TREND MICRO™

Hosted Email Security

Integrated email threat protection in a hosted service

Web Services Guide

Messaging Security

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before using this service and installing the software, please review the latest version of the applicable user documentation, which is available from the Help drop-down list at the top of the screen (**Help > Download Manual**).

Trend Micro, the Trend Micro t-ball logo, TrendLabs, Trend Micro Control Manager, and Trend Micro Damage Cleanup Services are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 2008-2010 Trend Micro Incorporated. All rights reserved.

Document Part No. HSEM04284_91229

Publication Date: March 18, 2010

Protected by U.S. Patent No. 5,623,600; 5,951,698; 5,983,348; 6,272,641

The user documentation for Trend Micro™ Hosted Email Security is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at the Trend Micro web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

Contents

Preface

Chapter 1: Installing the Hosted Email Security Web Services Client

Chapter 2: Using the Hosted Email Security Web Services Client

Chapter 3: Troubleshooting

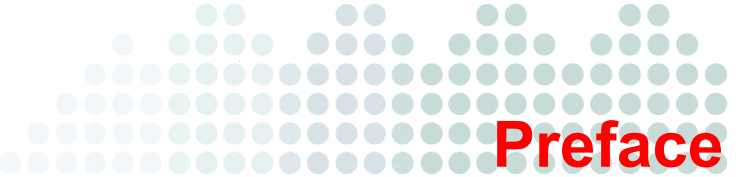
Appendix A: Hosted Email Security Web Services Applications

Appendix B: ActiveDirectory Sync Client Architecture

Appendix C: ActiveDirectory Sync Client Installation and Configuration

Appendix D: Hosted Email Security Web Services Command-Line Reference and Programming Guide

List of Figures



Preface

Welcome to the *Trend Micro™ Hosted Email Security Web Services Guide*. This book contains information about automating Hosted Email Security administrative tasks.

This preface discusses the following topics:

Hosted Email Security Documentation

The Trend Micro™ Hosted Email Security documentation consists of the following:

Online Help—Helps you configure all features through the user interface. You can access the online help by opening the web console and then clicking the help icon ().

Quick Start Card—Helps you quickly get your service set up.

Administrator's Guide—Helps you plan for deployment and configure all service settings.

Web Services Guide—Helps you to automate Hosted Email Security administrative tasks.

Web End User Quarantine User Guide—Helps you understand how to manage spam mail held in quarantine using the Trend Micro Web End User Quarantine.

The *Administrator's Guide* and the *Web End User Quarantine User Guide* are available at:
http://us.trendmicro.com/us/products/enterprise/hosted-email-security

Audience

The Hosted Email Security documentation is written for Hosted Email Security administrators who want to automate tasks without visiting the web console. The documentation assumes that the reader has in-depth knowledge of email messaging networks, including details related to the following:

- SMTP protocol
- Message Transfer Agents (MTAs)

The documentation does not assume the reader has any knowledge of antivirus or anti-spam technology.

Document Conventions

To help you locate and interpret information easily, the Hosted Email Security documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

Chapter 1

Installing the Hosted Email Security Web Services Client

Trend Micro™ Hosted Email Security Web Services provide the mechanism for automating administrative tasks such as importing valid recipient email addresses into Hosted Email Security.

This document guides you through the steps to set up a client to communicate with Hosted Email Security Web Services and to customize the automation of supported Hosted Email Security administrative tasks.

Supported Hosted Email Security Web Services Applications

One of the most troubling spam problems these days is the reverse NDR attack (Non-Delivery Receipt or bounce message) or more commonly known as backscatter spam. Spammers are exploiting mail servers that reply with courtesy NDRs by sending out spam messages with "spoofed" senders and recipients. The spoofed sender is the actual target of the spam. Mail servers that send NDRs unknowingly become the sources for such backscatter spam.

The most effective way to thwart such an attack is to import your valid recipient email addresses to Hosted Email Security service. The advantage is significant, reducing the risk of being listed by email abuse reputation services such as Trend Micro Email Reputation Services. In addition, this measure greatly reduces the bandwidth consumption in your operating environment due to directory harvest attacks (DHA).

The Hosted Email Security administrative console provides a user directory import function for the mail administrators to import and maintain their valid recipient email addresses. LDIF (LDAP Data Interchange Format) file or CSV (comma-separated value) file formats are accepted. However, if you choose not to use the administrative console, you can use the Hosted Email Security Web services application. In addition to accepting an LDIF and CSV file of valid mail recipients, a sample ActiveDirectory plug-in client (Hosted Email Security ActiveDirectory Sync Client) is also provided for customers who use ActiveDirectory.

The mail administrator selects a client program that is suitable for the mail environment to communicate with Hosted Email Security Web services. The client program can import valid mail recipients or list current valid mail recipients in effect in Hosted Email Security for the mail domain. Currently, the following Hosted Email Security Web service clients are available for download:

- Hosted Email Security ActiveDirectory Sync Client, a Microsoft ActiveDirectory client, is available for the Windows environment with ActiveDirectory. This program is a single-purpose client program for importing valid email addresses into the Hosted Email Security service.
- The Hosted Email Security Web service client (imhs_web_svc_client) is an OS-independent, command-line client that supports various Hosted Email Security Web services applications. Currently, the Hosted Email Security Web service client supports Hosted Email Security email account sync for importing valid recipient email addresses in CSV formats. Hosted Email Security email account sync is functionally equivalent to the user directory import feature on the administrative console.

For details on how to download and install a Hosted Email Security Web services client, see *Installing the Web Services Client* on page 1-4.

Installing the Web Services Client

The Hosted Email Security Web services client programs are sample implementations of how you can communicate with Hosted Email Security Web services applications from your operating environment.

The topics in this chapter guide you through selecting, installing, configuring, and using an Hosted Email Security Web services client program, including how to:

- Choose a Hosted Email Security Web services client program
- Install the Hosted Email Security Web services client
- Use the Hosted Email Security Web services client to automate your Hosted Email Security administrative tasks

Choosing a Hosted Email Security Web Services Client Program

Two Hosted Email Security Web services client programs are available:

- A sample implementation (imhs_web_svc_client - Hosted Email Security Web services client) for communicating with Hosted Email Security Web services applications
- An ActiveDirectory-specific (single-purpose) plug-in client program (Hosted Email Security ActiveDirectory Sync Client) for customers who maintain their valid email recipients using ActiveDirectory in the Windows environment

Which Hosted Email Security Web services client program is right for you depends on your needs.

If you are interested in automating other Hosted Email Security administrative tasks using Hosted Email Security Web services, you should install the sample client program (imhs_web_svc_client - Hosted Email Security Web services client).

If you are using ActiveDirectory to maintain your valid mail recipients and want to automate the process of importing valid recipient email addresses into the Hosted Email Security service for your managed domains, you should install the Hosted Email Security ActiveDirectory plug-in client (Hosted Email Security ActiveDirectory Sync Client) for importing valid recipient email addresses.

Whereas the ActiveDirectory plug-in runs only in the Windows environment, the Hosted Email Security Web services client is OS independent.

System Requirements

Before downloading the selected Hosted Email Security Web services client as described in the next section, check the minimum system requirements below.

Microsoft ActiveDirectory Plug-In Client

Hosted Email Security ActiveDirectory Sync Client is the Microsoft ActiveDirectory plug-in client. Before installing the client, you should first check the minimum system requirements. Minimum system requirements and installation:

- Windows 2003 Server or Windows XP Professional SP2
- Minimum 512MB memory
- Minimum 100MB available disk space
- Internet Explorer 6.0
- End-user email addresses are maintained in ActiveDirectory
- Network access to:
  - **https://us.imhs-ws.trendmicro.com** if your Hosted Email Security administrative console is **https://us.emailsec.trendmicro.com**
  - **https://imhs-ws.trendmicro.eu** if your Hosted Email Security administrative console is **https://emailsec.trendmicro.eu**

If you choose to install Hosted Email Security ActiveDirectory Sync Client, the Microsoft ActiveDirectory plug-in client, execute the downloaded self-extracting Windows ***setup.exe*** installation program. Follow the on-screen instructions to complete the installation.

For more information about the installation, please refer to *Using ActiveDirectory Plug-In Client to Synchronize ActiveDirectory Email Accounts* on page 2-3.

OS-Independent Hosted Email Security Web Services Client

A sample implementation of Hosted Email Security Web services client, imhs_web_svc_client, is provided for your convenience. The client is written in the Ruby scripting language. It is supported across most operating systems.

Minimum System Requirements and Installation

Linux or Unix

- Ruby v1.8.6 or later (if Ruby is already installed, you can enter **ruby -v** on a command line to find out the version). If Ruby has not been installed, download Ruby from `http://www.ruby-lang.org/en/downloads/`. For you convenience, it is included in the Linux/Unix Hosted Email Security Web services client package that you downloaded.
- Follow the instructions to install Ruby.
- Ruby gem (Ruby utility to install additional package) for rest-open-uri. Ruby rest-open-uri gem is an open source Ruby utility that you will need. You can download rest-open-uri gem from `http://rubyforge.org/frs/?group_id=2778&release_id=8581`. For you convenience, it is included in the Linux/Unix Hosted Email Security Web services client package you downloaded.
- Install ***`rest-open-uri gem`***: execute **gem install rest-open-uri** on a command line.
- RPM environment for Linux or ***`.deb`*** files for Debian, Ubuntu, and others.
- Hosted Email Security Web services client assumes default Ruby install path is `/usr/bin/ruby`
- Network access to:
  - `https://us.imhs-ws.trendmicro.com` if your Hosted Email Security administrative console is `https://us.emailsec.trendmicro.com`
  - `https://imhs-ws.trendmicro.eu` if your Hosted Email Security administrative console is `https://emailsec.trendmicro.eu`
- If the Ruby environment is behind a firewall, execute **gem install -p <your-proxy-url> rest-open-uri** on a command line after installation. **<your-proxy-url>** is the URL of the proxy server commonly in the form of ***`http://proxy.yourdomain.com:proxy-port`***. For example: ***`http://proxy.example.com:8080`***. The current rest-open-uri is v1.0.0.

