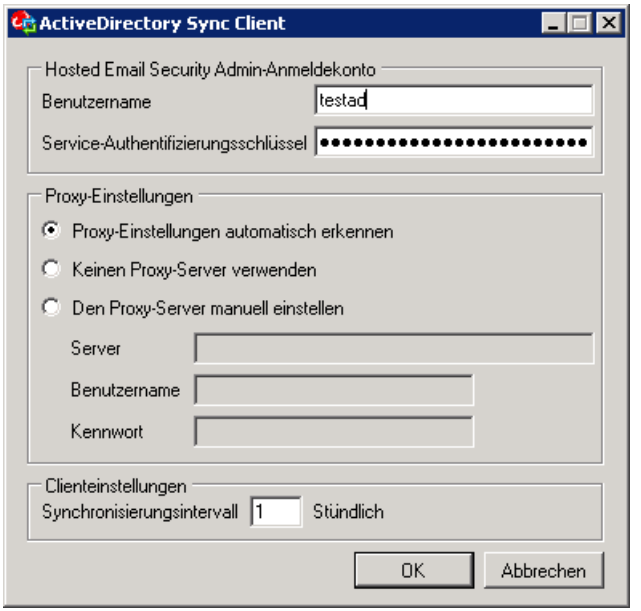


ABBILDUNG C-10. Das Dialogfeld „Netzwerkeinstellungen“

Das Anmeldekonto enthält die Anmeldedaten für den Zugriff auf die Web-Services:

- „Benutzername“ ist der Anmeldename, mit dem der Benutzer auf die Hosted Email Security Administrationskonsole zugreift. Hinweise hierzu finden Sie im Begrüßungsschreiben, das Sie bei der Anmeldung an den Hosted Email Security Service erhalten haben.
- „Service-Authentifizierungsschlüssel“ ist der APIKEY, der auf der Hosted Email Security Administrationskonsole zur Authentifizierung des Hosted Email Security Web-Services-Zugriffs generiert wurde.

Proxy-Einstellungen

Zurzeit werden nur HTTP-Proxy-Server unterstützt. Es können drei unterschiedliche Proxy-Einstellungen konfiguriert werden:

- Keinen Proxy-Server verwenden.
- Proxy-Einstellungen automatisch erkennen. Die Proxy-Einstellung des Microsoft Internet Explorers verwenden.
- Den Proxy-Server manuell einstellen. Geben Sie in die Textfelder unter **Den Proxy-Server manuell einstellen** die erforderlichen Daten ein.

Wenn Sie auf **OK** klicken, um die Proxy-Einstellungen zu bestätigen, versucht der Hosted Email Security ActiveDirectory Sync Client, eine Testverbindung zu den Hosted Email Security Web-Services herzustellen. Kann keine Verbindung zu den Hosted Email Security Web-Services hergestellt werden, wird die folgende Fehlermeldung angezeigt:

ABBILDUNG C-11. Fehlermeldung „Web-Services nicht erreichbar“

Synchronisierungsintervall

Das Synchronisierungsintervall bestimmt die Häufigkeit, mit der der Hosted Email Security ActiveDirectory Sync Client im Active Directory nach Updates der Benutzerkonten sucht. Die erste Synchronisierung beginnt ein Intervall nach dem Start des AD Sync Clients. Das Mindestintervall beträgt 1 Stunde. Es wird empfohlen, maximal 24 Stunden als Intervall einzustellen.

Enthält das ActiveDirectory sehr viele Benutzer, sollte das Synchronisierungsintervall auf mindestens 4 Stunden eingestellt werden, damit der Vorgang innerhalb des angegebenen Intervalls vollständig ausgeführt werden kann. Sich überschneidende Synchronisierungsintervalle werden nacheinander ausgeführt. Es wird jedoch empfohlen, ein ausreichend langes Synchronisierungsintervall zu wählen.

Funktion „Jetzt synchronisieren“

Falls erforderlich, können Sie eine Synchronisierung auch vorziehen, indem Sie im AD Sync Client auf die Schaltfläche **Jetzt synchronisieren** klicken (siehe die unten stehende Abbildung C-12).

Hinweis: Wenn Sie während einer zeitgesteuerten Synchronisierung auf **Jetzt synchronisieren** klicken, erfolgt die neue Synchronisierung nach Abschluss des zeitgesteuerten Vorgangs.

