Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before deploying and using the appliance, please review the readme files, release notes and the latest version of the Deployment Guide and Administrator’s Guide, which are available from Trend Micro’s Web site at:

www.trendmicro.com/download/documentation/

NOTE: A license to the Trend Micro Software usually includes the right to minor product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be renewed on an annual basis at Trend Micro’s then-current Maintenance fees.

Trend Micro, the Trend Micro logo, InterScan, and Control Manager 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 © 2007 Trend Micro Incorporated. All rights reserved.

Document Part Number: MSEM73166/70423

Release Date: December 2007

Patents Pending
The Administrator’s Guide for Trend Micro InterScan Messaging Security Appliance 7.0 (IMSA) is intended to provide you with instructions on how to configure and administer IMSA to ensure that your network is well-protected against various malware. You should read through this document after deploying IMSA. For instructions on deploying IMSA, please refer to the IMSA Deployment Guide.

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

www.trendmicro.com/download/documentation/rating.asp
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Enabling NRS and IP Profiler</td>
<td>2-5</td>
</tr>
<tr>
<td>Step 2: Enabling IP Profiler Rules</td>
<td>2-6</td>
</tr>
<tr>
<td>Step 3: Configuring NRS</td>
<td>2-7</td>
</tr>
<tr>
<td>Step 4: Adding IP Addresses to the Approved List</td>
<td>2-8</td>
</tr>
<tr>
<td>Step 5: Adding IP Addresses to the Blocked List</td>
<td>2-8</td>
</tr>
<tr>
<td>Querying IP Filtering Logs</td>
<td>2-10</td>
</tr>
<tr>
<td>Scanning SMTP Messages</td>
<td>2-11</td>
</tr>
<tr>
<td>Configuring SMTP Routing</td>
<td>2-11</td>
</tr>
<tr>
<td>Configuring SMTP Settings</td>
<td>2-11</td>
</tr>
<tr>
<td>Configuring Connections Settings</td>
<td>2-12</td>
</tr>
<tr>
<td>Configuring Message Rule Settings</td>
<td>2-13</td>
</tr>
<tr>
<td>Configuring Domain-based Delivery Settings</td>
<td>2-15</td>
</tr>
<tr>
<td>Scanning POP3 Messages</td>
<td>2-17</td>
</tr>
<tr>
<td>Understanding POP3 Scanning</td>
<td>2-17</td>
</tr>
<tr>
<td>Requirements</td>
<td>2-18</td>
</tr>
<tr>
<td>Enabling POP3 Scanning</td>
<td>2-18</td>
</tr>
<tr>
<td>Configuring POP3 Settings</td>
<td>2-19</td>
</tr>
<tr>
<td>Managing Policies</td>
<td>2-21</td>
</tr>
<tr>
<td>How the Policy Manager Works</td>
<td>2-21</td>
</tr>
<tr>
<td>Understanding Address Groups</td>
<td>2-23</td>
</tr>
<tr>
<td>Managing Address Groups</td>
<td>2-24</td>
</tr>
<tr>
<td>Adding an Address Group</td>
<td>2-24</td>
</tr>
<tr>
<td>Editing or Deleting an Address Group</td>
<td>2-26</td>
</tr>
<tr>
<td>Searching for an LDAP User or Group</td>
<td>2-28</td>
</tr>
<tr>
<td>Configuring Internal Addresses</td>
<td>2-30</td>
</tr>
<tr>
<td>Adding Policies</td>
<td>2-32</td>
</tr>
<tr>
<td>Specifying a Route</td>
<td>2-32</td>
</tr>
<tr>
<td>Specifying Scanning Conditions</td>
<td>2-34</td>
</tr>
<tr>
<td>Specifying Actions</td>
<td>2-38</td>
</tr>
<tr>
<td>Specifying Priority</td>
<td>2-41</td>
</tr>
<tr>
<td>Example 1</td>
<td>2-43</td>
</tr>
<tr>
<td>Example 2</td>
<td>2-47</td>
</tr>
<tr>
<td>Using the Asterisk Wildcard</td>
<td>2-51</td>
</tr>
<tr>
<td>Updating Scan Engine and Pattern Files</td>
<td>2-53</td>
</tr>
<tr>
<td>Specifying an Update Source</td>
<td>2-53</td>
</tr>
<tr>
<td>Performing a Manual Update</td>
<td>2-54</td>
</tr>
<tr>
<td>Rolling Back a Component Update</td>
<td>2-55</td>
</tr>
</tbody>
</table>
Chapter 5: Using EUQ

About EUQ .................................................................5-2
Step 1: Configuring and Enabling LDAP .........................5-2
Step 2: Enabling EUQ ......................................................5-5
Step 3: Starting the EUQ Service .....................................5-7
Step 4: Enabling End-User Access ...................................5-8
Step 5: Opening the End-User Quarantine Console ...........5-10
  Logon Name Format ....................................................5-10
Disabling EUQ ..............................................................5-11

Chapter 6: Using the Command Line Interface

Using the CLI ...............................................................6-2
Entering the CLI ..............................................................6-2
CLI Overview .................................................................6-4
  CLI Navigation ..............................................................6-5
Viewing Device Information and Status .........................6-6
Configuring Network Settings .......................................6-7
  Network Settings Examples and Limitations ...................6-8
    Hostname Format ......................................................6-8
    IP Address Format ....................................................6-9
    Subnet Mask Format ..................................................6-9
    Default Gateway Address Format ...............................6-9
Performing Basic Maintenance ......................................6-9
Entering the Linux-like Shell Environment .......................6-10
Changing Time and Date Settings ................................ 6-10
Enabling and Disabling Web Console and SSH Access .......6-11
Shutting Down IMSA ....................................................6-11

Chapter 7: Modifying IMSA Deployment

Adding and Removing Devices ....................................7-2
  Adding a Child Device to a Group .................................7-2
  Removing a Child Device from a Group .........................7-2
Resetting Child Devices When the Parent-Child Connection is Broken .........................................................7-3
Changing Device Roles .................................................7-3
  Changing the Device Role from Parent to Child ..............7-4
  Changing the Device Role from Child to Parent ..............7-4
Chapter 8: Updating and Rescuing the System and Application

Updating the System and Application ............................................... 8-2
Rescuing IMSA ........................................................................ 8-4
Operating System Rescue Overview ........................................... 8-4
Application Rescue Overview ...................................................... 8-4
Entering Rescue Mode .................................................................. 8-5
Rescuing the Operating System .................................................... 8-6
Rescuing the Application ............................................................ 8-6
Installing a New OS and Application After Changing Hard Disks 8-7

Chapter 9: Troubleshooting, FAQ, and Support

Troubleshooting ........................................................................... 9-2
Troubleshooting Utilities .............................................................. 9-2
Troubleshooting Issues ............................................................... 9-2
Frequently Asked Questions .......................................................... 9-10
Postfix MTA Settings ................................................................ 9-10
IP Profiler ................................................................................ 9-10
Mail Areas and Queues ............................................................ 9-11
Importing and Exporting .......................................................... 9-12
End-User Quarantine .................................................................. 9-14
Transport Layer Security (TLS) .................................................. 9-16
Spam Protection Service .......................................................... 9-16
ActiveUpdate ........................................................................ 9-17
Others ..................................................................................... 9-17
Using the Knowledge Base ........................................................ 9-20
Contacting Support ....................................................................... 9-20

Appendix A: IMSA Scripts

Invoking IMSA Scripts ............................................................... A-2
Appendix B:  Default Directory Locations

Default Mail Queues ................................................................. B-2
eManager, Virus and Program Logs ......................................... B-3
Temporary Folder ..................................................................... B-3
Notification Pickup Folder ...................................................... B-3

Appendix C:  Transport Layer Security

How Transport Layer Security Works .................................... C-2
Transport Layer Security Related Terms ............................... C-2
Prerequisites to Using Transport Layer Security with IMSA .... C-3
Configuring Transport Layer Security Settings ...................... C-4
  Scenario on Configuring Site-Specific TLS Settings .......... C-4
Incoming Transport Layer Security Levels ............................. C-6
  Scenario on Configuring Incoming Transport Layer Security
    Settings ........................................................................... C-6
Outgoing Transport Layer Security Levels ............................. C-7
  Scenario on Configuring Outgoing Transport Layer Security
    Settings ........................................................................... C-7

Index
Welcome to the *Trend Micro™ InterScan™ Messaging Security Appliance 5000 7.0 Administrator’s Guide*. This manual contains post-deployment information to get InterScan Messaging Security Appliance (IMSA) up and running. Please refer to the Online Help in the Web management console for detailed information on each field on the user interface.

This preface discusses the following topics:

- *InterScan Messaging Security Appliance 5000 7.0 Documentation* on page viii
- *Audience* on page viii
- *Document Conventions* on page x
InterScan Messaging Security Appliance 5000 7.0 Documentation

The InterScan Messaging Security Appliance 5000 7.0 (IMSA) 5000 7.0 documentation consists of the following:

- **Quick Start Guide**—Helps you set up InterScan Messaging Security Appliance and connect it to your network.
- **Deployment Guide**—Contains information about IMSA features and system requirements, and describes how to deploy and upgrade IMSA in various network environments.
- **Administrator’s Guide**—Helps you get IMSA up and running with post-deployment instructions on how to configure and administer IMSA.
- **Online Help**—Provides detailed information about each field on the Web management console and instructions on how to configure all features through the user interface. To access the online help, open the Web management console and then click the help icon (icontext). The Quick Start Guide, Deployment Guide, Administrator’s Guide, Hardware Maintenance Sheet and Readme file are available on the InterScan Messaging Security Appliance 5000 Solutions CD and at http://www.trendmicro.com/download.

- **Readme File**—Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, deployment tips, known issues, and product release history.
- **Hardware Maintenance Sheet**—Shows you how to change fans, hard disks, and power supplies.
- **Third-party License Agreements**—Contains a list of license agreements from third party companies whose products IMSA uses.

The **Audience**

The InterScan Messaging Security Appliance documentation is written for IT managers and email administrators in medium and large enterprises. The documentation assumes that the reader has in-depth knowledge of email messaging networks, including details related to the following:

- SMTP and POP3 protocols
• Message transfer agents (MTAs), such as Postfix
• LDAP
• Database management

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 IMSA documentation uses the following conventions.

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL CAPITALS</td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Menus and menu commands, command buttons, tabs, options, and other user interface items</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>References to other documentation</td>
</tr>
<tr>
<td>Monospace</td>
<td>Examples, sample command lines, program code, Web URL, file name, and program output</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Configuration notes</td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
<td>Recommendations</td>
</tr>
<tr>
<td><strong>WARNING!</strong></td>
<td>Reminders on actions or configurations that must be avoided</td>
</tr>
</tbody>
</table>
Getting Started

This chapter explains how to log on to the Web management console and provides instructions on what to do immediately after deployment to get InterScan Messaging Security Appliance (IMSA) 7.0 up and running.

Topics include:
• Opening the IMSA Web Management Console on page 1-2
• Setting Up a Single Parent Device on page 1-4
• Setting Up a Child Device on page 1-16
• IMSA Services on page 1-18
Opening the IMSA Web Management Console

You can view the IMSA management console with a Web browser from the server where you deployed the program, or you can view the management console remotely across the network.

To view the console in a browser, go to the following URL:

• https://<target server IP address>:8445

An alternative to using the IP address is to use the target server’s fully qualified domain name (FQDN).

The default logon credentials are as follows:

• Administrator user name: admin
• Password: imsa7.0

Type the logon credentials the first time you open the management console and click the Enter button.

Note: If you are using Internet Explorer (IE) 7.0 to access the Web management console, IE will block the access and display a popup dialog box indicating that the certificate was issued from a different Web address. Simply ignore this message and click Continue to this Web site to proceed.

Tip: To prevent unauthorized changes to your policies, Trend Micro recommends changing the password regularly.
Getting Started

Using the Online Help

The IMSA Web management console comes with an Online Help that provides a description of each field on the user interface.

To access page-specific Online Help from the IMSA Web management console, click the Help icon located at the top right corner of the page.

To access the table of contents for the Online Help, click the Help icon next to the Log Off hyperlink on the right of the page header.

Viewing the Web Management Console Using Secure Socket Layer

The IMSA Web management console supports encrypted communication, using SSL. After deploying IMSA, SSL communication should work because the device contains a default certificate. Trend Micro suggests creating your own certificate to increase security.

If you want to use your own certificate, replace the following:

/opt/trend/imss/UI/tomcat/sslkey/.keystore

Creating an SSL Certificate

Do the following:

1. Create the Tomcat SSL certificate as follows:
   
   keytool -genkey -alias tomcat -keyalg RSA -keystore 
   /opt/trend/imss/UI/tomcat/sslkey/.keystore 
   
   For more details on SSL configuration in Tomcat, please visit:
   
   http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html

2. Create the Apache SSL certificate as follows:
   
   a. Generate a Private Key and Certificate Signing Request (CSR)
openssl req -new > new.cert.csr

b. Remove pass-phrase from the key
openssl rsa -in privkey.pem -out new.cert.key

c. Generate a Self-Signed Certificate
openssl x509 -in new.cert.csr -out new.cert.cert -req -signkey new.cert.key -days 1825

d. Copy the certificate and key to the Apache path
   cp new.cert.cert
   /opt/trend/imss/UI/apache/conf/ssl.crt/server.crt
   cp new.cert.key
   /opt/trend/imss/UI/apache/conf/ssl.key/server.key

Setting Up a Single Parent Device

IMSA provides a configuration wizard to help you configure all the settings you need to get IMSA up and running.