Windows

- Ruby v1.8.6 or later (if Ruby is already installed, you may enter **ruby -v** on a command line to find out the version). If Ruby has not been installed, download Ruby from http://www.ruby-lang.org/en/downloads/. For you convenience, it is included in the Windows Hosted Email Security Web services client package that you downloaded.
- Follow the instructions to install Ruby.
- Ruby gem (Ruby utility to install additional package) for rest-open-uri. Ruby rest-open-uri gem is an open source Ruby utility that you will need. You can download rest-open-uri gem from http://rubyforge.org/frs/?group_id=2778&release_id=8581. For you convenience, it is included in the Windows Hosted Email Security Web services client package that you downloaded.
- Install ***rest-open-uri gem***: Enter **gem install rest-open-uri** at a DOS command prompt.
- Network access to:
  - https://us.imhs-ws.trendmicro.com if your Hosted Email Security administrative console is https://us.emailsec.trendmicro.com
  - https://imhs-ws.trendmicro.eu if your Hosted Email Security administrative console is https://emailsec.trendmicro.eu
- If the Ruby environment is behind a firewall, execute **gem install -p <your-proxy-url> rest-open-uri** at a DOS command prompt after installation. **<your-proxy-url>** is the URL of the proxy server commonly in the form of http://proxy.yourdomain.com:proxy-port. For example, http://proxy.example.com:8080. The current open source Ruby utility rest-open-uri gem is v1.0.0.

Downloading a Client Program

To download the client program:

1. Log on to the Hosted Email Security administrative console at one of the following addresses:
   - **European region:** https://emailsec.trendmicro.eu
   - **Other regions:** https://us.emailsec.trendmicro.com

   From the Hosted Email Security menu, select **Administration** > **Web Services**.

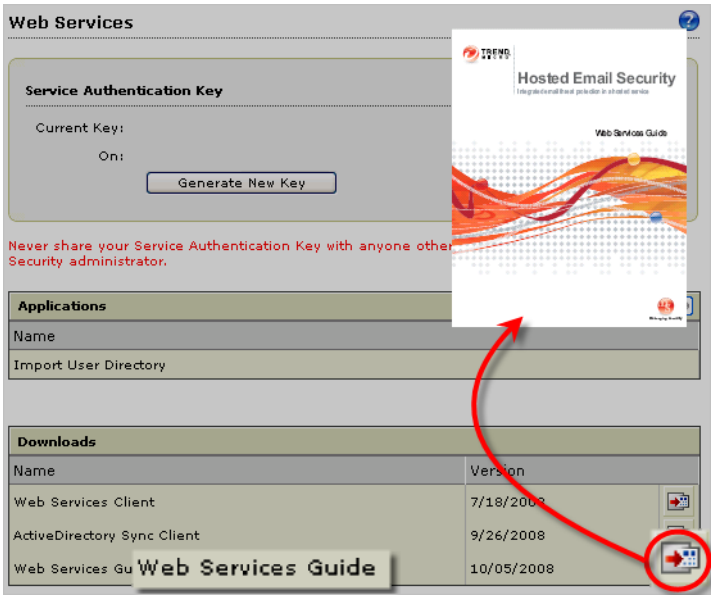


FIGURE 1-1. Downloading this manual from the Hosted Email Security Web Services screen

2. Select the client that is suitable for your operating environment.

Chapter 2

Using the Hosted Email Security Web Services Client

Using Hosted Email Security Web services programs is an effective way to automate some Hosted Email Security administrative tasks such as periodic import of valid mail recipient email addresses for your mail domains.

There are several things you should be aware of before customizing and using your Hosted Email Security Web services client to communicate with Hosted Email Security Web services.

Enabling Hosted Email Security Web Services

Web services programs in Hosted Email Security are disabled for your mail domains by default. In order to allow the Hosted Email Security Web services client to communicate with them for your managed mail domains, log on to the Hosted Email Security administrative console and enable Hosted Email Security Web services. If access to Hosted Email Security Web services has not been enabled, your installed Hosted Email Security Web services client(s) will be unable to communicate with Hosted Email Security Web services.

To enable Hosted Email Security Web services:

1. From the Hosted Email Security menu, select **Administration** > **Web Services**.
2. If Hosted Email Security Web services applications are not already enabled ("Disabled" is displayed on the Web Services screen), you will need to enable Hosted Email Security Web services. To enable the Web services applications, you need to have an APIKEY.

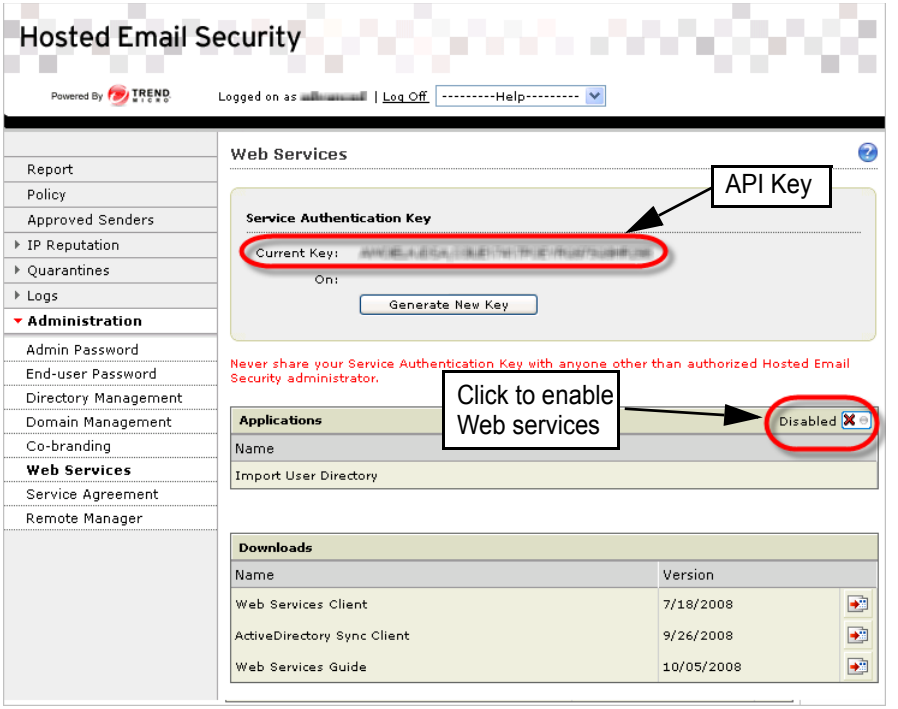


FIGURE 2-1. Hosted Email Security Web Services screen

3. Make sure you have an APIKEY displayed for Current Key, and then click the **Disabled** toggle button to allow your Hosted Email Security Web Services client to communicate with Hosted Email Security Web services applications.

   The Hosted Email Security Web services client uses the APIKEY to authenticate the communication. If an APIKEY is already generated on your administrative console, copy or cut and paste the APIKEY to the Hosted Email Security Web

services client program. Without the APIKEY, your Web services client will be unable to communicate with Hosted Email Security Web services applications.

4. Click **Generate New Key** if no APIKEY was generated before.

For added security, you may choose to periodically generate a new APIKEY by clicking **Generate New Key.** You will then update your Hosted Email Security Web services client with the new authentication APIKEY. Note that once a new APIKEY is generated, the old key becomes obsolete.

Rate Limit for Hosted Email Security Web Services Access

Since the Web services client communicates with Hosted Email Security Web services programmatically (not through the administrative console on a web browser), Hosted Email Security adopts access rate limiting to prevent unintended access such as denial-of-service attacks or programming errors (for example, infinite loop) in customized Hosted Email Security Web services client programs. Such rate limits protect you from being affected by the Web service client programs of others.

Each customer is limited to a maximum of 50 Web service email account synchronization requests per domain per day (UTC time).

Using ActiveDirectory Plug-In Client to Synchronize ActiveDirectory Email Accounts

If your organization utilizes ActiveDirectory to manage your users' email accounts, you can install the ActiveDirectory plug-in client, Hosted Email Security ActiveDirectory Sync Client, on a Windows machine to automate the import of the valid mail recipient user directory into Hosted Email Security to:

- Thwart DHA (directory harvest attack)
- Reduce backscatter spam (reverse NDR attack)

ActiveDirectory Size Limitation

WARNING! Before configuring your Hosted Email Security ActiveDirectory Sync Client, be aware of its limitations, detailed below.

The User Base in your ActiveDirectory May Be Too Large

Under normal conditions, the current version of the ActiveDirectory Sync Client can process up to 250,000 users email addresses of average address length. If you have a very large number of user email addresses in your ActiveDirectory, Hosted Email Security ActiveDirectory sync may not be able to process them.