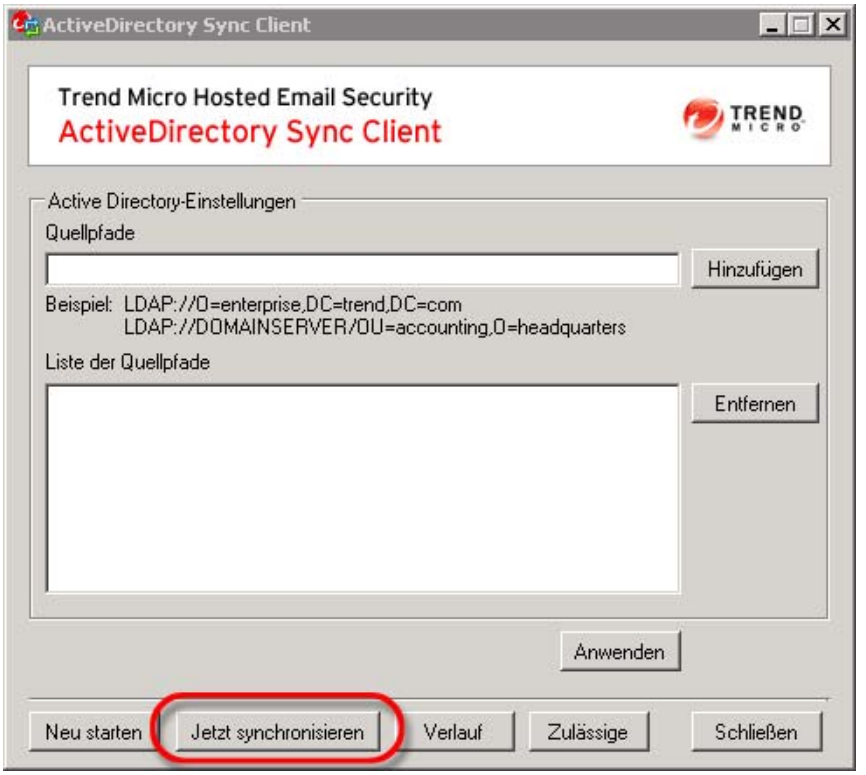


ABBILDUNG C-12. Hosted Email Security AD Sync Client mit der Schaltfläche „Jetzt synchronisieren“

Suchkriterien ändern

Standardmäßig sucht der Hosted Email Security ActiveDirectory Sync Client nach einer Objektklasse **`User`** und den dazugehörigen drei Attributen:

- `displayName`
- `mail`
- `proxyAddresses`

Diese Standardeinstellungen sind in der XML-Konfigurationsdatei ***IMHS_AD_ACL.config*** festgelegt. Der Inhalt dieser Datei wird in der unten stehenden Abbildung C-13 angezeigt. Alle Pfade, die über die Benutzeroberfläche geändert werden, verwenden diese Standardeinstellungen.

IMHS_AD_ACL.config

```
<?xml version="1.0" encoding="utf-8"?>
<ad_acl>
    <ldap_path name="default">
        <objectClass name="User">
          <displayNameAttr>displayName</displayNameAttr>
          <emailAttr>mail</emailAttr>
          <emailAttr>proxyAddresses</emailAttr>
        </objectClass>
    </ldap_path>
</ad_acl>
```

ABBILDUNG C-13. Standardwerte der Datei IMHS_AD_ACL.config

Der Client bietet jedoch die Möglichkeit, diese Standardwerte bei Bedarf zu ändern. Wenn der Client z. B. aus Vertraulichkeitsgründen ausschließlich Proxy-Adressen (keine E-Mail-Adressen oder Anzeigenamen) suchen soll, können diese Einstellungen in der Konfigurationsdatei geändert werden. Dies zeigt die unten stehende Abbildung C-14.

IMHS_AD_ACL.config*

```
<?xml version="1.0" encoding="utf-8"?>
<ad_acl>
    <ldap_path name="default">
        <objectClass name="User">
          <emailAttr>proxyAddresses</emailAttr>
        </objectClass>
    </ldap_path>
</ad_acl>
```

ABBILDUNG C-14. IMHS_AD_ACL.config mit geänderten Werten

Sie können den Standardwert unverändert lassen und weitere alternative Pfadnamen wie in Abbildung C-15 hinzufügen.

```
<?xml version="1.0" encoding="utf-8"?>

<ad_acl>
     <ldap_path name="default">
       <objectClass name="user">
         <displayNameAttr>displayName</displayNameAttr>
          <emailAttr>mail</emailAttr>
          <emailAttr>mail</emailAttr>
       </objectClass>
       <objectClass name="group">
         <displayNameAttr>displayName</displayNameAttr>
          <emailAttr>mail</emailAttr>
       </objectClass>
     </ldap_path>

     <ldap_path name="LDAP://OU=fake,O=cup,C=us">
       <objectClass name="user">
         <displayNameAttr>displayName</displayNameAttr>
          <emailAttr>mail</emailAttr>
          <emailAttr>mail</emailAttr>
       </objectClass>
       <objectClass name="contact">
         <displayNameAttr>displayName</displayNameAttr>
          <emailAttr>mail</emailAttr>
       </objectClass>
     </ldap_path>
<ad_acl>
```