**To set up a single parent device:**

1. Connect your management computer to the Managed port with the included Crossover cable. The IP address of the Managed port is 192.168.252.1, so your computer’s IP address must be in network segment 192.168.252.0/24 (such as 192.168.252.2) and have the subnet mask 255.255.255.0.

2. On the management computer, open Internet Explorer (version 6.0 or later) or Firefox (version 2.0 or later).

3. Enter the following URL (accept the security certificate if necessary):
   https://192.168.252.1:8445
   The login screen appears.

4. Select the “Open Configuration Wizard” check box.

5. Type the following default user name and password:
   - User name: **admin**
   - Password: **imsa7.0**
   The Configuration Wizard screen appears.
6. Continue through the Wizard screens to configure the settings.

**Step 1: Configuring the System Settings**

1. After you read the welcome screen, click **Next**. The Local System Settings screen appears.
2. Modify the device host name, IP address, and netmask if necessary. Also, configure your network settings and set the device system time.

**Note:** The local system settings take effect immediately when you click the **Next** button. If the IP address or time settings are changed, IMSA will restart. Wait until IMSA is online and then log on again.
Step 2: Configuring the Deployment Settings

1. Click **Next**. The Deployment Settings screen appears.

![Deployment Setting Screen](image.png)

2. Select Parent or Child. If this is the first device you are setting up, you must select Parent. You can configure additional child devices at a later time.

To deploy the device between upstream and downstream MTAs, clear the gateway deployment check box.

Also, decide if you want to use EUQ or NTP services.
Step 3: Configuring the SMTP Routing Settings

1. Click Next. The SMTP Routing Settings screen appears.

2. Add all SMTP server domains and their corresponding SMTP server names to the relay domain list. IMSA needs this information to pass email to SMTP servers for delivery.
Step 4: Configuring the Notification Settings

1. Click Next. The Notification Settings screen appears.

   ![Configuration Wizard Step 4 of 10](image)

   **Notification Settings**

   Configure email and SNMP trap notifications for default system notifications.

   **Email Settings**
   - To address(es):
   - Use a semicolon “;” to separate multiple addresses
   - Sender's email address:
   - Server name or IP address:
   - SMTP server port:
   - Preferred charset:
   - Message header:
   - Message footer:

   **SNMP Trap**
   - Server name (IP or FQDN):
   - Community:
   - Public:

2. If you want to receive notifications for system and policy events, configure the Email or SNMP trap notification settings.
Step 5: Configuring the Update Source

1. Click **Next**. The Update Source screen appears.

2. Configure the following update settings, which will determine from where IMSA will receive its component updates and through which proxy (if any) IMSA needs to connect to access the Internet:
   - **Source**—Click Trend Micro ActiveUpdate (AU) server to receive updates directly from Trend Micro. Alternatively, click Other Internet source and type the URL of the update source that will check the Trend Micro AU server for updates. You can specify an update source of your choice or type the URL of your Control Manager server, if applicable.
   - **Proxy Settings**—Select the Use proxy server check box and configure the proxy type, server name, port, user name, and password.
Step 6: Configuring the LDAP Settings

1. Click Next. The LDAP Settings screen appears.
2. Configure LDAP settings only if you will use LDAP for user-group definition, administrator privileges, or Web quarantine authentication.

   a. For **LDAP server type**, select one of the following:
      - Microsoft Active Directory
      - Domino
      - Sun iPlanet Directory

   b. To enable one or both LDAP servers, select the check boxes next to **Enable LDAP 1** or **Enable LDAP 2**.

   c. Type the names of the LDAP servers and the port numbers they listen on.

   d. Under **LDAP Cache Expiration for Policy Services and EUQ services**, type a number that represents the time to live next to the **Time To Live in minutes** field.

   e. Under **LDAP Admin**, type the administrator account, its corresponding password, and the base-distinguished name. See Table 1-1 for a guide on what to specify for the LDAP admin settings.

<table>
<thead>
<tr>
<th>LDAP Server</th>
<th>LDAP Admin Account (examples)</th>
<th>Base Distinguished Name (examples)</th>
<th>Authentication Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>* Without Kerberos: <a href="mailto:user1@domain.com">user1@domain.com</a> (UPN) or domain\user1</td>
<td>dc=domain, dc=com</td>
<td>• Simple</td>
</tr>
<tr>
<td></td>
<td>* With Kerberos: <a href="mailto:user1@domain.com">user1@domain.com</a></td>
<td></td>
<td>• Advanced (with Kerberos)</td>
</tr>
<tr>
<td>Domino</td>
<td>user1\domain</td>
<td>Not applicable</td>
<td>Simple</td>
</tr>
<tr>
<td>Sun iPlanet Directory</td>
<td>uid=user1, ou=people, dc=domain, dc=com</td>
<td>dc=domain, dc=com</td>
<td>Simple</td>
</tr>
</tbody>
</table>

   **TABLE 1-1. LDAP admin settings**

   f. For **Authentication method**, click **Simple** or **Advanced** authentication. For Active Directory advanced authentication, configure the Kerberos authentication default realm, Default domain, KDC and admin server, and KDC port number.
Note: Specify LDAP settings only if you will use LDAP for user-group definition, administrator privileges, or Web quarantine authentication. You must enable LDAP to use End-User Quarantine.

Step 7: Configuring the Internal Addresses

1. Click Next. The Internal Addresses screen appears.

2. IMSA uses the internal addresses to determine whether a policy or an event is inbound or outbound.
   - If you are configuring a rule for outgoing messages, the internal address list applies to the senders.
   - If you are configuring a rule for incoming messages, the internal address list applies to the recipients.

To define internal domains and user groups, do one of the following:
• Select **Enter domain** from the drop-down list, type the domain in the text box, and then click `>>`.

• Select **Search for LDAP groups** from the drop-down list. A screen for selecting the LDAP groups appears. Type an LDAP group name for which you want to search in the text box and click **Search**. The search result appears in the list box. To add it to the **Selected** list, click `>>`.

**Step 8: Configuring TMCM Server Settings**

1. Click **Next**. The TMCM Server Settings screen appears.

2. If you will use Control Manager to manage IMSA, do the following:
   a. Select **Enable TMCM Agent** (included with IMSA by default).
   b. Next to **Server**, type the TMCM IP address or FQDN.
c. Next to Communication protocol, select HTTP or HTTPS and type the corresponding port number. The default port number for HTTP access is 80, and the default port number for HTTPS is 443.

d. Under Web server authentication, type the user name and password for the Web server if it requires authentication.

e. If a proxy server is between IMSA and TMCM, select Enable proxy.

f. Type the proxy server port number, user name, and password.

Step 9: Activating the Product

1. Click Next. The Product Activation screen appears. You must activate the Antivirus and Content Filter to enable scanning and security updates. If you want to scan email traffic for spam or use IP Filtering (NRS and IP Profiler), enter the SPS Activation Code.

2. Type the Activation Codes for the products you want to activate. If you do not have an Activation Code, click Register Online and follow the directions at the Trend Micro Registration Web site.
Step 10: Reviewing the Settings

1. Click Next. The Review Settings screen appears.

2. If your settings are correct, click Finish. To modify any of your settings, click Back and keep moving through the screens until your settings are complete. IMSA will be operational after you click Finish and exit the Wizard.

Setting Up a Child Device

This section explains how to set up a child device and register it to the parent device.

To set up a child device:

1. Determine the IP address of the child device.
2. On the parent device, do the following:
   a. After you set up a parent device (see Setting Up a Single Parent Device on page 1-4), make sure the parent device is operational.
b. Log on to the Web console. Make sure that you are logging on the parent device Web console.

c. Choose Administration > IMSA Configuration > Connections > Child IP.

d. Under Add IP Address, add the IP address of the child device.

3. On the child device, do the following:

   a. Just as you did for the parent device, connect a management computer to the child device and log on to the Web console. All IMSA devices have the same default IP addresses and Web console login credentials.

   b. In the Setup Wizard, configure the local system settings and then click Next>.

   c. On the Deployment Settings screen, select Child Server and add the Parent device IP address.

   d. Click Finish.

4. On the parent device, do the following:

   a. Choose Summary > System from the menu.

   b. Verify that the child device appears under Managed Services and that a green check box appears under Connection. You can start or stop Scanner, Policy, or EUQ services.

   **Note:** If you enabled EUQ on the parent, it will also be enabled on the child.

5. If you want to use EUQ on the child device, redistribute the data across the EUQ databases:

   a. On the parent device, choose Administration > End-User Quarantine.

   b. Choose Redistribute all or Only redistribute to approved senders. Trend Micro recommends choosing Redistribute all.

   c. Click Redistribute.
Note: If you registered an EUQ-enabled child device to its parent device, add senders to the approved senders list, and then re-distribute EUQ data, some of the newly added approved senders might not appear. Trend Micro recommends the following:
- After redistributing EUQ, the administrator informs all end users to verify that the newly added approved senders are still available.
- That the administrator notifies all end users not to add EUQ approved senders list when the administrator is adding a child device and redistributing EUQ.

IMSA Services

The scanner and policy services must be started in order to protect your network using IMSA. You can however, choose whether to start the EUQ service.

- **Scanner Services**—Performs scanning of SMTP/POP3 traffic.
- **Policy Services**—Acts as a remote store of rules for the scanner services to enhance rule lookups.
- **EUQ Services**—Hosts a Web-based console to enable end-users to view, delete, and release spam messages addressed to them.

For more information on these services, refer to the IMSA Deployment Guide.
Starting or Stopping Services

After you have successfully activated IMSA and configured the various settings, ensure that the IMSA services are started so that IMSA can begin scanning for malware and other threats. Likewise, you may need to stop IMSA services prior to performing an upgrade or backup function.

1. Choose Summary from the menu. The Real-time Statistics tab appears by default.

2. Click the System tab.

3. Under the Managed Services section, click the Start or Stop button for the service(s) that you would like to start or stop.
Chapter 2

Configuring IMSA Settings

This chapter provides general descriptions on the various configuration tasks that you need to perform to get IMSA up and running. For more details, please refer to the Online Help accessible from the Web management console.

- *IP Filtering Service* on page 2-2
- *Scanning SMTP Messages* on page 2-11
- *Scanning POP3 Messages* on page 2-17
- *Managing Policies* on page 2-21
- *Updating Scan Engine and Pattern Files* on page 2-53
- *Configuring Log Settings* on page 2-57
IP Filtering Service

The IP Filtering service has two individual components: Network Reputation Service and IP Profiler.

- Network Reputation Service filters spam senders at the connection layer.
- IP Profiler helps protect the mail server from attacks with smart profiles (SMTP) Intrusion Detection Service (IDS).

**Tip:** Trend Micro recommends deploying IP Filtering as the first line of defense in your messaging infrastructure.

Although most email messaging systems have a multi-layer structure that often includes some pre-existing IP blocking, spam filtering, and virus filtering, Trend Micro recommends completely removing other IP blocking techniques from the messaging environment. IP Filtering should act as the precursor to any application filtering you might use.

Using Network Reputation Services

Trend Micro maintains a list of IP addresses belonging to known spam senders in a central database. Network Reputation Services (NRS) filters spam by blocking the IP addresses stored in this database.

Using the SPS Activation Code

IP Filtering Service, which includes NRS and IP Profiler, uses the same license as Spam Prevention Solution (SPS). If you purchase the full SPS service package, you will receive a registration key that will allow you to create a customer account with Trend Micro and upon completion of the registration process, you will receive your Activation Code.

The Activation Code enables you to access the level of services according to your registration. When you activate SPS, the licensing information for IP Filtering will then appear.

For details on configuring NRS, see *Configuring IP Filtering* on page 2-5
Preparing Your Message Transfer Agent for use with Network Reputation Services

To prepare your MTA for use with NRS:

- **RBL+ Service**—Configure the MTA to reject connections that have a 550 level error code (connection refused). This error code indicates that a positive response was received from the RBL+ database. Listings in the RBL+ database are known to be spammers or sources that should not be sending email. Therefore, the standard method for handling these spammers is to reject the connections outright.

  For more information, see the following URL:


- **Network Anti-Spam Service**—Configure your MTA to make 2 potential DNS queries, first to the QIL database and then to the RBL+ database.

  The QIL (Quick IP Lookup) database is a real-time dynamic database that contains a list of suspicious IP addresses that are sending spam. These IP addresses will be removed from the QIL database once spam stops coming from these addresses. If the QIL database does not receive a positive response, the MTA will need to make a second query to the RBL+ database, which contains a more stable list of blacklisted IP addresses.

  The MTA should temporarily deny connections that have a 450 level error code (server temporarily unavailable, please retry), when a positive response is received from the QIL database. The IP listings in this database are occasionally legitimate mail servers that may have compromised hosts behind them temporarily sending spam. If the connection request is from a legitimate mail server, it will re-queue and try sending the message at a later time. This will cause a short delay in mail delivery until the listing expires, but will not permanently block the mail.

  For more information, see the following URL:

Using the NRS Management Console

Log on to the Network Reputation Services management console to access global spam information, view reports, create or manage Approved Sender IP and Blocked Sender IP lists, and perform administrative tasks.