If you have a very large user email address base in a single ActiveDirectory, try separating the users into multiple LDAP paths to smaller ActiveDirectory databases.

Use of Multiple ActiveDirectory Sync Clients

Trend Micro recommends that you schedule to synchronize only one ActiveDirectory at a time not to overlap the synchronization.

If you use more than one sync client, make sure that they do not sync the same email domain. Otherwise, one client may interfere with the synchronization result of another client.

Handling of Multiple ActiveDirectory Paths or Servers

If you have multiple ActiveDirectory paths or servers for the same email domain to be synchronized, use a single sync client and configure multiple LDAP paths, as shown in *Figure C-16* on page C-17.

For example, if you have two ActiveDirectory paths: A and B. According to the ACL setting, some email addresses of ***abc.com*** will be retrieved from path A. Also in path B there are some other email addresses of ***abc.com***. If you use two sync clients (C1 and C2) to synchronize from A and B separately, then C1 will refresh the server and put on all its result from A, so any email addresses from B will be deleted (and vice-versa). In a case like the above, use a single sync client and configure LDAP path A and B to synchronize their data to the server.

Email Addresses Accepted

In the mail attribute we accept three types of email address:

1. SMTP address with "smtp:" prefix. Email with other prefixes (like X500:) or invalid SMTP address (like person@domain) will be rejected.

Example: ***smtp:person@domain.com***

2. SMTP address.

   Example: ***person@domain.com***

3. Any combination of types 1 and 2 above, separated by a comma (,) or a semicolon (;).
   Example: ***person@domain.com;smtp:Staff_A@domain.com, SMTP:Staff_B@domain.com***

   In the example above, the value will separated into three email addresses.

WARNING! **Almost all email addresses compliant with RFC 822 can be accepted by the ActiveDirectory Sync Client. The only exceptions are those email addresses containing any of the following special characters to the left or right of the "@" sign:** `( ) < > @ , ; : \ " [ ]`

Any email address containing one of the above special characters will be rejected. See *Identifying Invalid Email Addresses* **on page 3-2 for more information.**

All-or-None Synchronization

If you configure multiple LDAP paths, the data synchronization from these LDAP paths will be taken as an "all or none" transaction. If the data synchronization on one or more LDAP paths fails, then the entire synchronization will fail and no data will be synchronized to the server.

Because of this feature, there is no need to provide a failover ActiveDirectory server LDAP path in the AD Sync Client configuration. In fact, doing so is inadvisable, because when more paths are configured, there is a higher chance that one of the paths will fail.

Note: In the event of a failed synchronization, the server will retain the existing data.

If your AD synchronization is continually failing, verify that all LDAP paths are valid and reachable. If the cause is a network or AD server problem (as indicated in the AD Sync Client History list), fix the connectivity problem as soon as possible, so that a complete synchronization can occur.

If You Change the Time on Your Computer, You Must Restart the Hosted Email Security ActiveDirectory Sync Client Service

The Synchronization Interval Must Not Be Smaller than the Time Required to Synchronize the ActiveDirectory Users

If you have a very large ActiveDirectory user base, set your synchronization interval to 4 hours or longer so that the synchronization can be completed within the interval specified. Overlapping synchronization would create error conditions and so is not supported.

To customize your periodic valid mail recipient email addresses import:

1. Start the configuration program and customize your periodic import of valid mail recipient email addresses into the Hosted Email Security ActiveDirectory Sync Client dialog box:

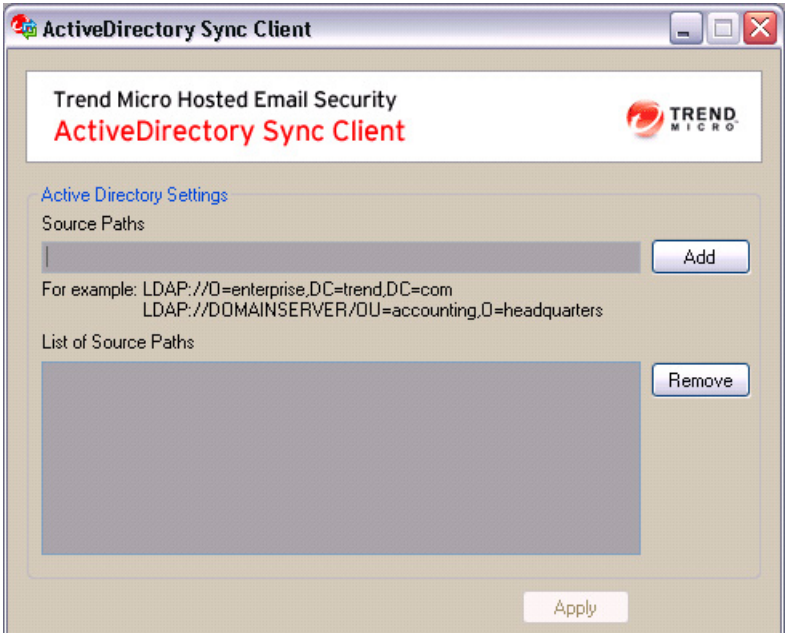


FIGURE 2-2. Hosted Email Security ActiveDirectory Sync Client

2. Follow the guidance on installation and initial configuration of Hosted Email Security ActiveDirectory Sync Client in Appendix C, ActiveDirectory Sync Client Installation and Configuration starting on page C-1.

Example of Periodic Synchronizing User Email Addresses

The following is an example of periodic synchronizing user email addresses from your ActiveDirectory to Hosted Email Security using the ActiveDirectory Sync Client. In this example, **test.com** domain has two users: **abc** and **adam-paul**. You can verify whether Hosted Email Security service has the same information.

To run the example:

1. Enter one of the following URLs in your Web browser:
   - For customers in Europe:
     `https://imhs-ws.trendmicro.eu/imhs/v1.0/en/domains/test.com/users`
   - For customers in other regions:
     `https://us.imhs-ws.trendmicro.com/imhs/v1.0/en/domains/test.com/users`

   A logon pop-up window appears.
2. Enter your Hosted Email Security administrator account name for the user name and your APIKEY for the password.
3. Add a new user named "angel" with the email address **angel@test.com**. For information on how to insert a new user into your ActiveDirectory, consult your ActiveDirectory administrator.

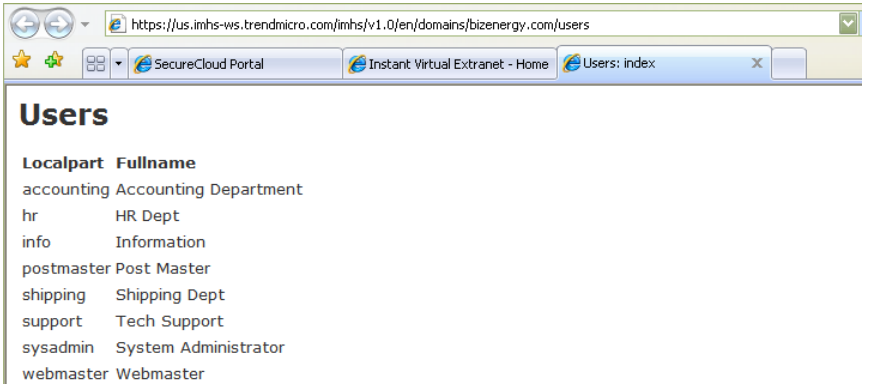


FIGURE 2-3. Viewing email users

The steps to update your ActiveDirectory may be similar to what is described in this example; however, this description is provided for reference only.

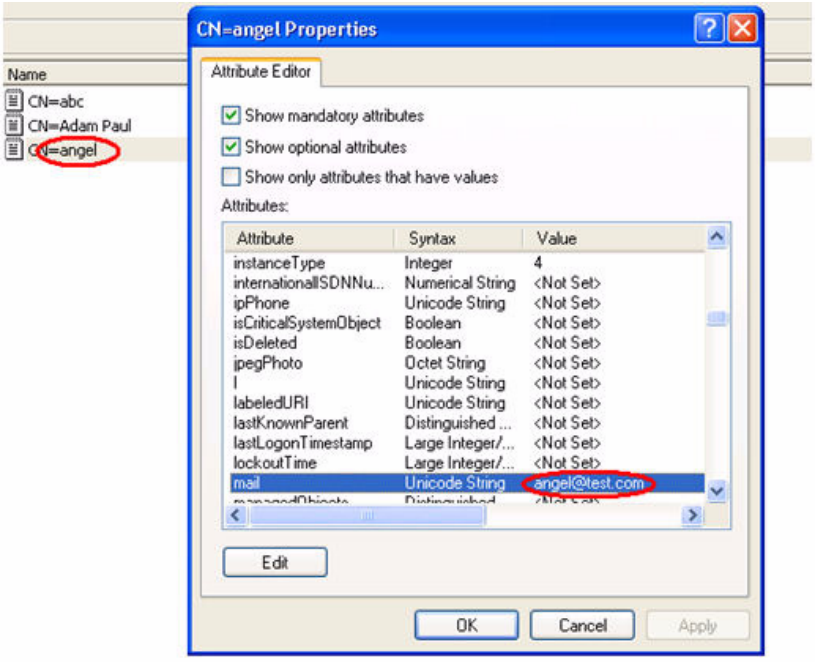


FIGURE 2-4. Example Properties dialog box

In the next synchronized interval—for example, in about 1 hour—Hosted Email Security ActiveDirectory Sync Client will check your ActiveDirectory for changes since the last update and will find **angel@test.com**. It will then push **angel@test.com** to the Hosted Email Security service through Hosted Email SecurityWeb services interface.