ABBILDUNG C-15. IMHS_AD_ACL.config mit unverändertem Standardwert und neu hinzugefügten Pfadnamen

Sie können außerdem benutzerdefinierte Objektklassen oder Attributnamen hinzufügen. Wenn Sie die Konfigurationsdatei ändern, speichern Sie die Änderungen, und starten Sie den Client neu, damit die Änderungen wirksam werden.

Hinweis: Das Tag **<ad_acl>** ist das Root-Tag in dieser XML-Datei. Sie können zwar mehrere **<ldap_path>**-Blöcke hinzufügen, es dürfen jedoch nur ein öffnendes **<ad_acl>**-Tag und ein schließendes **</ad_acl>**-Tag in der `IMHS_AD_ACL.config`-Datei vorhanden sein.

Objektklassen vererben

Im Active Directory Schema können Objektklassen vererbt werden. Wird eine Objektklasse in ***`IMHS_AD_ACL.config`*** konfiguriert, werden auch die Objekte der untergeordneten Klassen über diesen LDAP-Pfad abgerufen. Dies sollte bei einer Änderung der ACL-Konfigurationsdatei beachtet werden.

In der Konfigurationsdatei A, der ersten der beiden in Abbildung C-16 angezeigten Beispieldateien, ist die Klasse **inetOrgPerson** eine Subklasse von **user**. Wird für denselben LDAP-Pfad die Objektklasse **user** wie in der Beispieldatei B konfiguriert, berücksichtigt die Abfrage auch **inetOrgPerson** Objekte. Beide Konfigurationsdateien würden also dieselben Objekte zurückgeben.

Beispieldatei A

```
<?xml version="1.0" encoding="utf-8"?>
   <ad_acl>
      <ldap_path name="default">
         <objectClass name="user">
         …….
         </objectClass>
         <objectClass name="inetOrgPerson">
         …….
         </objectClass>
      </ldap_path>
   </ad-acl>
```

Beispieldatei B

```
<?xml version="1.0" encoding="utf-8"?>
   <ad_acl>
      <ldap_path name="default">
         <objectClass name="user">
         …….
         </objectClass>
      </ldap_path>
   </ad-acl>
```

ABBILDUNG C-16. Zwei IMHS_AD_ACL.config Beispieldateien zur Veranschaulichung, wie der Client mit Vererbung umgeht

Die Konfiguration von **inetOrgPerson** ist nicht erforderlich. Wenn jedoch **inetOrgPerson** aus der ACL-Datei entfernt und **user** beibehalten wird, werden Objekte der Klasse **inetOrgPerson** weiterhin abgerufen. Wenn eine Objektklasse

also aus der ACL-Datei entfernt wird, werden die dazugehörigen Einträge auf dem Server ebenfalls gelöscht, sofern sie nicht in anderen Objektklassen in der ACL-Datei angegeben sind.

Hinweis: Hosted Email Security speichert diese Konfigurationsdatei, um sie später wieder zu verwenden. Dies gilt auch bei einer erneuten Installation des Clients.

Verlaufsprotokoll anzeigen

Der Hosted Email Security ActiveDirectory Sync Client protokolliert Transaktionen. Sie können die letzten Transaktionen anzeigen, indem Sie auf **Verlauf** klicken.

Die Verlaufsinformationen enthalten drei Spalten: Zeitstempel, Ereignis und Gründe, wie in Abbildung C-17 angezeigt.