This section includes basic instructions for using the NRS console. For detailed instructions on configuring the settings for each screen, see the NRS console online help. Click the help icon in the upper right corner of any help screen to access the online help.

To use the NRS Management Console:

1. Open a browser and access the following address:
   https://nrs.nssg.trendmicro.com/
2. Select Global Spam Update from the menu.
3. Click any of the following tabs:
   - Spam Alert—Provides a brief overview and discussion of current spamming tactics and the implications for organizations. It also describes how new tactics are deployed, how they evade Trend Micro systems, and what Trend Micro is doing to respond to these new threats.
   - ISP Spam.x—The total spam volume from the top 100 ISPs for a specific week. The networks that are producing the most spam are ranked at the top. The ranking of the ISP’s will change on a daily basis.
4. To view reports that summarize the query activity between your MTA and the Network Reputation Services database servers, do the following:
   a. Select Report from the menu.
   b. Click Percentage queries, Queries per hour, or Queries per day.
5. To create or manage Approved Sender IP and Blocked Sender IP lists, choose Policy from the menu. You can define your Approved Senders by individual IP address and CIDR by Country, or by ISP.
6. To add an ISP to the list, choose New ISP from the menu.
   To change your password or Activation code, choose Administration from the menu.
Configuring IP Filtering

To completely configure IP Filtering, perform the following steps:

**Step 1:** Enable NRS and IP Profiler

**Step 2:** Enable IP Profiler Rules

**Step 3:** Configure NRS

**Step 4:** Add IP Addresses to the Approved List

**Step 5:** Add IP Addresses to the Blocked List

**Step 1: Enabling NRS and IP Profiler**

To enable NRS and IP Profiler:

1. Choose **IP Filtering > Overview** from the menu. The IP Filtering Overview screen appears.

   **IP Filtering Overview**

   ![IP Filtering Overview Screen]

   - **DHA Attack**:
     - Domain: IP
     - Dropped Connections: No malicious domains or IP addresses have been found for the last 1 day(s).

   - **Bounced Mail**:
     - Domain: IP
     - Dropped Connections: No malicious domains or IP addresses have been found for the last 1 day(s).

   - **Virus**:
     - Domain: IP
     - Dropped Connections: No malicious domains or IP addresses have been found for the last 1 day(s).

   - **Spam**:
     - Domain: IP
     - Dropped Connections: No malicious domains or IP addresses have been found for the last 1 day(s).

   - **Manual**:
     - Domain: IP
     - Dropped Connections: No malicious domains or IP addresses have been found for the last 1 day(s).
2. Select the **Enable IP Filtering** check box. This will select both the NRS and IP Profiler check boxes.

3. Clear the NRS or **IP Profiler** check box, if you do not require them.

4. Click Save.

**Step 2: Enabling IP Profiler Rules**

IP Profiler can defend against four types of attacks.

**To enable IP Profiler rules:**

1. Choose **IP Filtering > Rules** from the menu. The Rules screen appears with 4 tabs, one for each type of threat.

2. Select the desired tab to configure the rule settings for that threat.

3. Select the **Enable** check box.
4. Specify the required parameters (consult the online help for details).
5. Click Save.

Step 3: Configuring NRS

To configure NRS:

1. Choose IP Filtering > NRS from the menu. The NRS screen appears.

2. Select the Enable check box.
3. Click a radio button next to one of the following:
   - **Default intelligent action**—NRS permanently denies connection (550) for RBL+ matches and temporarily denies connection (450) for Zombie (Quick IP Lookup) matches.
   - **Take customized action for all matches**
     - **SMTP error code**—Reject any connections that have a certain SMTP code. Type an SMTP code.
     - **SMTP error string**—Type the message associated with the SMTP error code.

**Note:** The above SMTP error code and error string will be sent to the upstream MTA that will then take the necessary preconfigured actions, such as record the error code and error string in a log file.
4. Click Save.

Step 4: Adding IP Addresses to the Approved List
IMSA does not filter IP addresses or domains that appear in the Approved List.

To add an IP address to the approved list:

1. Choose IP Filtering > Approved List from the menu. The Approved List screen appears.

2. Click Add. The Add IP/Domain to Approved List screen appears.

3. Select the Enable check box.

4. Type the domain or IP address that you would like to add to the Approved List.

5. Click Save. The domain or IP address appears in the Approved List.

Step 5: Adding IP Addresses to the Blocked List
IMSA blocks IP addresses that appear in the Blocked List.
To add an IP address to the Blocked List:

1. Choose **IP Filtering > Blocked List** from the menu. The Blocked List screen appears.

2. Click **Add**. The Add IP/Domain to Blocked List screen appears.

3. Select the **Enable** check box.

4. Type the domain or IP address.

5. Select **Block temporarily** or **Block permanently**.

6. Click **Save**. The domain or IP address is added to the blocked list.
Querying IP Filtering Logs

IP Filtering records events on your network as the events occur. You can query the IP Filtering action history.

To query IP filtering logs:
1. Choose Logs > Query from the menu. The Log Query screen appears.
2. For Type select IP Filtering.

3. Specify the search data (leave blank to show all data). IMSA performs an exact match by default. Separate multiple conditions with a semicolon “;”.
4. Click Display Log to see the results.
Scanning SMTP Messages

If you have deployed multiple scanner services, you can manage the SMTP routing settings for the scanner services centrally. From the IMSA Web management console, you can configure the SMTP settings and apply the same settings to all scanners.

Configuring SMTP Routing

Configuring SMTP routing involves four steps as follows:

Step 1: Configure the SMTP settings
Step 2: Configure the Connections settings
Step 3: Configure the Message Rule settings
Step 4: Configure the Domain-based Delivery settings

Configuring SMTP Settings

To specify the SMTP settings:

1. Choose Administration > IMSA Configuration > SMTP Routing from the menu. The SMTP Routing screen appears.

2. Specify the SMTP server Greeting Message (displays when a session is created).
3. Click Save.
Configuring Connections Settings

To specify the Connections settings:

1. Choose **Administration > IMSA Configuration > SMTP Routing** from the menu.

2. Click the **Connections** tab. The Connections screen appears.
3. Specify the SMTP Interface and Connection Control parameters.
5. Click Save.

Configuring Message Rule Settings

To specify the Message Rules:

1. Choose Administration > IMSA Configuration > SMTP Routing from the menu.
2. Click the Message Rule tab. The Message Rule screen appears.
3. Specify the **Message Limits** parameters to set restrictions on the messages that IMSA will process.
4. Specify the Relay Control parameters to have IMSA reject messages matching the selected condition.
5. Specify the Relay Domains. IMSA relays the messages to the listed domains.
6. Specify the Permitted Senders of Relayed Mail.
7. Click Save.

Configuring Domain-based Delivery Settings

Specify settings for the next stage of delivery. IMSA finds the recipient mail domain and sends the mail to the next SMTP host for the matched domain.

To specify the Domain-based Delivery:
1. Choose Administration > IMSA Configuration > SMTP Routing from the menu.
2. Click the Domain-based Delivery tab. The Domain-based Delivery screen appears.

3. Click Add. The Destination Domain screen appears.
4. Specify the **Destination Domain** and **Delivery Method**.
5. Click **OK**.
6. Click **Save**.
Scanning POP3 Messages

In addition to SMTP traffic, IMSA can scan POP3 messages at the gateway as clients in your network retrieve them. Even if your company does not use POP3 email, your employees might access their personal POP3 email accounts using mail clients on their computers. Hotmail® or Yahoo® accounts are some examples of POP3 email accounts. This can create points of vulnerability on your network if the messages from those accounts are not scanned.

Understanding POP3 Scanning

The IMSA POP3 scanner acts as a proxy server (positioned between mail clients and POP3 servers) to scan messages as the clients retrieve them.

![Figure 2-1 Scanning POP3 messages](image)

To scan POP3 traffic, configure your email clients to connect to the IMSA server POP3 proxy, which connects to POP3 servers to retrieve and scan messages.

You can set up the following connection types:
• **Generic**—Allows you to access different POP3 servers using the same port, typically 110, the default port for POP3 traffic.

• **Dedicated**—Accesses the POP3 server using a specified port. Use these connections when the POP3 server requires authentication using a secure logon, such as APOP or NTLM.

**Requirements**

For IMSA to scan POP3 traffic, a firewall must be installed on the network and configured to block POP3 requests from all the computers except IMSA on your network. This configuration ensures that all POP3 traffic passes through the firewall only to IMSA and that IMSA scans the POP3 data flow.

**Enabling POP3 Scanning**

Before IMSA can begin scanning POP3 traffic, you will need to enable POP3 scanning and configure POP3 settings.

**To enable POP3 scanning:**

1. Choose **Summary** from the menu. The Real-time Statistics tab appears by default.
2. Click the **System** tab.
3. Select the check box next to Accept POP3 connections.
4. Click Save.

Configuring POP3 Settings

You can specify the IMSA server ports that clients will use to retrieve POP3 traffic. The default POP3 port is 110. However, if your users need to access a POP3 server through an authenticated connection, (through the APOP command or using NTLM) you may also set up a dedicated connection with a customized port assignment.

To add a POP3 connection:

1. Choose Administration > IMSA Configuration > Connections from the menu.
   The Components tab appears by default.
2. Click the POP3 tab.
3. Do one of the following:
   - To accept any POP3 server requested by user, type the incoming IMSA port number, if it is different from the default port 110.
   - To access the POP3 server using a specific port for authentication purposes, click **Add** to create a new dedicated POP3 connection. Provide the required information and click **OK**.
4. Click **Save**.
Managing Policies

IMSA policies are rules that are applied to incoming/outgoing email messages. Create rules to enforce your organization’s antivirus and other security goals. This section gives you an overview of how the policy manager enables you to manage IMSA policies.

How the Policy Manager Works

You can create multiple antivirus and other types of rules to filter and reduce security and productivity threats to your messaging system.

An IMSA policy has the following components:

- The **Route**—A set of sender and recipient email addresses or groups to which the policy is applied. You can use the asterisk (*) to create wildcard expressions and simplify route configuration.

- The **Filter**—A rule or set of rules that apply to a specific route, also known as scanning conditions. IMSA contains predefined filters that you can use to combat common virus and other threats. You can modify these predefined filters or define your own filters.

- The **Action**—The action that IMSA should take if the filter conditions are met. Depending on the filter result, a filter action is performed that determines how the message is finally processed.

For more information on how to create a policy, see *Adding Policies* on page 2-32.
FIGURE 2-2. Simplified policy manager process flow
Understanding Address Groups

An address group is a list of email addresses to which your policy applies.

For example, suppose that you have identified three types of content that you want to block from being transmitted through your company’s email system and have defined three filters (in parentheses) to detect these types of content:

- Sensitive company financial data (FINANCIAL)
- Job search messages (JOBSEARCH)
- VBS script viruses (VBSCRIPT)

Now consider the following address groups within your company:

- All Executives
- All HR Department
- All IT Development Staff

The filters that you use in the policies will be applied to these groups as follows:

<table>
<thead>
<tr>
<th>Address Groups</th>
<th>FINANCIAL</th>
<th>JOBSEARCH</th>
<th>VBSCRIPT</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Executives</td>
<td>Not applied</td>
<td>Applied</td>
<td>Applied</td>
</tr>
<tr>
<td>All HR Department</td>
<td>Applied</td>
<td>Not applied</td>
<td>Applied</td>
</tr>
<tr>
<td>All IT Development Staff</td>
<td>Applied</td>
<td>Applied</td>
<td>Not applied</td>
</tr>
</tbody>
</table>

Executives, HR staff, and IT developers have legitimate business reasons to send financial information, job search-related correspondence, and VBS files, respectively, so you would not apply some filters to those groups.

In IMSA, email addresses identify the different members of your organization and determine the policies that are applied to them. Defining accurate and complete address groups ensures that the appropriate policies are applied to the individuals in those groups.
Managing Address Groups

Address groups allow you to organize multiple email addresses into a single group and apply the same policy to every address in the group.

Adding an Address Group

You can create an address group when specifying the route during policy creation. You can also add an address group when modifying an existing policy. This can be done by adding email addresses individually or importing them from a text file. The following provides instructions on adding an address group when creating a new policy.

To add an address group:

1. Choose Policy > Policy List from the menu.
2. Click the Add button.
3. Select Antivirus or Other from the drop-down list to create an antivirus rule or a rule against other threats respectively.
4. Click on the Recipients or Senders link. The Select Addresses screen appears.
5. Choose Select Address Groups from the drop-down list.
6. Click the **Add** button. The Add Address Group screen appears.

7. Type a group name, then do any of the following:
• Type an email address and click Add to add email addresses individually. You can also use wildcard characters to specify the email address. For example, *@hr.com.
• Click the Import button to import a text file containing a list of predefined email addresses.

Note: IMSA 7.0 can only import email addresses from a text file. Ensure that the text file contains only one email address per line. You can also use wildcard characters to specify the email address. For example, *@hr.com.

8. Click Save.

Editing or Deleting an Address Group
You can edit or delete an address group by editing an existing policy.

To edit or delete an address group:
1. Choose Policy > Policy List from the menu.
2. Click the link for an existing policy.
3. Click the If recipients and senders are link.
4. Click the Recipients or Senders link. The Select addresses screen appears.
5. Choose **Select address groups** from the drop-down list.
6. Select the desired address group and click the **Edit** or **Delete** button accordingly.