4. To verify the result after the synchronization interval, enter one of the following URLs into your Web browser:
   - For customers in Europe:
     `https://imhs-ws.trendmicro.eu/imhs/v1.0/en/domains/test.com/users`
   - For other regions:
     `https://us.imhs-ws.trendmicro.com/imhs/v1.0/en/domains/test.com/users`

   A logon pop-up window appears.

5. Enter your Hosted Email Security administrator account name for the user name and your APIKEY for the password.

   The email address is displayed as shown below.

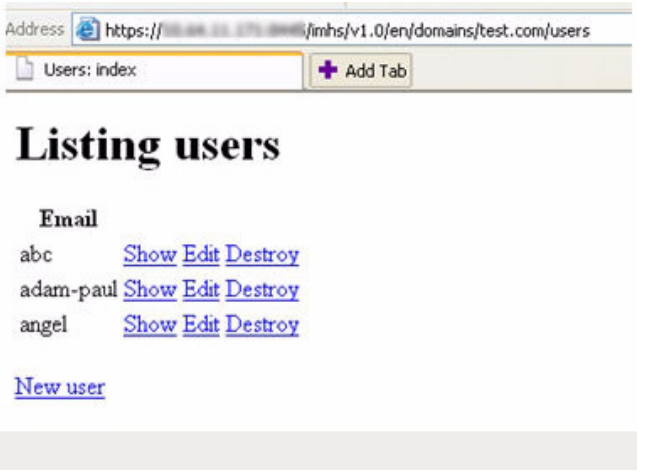


FIGURE 2-5. Result after synchronization

Using Command-Line Hosted Email Security Web Services Client to Synchronize Valid Recipient Email Addresses

If your organization does not utilize ActiveDirectory to manage your users' email accounts, you may import valid mail recipients in plain-text CSV (comma-separated value). Most LDAP servers have a utility to export the contents of the LDAP database into a CSV file.

The following is an example of periodic importing of user email addresses in a CSV file to Hosted Email Security using the OS-independent Hosted Email Security Web services client, ***`imhs_web_svc_client`***.

FIGURE 2-6. Client import CSV

Summary

Here is a quick summary of how to use Hosted Email Security Web services:

1. Log on to the Hosted Email Security administrative console **Administration > Web Services** screen. Remember the current APIKEY on this screen. If this is a new administrator account, there will be no APIKEY.
2. Click **Generate New Key** to generate an APIKEY.
3. Verify that an APIKEY is available and then make sure that Web services applications are "Enabled."
4. Download the Hosted Email Security Web services client program.
5. Follow the Hosted Email Security Web services client installation procedure to set up the client program. You will need the APIKEY for the setup.
6. Configure the client program for your organization.

Chapter 3

Troubleshooting

This chapter describes possible Hosted Email Security Web services issues and solutions for each.

Topics in this chapter include:

Using the AD Sync Client Debug Log

The Active Directory Sync Client keeps debug logs for troubleshooting purposes. The debug log files reside in the following directory:

`[Your_AD_Client_InstallFolder]\log`

There are three types of debug log:

1. History log (under `\log\PluginHistory`)
2. Monitor log (under `\log\PluginMonitor`)
3. Plug-in service log (under `\log\PluginService`)

By default, all three log types are saved for 7 days.

The debug logs are named with the following convention:

{Type of log}-{year}-{month}-{day}.log

For example:

```
YourADSyncClientInstall\log\PluginHistory\PluginHis
tory-2008-5-9.log
YourADSYncClientInstall\log\PluginService\PluginSer
vice-2008-10-24.log
```

Tip: Please submit the relevant log files when contacting Support. Supplying those files will help Trend Micro to resolve the issue faster.

Identifying Invalid Email Addresses

Every time you use the AD Sync Client to synchronize with your AD server, the client keeps a record of any email addresses in your AD server that could not be accepted by inbound or upstream mail servers. (For details as to which email addresses are considered invalid, please see *Email Addresses Accepted* on page 2-4.)

To assist you with identifying such addresses, the AD Sync Client generates a file named `InvalidUsers.txt`, which is placed in your AD Sync Client installation directory.

This file is generated during synchronization, each time completely replacing any previous file of that name. If there are no invalid addresses upon synchronization, an empty file is created. Email addresses are grouped by domain.

Frequently Asked Questions

How do I know whether the sync client program runs properly?

First, you can query the users with a Web browser as in the example in section *Example of Periodic Synchronizing User Email Addresses* on page 2-7.

Also, you can check the history info. If data is successfully synchronized, you will find the successful transaction in the log. If it failed, you will find a failure or error message. You can use the transaction log's "reasons" to aid in diagnosing problems. If no info is recorded, it means no change for the user data. Thus, no synchronization occurred.

What should I do if synchronization failed?

First, check the history info to get the failure reason. If the reason for the synchronization failure is that Hosted Email Security failed to retrieve Active Directory data, try to confirm whether the LDAP path is still valid.

If the reason concerns the Web service, check the proxy setting, user name, and key. If the key is invalid, get the valid key from the Hosted Email Security administrative console or generate a new one.

How long should I set the sync interval?

The default value (1 hour) works in most cases. You do not need to modify it. However, if the ActiveDirectory data is very large (more than 250,000 recipient email messages), increase the interval value.

Tip: Trend Micro recommends setting the sync interval to 4 hours in such cases.

Can I do a directory import from the admin console with a Web service client running?

While a Web service client is actively doing a sync, it locks the domain that is the target of the sync and prevents a directory import from the admin console. If the Web service fails in the middle of its synchronization attempt and cannot close/rollback the

synchronization, then the Web service server waits for 2 hours before timing out the sync transaction and releasing the lock on the domain that is being synchronized.

Why can't the sync service be started and why is it reporting the error "Error 1069: The service did not start due to a logon failure"?

Check whether the domain account password has been changed. If the password has been changed, you must also change the service logon information as follows:

1. Open **Control Panel** and select **Administrative Tools** > **Services**.
2. In the Service window, find the **Hosted Email Security ActiveDirectory Sync Service** service.
3. Right-click the service and select **Properties**.
4. In the Logon window, make sure that **Log on as this account** is selected and enter the correct logon information (domain, user name, and password).

Appendix A

Hosted Email Security Web Services Applications

The information in this appendix is intended for value-added resellers, professional services providers, and software development partners of Trend Micro. It is not intended for other Hosted Email Security service customers.

The topics in this appendix provide additional information for you to customize and program your Hosted Email Security Web services client to communicate with Hosted Email Security Web services applications. These topics serve as a reference for the sample client program provided by Trend Micro.

Note: Not all APIs are available at the time of writing.

Web Service Security

The connection to Hosted Email Security Web services is initiated by the client and is done through SSL. On top of this, HTTP basic authentication is used with the customer account Activation Code, administrator user account name, and a Hosted Email Security-generated APIKEY for the password. The APIKEY can be regenerated at your discretion as long as the client program configuration is updated with the current APIKEY.

Web Services Applications

Hosted Email Security Web services provide a set of Application Programming Interfaces (APIs) in REST-ful Web application architecture. The focus of the APIs is on automating repetitive Hosted Email Security administrative tasks.

Provisioning

Maintaining email user accounts and keeping them consistent across the company mail servers and Hosted Email Security is a repetitive administrative task. Hosted Email Security Web services provide User Directory Management APIs for automating such tasks, including:

- Adding user email address to a managed domain on Hosted Email Security service
- Deleting user email address from a managed domain on Hosted Email Security service
- Listing user email addresses of a managed domain on Hosted Email Security service
- Bulk addition of user email addresses to a Hosted Email Security administrator account
- Listing domain names managed by a Hosted Email Security administrator account
- Listing user email addresses managed by a Hosted Email Security administrator account

Web Services Clients

Hosted Email Security ActiveDirectory Sync Client

For users with Active Directory (AD) setups, Trend Micro provides the Hosted Email Security ActiveDirectory Sync Client (a Microsoft Active Directory plug-in or an AD Connector), developed under .NET. It acts as a one-way pipe (that is, moving data from the user's Active Directory to Hosted Email Security Web services) between the user's AD and the Web service to carry provisioning data (for example, limited to deltas of valid users for Web services version 1.0). The Hosted Email Security ActiveDirectory Sync Client polls the user's AD servers at configurable intervals to determine additions and deletions of valid users. The AD Connector then syncs up the Hosted Email Security user data relating to the user's account with a Web service API call.

Hosted Email Security Web Services Client

For general-purpose Hosted Email Security Web services communications, Trend Micro provides a sample OS-independent implementation of the Web service client: **imhs_web_svc_client**.

Hosted Email Security Web services client (**imhs_web_svc_client**) is written in the Ruby OS-independent scripting language. The Ruby client is a full Web service client, with access to both the reporting and provisioning resources of the Hosted Email Security Web services. As such, for provisioning-related deployment, it can act as the upload component by uploading a CSV file of valid user email addresses or by performing a single call to the Web service for each user added or deleted.