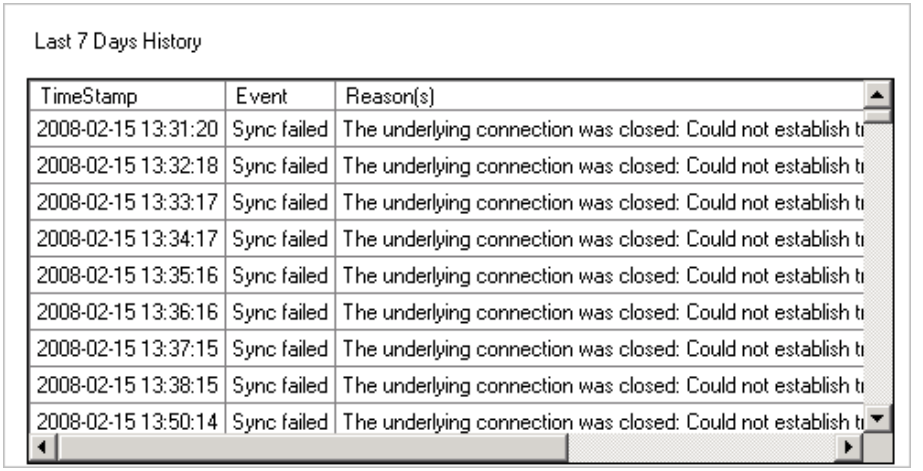


ABBILDUNG C-17. Verlaufsprotokoll

Anhang D

Hosted Email Security Web-Services Befehlszeilen-Referenz und -Programmierhandbuch

Dieser Anhang richtet sich nur an erfahrene Hosted Email Security Administratoren. Wenn Sie planen, die Hosted Email Security Web-Services über eine Befehlszeile in einer Unix-/Linux- oder Windows Umgebung zu verwenden und den Import gültiger E-Mail-Empfängeradressen zu automatisieren, können Sie diesen Befehlszeilen-Client in einem Cron-Job oder einem zeitgesteuerten Task verwenden.

Hinweis: Zielgruppe für dieses Handbuch sind erfahrene Hosted Email Security Administratoren und Tool-Entwickler. Der Leser sollte mit der Programmierung in Skriptsprachen und dem Testen von Software vertraut sein, um die vorliegenden Informationen zu verstehen.

Gültige E-Mail-Empfänger warten und mit Hosted Email Security synchronisieren

Wenn Sie eine Liste gültiger E-Mail-Empfänger für verwaltete E-Mail-Domains in einer kommaseparierten (CSV) Datei verwalten, können Sie diese Benutzerbereitstellung für Hosted Email Security mit Hilfe des Web-Services-Clients automatisieren.

Die meisten Hosted Email Security Administratoren werden ausschließlich die Aktion **sync-users** des Web-Services-Clients verwenden. Vielleicht warten Sie Ihre verwaltete Domain `example.com` in einer CSV-Datei ***`example_com.txt`***, wie in dem folgenden Beispiel:

```
alligator@example.com, Alli Gator
buffalo@example.com, Buffa Lo
crocodile@example.com, Croc O'Dile
donkey@example.com, Don Key
```

ABBILDUNG D-18. Beispieltextdatei

Erstellen Sie einfach einen **Cron**-Job, der eine Befehlszeilenaktion wie die folgende ausführt:

```
[imhs_admin@localhost]#./imhs-cmd -a sync-users -t csv -f example_com.txt
```

ABBILDUNG D-19. Beispiel für eine Befehlszeilenaktion in einem Cron-Job

Hierfür brauchen Sie die E-Mail-Benutzer nur fortlaufend in der Textdatei zu warten. Die E-Mail-Adressen werden mit dem Hosted Email Security Service in regelmäßigen Intervallen (entsprechend des crontab-Zeitplans) synchronisiert.

Einen benutzerdefinierten Hosted Email Security Web-Services-Client programmieren

Trend Micro unterstützt zurzeit keine Programmierumgebung für Kunden, die benutzerdefinierte Hosted Email Security Web-Services-Clients erstellen wollen.

ACHTUNG! **Wenn Sie sich dafür entscheiden, Ihre eigenen Hosted Email Security Web-Services aufzubauen, können die Mitarbeiter des Trend Micro Rundum-Supports Sie bei Erstellung, Verwaltung oder Test des Client-Programms nicht unterstützen.**

Handbuch zur Verwendung von Client-Befehlen für die Hosted Email Security Web-Services

Die folgenden Abschnitte beschreiben die Verwendung von `imhs-cmd.rb`.

Verwendung:

```
imhs-cmd.rb [Optionen]
```

TABELLE D-1. Spezifische Optionen

OPTION	BESCHREIBUNG
`-a, --action AKTION`	Verzeichnisaktionen {list-domains|list-users|add-user|delete-user|delete-users|replace-users|merge-users|sync-users}
`-u, --user [BENUTZER-E-MAIL]`	E-Mail-Adresse des Benutzers
`-n, --name [VOLLSTÄNDIGER NAME]`	E-Mail-Adresse des Benutzers
`-d, --domain [DOMAIN-NAME]`	Name der Domain
`-t, --type [DATEITYP]`	Typ der Eingabedatei {csv}

TABELLE D-1. Spezifische Optionen

OPTION	BESCHREIBUNG
`-f, --file [DATEIPATH]`	Pfad der Eingabedatei
`-c, --config [PFAD DER CONFIG-DATEI]`	Alternative imhs-config.rb-Datei

Hinweis: Erstellen Sie vor der Verwendung in `imhs-config.rb` den Kontonamen und den APIKEY.