### Searching for an LDAP User or Group

When specifying the route for a policy, instead of entering an individual email address or address group, you can also perform a search for a Lightweight Directory Access Protocol (LDAP) user or group.

IMSA supports the following three (3) types of LDAP servers:

- Microsoft™ Active Directory 2000 or 2003
- IBM Lotus™ Domino™ 6.0 or above
- SUN™ One LDAP

The following steps provide instructions on adding an LDAP user or group when creating a new policy.

**To add an LDAP user or group:**

1. Choose **Policy > Policy List** from the menu.
2. Click the **Add** button.
3. Select **Antivirus** or **Other** from the drop-down list to create an antivirus rule or a rule against other threats respectively.
4. Click on the **Recipients** or **Senders** link. The Select Addresses screen appears.
5. Choose **Search for LDAP users or groups** from the drop-down list.

   ![Select addresses](image)

   6. Type the LDAP user or group that you are looking for.

   **Note:**
   
   1. You can use the asterisk wildcard when performing a search. See *Using the Asterisk Wildcard* on page 2-51.
   
   2. You can also search for LDAP groups when adding internal addresses. For more information, see *Configuring Internal Addresses* on page 2-30.

   7. Click the **Search** button.
   
   8. IMSA will display the LDAP user or group if a matching record exists on the LDAP server.
   
   9. Select the user or group and click the **Add** button to add it to the recipient or sender list.
Configuring Internal Addresses

For reporting and rule creation, IMSA uses internal addresses to determine which policies and events are Inbound and Outbound.

Senders and recipients must be on the Internal Addresses list if you select incoming messages or outgoing messages when adding a new rule or modifying an existing rule:

- If you are configuring a rule for outgoing messages, the Internal Address list applies to the senders.
- If you are configuring a rule for incoming messages, the Internal Address list applies to the recipients.

To set internal addresses:

1. Choose Policy > Internal Addresses from the menu. The Internal Addresses screen appears.

2. Do any of the following:
• Type an internal domain name and click the >> button to add the domain to the list of internal addresses.

Note: You can also search for LDAP groups when adding internal addresses. For more information, see *Searching for an LDAP User or Group* on page 2-28.

• Click the **Import from File** button to import a list of internal domains from a text file.

3. Click **Save**.
Adding Policies

Before creating a policy, ensure that you have configured the internal addresses. For more information, see Configuring Internal Addresses on page 2-30.

Creating a policy involves four (4) steps:

Step 1: Specifying a Route
Step 2: Specifying Scanning Conditions
Step 3: Specifying Actions
Step 4: Specifying Priority

Tip: To prevent a virus leak and ensure that all messages are scanned, Trend Micro recommends that you maintain at least one antivirus rule that applies to "all messages". Select "all messages" from the drop-down list when specifying the route for an antivirus rule.

Specifying a Route

To add a new policy:

2. Click Add.
3. Select Antivirus or Other from the drop-down list.
Note: The Antivirus rule scans messages for viruses and other malware such as spyware and worms. The Other rule scans spam or phishing messages, message content, and other attachment criteria.

4. The Add Rule screen appears.

5. Select the policy route type from the drop-down list next to This rule will apply to.
   - incoming messages
   - outgoing messages
both incoming and outgoing messages
POP3
all messages (only available when creating an antivirus rule)

6. Select the recipients and senders:
   • For incoming messages, specify the recipient’s address, which is in range of the internal addresses. (for example: internal address is *@domain.com, valid recipients include jim@domain.com, bob@domain.com)
   • For outgoing messages, specify the sender’s address, which is in range of the internal addresses. (for example: internal address is *@domain.com, valid senders include jim@domain.com, bob@domain.com)
   • For both incoming and outgoing messages, the rule applies to senders or recipients that match the mail address.

**Note:**
1. You can use the asterisk wildcard when specifying an email address. For more information, see *Using the Asterisk Wildcard* on page 2-51.
2. If you selected POP3, you cannot configure the route. The rule applies to all routes.
3. If you selected “all messages” for an antivirus rule, the rule applies to messages from any sender to any recipient.

---

**Specifying Scanning Conditions**

To specify scanning conditions:

1. Click **Next**. The Step 2: Select Scanning Conditions screen appears.
2. Select the check boxes as desired. The categories of scanning conditions for the Antivirus and the Other rule types vary as follows:
Antivirus rule

- **Files to Scan**—Sets the default method for scanning messages and specific file types containing viruses and other malware. Also uses IntelliScan to identify malicious code that can be disguised by a harmless extension name.
• **IntelliTrap Setting**—Scans compressed files for viruses/malware and sends samples to TrendLabs for investigation.

• **Spyware/Grayware Scan**—Scans other types of threats such as spyware and adware.
• **Other rule**
  • **Spam/phishing emails**—Scans messages identified as spam and phishing messages. Spam messages are generally unsolicited messages.
containing mainly advertising content. Phishing messages, on the other hand, originate from senders masquerading as trustworthy entities.

- **Attachment**—Scans messages for file attachments that match the selected criteria, such as attachments with specific extensions or belonging to a certain true file type.
- **Size**—Scans messages that match the specified message size.
- **Content**—Scans messages containing the keyword expressions that match those expressions specified in the subject, body, header, or attachment content keyword expressions links.
- **Others**—Scans messages in which the number of recipients match the specified number. Also scans messages that are received within the specified time range.

### Specifying Actions

**To set the actions:**

1. Click **Next**. The Step 3: Select Actions screen appears.

   **Note:** The user interface that appears in this step depends on the type of rule that you are creating. The antivirus rule contains two tabs that allow you to configure the main actions and the actions for special viruses.

2. The main actions for both the Antivirus and Other rule are similar, although there are minor differences in the options listed. Select the desired action(s) from the following categories:
   - **Intercept**—Allows you to choose whether you would like IMSA to intercept the messages and prevent them from reaching the recipients. Choosing the intercept option allows you to specify an action for IMSA to take on intercepted messages.
   - **Modify**—Instructs IMSA to make some alterations to the messages or the attachments, such as inserting a stamp or tagging the subject.
   - **Monitor**—Instructs IMSA to send a notification, archive, or blind copy the messages if you would like to further analyze them.

**To specify actions for an Antivirus rule:**

Specify the main actions or actions for special viruses by clicking the respective tabs.
1. **Main Actions**—Allows you to specify the default actions that IMSA takes when messages match the scanning conditions specified in Step 2: Scanning Conditions.

2. **Special Viruses**—Allows you to specify the actions that IMSA takes if the messages match any of the following criteria. The actions specified on this screen will override the default actions specified on the Main Actions tab.
• **Mass mailing**—IMSA takes the actions specified in this section if it detects mass mailing messages.

• **Spyware/grayware**—Allows you to specify the corresponding actions if you have selected any of the Additional Threats Scanning options on the Scanning Conditions screen in step 2. See *Specifying Scanning Conditions* on page 2-34. If IMSA detects spyware/grayware in a message, it takes the actions that are specified here.

  **Note:** IMSA takes the default action for messages matching the Additional Threats Scanning conditions if you do not select alternative actions.

• **IntelliTrap**—Allows you to specify the corresponding actions if you have selected the IntelliTrap Setting options on the Scanning Conditions screen in step 2. See *Specifying Scanning Conditions* on page 2-34.

  **Note:** IMSA takes the default action for messages matching the IntelliTrap conditions if you do not select alternative actions.

To specify actions for the Other rule:

The Select Actions screen when creating an Other rule appears as follows.
Specifying Priority

Setting the priority of a rule allows you to control the order in which IMSA matches the messages against a list of policies that you have created.

To specify a priority:

1. Click Next. The Step 4: Name and Order screen appears.
2. Select the **Enable** check box to activate the rule.
3. Type a name for the rule in the **Rule Name** field.
4. In the **Order Number** field, specify the priority in which IMSA will perform the scan. IMSA applies the rule to messages according to the order you specify.
5. Click the **Notes** tab. The Notes screen appears.
6. Type a note to distinguish the new rule from other rules.
7. Click Finish.

Example 1

How do I create a rule to delete attachments with specific file names or extensions and then stamp the affected incoming message with an explanation to the recipients?

Step 1: Specify the Route
1. Choose Policy > Policy List from the menu.
2. Click Add.
3. Select Other from the drop-down list. The Step 1: Select Recipients and Senders screen appears.
4. Next to This rule will apply to, select incoming messages from the drop-down list.
5. Click the Recipients link. The Select addresses screen appears.
   a. To apply this rule to any recipients, select Anyone.
b. To apply this rule to specific recipients, choose **Any of the selected addresses**, and then specify the target email address or group.

c. Click **Save**. The Step 1: Select Recipients and Senders screen re-appears.

**Step 2: Specify the Scanning Conditions**

1. Click **Next**. The Step 2: Select Scanning Conditions screen appears.
2. Next to **Take rule action when**, select **any condition matched (OR)**.
3. To enable the **Name or extension** condition, select the check box next to it.
4. Click **Name or extension**. The Attachment Name or Extension screen appears.
5. Select the file extensions to block or consider blocking.
6. Click Save. The Step 2: Select Scanning Conditions screen re-appears.

**Step 3: Specify the Actions**
1. Click Next. The Step 3: Select Actions screen appears.
2. Under Modify, to enable the **Delete attachment** action, select the check box next to it.
3. Select **Matching attachment** from the drop-down list if it is not already selected.
4. Select the check box next to **Insert stamp in body**.
5. If there is no suitable stamp available from the drop-down list, click **Edit**. The Stamps screen appears.
6. Click **Add** to create a new stamp. The New Stamp screen appears.

7. Provide the required information.
8. Click **Save**. The Stamps screen re-appears.
9. Click **Done**. The Select Actions screen re-appears.
10. Select the newly created stamp from the drop-down list.

**Step 4: Specify the Priority**
1. Click **Next**. The Step 4: Name and Order screen appears.
2. Type the rule name and order number.
3. Click Finish. The newly created rule will appear highlighted in the Policy list screen.

Example 2

How do I create a rule that quarantines messages containing specific keywords in the subject or body and then apply this rule to all recipients except administrators?

Step 1: Specify the Route

2. Click Add.
3. Select Other from the drop-down list. The Step 1: Select Recipients and Senders screen appears.
4. Next to This rule will apply to, select incoming messages from the drop-down list.
5. Click the Recipients link. The Select addresses screen appears.
7. Click Save. The Step 1: Select Recipients and Senders screen re-appears.
8. Click the Sender to Recipient link next to Exceptions. The Exceptions screen appears.
9. Under **From (sender)**, type *@* to specify any sender.
10. Under **To (recipient)**, type the administrator’s email address.
11. Click **Add**. The sender-recipient pair appears in the list.
12. To add other administrators or recipients, repeat steps 9 to 11.
13. Click **Save** after you finish adding all the desired recipients. The Step 1: Select Recipients and Senders screen re-appears.

**Step 2: Specify the Scanning Conditions**

1. Click **Next**. The Step 2: Select Scanning Conditions screen appears.
2. Next to **Take rule action when**, select **any condition matched (OR)**.
3. To enable the **Subject Keyword Expressions** condition under **Content**, select the check box next to it.
4. Click **Subject Keyword Expressions**. The Keyword Expressions screen appears.
5. If the desired keywords are not available from the existing list, click **Add** to create a new keyword list. The New Keyword Expression screen appears.

6. Specify the required information.
7. To add an individual keyword expression, click **Add**. The Add Keyword Expressions screen appears.
8. Type the desired keyword expression and click **Save**. The New Keyword Expression screen re-appears.

9. Repeat steps 7 and 8 for additional keyword expressions.

10. After you have added all the required keyword expressions, click **Save**. The Keyword Expressions screen re-appears with the newly created keyword list.

11. Select the new list and click >> to insert the list into the Selected box.

12. Click **Save**. The Step 2: Select Scanning Conditions screen re-appears.

13. To enable the **Body Keyword Expression** condition, select the check box next to it.

14. Click **Body Keyword Expression**. The Keyword Expressions screen appears.

15. Select the new keyword list and click >> to insert the list into the Selected box.

16. Click **Save**. The Step 2: Select Scanning Conditions screen re-appears. Ensure that both the Subject keyword and Body keyword expressions are selected.
Step 3: Specify the Actions
1. Click Next. The Step 3: Select Actions screen appears.
2. Under Intercept, select Quarantine to.
3. Accept the Default Quarantine area or click the drop-down list to select the desired quarantine area.

Step 4: Specify the Priority
1. Click Next. The Step 4: Name and Order screen appears.
2. Type the rule name and order number.
3. Click Finish. The newly created rule will appear highlighted in the Policy list screen.

Using the Asterisk Wildcard
You can use the asterisk (*) as a wildcard in email addresses when defining routes and in file names.

Wildcards in Email Addresses
Wildcards can appear in the name or domain sections of an email address. The following are valid examples:
• *—Valid representation of all email addresses.
• *@domain.tld, name@*.tld—Valid representation of the whole name or the domain (not the top level domain (TLD)).
• *@*.tld—Valid representation of both the name and the domain (not the TLD).

Wildcards cannot appear in a sub domain or the top-level domain. Wildcards also cannot appear with other letters; they must appear alone. The following are invalid examples:
• name@domain.*.tld—Invalid representation of a sub domain.
• name@domain.*—Invalid representation of a TLD.
• *name@domain.tld—Invalid use in conjunction with a name.