For report extraction, the Ruby client can be called with the appropriate parameters to extract the required type of report in either XML or CSV format for saving to a local file. The supporting library of the Ruby client can also be called directly if you want to assemble a custom client-based application. There are Ruby ports for running on *nix or Windows platforms.

Appendix B

ActiveDirectory Sync Client Architecture

This appendix describes the software architecture behind Hosted Email Security ActiveDirectory Sync client. It is intended to provide more information to help you understand the client design.

Overview

The Hosted Email Security ActiveDirectory Sync client is a Microsoft ActiveDirectory plug-in connector. It is installed in your environment and has access to your Active Directory. It periodically queries the user email accounts from data sources in the Active Directory and reports the changes to the Hosted Email Security service. The high-level architecture is as follows:

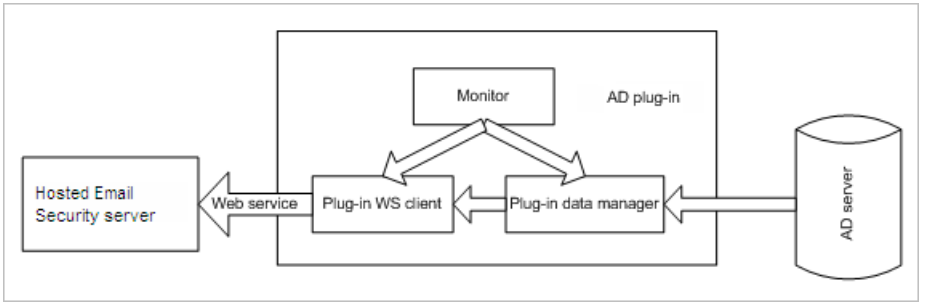


FIGURE B-1. Hosted Email Security ActiveDirectory Sync client architecture

Hosted Email Security includes the following three main components:

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

These are each described in the following sections.

Plug-In Data Manager

The Plug-in Data Manager retrieves data from Active Directory. Currently, only user email addresses are retrieved. The Plug-in Data Manager runs as a Windows service named Hosted Email Security ActiveDirectory Sync service.

Plug-In WS Client

Plug-in WS Client is a stateless library that communicates with the Web service server. It sends Web requests to the server and receives the responses.

Monitor

Monitor is a health monitor of the Hosted Email Security ActiveDirectory Sync service. It monitors the health of the plug-in data manager and plug-in WS client services. Monitor itself runs as a Windows service named Hosted Email Security ActiveDirectory Sync Agent.

Operating Environment

Hosted Email Security ActiveDirectory Sync should work properly under Windows XP and Windows Server 2003 and can access various AD servers under Windows Server 2003. The .NET Framework 2.0 must be installed on the client computer. Without the .NET Framework 2.0 installed properly, various installation and runtime issues will be encountered.

Tip: Trend Micro recommends at least 512MB of memory and 100MB of free hard disk space for the Hosted Email Security ActiveDirectory Sync.

Hosted Email Security ActiveDirectory Sync client is written using .NET C# as the developing platform and language.

Appendix C

ActiveDirectory Sync Client Installation and Configuration

This appendix provides an overview of how to install, configure, and customize your Hosted Email Security ActiveDirectory Sync client.

Installing the Hosted Email Security ActiveDirectory Sync Client

If you have not downloaded the latest Hosted Email Security ActiveDirectory Sync client, log on to the Hosted Email Security administrative console, click **Administration > Web Services,** and download the latest client.

The Hosted Email Security ActiveDirectory Sync client program requires Microsoft .NET Framework 2.0 in order to install and run properly. You will be prompted during the installation process to install .NET Framework 2.0 if it is not already installed on your computer.

To install Hosted Email Security ActiveDirectory Sync Client:

1. If prompted to install Microsoft .NET Framework 2.0, click **Accept** to start downloading the .NET Framework from the Microsoft Web site. This may take several minutes depending on your Internet connection speed. (Skip to Step 2 if you already have .NET Framework 2.0 installed).

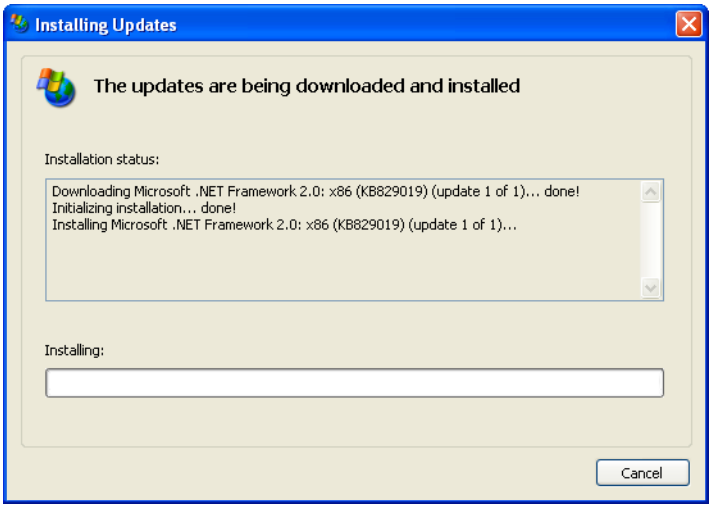


FIGURE C-2. Downloading and installing Microsoft .NET 2.0

Installation of the .NET Framework 2.0 automatically starts after the download completes. This installation step takes about 10 minutes.

After installing the .NET Framework 2.0—or if it was already installed on your computer—the Hosted Email Security ActiveDirectory Sync Client begins the installation process by displaying the following screen:

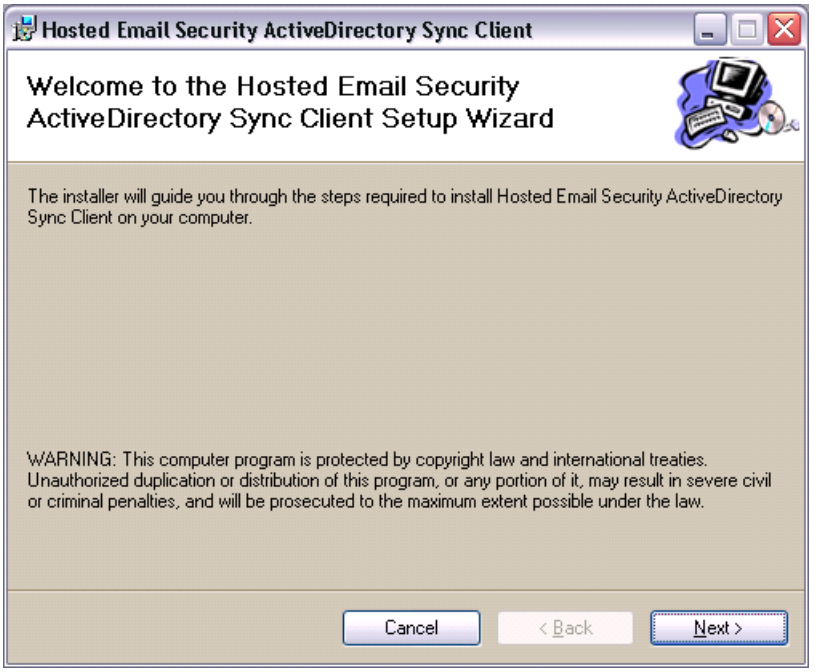


FIGURE C-3. Welcome screen

2. Click **Next** to review the Licensing Agreement.
   The License Agreement screen is displayed:

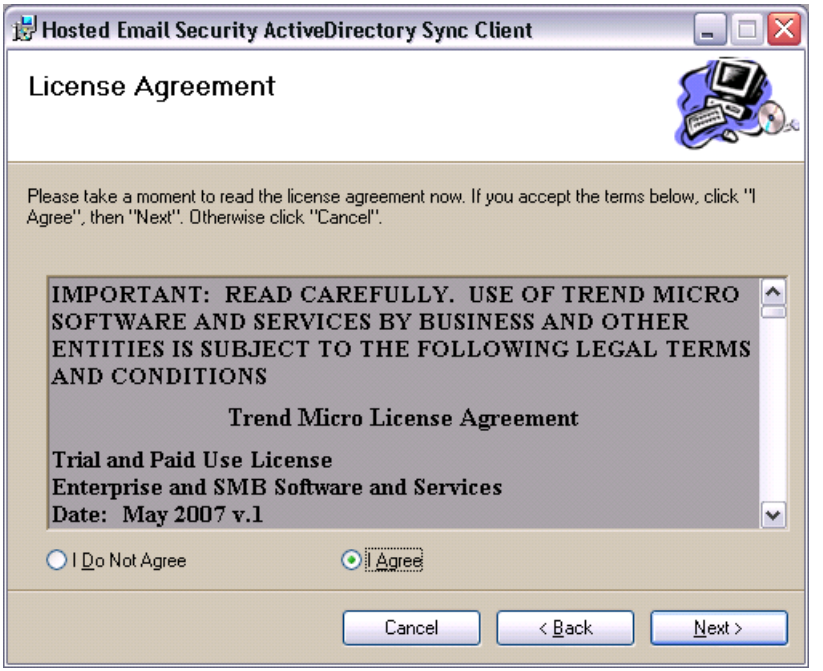


FIGURE C-4. License Agreement screen

3. Select **I Agree** and click **Next** to continue.

The Enter Domain Account screen appears:

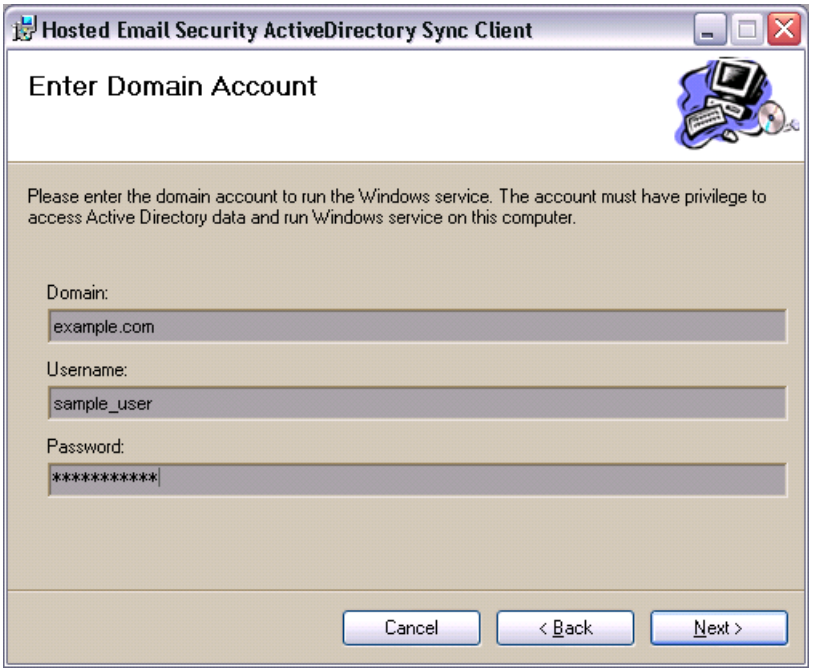


FIGURE C-5. Enter Domain Account screen

4. Enter your domain account, which has the privilege to access your Active Directory server and to run Windows services on your computer. Click **Next**.

Note: This is an important criterion. If you enter an account that does not have the access privilege to either of the above, your installed Hosted Email Security ActiveDirectory Sync Client will not function properly.

The Select Your Destination screen appears:

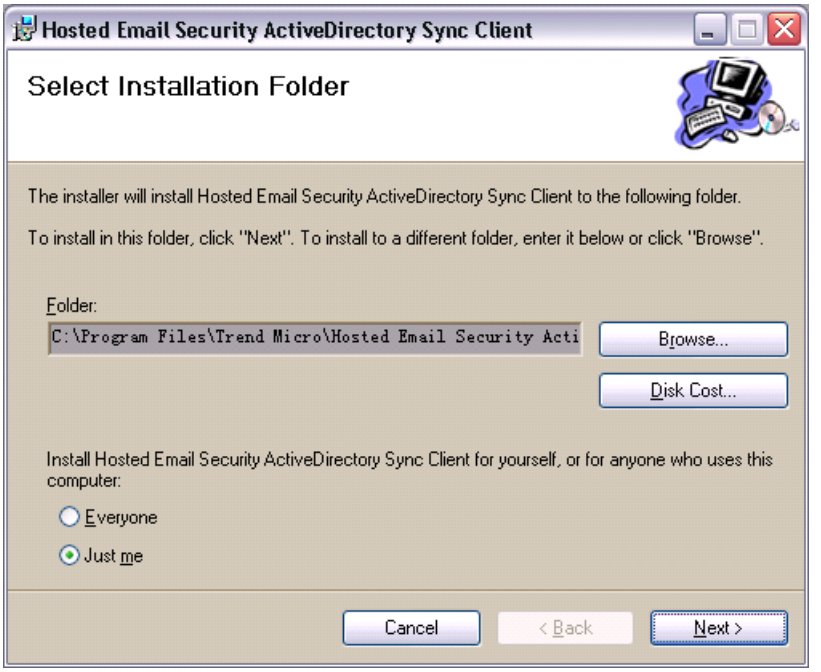


FIGURE C-6. ActiveDirectory Sync Client Select Installation Folder screen

5. Choose the install folder and target user. As far as using the Hosted Email Security ActiveDirectory Sync client is concerned, there is very little difference between "Everyone" and "Just me." In either case, the login user can use the Web service client. The only difference is that for "Just me," the client program menu group will be created only for the current user. Otherwise, it will be created for all users.

6. Click **Next**. The Confirm Installation screen appears:

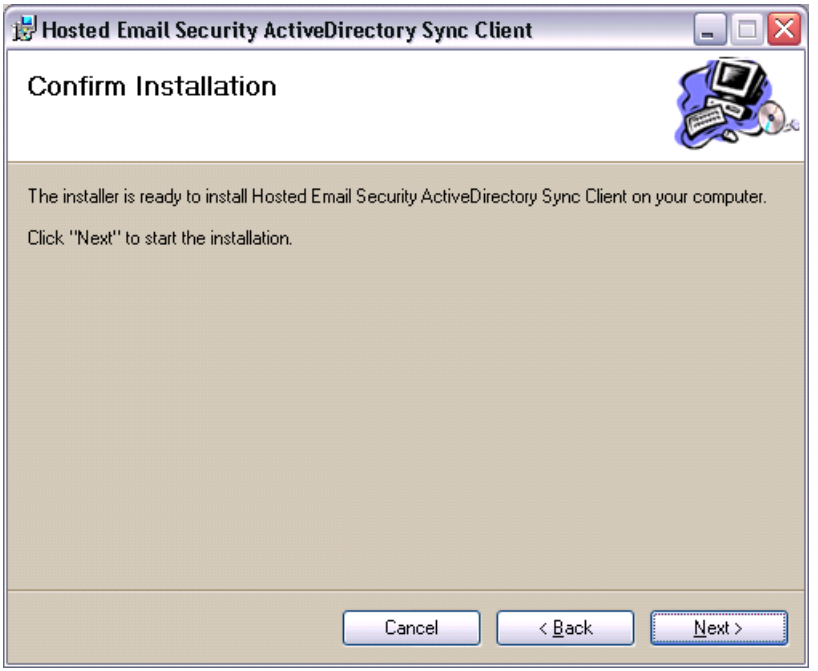


FIGURE C-7. Confirm Installation scree

7. Click **Next** to continue.
   Installation begins and the installer displays the following screen:

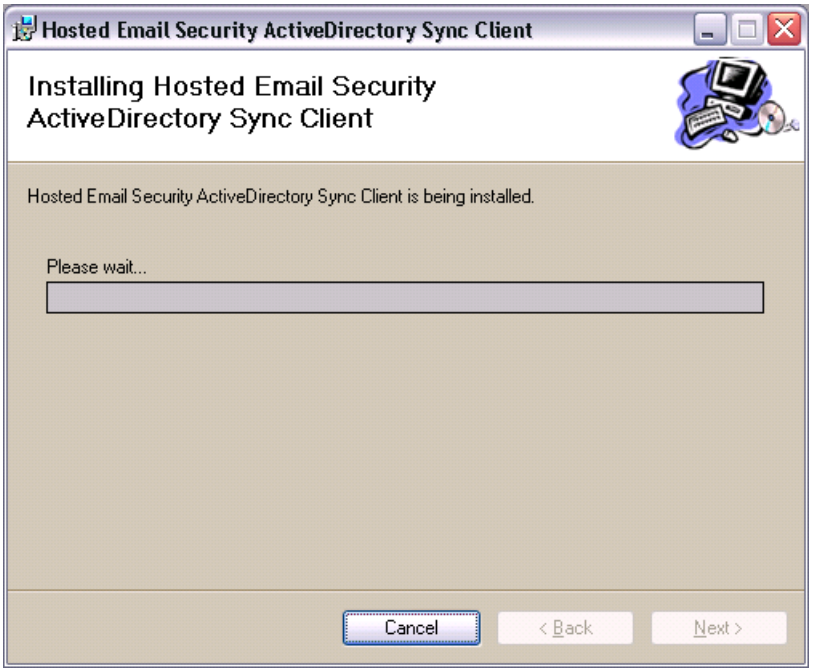


FIGURE C-8. Installing screen

The installer displays the following screen when installation is complete.

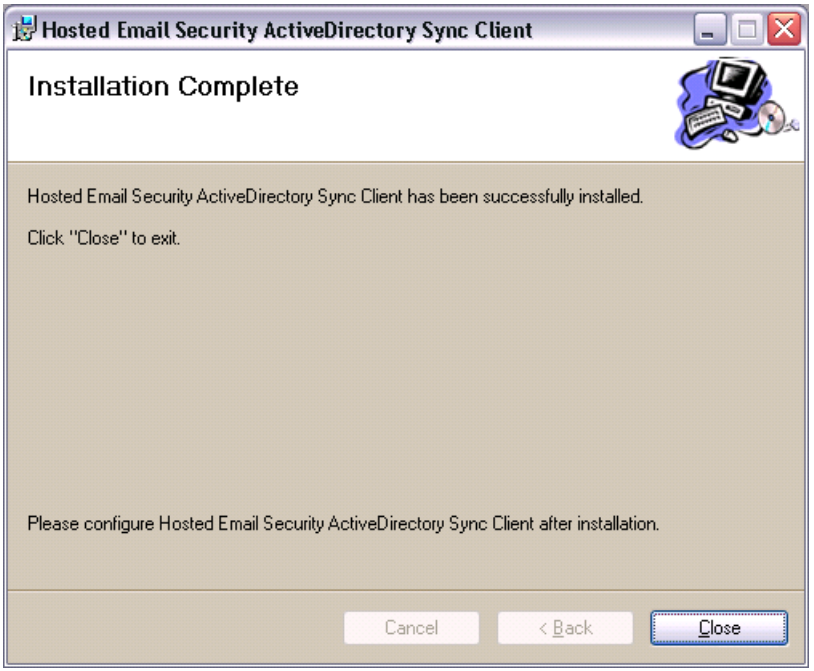


FIGURE C-9. Installation Complete screen

8. Click **Close** to exit the installation and enter initial configuration of Hosted Email Security ActiveDirectory Sync client.