TABELLE D-2. Allgemeine Optionen

OPTION	BESCHREIBUNG
`-h, --help`	Diese Nachricht anzeigen
`--version`	Version anzeigen

Beispiele

Dieser Abschnitt enthält Verwendungsbeispiele für Client-Befehle.

Benutzerverzeichnis aus einer Datei synchronisieren

example_com.txt ist ein Beispiel für die Synchronisierung des Benutzerverzeichnisses aus einer CSV-Datei. ***example_com.txt*** ist eine CSV-Datei mit folgendem Inhalt:

```
alligator@example.com, Alli Gator

buffalo@example.com, Buffa Lo

crocodile@example.com, Croc O'Dile

donkey@example.com, Don Key

[imhs_admin@localhost]# ./imhs-cmd.rb -a sync-users -t csv -f example_com.txt

SUCCESS REPLACE: example.com with 4 users
```

Mail-Domains anzeigen

Das folgende Beispiel zeigt die verwalteten Mail-Domains an:

```
[imhs_admin@localhost]# ./imhs-cmd.rb -a list-domains example.com
```

Das gesamte Benutzerverzeichnis ersetzen

Im Beispiel ***UserDirReplaceExample.txt*** wird das gesamte Benutzerverzeichnis einer verwalteten Mail-Domain (***example.com***) aus einer kommaseparierten CSV-Datei ersetzt. ***UserDirReplaceExample.txt*** ist eine CSV-Datei mit folgendem Inhalt:

```
hr@example.com,Human Resource Dept
jack_customer@example.com,Jack Customer
jill_user@example.com,Jill Manager
tech_support@example.com,Tech Support
us_sales@example.com,US Sales Team
[imhs_admin@localhost]# ./imhs-cmd.rb -a replace-users -t csv
-f UserDirReplaceExample.txt
SUCCESS REPLACE: example.com with 5 users
```

Die Benutzer einer Mail-Domain anzeigen

Das folgende Beispiel zeigt die Benutzer einer verwalteten Mail-Domain an:

```
[imhs_admin@localhost]# ./imhs-cmd.rb -a list-users -d
example.com
hr@example.com,Human Resource Dept
jack_customer@example.com,Jack Customer
jill_user@example.com,Jill Manager
tech_support@example.com,Tech Support
us_sales@example.com,US Sales Team
```

Benutzer einfügen

Im Beispiel ***UserDirMergeExample.txt*** werden Benutzer einer verwalteten Mail-Domain (**example.com**) aus einer CSV-Textdatei eingefügt. ***UserDirMergeExample.txt*** ist eine CSV-Datei mit folgendem Inhalt:

```
bonnie_clyde@example.com,Bonnie Anne Clyde

leo_da_vinci@example.com,Leonardo da Vinci

w_a_mozart@example.com,Wolfgang Amadeus Mozart

[imhs_admin@localhost]# ./imhs-cmd.rb -a merge-users -t csv -f
UserDirMergeExample.txt

SUCCESS MERGE: example.com with 3 users
```

Einen einzelnen Benutzer hinzufügen

Im folgenden Beispiel wird ein einzelner Benutzer, `orville_wilbur@example.com`, zu einer verwalteten E-Mail-Domain (**example.com**) hinzugefügt:

```
[imhs_admin@localhost]# ./imhs-cmd.rb -a add-user -u
orville_wilbur@example.com

SUCCESS ADDUSER orville_wilbur@example.com
```

Einen einzelnen Benutzer löschen

Im folgenden Beispiel wird ein einzelner Benutzer, `bonnie_clyde@example.com`, aus einer verwalteten E-Mail-Domain (**example.com**) gelöscht:

```
[imhs_admin@localhost]# ./imhs-cmd.rb -a delete-user -u
bonnie_clyde@example.com

SUCCESS DELETEUSER bonnie_clyde@example.com.
```

Ausgewählte Benutzer löschen

Im Beispiel ***UserDirDeleteExample.txt.*** werden ausgewählte Benutzer aus einer verwalteten Mail-Domain (**example.com**) entsprechend der angegebenen Datei gelöscht. ***UserDirDeleteExample.txt*** ist eine CSV-Datei mit folgendem Inhalt:

```
jack_customer@example.com,Jack Customer

jill_user@example.com,Jill Manager

[imhs_admin@localhost]# ./imhs-cmd.rb -a delete-users -t csv -f
UserDirDeleteExample.txt

SUCCESS DELETE: example.com with 2 users
```