Wildcards in File Names
You can use wildcard characters in file names the same way you can use them in email addresses. Use an asterisk in the name or the extension sections of a filename,
but not in conjunction with a partial name or extension. The following are valid examples:

•  *.*—Valid representation of all files.
•  *.extension—Valid representation of all files of a certain extension.
•  name.*—Valid representation of files with a specific name but with any extension.

The following are invalid examples:

•  *name.*—Invalid representation of a name.
•  name.*extension—Invalid representation of an extension.
**Updating Scan Engine and Pattern Files**

To ensure that your network is well protected against the latest malware, ensure that you update IMSA components such as the scan engine and virus pattern files on a regular basis. You can choose to perform a manual or scheduled update of the components.

**Specifying an Update Source**

Before you can update the IMSA scan engine and pattern files, you need to specify the update source. By default, IMSA downloads components from the Trend Micro ActiveUpdate server, which is the only source for up-to-date components. However, if you are using Trend Micro Control Manager (TMCM) to manage IMSA, you can update the components from the Control Manager server.

If you did not specify the Update Source when configuring IMSA using the Configuration Wizard, enter the update source and/or any proxy settings as follows:

1. Choose **Administration > Updates > Components** from the menu. The Schedule tab appears by default.
2. Click the **Source** tab.
3. Make your selection and provide the required information.
4. Click Save.

Performing a Manual Update

You may perform a manual update of IMSA components under the following circumstances:

- If you have just deployed or upgraded IMSA.
- If you suspect that your network’s security has been compromised by malware and would like to update the components immediately.

To perform a manual update:

1. Choose Summary from the menu. The Real-time Statistics tab appears by default.
2. Click the System tab.
3. To update all components, select the first check box on the column header next to the Name field. Otherwise, to update specific component(s), select the check box next to the desired component.

4. Click the Update button.

**Rolling Back a Component Update**

If you encounter any system issues after updating IMSA components, you can roll back to the previous version.

**To roll back a component update:**

1. Choose Summary from the menu. The Real-time Statistics tab appears by default.
2. Click the **System** tab.
3. To roll back all components to the previous versions, select the first check box on the column header next to the Name field. Otherwise, to roll back specific component(s), select the check box next to the desired component.
4. Click the **Rollback** button.

**Configuring Scheduled Update**

To have IMSA automatically update the components at specified intervals, configure the update schedule.

**To configure a scheduled update:**

1. Choose **Administration > Updates > Components** from the menu. The Schedule tab appears by default.

2. Specify the required information.
3. Click **Save**.
Configuring Log Settings

To define the duration for which IMSA retains database logs for query and application logs for troubleshooting purposes, configure the log settings.

1. Choose **Logs > Settings** from the menu. The Log Settings screen appears.

   ![Log Settings Screen](Image)

   **Log Settings**

   Reporting Logs (Stored in Database)

   - Database log update interval: 01 minutes
   - Number of days to keep logs for queries: _days_

   Log Files

   - Application log detail levels: Normal
   - Number of days to keep log files: _days_
   - Maximum log file size for each service: _MB_

2. Specify the required information.
3. Click **Save**.
Chapter 3

Backing Up, Restoring, and Replicating Settings

This chapter provides instructions on how you can back up and restore IMSA configuration settings as a precaution against system failure. If you have deployed multiple IMSA devices and are using Trend Micro Control Manager simultaneously, you can also replicate IMSA settings without having to reconfigure settings for each new scanner.

Topics include:

• Import/Export Notes on page 3-2
• Backing Up IMSA Settings on page 3-2
• Restoring IMSA Settings on page 3-4
• Replicating Settings on page 3-6
Import/Export Notes

To back up IMSA settings, export the settings from the Web management console. In the event of system failure, you can restore the settings by importing the configuration file that you have backed up previously. Note the following when importing/exporting settings:

• You cannot import or export the component list and child device registration information.
• When exporting/importing your settings, the database will be locked. Therefore, all IMSA actions that depend on database access, such as performing a mail trace, will not function.
• SMTP Routing Settings that were exported from IMSA 1.0 or IMSA 7.0, and subsequently imported into IMSA 7.0, will overwrite existing settings in the current IMSA version.

Trend Micro strongly suggests that you:

• Adjust the component list and child device registration information after import if necessary
• Backup a copy of current configuration before each import operation, in order to recover from mistaken import processes.
• Perform import/export when IMSA is idle because importing and exporting affects IMSA performance.

Backing Up IMSA Settings

Trend Micro recommends exporting your settings to:

• **Keep a backup**—In case a problem occurs with the IMSA application file and you need to rescue the application. Importing your configuration backup will prevent you from having to configure all settings again.
• **Replicate settings across several devices**—If you have several devices on your network, you do not need to configure most settings on each of them separately.

**To export settings:**

1. Choose **Administration > Import/Export** from the menu.
2. Click **Export**.

3. When the File Download dialogue box appears, click **OK** to save the configuration file to your computer.

4. To return to the Import/Export screen, click **Return**.

During export, do not:

- Access other Web console screens or modify any settings.
- Perform any database operations.
- Start/stop any services on the device or in the group to which the device belongs.
- Register/unregister any child devices into/from the group to which the device belongs.
- Launch other export or import tasks.
Restoring IMSA Settings

To restore IMSA settings, import the configuration files that you have backed up previously.

**To import settings:**

1. Choose **Summary** from the menu. The Real-time Statistics tab appears by default.
2. Click the **System** tab.
3. Verify that no services are starting or stopping. If services are starting or stopping, wait until they are stable.
4. Choose **Administration > Import/Export** from the menu.
5. Under **Import Configuration Files**, click **Browse...** and locate the file.
6. Click **Import**. The original settings and rules, such as domain-based delivery settings, will be deleted and replaced by the imported settings and rules. All services on each device in the group will be restarted to apply the imported settings and rules. Wait until all services are restarted.

During import, do not:

- Access other Web console screens or modify any settings.
- Perform any database operations.
- Start/stop any services on the device or in the group to which the device belongs.
- Register/unregister any child devices into/from the group to which the device belongs.
- Launch other export or import tasks.
Settings That Cannot Be Restored

- Control Manager Settings
- EUQ approved senders
- Administrator Accounts & Password
- Activation Code & license information
- ActiveUpdate server information
- IP and network settings
- Group member list
Replicating Settings

If you have deployed multiple IMSA groups, you can use the Trend Micro Control Manager to replicate settings across these groups without having to configure each group separately.

Do the following if you intend to replicate settings using Control Manager:

**Step1:** Back up IMSA settings. For details, see *Backing Up IMSA Settings* on page 3-2.

**Step2:** Enable the Control Manager agent.

**Step3:** Replicate settings from the Control Manager Web console.

Enabling Control Manager Agent

To integrate with Control Manager, all you need to do is provide the Control Manager server details and enable the agent from the Web management console.

To configure Control Manager Server settings:

1. Choose **Administration > IMSA Configuration > Connections** from the menu. The Components tab appears by default.
2. Click the **TMCM Server** tab. The TMCM Server Settings screen appears.
3. Provide the required information.
4. Select the check box next to **Enable TMCM Agent**.
5. Click **Save**.

**Replicating Settings from Control Manager**

After enabling the Control Manager agent from the IMSA Web management console, you can start to replicate IMSA settings by logging on to the Control Manager Web console.

**To replicate IMSA settings:**

1. Choose **Products** from the Control Manager menu.
2. Locate the source IMSA scanner from the Product Directory on the left of the user interface.
3. Click the **Tasks** tab.
4. Select **Configuration Replication** from the drop-down list.

5. Click **Next**.

6. Select the check box next to the target server.
7. Click the Replication button.
Maintaining IMSA

This chapter provides you with general instructions on the tasks that you need to perform for the day-to-day maintenance of IMSA. For more information on each field on the Web management console, please refer to the Online Help.

Topics include:

- *Monitoring Your Network* on page 4-2
- *Logs* on page 4-13
- *Mail Areas and Queues* on page 4-15
- *Configuring NTP Setting* on page 4-23
- *Configuring Database Maintenance Schedule* on page 4-24
- *Event Notifications* on page 4-19
- *Managing Administrator Accounts* on page 4-25
- *Configuring Policy Connections* on page 4-28
Monitoring Your Network

IMSA provides a complete set of tools that enable you to monitor your network traffic. You can obtain useful information such as the statistics on the performance of IMSA components, or generate reports that display a breakdown of messages matching various scanning conditions.

Viewing the Real-time Statistics

You can obtain up to the last 24 hours’ of statistics on the performances of IMSA scanners and IP profilers. These statistics provide useful information to help you better manage your IMSA policies and enhance the security of your network.

To view the statistics:

1. Choose Summary from the menu. The Real-time Statistics tab appears by default.
2. Select the device from the Host drop-down list.
3. Select the desired last # minutes/hours from the Show drop-down list.

Note: IMSA automatically updates these statistics in its database every 5 minutes.
Interpreting the Real-time Statistics

IMSA presents performance statistics in both graphical and table formats. This section explains how the values in the System Overview, IMSA Scan Performance, and IP Filtering Performance sections on the Real-time Statistics tab are derived.

Note: In the table, the total number of messages matching each scanning condition or IP filtering type consists of overlaps. For example, if a message matches more than one scanning condition, such as spam and attachment, this message will be counted twice, once in the total number for spam and a second time in the total number for attachment. Values in the chart, however, do not include such overlaps.

System Overview

This section shows the system information of the devices that you select from the Host drop-down list. If you select All servers, IMSA will display the system information for all the devices within a group.

Note: 1. The data partition stores IMSA logs and databases.
2. The queue partition stores messages in the delivery, quarantined, postponed, and deferred queues.
**IMSA Scan Performance**

This section shows a breakdown of the total number of messages processed in terms of the following:

- Number of incoming and outgoing messages, and their corresponding values in percentages of the total.
- Number of messages matching various types of scanning conditions specified in the policy rules, and their corresponding values in percentages of the total.

The chart and table are interpreted as follows:

- **Chart**
  
  IMSA displays a maximum of 12 bars in the chart. The duration represented by each bar depends on the period you select from the **Show** drop-down list. For example, if you choose to view the scan performance of the **Last 60 minutes**, each bar represents 5 minutes’ worth of messages scanned.

  You can choose to view the statistics for messages matching all the scanning conditions, or for messages matching only selected conditions.

  **To view the statistics for messages matching only specific scanning conditions:**
  
  - Select the check box(es) next to the desired scanning condition(s).
  - Click **Apply**.

- **Table**
  
  Numbers in the table show the messages matching each scanning condition.
### IMSA Scan Performance

- **Messages Processed**
  - **Total**
    - **Total**: 68312
    - **%**: 100%
    - **Average Speed (msgs/min)**: 1.855
  - **Incoming**: 33577
    - **%**: 48%
    - **Average Speed (msgs/min)**: 559
  - **Outgoing**: 24735
    - **%**: 31.56%
    - **Average Speed (msgs/min)**: 295

### Scanning Conditions

- **Malicious code**: 8500
  - **%**: 6.49%
- **Spam/grayware**: 4750
  - **%**: 6.85%
- **Spam**: 13000
  - **%**: 18.91%
- **Phish**: 4410
  - **%**: 6.26%
- **Attachment**: 2500
  - **%**: 3.65%
- **Size**: 4090
  - **%**: 5.77%
- **Content**: 3990
  - **%**: 5.76%
- **Others**: 3050
  - **%**: 4.45%
- **Scanning exceptions**: 3400
  - **%**: 4.92%
IP Filtering Performance

This section shows the number of connections blocked based on the following:

- The four types of IP Filtering rules, namely, spam, malicious code, DHA attack, and bounced mail.
- IP addresses that you have manually entered.
- NRS.

<table>
<thead>
<tr>
<th>IP Filtering Type</th>
<th>Total Blocked Connections</th>
<th>Blocked %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>10493</td>
<td>100%</td>
</tr>
<tr>
<td>Spam (IP Profile)</td>
<td>2790</td>
<td>27.18%</td>
</tr>
<tr>
<td>Malicious code (IP Profile)</td>
<td>1210</td>
<td>11.70%</td>
</tr>
<tr>
<td>DHA attack (IP Profile)</td>
<td>1000</td>
<td>9.61%</td>
</tr>
<tr>
<td>Bounced mail (IP Profile)</td>
<td>1600</td>
<td>15.09%</td>
</tr>
<tr>
<td>Manual (IP Profile)</td>
<td>1205</td>
<td>11.41%</td>
</tr>
<tr>
<td>Network Reputation Services</td>
<td>1220</td>
<td>11.72%</td>
</tr>
</tbody>
</table>
Generating Reports

Depending on your needs, you can choose to generate a one-time report on demand or schedule a report to be run at specific intervals. IMSA offers you the flexibility of specifying the content for each report and the option of viewing or saving the result in HTML or CSV format.