Configuring the ActiveDirectory Sync Client

After installing the Hosted Email Security ActiveDirectory Sync client, you need to configure some parameters before you start using the client to synchronize user email addresses to the Hosted Email Security service.

The Hosted Email Security ActiveDirectory Sync client starts automatically upon the completion of installation. There are three configuration steps to perform:

Setting the LDAP (ActiveDirectory) Path

The main screen is for setting the LDAP path. Enter the LDAP (ActiveDirectory) path by which this client can retrieve the email address data.

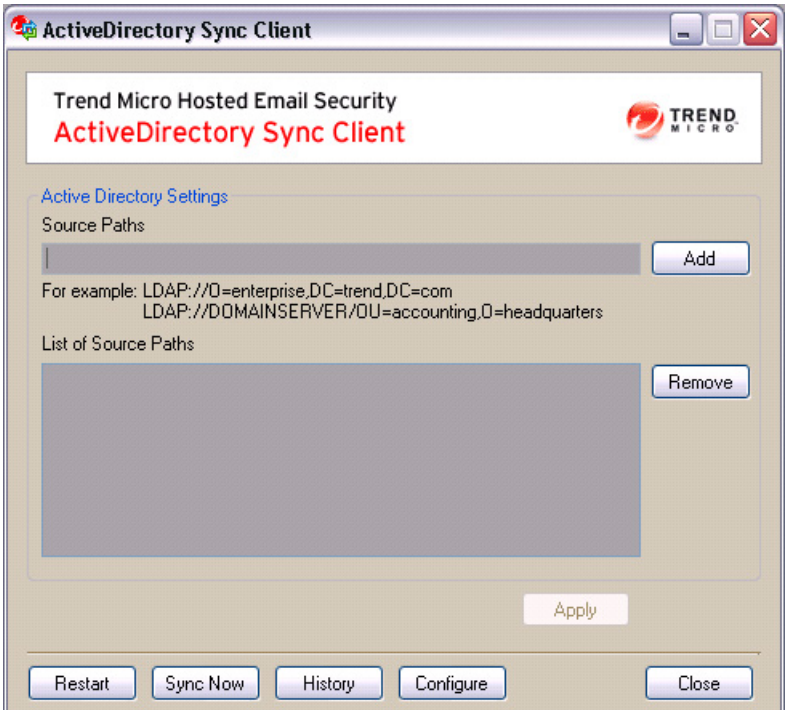


FIGURE C-10. Setting the Hosted Email Security ActiveDirectory path

You can enter one or more LDAP paths by which the sync client program can retrieve the user email address (mail record) data.

Configuring the Network Settings

Configuring the network includes setting the following:

- *Access Authentication* on page C-12
- *Proxy Settings* on page C-13
- *Sync Interval* on page C-13
- *Sync Now Function* on page C-14

Access Authentication

To access Hosted Email Security Web services applications, you must provide the network parameters. To configure the network settings, click **Configure** at the bottom of the main screen. The Network Settings dialog box appears.

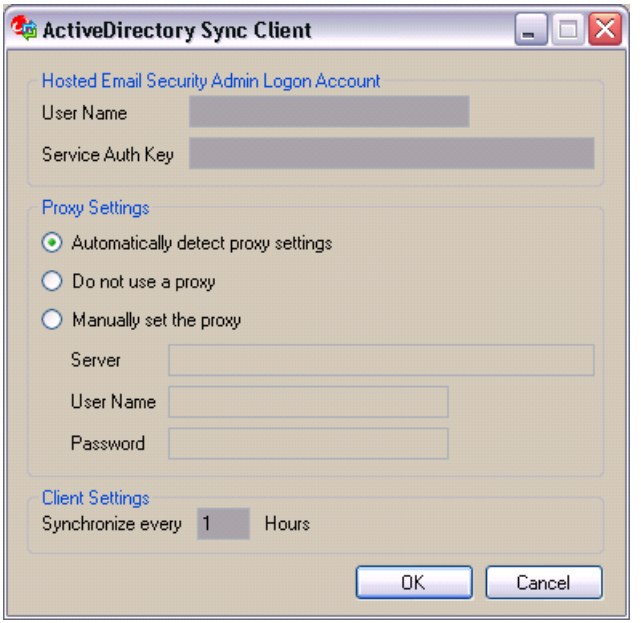


FIGURE C-11. Network Settings dialog box

The login account is the account credentials to access the Web services:

- User Name is the log on user name given to you for accessing the Hosted Email Security administrative console. Refer to your welcome letter, sent when you subscribed to the Hosted Email Security service.
- Service Auth Key is the APIKEY that you generated on the Hosted Email Security administrative console for authenticating Hosted Email Security Web services access.

Proxy Settings

Currently, only HTTP proxy is supported. You can configure three different kinds of proxy settings:

- Do not use a proxy.
- Automatically detect proxy settings. Use the proxy setting of Microsoft Internet Explorer.
- Manually set the proxy. Input the proxy information in the text boxes under **Manually set the proxy**.

When you click **OK** to configure the proxy settings, Hosted Email Security ActiveDirectory Sync client attempts to make a test connection to Hosted Email Security Web services. If Hosted Email Security Web services are unreachable, the following error message appears:

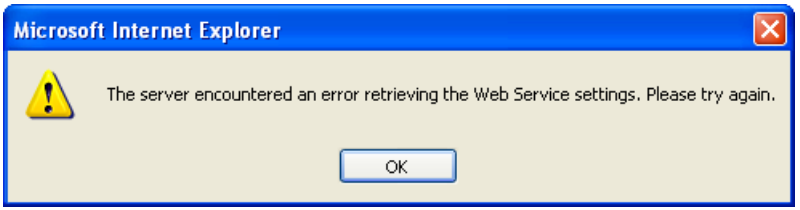


FIGURE C-12. Web Services unreachable error message

Sync Interval

Sync interval is the frequency with which the Hosted Email Security ActiveDirectory Sync client checks for user account updates in Active Directory. The first synchronization starts one interval after you start the AD Sync Client. The minimum interval is 1 hour. We suggest that you set the interval no higher than 24 hours.

If you have a very large ActiveDirectory user base, set your synchronization interval to 4 hours or longer so that the synchronization can be completed within the interval specified. Overlapping synchronization intervals will be executed in serial order, however Trend Micro recommends that you do not set too short a sync interval.

Sync Now Function

If you need to see the sync result sooner than the next scheduled synchronization, you can execute a synchronization immediately by clicking **Sync Now** in the AD Sync Client, as shown in Figure C-13 below.

Note: If you click **Sync Now** while a scheduled synchronization is in progress, the new sync action will begin after the scheduled synchronization is complete.

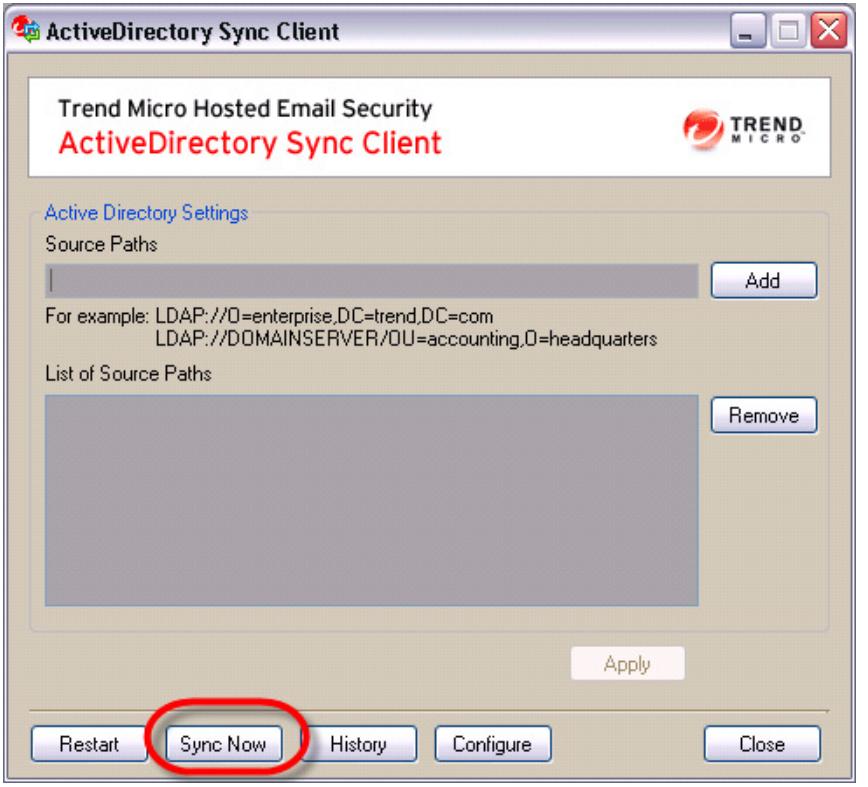


FIGURE C-13. Hosted Email Security AD Sync Client showing the Sync Now button

Modifying Search Criteria

By default, the Hosted Email Security ActiveDirectory Sync Client searches for an object class "**`User`**" and its three attributes:

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

These defaults are set in an XML configuration file called ***`IMHS_AD_ACL.config`***, whose contents are shown in Figure C-14 below. Any paths that you modify in the user interface make use of these defaults.