Types of Report Content

You can choose from the following types of content to be included in the report:

<table>
<thead>
<tr>
<th>Report Content</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy and traffic summary</td>
<td>Shows the total number and size of incoming and outgoing messages. Also shows the number of messages matching specific scanning conditions.</td>
</tr>
<tr>
<td>Virus and malicious code summary</td>
<td>Shows a summary of the virus message count by actions.</td>
</tr>
<tr>
<td>Spam summary</td>
<td>Shows a summary of the total spam message count by anti-spam engine, NRS, IP Profiler, and actions.</td>
</tr>
<tr>
<td>Sender IP address blocking summary</td>
<td>Includes &quot;IP Profiler Blocking Summary&quot; and &quot;NRS Blocking Summary&quot;. The former shows a summary of the total number of sender connections that reached IP Profiler and are blocked by the different IP Filtering rules. The latter shows the total sender connections that reached NRS and are blocked by NRS.</td>
</tr>
<tr>
<td>Top 10 traffic email addresses</td>
<td>Shows the top 10 email addresses ranked by the total sent and received message count.</td>
</tr>
<tr>
<td>Top 10 virus names</td>
<td>Shows the top 10 virus names ranked by their detected count.</td>
</tr>
<tr>
<td>Top 10 IP addresses for DHA attack addresses</td>
<td>Shows the top 10 IP addresses ranked by the blocked count for DHA attack.</td>
</tr>
<tr>
<td>Top 10 IP addresses for bounced mail attack addresses</td>
<td>Shows the top 10 IP addresses ranked by the blocked count for bounced mail attack.</td>
</tr>
<tr>
<td>Top 10 virus recipients and senders</td>
<td>Shows the top 10 virus recipients and senders ranked by their total received and sent virus message count respectively.</td>
</tr>
</tbody>
</table>

**TABLE 4-1. Report content descriptions**
Adding One-time Reports

You can generate one-time reports on demand to help monitor the traffic on your network.

To create a one-time report:
1. Choose Reports > One-time Report from the menu.
2. Click Add.
3. Provide the required information.

4. Click Save. The report takes several minutes to generate. The message In progress appears in the report table.

After the report generates, the hyperlinks HTML and CSV display in the report table.
5. Click **HTML** to display the report in HTML format.
6. Click **CSV** to export the report data to a csv file.

**Note:** Report generation occurs once every five minutes. This means that report generation could require as much as five minutes in addition to the time required to aggregate reporting data and make the necessary calculations.

### Configuring Scheduled Reports
Scheduled reports generate automatically according to the intervals you configure.

**To create a scheduled report:**

1. Choose **Reports > Settings** from the menu. The Scheduled Report Settings screen appears.

   **Scheduled Report Settings**

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Status</th>
<th>Schedule</th>
<th>Configure</th>
<th># to Save</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily reports</td>
<td>🟢</td>
<td>2:00</td>
<td>Settings</td>
<td>60</td>
</tr>
<tr>
<td>Weekly reports</td>
<td>🟢</td>
<td>Sunday at 2:00</td>
<td>Settings</td>
<td>20</td>
</tr>
<tr>
<td>Monthly reports</td>
<td>🟢</td>
<td>Date 1st 2:00</td>
<td>Settings</td>
<td>5</td>
</tr>
</tbody>
</table>

2. Click the **Settings** link for one of the following report types:
   - Daily reports
   - Weekly reports
• Monthly reports

The Report Settings screen appears.

3. Specify your settings for the report.

Note: When configuring monthly report settings, if you choose to generate the report on the 29th, 30th, or 31st day, IMSA will generate the report on the last day of the month for months with fewer days. For example, if you select 31, IMSA will generate the report on the 28th (or 29th) in February, and on the 30th in April, June, September, and November.

4. Click Save. The report status changes.
5. Specify the number for each type of report that you would like to retain. Click \textit{Save}.

6. Choose \textit{Reports} > \textit{Scheduled Reports} from the menu. The Scheduled Reports screen appears.

\textbf{Note:} The report has not generated yet.

7. After the report generates, you can click \textit{HTML} or \textit{CSV} to view the report.
Logs

Logs are a useful means of enabling you to monitor various types of events and information flow within IMSA. They also serve as an important resource for troubleshooting purposes.

To enable logs and benefit from the information, do the following:

Step 1: Configure the log settings. For details, see Configuring Log Settings on page 2-57.

Step 2: Perform log query.

Querying Logs

You can perform queries on five types of events or information:

- **Message tracking**—Records message details such as the sender, recipient(s), message size, and the final action that IMSA has taken. In the case of quarantined messages, the query result will also indicate the name and type of the policy rule that was triggered.
- **System events**—Tracks the time of system events such as user access, modification of rules, registration of Control Manager agent and so on.
- **Policy events**—Provides details on the policy rules that were triggered, the actions taken, and the message details.
- **MTA logs**—Provides connection details of Postfix on the selected parent or child device.
- **IP Filtering**—Provides the time when IMSA started and stopped blocking email messages from the queried IP address.

For most log queries, IMSA supports wildcards (*) and exact matches (for example, to view mail recipients whose name includes A or B, set the recipient(s) to “*A*;*B*”). IMSA uses exact matching by default. Leaving the search condition blank displays all logs. For multiple-conditions items, use semicolons (;) to separate the entries for recipient(s) and attachment(s).

To query logs:

1. Choose **Logs > Query** from the menu. The Log Query screen displays.
2. Select the type of logs to query from the **Type** drop-down list.
3. Specify the query details.
4. Click Display Log.
Mail Areas and Queues

IMSA stores messages matching specific policy rule actions in the following areas and queues:

- **Quarantine Area**—Stores messages that you would like to analyze before deciding whether to delete or release to the intended recipient(s).
- **Archive Area**—Stores messages for future reference.
- **Postponed Queue**—Stores messages that will be delivered at a specified time.
- **Deferred Queue**—Stores messages that IMSA is unable to deliver to the next MTA. IMSA will try to resend the message every 1000 seconds. If IMSA is still unable to deliver the message within 24 hours, the message will be returned to the sender.

Configuring Quarantine and Archive Settings

Quarantine and archive settings allow you to manage these areas and allocate the amount of disk space per scanner for storing quarantined or archived messages.

**To configure quarantine and archive settings:**

1. Choose **Mail Areas & Queues > Settings** from the menu. The Quarantine and Archive Settings screen appears.

   ![Quarantine and Archive Settings](image)

<table>
<thead>
<tr>
<th>Quarantine</th>
<th>Archive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk quota (per scanner): 10 GB</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Delete</td>
</tr>
<tr>
<td>Area</td>
<td>Expiration</td>
</tr>
<tr>
<td>Default Quarantine</td>
<td>30 day(s)</td>
</tr>
</tbody>
</table>

2. Specify the disk quota per scanner.
3. Click **Add**. The Add Quarantine screen appears.
4. Specify the required information.
5. Click Save. To configure archive settings, click the Archive tab accordingly.
Managing Mail Areas and Queues

You can perform a query on quarantined, archived, postponed, or deferred messages before deciding on the action to be taken. After viewing the message details, you can then choose to release or delete the messages.

To manage mail areas and queues:

1. Choose Mail Areas & Queues > Query from the menu. The Quarantine tab appears by default.

   ![Mail Areas & Queues Management](image)

   2. To query quarantined, archived, postponed, or deferred messages, click the respective tab.
   3. Specify the search criteria.
   4. Click Display Log.
   5. Click the Timestamp hyperlink for a result item. The item details display.
6. Click Release or Delete to release or delete the message respectively.
Event Notifications

You can configure IMSA to send an email or SNMP notification to you or specific email users upon the occurrence of the following categories of event:

- **System Status**—Informs you when certain IMSA performances fall below the desired level. For example, when a scanner service stops working, or when the number of messages in the delivery queue exceeds the desired quantity.

- **Scheduled Update Event**—Alerts you when IMSA is able or unable to perform a scheduled update of the scan engine or pattern files from the update source onto the admin database.

- **Scanner Update Result**—Alerts you when IMSA is unable to update the engine or pattern files on any scanner.

- **Hardware Events**—Alerts you when hardware events such as CPU temperature and fan speed exceed or fall below the specified thresholds.

**Note:** Component update is a 2-step process:
1. At the scheduled time, the IMSA admin database will first check the update source for new engine or pattern files.
2. IMSA scanners will then check the admin database at regular intervals for updated components. The default interval is three (3) minutes.
Configuring Delivery Settings

The delivery settings allow you to specify the sender, recipient(s) and other settings required for delivering the notification message when certain events are triggered.

To configure the delivery settings:

1. Choose **Administration > Notifications** from the menu. The Events tab appears by default.
2. Click the **Delivery Settings** tab.
3. Provide the required information.
4. Click Save.

Configuring Event Criteria and Notification Message

You can set the criteria under which IMSA will trigger a notification message and also customize the message content for each event.

To configure the criteria and message content:

1. Choose Administration > Notifications from the menu. The Events tab appears by default.
2. Specify the desired criteria under the System Status section.

3. Select the Email and/or SNMP check boxes according to how you would like to receive the notification.

4. To customize the message content, click on the hyperlink for the specific event. The Message Edit screen appears.
Configuring NTP Setting

The Network Time Protocol (NTP) synchronizes the clocks of computer systems across the Internet. To synchronize the computer clock of an IMSA device with the clock of an NTP server, configure the NTP setting.

To configure NTP setting:

1. Choose Administration > IMSA Configuration > Connections from the menu. The Components tab appears by default.
2. Click the NTP Setting tab.
3. Select the **Enable NTP** check box.
4. Type the domain name or IP address of the NTP server.
5. Click **Save**.

### Configuring Database Maintenance Schedule

You may want to re-index the IMSA database tables if you encounter slow performance when performing queries. As re-indexing can impact the scanner performance, Trend Micro recommends that you do this during off-peak hours.

**To re-index database tables:**

1. Choose **Administration > Database Maintenance** from the menu. The Database Maintenance Schedule screen appears.

2. Select the **Re-index database tables** check box.
3. Select the weekly or monthly schedule from the drop-down boxes.
4. Click **Save**.
Managing Administrator Accounts

To reduce bottlenecks in administering IMSA, you can delegate administrative tasks to other staff by creating new administrator accounts and assigning the desired permissions to the various areas of the Web management console.

Adding Administrator Accounts

To add administrator accounts:

1. Choose Administration > Admin Accounts from the menu. The Admin Accounts screen appears.

2. Click Add. The Add Administrator Account screen appears.

3. Provide the required information on the Authentication tab.
4. Click the Permissions tab. The Permissions screen appears.
5. Select the desired permissions to the various access areas of the Web management console and the command line interface.

6. Click Save.

**Note:**
1. Only the default IMSA administrator account can add new administrator accounts. Delegate administrator accounts cannot do so even if you assign full permission to the Administration area.

2. Delegate administrator accounts with full administration rights can only change their own IMSA passwords. If you forget the default administrator account password, please contact Trend Micro’s technical support to reset the password.

**Editing or Deleting Administrator Accounts**

You can change or delete the permissions of a delegate whenever there is a revision of roles or other organizational changes.

**To edit an administrator account:**

1. Choose Administration > Admin Accounts from the menu. The Admin Accounts screen appears.

2. To edit an administrator account, click the account name hyperlink.

3. Make the required changes.
4. Click Save.

**To delete an administrator account:**

1. To delete an administrator account, select the check box next to the account to be removed.
2. Click **Delete**.
3. Click **OK** to confirm the deletion or **Cancel** to withdraw.

---

**Note:** You can only delete the delegate administrator account but not the default IMSA administrator account.
Configuring Policy Connections

To enhance the performance of rule lookups by the policy services, configure the connection settings.

To configure scanner and policy connections:

1. Choose Administration > IMSA Configuration > Connections from the menu. The Components tab appears by default.

2. Specify the required settings.

3. Click Save.
Using EUQ

This chapter explains how to use End-User Quarantine (EUQ).

Topics include:

- *About EUQ* on page 5-2
- *Step 1: Configuring and Enabling LDAP* on page 5-2
- *Step 2: Enabling EUQ* on page 5-5
- *Step 3: Starting the EUQ Service* on page 5-7
- *Step 4: Enabling End-User Access* on page 5-8
- *Step 5: Opening the End-User Quarantine Console* on page 5-10
- *Disabling EUQ* on page 5-11
About EUQ

IMSA provides Web-based EUQ to improve spam management. The Web-based EUQ service allows end-users to manage their own spam quarantine. Messages that are determined to be spam are placed into quarantine. These messages are indexed into a database by the EUQ agent and are then available for end-users to review, delete, or approve for delivery.

To use EUQ, you must do the following:

**Step 1:** Configure and enable LDAP
**Step 2:** Enable EUQ
**Step 3:** Start EUQ service
**Step 4:** Enable end-user access
**Step 5:** Open the EUQ console

**Step 1: Configuring and Enabling LDAP**

To use EUQ, you must configure and enable LDAP.

**To enable and configure LDAP:**

1. You can configure and enable LDAP settings in 2 ways:
   - Choose Administration > IMSA Configuration > Connections from the menu, then click the LDAP tab.
## Connections

<table>
<thead>
<tr>
<th>Components</th>
<th>LDAP</th>
<th>POP3</th>
<th>IRC Server</th>
<th>NTP Setting</th>
<th>Child IP</th>
</tr>
</thead>
</table>

### LDAP Settings

Enter LDAP settings if you wish to use them for user-group definition, administrator privileges, or end-user quarantine authentication.

**LDAP server type:** Microsoft Active Directory

- **Enable LDAP1**
  - LDAP server: Example: example.com or 123.123.123.123

- **Enable LDAP2**
  - LDAP server: Example: example.com or 123.123.123.123

**Note:** Please use the global catalog port 3268 if the LDAP server type is Microsoft Active Directory.

### LDAP Cache expiration for policy services and EUQ services

**Time to live in minutes:** 1440

### LDAP admin

**LDAP admin account:** Example: Domain_name\Account_Name or Account_Name@Domain_Name

**Password:** ********

**Base distinguished name:** Example: DC=foo, DC=example, DC=com

**Authentication methods:**
- Simple

**Kerberos authentication default realm:**

**Default domain:**

**KDC and admin server:**

**KDC port number:**

---

5-3
Choose Administration > IMSA Configuration > Configuration Wizard from the menu.

2. Configure all LDAP settings.
Step 2: Enabling EUQ

To enable EUQ:

1. You can enable EUQ in 2 ways:
   - Choose Administration > End-User Quarantine from the menu.
Choose Administration > IMSA Configuration > Configuration Wizard from the menu, then go to Step 2: Deployment Settings.

2. Select the Enable End-User Quarantine check box.
3. Click Save at the EUQ Management tab. If you are using the wizard, progress through the wizard screens and click Finish.
4. At the EUQ Management tab, click Redistribute to redistribute the EUQ data among the devices in the group.

*Note:* Any time you enable EUQ in a group, you should redistribute EUQ data.
Step 3: Starting the EUQ Service

To start the EUQ service:

1. Choose Summary from the menu. The Real-time Statistics tab appears.
2. Click the System tab.
3. In the Managed Services table, click Start under EUQ Service.

4. Choose Administration > End-User Quarantine from the menu. The EUQ Management tab appears.
5. Click Redistribute to redistribute the EUQ data among the devices in the group.
6. Choose Summary > System from the menu and verify that the EUQ service is active (or inactive).
Step 4: Enabling End-User Access

Enable end-user access to allow your users to access quarantined spam items that IMSA might have misidentified as spam. The clients use LDAP authentication to access the IMSA EUQ service.

To configure and enable end-user access:

1. Choose Administration > End-User Quarantine from the menu. The EUQ Management tab appears.
2. Click the User Quarantine Access tab.
3. Select Enable access.
4. Select the number of days to keep quarantined spam.
5. Select the maximum number of approved senders per end-user.
6. Type a login page message that appears on your user's browser when he/she starts to access the quarantined email messages.
7. Under Select LDAP groups, select the check box next to Enable all to allow all LDAP group users to access quarantined spam.
8. To add individual LDAP groups, clear the Enable all check box and do either of the following:
   • Search for groups:
     a. From the drop-down list, select Search LDAP groups.
     b. Type the group name.
     c. Click Search. The groups appear in the table below.
     d. Click the LDAP groups to add.
     e. Click >>. The groups appear in the Selected Groups table.
   • Browse existing groups:
     a. From the drop-down list, select Browse LDAP groups. The groups appear in the table below.
     b. Click the LDAP groups to add.
     c. Click >>. The groups appear in the Selected Groups table.
     d. Click Save.
Step 5: Opening the End-User Quarantine Console

You can view the EUQ Web console from the computer where the program was deployed or you can view the EUQ Web console remotely across the network.

To view the console from another computer on the network, go to:

- Primary EUQ service—https://<target server IP address>:8447
- Secondary EUQ service—https://<target server IP address>:8446

**WARNING!** To successfully access all Web consoles on secondary EUQ services, you must synchronize the system time of all EUQ services on your network.

An alternative to using the IP address is to use the target server’s fully qualified domain name (FQDN).

Logon Name Format

The format of the user logon name for accessing the EUQ Web console differs according to the LDAP server type you have selected when configuring LDAP settings. Following are some examples of the logon name format for the three (3) types of supported LDAP servers:

- **Microsoft Active Directory**
  - Without Kerberos—user1@domain.com (UPN) or domain\user1
  - With Kerberos—user1@domain.com
- **Domino**—user1/domain
- **Sun iPlanet Directory**—uid=user1, ou=people, dc=domain, dc=com
Disabling EUQ

Before disabling EUQ, inform your users that they should handle their quarantined spam.

To disable EUQ:

1. To access the EUQ configuration screen, do one of the following:
   • Choose Administration > End-User Quarantine from the menu. The EUQ Management tab appears.
   • Choose Administration > IMSA Configuration > Configuration Wizard from the menu, then go to Step 2: Deployment Settings.
2. Clear the Enable End-User Quarantine check box.
3. To save disk space on each device, you have the option of removing all EUQ data from each device. To do so, click Remove on the EUQ Management tab.
4. Click Save at the EUQ Management tab. If you are using the wizard, progress through the wizard screens and click Finish.
5. Choose Summary from the menu.
6. Click the System tab and verify that the EUQ service is inactive.
Using the Command Line Interface

This chapter explains how to use the command line interface (CLI) to configure IMSA settings and perform other IMSA device related functions.

Topics include:

• Using the CLI on page 6-2
• Entering the CLI on page 6-2
• CLI Overview on page 6-4
• Viewing Device Information and Status on page 6-6
• Configuring Network Settings on page 6-7
• Performing Basic Maintenance on page 6-9
• Entering the Linux-like Shell Environment on page 6-10
• Changing Time and Date Settings on page 6-10
• Enabling and Disabling Web Console and SSH Access on page 6-11
• Shutting Down IMSA on page 6-11
Using the CLI

Use the CLI to do the following:

• Configure initial settings, such as the device IP address and host name
• Restart the device
• Rescue the application
• View device status
• Debug and troubleshoot the device

---

Note: Do not enable scroll lock on your keyboard when using HyperTerminal. If scroll lock is enabled, you cannot enter data.

---

Entering the CLI

To enter the CLI:

1. Connect a computer to one of the following ports:
   • Management—Use the crossover cable provided and connect it to the port labeled MANAGED (also known as the management port). You must have an application that supports SSH communications, such as SecureCRT.

   ---

   Note: Your computer’s IP address must be in the same subnet as the management port’s IP address.

   ---

   • Console—Use the RS232 serial cable provided and connect it to the port labeled CONSOLE. You must have an application that supports serial communications, such as HyperTerminal.

   If you want to connect to IMSA from another computer on your network (not directly connected to the device), you can access the data port.

   If you are accessing the data port for the first time, do the following:

   a. Configure the data port network settings (see Configuring Network Settings on page 6-7).
b. Enable the SSH service (see Enabling and Disabling Web Console and SSH Access on page 6-11).

c. Log on to a computer on your network that can access the device.

2. For an SSH connection, use the following information:
   - IP address (MANAGED port)—192.168.252.1
     IP address (DATA port)—The IP address you configured in the previous step.
   - Port number —22

3. For a HyperTerminal connection, use the following information:
   - Bits per second—115200
   - Data bits—8
   - Parity—None
   - Stop bits—1
   - Flow control—None

4. Enter the logon information.
   - User name—The default user name is root.
   - Password—The default password is imsa7.0.
CLI Overview

After you open the CLI menu, it displays the following:

```
# Interscan Messaging Security Appliance (TMSA) #
# Model: 5000 #
# OS Version: 7.0.0.1112 #
#
Role: parent
NTP: enabled

[Main Menu]
0) Exit
1) Device Information and Status
2) Network Settings
3) Maintenance
4) Utility
5) Shutdown

Notice: [ Ctrl + \ ] can return to the main menu
Select an option (0-5) [0]: 1
```

0) **Exit**—Leaves the CLI.

1) **Device Information and Status**—Monitor hardware items, such as CPU usage, hard disk status, and disk space.

2) **Network Settings**—Modify the device host name, IP address, subnet mask, and the network default gateway address and DNS servers. You can also select the active data port.

3) **Maintenance**—Restarts the device, rescues the application, unregisters from the parent, or re-registers to the parent if the parent IP address was modified.

4) **Utility**—Modifies access to the Web console and SSH access to the Data port. You can also enter the Linux-like shell environment for debugging and modify the device time zone, date, and time.

5) **Shutdown**—Reboots or powers off the device.
CLI Navigation

To navigate the CLI, type the index number of the desired selection and press the Enter key.

To return to the Main Menu from any sub-menu, press the Ctrl and \ keys.

To skip an entry or keep the current value, press the Enter key.

To go back to the top of a menu tree or to exit the CLI from the Main Menu, enter 0.
Viewing Device Information and Status

View device information and status to monitor the performance of the items listed below.

1. Enter the CLI. The Main Menu appears.
2. Enter 1. The Device Information and Status screen appears.

```
[Device Information and Status]
RAID Status: OK
HD1: OK
HD2: OK

Memory Usage: 72.10%
CPU Usage
   CPU 0: 3.26%
   CPU 1: 1.84%
   CPU 2: 1.84%
   CPU 3: 1.84%

Free Disk Space
   MTA Queue Partition: 18180 M
   IM3A Data Partition: 198345 M

Mail Count in MTA Queue
Delivery Queue: 0
Referred Queue: 0
Press <ENTER> to return to Main Menu...
```
### Configuring Network Settings

You can modify device network settings in the CLI or through the Web console. For a list of valid network settings examples and limitations, see *Network Settings Examples and Limitations* on page 6-8.

**To modify network settings:**

1. Enter the CLI. The Main Menu appears.
2. Enter 2. The Network Settings menu appears.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID Status</td>
<td>Shows whether the hard disks are operational. If you swapped in a new hard disk, this field shows the disk build process percentage.</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>The percentage of the RAM memory currently in use.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>The percentage of CPU resources currently in use for both physical CPUs (four logical CPUs).</td>
</tr>
<tr>
<td>Free Disk Space</td>
<td>The amount of free space in MB for the MTA Queue partition and the application data partition.</td>
</tr>
<tr>
<td>Mail Count in MTA Queue</td>
<td>The number of email messages in the delivery queue (waiting to be delivered) and the deferred queue (deferred until further action is taken).</td>
</tr>
</tbody>
</table>
3. To change the host name:
   a. Enter 1. The Change Device Host Name menu appears.
   b. Enter the new host name.

4. To change the other network settings:
   a. Enter 2. The Change Device Network Settings menu appears.
   b. Enter a new IP address, subnet mask, default gateway IP address, and primary and secondary DNS server IP addresses.

5. To choose a different data port:
   a. Enter 3.
   b. Choose data port 1 or data port 2.

Network Settings Examples and Limitations

The following format rules apply to IMSA network settings.

Hostname Format

Use the Fully Qualified Domain Name (FQDN) for the hostname, for example:

hostname.domain_1.com

The host name can contain alphanumeric characters and dashes ("A-Z", "0-9", ")
IP Address Format

IP addresses should be in the format: XXX.XXX.XXX.XXX (where X is a decimal value). The IP address should not be in one of the following formats:

- AXX.XXX.XXX.XXX (A is in the range from 223 to 240) [Multicast Address]
- 0.0.0.0 [Local Hostname]
- 255.255.255.255 [Broadcast Address]
- 127.0.0.1 [Loop back Address]

Subnet Mask Format

The binary format of net mask starts with a sequence of continuous 1’s and ends with a sequence of continuous 0’s.

For example:

- 255.255.255.0—Binary format is 11111111.11111111.11111111.0000 0000
- 255.255.252.0—Binary format is 11111111.11111111.11111100.000 00000

Default Gateway Address Format

Gateway must be in the same subnet with IP address. The combination of the IP address and the subnet mask should not be the broadcast or network address.

Performing Basic Maintenance

If you encounter an error message that requires you to stop and restart the IMSA application services, use the Maintenance screen.

To perform basic device maintenance:

1. Enter the CLI. The Main Menu appears.
2. Enter 3. The Maintenance menu appears.
3. Choose one of the following:
   • **Restart IMSA**—Restarts the IMSA application only, not the device.
   • **Rescue IMSA**—Rescues the application only, not the operating system.
   • **Unregister from parent**—Makes the device a stand-alone, parent device by unregistering it from its previous parent.
   • **Change parent IP address**—Instructs the current (child) device to re-register to the new IP address of its parent device.
   • **Change root password**—Modifies the password you use to log on IMSA as a “root” user.

### Entering the Linux-like Shell Environment

**WARNING!** Enter the shell environment only if your support provider instructs you to perform debugging operations.

To enter the Linux-like shell environment:
1. Enter the CLI. The Main Menu appears.
2. Enter 4. The Utility menu appears.
3. Enter 1 and type y. The Linux-like shell environment interface appears.

### Changing Time and Date Settings

To change time and date settings:
1. Enter the CLI. The Main Menu appears.
2. Enter 4. The Utility menu appears.

```
[Utility]
0) Back to top
1) Enter shell environment
2) Set time zone
3) Set date and time
4) Enable Admin UI access on data port
5) Disable Admin UI access on data port
6) Enable SSH access on data port
7) Disable SSH access on data port
Select an option (0-7) [0]: 4
```

3. Enter 2 for Time Zone settings or 3 for Date settings.
4. Modify the settings as necessary.

## Enabling and Disabling Web Console and SSH Access

To manage IMSA remotely through the data port without being directly connected to the managed port, enable SSH from the CLI.

---

**Note:** By default, SSH access to the data port is disabled. To help retain device access security, Trend Micro recommends keeping SSH access to the data port disabled.

---

**To enable or disable Web console and SSH access:**

1. Enter the CLI. The Main Menu appears.
2. Enter 4. The Utility menu appears.
3. Enter 4, 5, 6, or 7.

## Shutting Down IMSA

To shut down the device safely, use the CLI. Do not merely turn off the power switch.

**To shut down IMSA:**

1. Enter the CLI. The Main Menu appears.
2. Enter 5. The Shutdown menu appears.

3. To restart the device, enter 1.
   To power off the device, enter 2.
Modifying IMSA Deployment

This chapter explains how to perform important maintenance tasks, such as changing the device role (parent to child or child to parent), changing a device IP address, and using the backup data port.