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>
```

FIGURE C-14. Default values of IMHS_AD_ACL.config

However, the client provides the flexibility for you to modify these defaults if you wish. For example, if for purposes of confidentiality you would like for the client to search only for proxy addresses but not email addresses or display names, you could modify these settings by revising the config file as shown in Figure C-15 below.

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>
```

FIGURE C-15. IMHS_AD_ACL.config showing modified values

You can leave the default value as is but add more alternate path names, for example, as shown in Figure C-16.

```
<?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>
       <objectClass name="group">
         <displayNameAttr>displayName</displayNameAttr>
          <emailAttr>proxyAddresses</emailAttr>
       </objectClass>
     </ldap_path>

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

FIGURE C-16. IMHS_AD_ACL.config with default path kept but new paths added

You can also add self-defined object classes or attribute names. If you modify this config file, save it and restart the client in order for your changes to take effect.

Note: The tag **<ad_acl>** is the root tag in this XML file. Although you can add multiple **<ldap_path>** blocks, there can be only one opening **<ad_acl>** tag and one closing **</ad_acl>** tag in the `IMHS_AD_ACL.config` file.

Inheritance of Object Classes

In Active Directory schema, object classes can be inherited. If an object class is configured in ***`IMHS_AD_ACL.config`***, then the objects of its subclasses under the same LDAP path will be retrieved as well. Take this into consideration when modifying the ACL configuration file.

For example, in config file sample A, the first of the two sample configuration files shown in Figure C-17 below, class **inetOrgPerson** is a subclass of **user**. If for the same LDAP path we configure the object class **user**, as in config file sample B, the query will also retrieve **inetOrgPerson** objects. Both of these configuration files would retrieve the same objects.

Config File Sample 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>
```

Config File Sample B

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

FIGURE C-17. Two sample IMHS_AD_ACL.config files, illustrating how the client handles inheritance

It is not necessary to configure **inetOrgPerson.** Whereas, if we remove **inetOrgPerson** from the ACL file but keep **user**, objects of **inetOrgPerson** will still be retrieved. In other words, if an object class is removed from ACL, its entries in the server will be removed if they are not in other object classes specified in ACL.

Note: Hosted Email Security preserves this config file for future use, even if you re-install the client.

Viewing the History Log

Hosted Email Security ActiveDirectory Sync Client provides transaction logging. You can view the recent transactions by clicking **History**.

The history information contains three columns: TimeStamp, Event and Reason(s), as shown in Figure C-18.

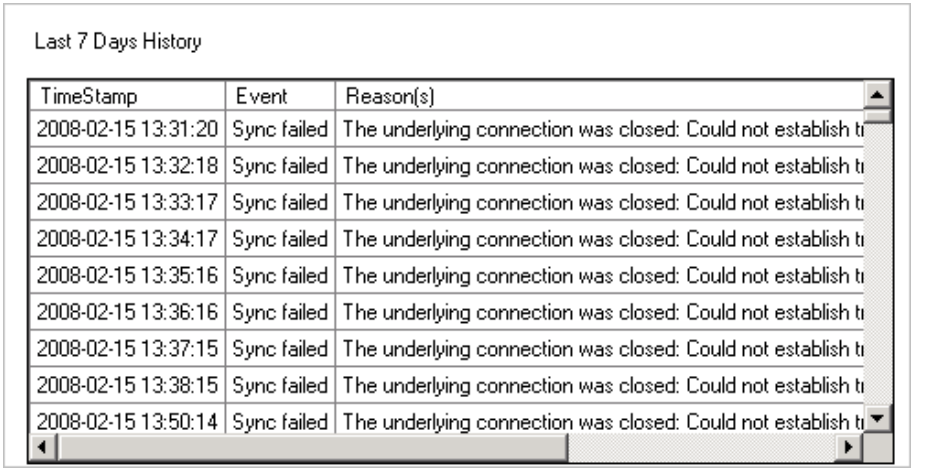


FIGURE C-18. History log

Appendix D

Hosted Email Security Web Services Command-Line Reference and Programming Guide

This appendix is for advanced Hosted Email Security administrators only. If your organization plans to use the Hosted Email Security Web services client from a command line in a Unix/Linux or Windows environment and you want to automate the valid email recipient addresses import, you can use this command-line client in a cron job or scheduled task.

Note: The target audience of the following usage guide is advanced Hosted Email Security administrators and tool developers. You should be familiar with programming in scripting languages and debugging software in order to understand this material.

Maintaining Valid Mail Recipients and Synchronizing to Hosted Email Security

If you maintain a list of valid mail recipients for your managed mail domains using a plain-text comma-separated values (CSV) file, you can automate such user provisioning to Hosted Email Security by using the Web services client.

For most Hosted Email Security administrators, only the Web services client command action **sync-users** will ever be used. For example, you maintain your managed domain `example.com` in a plain-text (CSV) file ***`example_com.txt`*** such as the following:

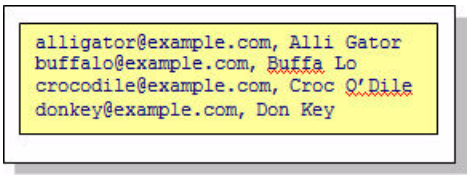


FIGURE D-19. Example plain text file

All you need to do is to set up a **cron** job that runs a command-line action similar to this:

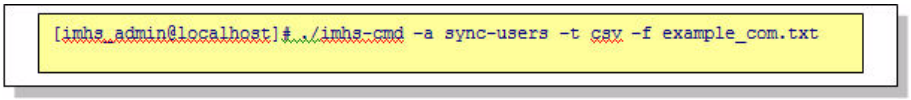


FIGURE D-20. Example cron job command-line action

All you have to do is to continue to maintain your email users in the plain-text file. Email addresses will be synchronized to the Hosted Email Security service periodically (according to your crontab schedule).

Programming your own Hosted Email Security Web Services Client

Trend Micro does not currently support a programming environment for customers who choose to create their own Hosted Email Security Web services clients.

WARNING! **If you choose to create your own** Hosted Email Security **Web services, the Trend Micro 24x7 Support staff will be unable to support you in creating, maintaining, or debugging your client program.**

Hosted Email Security Web Services Client Command Usage Guide

The following sections describe the usage of `imhs-cmd.rb`.

Usage:

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

TABLE D-1. Specific options

OPTION	DESCRIPTION
`-a, --action ACTION`	Directory actions {list-domains|list-users|add-user|delete-user|delete-users|replace-users|merge-users|sync-users}
`-u, --user [USEREMAIL]`	Email address of user
`-n, --name [FULLNAME]`	Email address of user
`-d, --domain [DOMAINNAME]`	Domain name
`-t, --type [FILETYPE]`	Type of input file {csv}

TABLE D-1. Specific options

OPTION	DESCRIPTION
`-f, --file [FILEPATH]`	Input file path <path_to_inputfile>
`-c, --config [CONFIG_FILEPATH]`	Alternate imhs-config.rb file <path_to_configfile>

Note: Set the account name and API KEY in `imhs-config.rb` before using.

TABLE D-2. Common Options

OPTION	DESCRIPTION
`-h, --help`	Show this message
`--version`	Show version

Examples

This section provides usage examples for client commands.

Synchronizing Your User Directory From a File

For an example of synchronizing your user directory from a plain text CSV file, see ***example_com.txt***. ***Example_com.txt*** is a CSV file that contains:

```
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
```

Listing the Mail Domains

The following is an example of listing the mail domains that you manage:

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

Replacing the Entire User Directory

For an example of replacing the entire user directory of your managed mail domain (***example.com***) from a plain-text CSV (comma-separated-values) file, see ***UserDirReplaceExample.txt***. ***UserDirReplaceExample.txt*** is a CSV file that contains:

```
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
```

Listing the Users of a Mail Domain

The following is an example of listing the users of a mail domain that you manage:

```
[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
```

Merging In Users

To merge in users of your managed mail domain (**example.com**) from a plain text CSV file, see ***UserDirMergeExample.txt***. ***UserDirMergeExample.txt*** is a CSV file that contains:

```
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
```

Adding a Single User

The following is an example of adding a single user, `orville_wilbur@example.com`, to your managed email domain (**example.com**):

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

SUCCESS ADDUSER orville_wilbur@example.com
```

Deleting a Single User

The following is an example of deleting a single user, `bonnie_clyde@example.com`, from your managed email domain (**example.com**):

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

SUCCESS DELETEUSER bonnie_clyde@example.com.
```

Deleting Selected Users

For an example of deleting selected users from your managed mail domain (**example.com**) according to the file specified, see ***UserDirDeleteExample.txt***. ***UserDirDeleteExample.txt*** is a CSV file that contains:

```
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.
```