Topics include:

• *Adding and Removing Devices* on page 7-2
• *Changing Device Roles* on page 7-3
• *Changing the Deployment* on page 7-4
• *Changing IP Addresses* on page 7-6
• *Changing the Data Port* on page 7-7
Adding and Removing Devices

This section explains how to add or remove a device from a group.

Adding a Child Device to a Group

To add a child device to a group:

1. Determine the device settings for the new device (IP address, net mask, gateway IP address, DNS server IP address, NTP server IP address if necessary).
2. Follow the instructions in Setting Up a Child Device on page 1-16.

Removing a Child Device from a Group

This section explains how to remove a device from a group. If the device is active, you must first stop all services running on it. If it is inactive, you can unregister it directly.

Note: When you remove a device that has EUQ enabled, all email messages in the EUQ quarantine area are deleted. Trend Micro suggests notifying your users to handle the email messages in the EUQ quarantine area before you remove the device.

To remove a child device from a group:

1. Choose Summary from the menu. The Real-time Statistics tab appears by default.
2. On the top of the screen next to Host, verify that there are no email messages in the delivery queue or deferred queue for the device you want to remove. If there are messages in the delivery queue or deferred queue, wait momentarily for IMSA to process them.
3. Click the System tab. The System Summary appears.
4. Under Managed Services, stop all services on the device you want to remove. When the services stop, the Unregister button appears.
Modifying IMSA Deployment

Note: If the device was using EUQ, redistribute the data across the remaining EUQ databases before you unregister the child device:
   a. Choose Administration > End-User Quarantine.
   b. Click Redistribute.

5. Click Unregister. The child will be automatically removed from the group.

Tip: Trend Micro recommends that you notify your users do not add members to the EUQ approved list while you are adding a child device and redistributing EUQ data.

Resetting Child Devices When the Parent-Child Connection is Broken
If the parent-child connection is broken, you must reset the child devices.

To reset child devices:
1. Connect to the child devices through an SSH connection.
2. Choose 1) Device Information and Status.
3. Verify that there are no email messages in the delivery queue or deferred queue for the device you want to remove. If there are messages in the delivery queue or deferred queue, wait momentarily for IMSA to process them.
4. Return to the main menu and select option 3) Maintenance.
5. Choose 4) Rescue IMSA.

Changing Device Roles
This section explains how to change device roles.
Changing the Device Role from Parent to Child

To change the device role from parent to child:

1. Remove all child devices from the group (see Removing a Child Device from a Group on page 7-2).
2. Register the former parent devices to another parent device (see Setting Up a Child Device on page 1-16).

Changing the Device Role from Child to Parent

To change a device from a child to a parent, simply unregister it from its parent. The device automatically becomes a parent.

To change the device role from child to parent:

1. Unregister the child from the parent by doing one of the following:
   - Use the Web console (see Removing a Child Device from a Group on page 7-2).
   - Use the CLI:
     a. Connect to the child device through an SSH connection.
     b. Choose 3) Maintenance.
     c. Choose 5) Unregister from parent.
2. Register other child devices to this device if necessary.

Changing the Deployment

This section explains how to change the deployment to and from a gateway/non-gateway setup.

Changing the Deployment from Gateway to Non-Gateway

Note: IMSA cannot use IP Filtering in a non-gateway setup.
Modifying IMSA Deployment

To change the deployment from gateway to non-gateway:

1. On the Web console, choose Administration > IMSA Configuration > Configuration Wizard from the menu.
2. Go to Step 2: Deployment Settings.
3. Clear the Gateway deployment check box.
4. Skip the rest of the wizard steps.
5. On the last wizard screen, click Finish.

Changing the Deployment from Non-Gateway to Gateway

Note: IMSA can use IP Filtering in a gateway setup only.

To change the deployment from non-gateway to gateway:

1. On the Web console, choose Administration > IMSA Configuration > Configuration Wizard from the menu.
2. Go to Step 2: Deployment Settings.
3. Select the Gateway deployment check box.
4. Skip the rest of the wizard steps.
5. On the last wizard screen, click Finish.
Changing IP Addresses

This section explains how to change the IP address of parent and child devices.

**Note:** When changing IP addresses in the Command Line Interface (CLI) through Secure Shell (SSH), do not close the SSH client until connection times out. Otherwise, the IP change script may not execute completely, causing inconsistencies in the settings.

### Changing the Parent IP Address

1. Connect to the parent device through an SSH connection and do the following from the CLI:
   b. Change the IP address.
2. Connect to each child device through an SSH connection and do the following:
   b. Enter the updated IP address.

### Changing the Child IP Address

1. On the parent device, do the following from the IMSA Web management console:
   a. Choose Administration > IMSA Configuration > Connections from the menu.
   b. Click the Child IP tab.
   c. Under Add IP Address, add the new IP address.
2. Connect to the child device through an SSH connection and do the following from the CLI:
   b. Change the IP address.
3. On the parent device, do the following:
a. Choose **Administration > IMSA Configuration > Connections** from the menu.

b. Click the **Child IP** tab.

c. Under **Add IP Address**, remove the old child IP address.

**Note:** If you have applied IMSA 7.0 Service Pack 1 (SP1), you are only required to perform step 2 as the parent device will automatically add new child IP addresses and remove old child IP addresses.

### Changing the Data Port

This section explains how to use the secondary data port. You can change the data port by connecting to the Console port using a serial connection, or connecting to the Managed port using an SSH connection. You cannot change the data port via an SSH connection to the data port.

**Note:** The second data port is for cold data port redundancy. You cannot use both data ports simultaneously.

1. Remove the Ethernet cable from the data port and plug it into the other data port.
2. Access the CLI (see *Entering the CLI* on page 6-2).
3. Choose 2) **Network Settings > 3) Select active data port**.
4. Select the data port.
5. To apply the setting, press Enter twice.
6. When you see the question “Did you already switch the Ethernet cable to the other port?” enter y to select yes.
Chapter 8

Updating and Rescuing the System and Application

This chapter explains how to update and rescue the system and application files when Trend Micro releases patches, service packs, and other updates.

Topics include:

- *Updating the System and Application* on page 8-2
- *Rescuing IMSA* on page 8-4
Updating the System and Application

When new operating system and application files become available from Trend Micro, deploy them to a parent IMSA device and all of its child devices. By default, child devices will be updated before the parent device.

Updating devices is a two-step process:

**Step 1:** Upload the file to the IMSA parent device.

**Step 2:** Deploy the file to selected devices.

**To upload a new system or application file:**

1. Choose Administration > Updates > System & Applications from the menu.

2. Under Upload, click Browse and locate the file.

3. Click Upload. After the file finishes uploading, the package type, build number, and title appear under Latest uploaded package.

**To deploy the system or application file:**

1. Select the check boxes next to the devices to which you want to deploy the update.

2. Click Update.

3. Accept the license agreement.
After an operating system update or upgrade, IMSA reboots. An application upgrade might force IMSA to automatically reboot.

4. If IMSA rebooted, wait for it to start up and log on again.

5. Choose Administration > Updates > System and Applications to view the summary screen.

Note:
1. During an update, do not modify any other settings. If you are updating several devices, you can click Cancel to stop the update of the next device.

2. If you have applied some patches on a child device, and later unregister this child device from the parent device, IMSA automatically rescues the system and application files, then re-applies the patches during unregistration. Due to the re-application of the patches, it might take some time before the Web management console for the new parent device (unregistered child device) becomes available.

If a device check box is grayed out, you cannot deploy the files to the device because the device:

• Already has the updated files.
• Has more up-to-date files than the ones you are trying to deploy.
• Is a child device and the patch requires you to upload the files and deploy them to the parent first, or vice versa.

To view update history for any device or to roll back an update:

1. Under Host Name, click the name of the device you want to view. A summary screen appears showing the updates and related log information.

2. To remove an update, click Rollback. You can only roll back the latest application updates.

3. To go back to the main screen, click OK.
Rescuing IMSA

Rescuing IMSA means that you reinstall either of the following items:

- IMSA operating system
- IMSA application

Operating System Rescue Overview

You might need to rescue the operating system if system files become corrupt or if a new version of the operating system is available. Rescuing the operating system re-images the device by overwriting all system files in the device's compressed flash memory with an operating system that you obtain from Trend Micro.

The IMSA operating system file has a `.S` extension. You can obtain all IMSA operating system file from the following locations:

- Trend Micro Web site—www.trendmicro.com/download
- The Solutions CD for IMSA 5000 version 7.0

Rescuing the operating system is not the same as updating the operating system.

- Rescuing—Replaces IMSA operating system kernel, utilities, and all operating system-related files, such as the boot loader.
- Updating—Replaces IMSA operating system kernel files and system utilities with new versions.

Application Rescue Overview

You might need to rescue the application if application files become corrupt. Rescuing the application reinstalls the IMSA application that instructs IMSA to scan traffic, carry out filter actions, and create logs.

IMSA uses the following files to run the application rescue:

- `imsa_app.tar.bz2`
- `install_imsa_app.sh`
- `uninstall_imsa_app.sh`

The application files are located on a data partition on the IMSA hard disk. You do not need to download the files.
Rescuing the application is not the same as applying a patch.

- Rescuing—Replaces all application files and deletes all settings.
- Applying a patch—Updates the existing application files to enhance features.

**WARNING!** All settings you configure through the Web console are deleted when you rescue the application, but not when you rescue the operating system. Before rescuing the application, create a backup of your settings.

## Entering Rescue Mode

Enter rescue mode to upload the new operating system file.

**To enter rescue mode for operating system rescue:**

1. Enter the CLI (see *Using the CLI* on page 6-2).
2. Select 5) **Shutdown** and 1) **Reboot**.
   
   The device restarts. While the device is booting up, a message appears on the device’s LCD display and on the CLI screen prompting you to enter rescue mode.
3. Do one of the following:
   - Press the button on the device.
   - Press `r` on your computer as instructed on the CLI window.

**WARNING!** Do not use the Reset or Power buttons on the back of the device to reboot the device. Doing so might damage the RAID disks.

A `tftp` prompt appears on the CLI of the computer connected to the Console port.

4. Connect a computer to the **Managed** port with the crossover cables. The computer IP address must be in the same subnet as the management port IP address (192.168.252.1). Valid IP addresses fall in the range 192.168.252.2 to 192.168.252.254.

**WARNING!** Do not power off the device while it is in rescue mode.
Rescuing the Operating System

When the rescue process is complete, IMSA automatically reboots. The following system items will be set to the factory defaults:

- Networking settings
- Password
- Time zone
- Interface settings

To rescue the operating system, use the Upload Utility.

**To rescue the operating system with the IMSA upload utility:**

1. Open the Solutions CD for IMSA 5000.
2. On the menu, click **IMSA Upload Utility**.
3. On the bottom of the window, click **Launch**. The utility opens.
4. With the device in rescue mode, click **Launch** at the bottom of the screen.
5. In the screen that appears, click **Browse** and then **Files of type:**.
6. Choose the operating system file:
   
   ![](image1)

   **Note:** If you are changing both hard disks, choose the operating system file
   
   ![](image2)
   
   This file will format the new hard disks and replace all IMSA operating system-related files.

7. Click **Upload** button to upload the image.
   
   After the upload, IMSA begins the operating system rescue. When the rescue is finished, the device will reboot automatically.

Rescuing the Application

**To rescue the application:**

1. Enter the CLI (see Using the CLI on page 6-2).
2. Select 3) Maintenance and 2) Rescue IMSA.
   A confirmation prompt appears.
3. Enter y to confirm that you want to rescue the application. IMSA automatically re-installs the application files located on the hard disk.

Installing a New OS and Application After Changing Hard Disks

If you are changing both hard disks, you must also install the operating system and application through the rescue procedure.

The steps for installing a new operating system are the same as rescuing the operating system (see Rescuing the Operating System on page 8-6).

To install a new operating system and application:

1. Export a backup of your settings on the Administration > Import/Export screen.
2. Power off the device and swap in the new hard disks.
3. Open the Solutions CD for IMSA 5000.
4. On the menu, click IMSA Upload Utility.
5. On the bottom of the window, click Launch.
   The utility opens.
6. With the device in rescue mode, click Launch at the bottom of the screen.
7. In the screen that appears, click Browse and then Files of type:
8. Choose the application file:
   IMSA_sys_rescue.7.0.####.en_US.A
9. Click Upload to upload the image.
10. Re-import the backup of your settings.
Troubleshooting, FAQ, and Support

This chapter explains how to troubleshoot common IMSA issues, search the Trend Micro Knowledge Base, and contact support.

Topics include:

• **Troubleshooting** on page 9-2
• **Frequently Asked Questions** on page 9-10
• **Using the Knowledge Base** on page 9-20
• **Contacting Support** on page 9-20
Troubleshooting

This section provides a list of IMSA troubleshooting utilities and solutions to issues you might encounter. If you have additional problems, check the Trend Micro Knowledge Base:

http://esupport.trendmicro.com

Troubleshooting Utilities

Use the following troubleshooting-related utilities and commands with caution. Trend Micro recommends contacting your support provider before modifying any internal IMSA files.

- Firewall setting check:
  `iptables -nvxL`

- PostgreSQL command line tool:
  `/opt/trend/imss/PostgreSQL/bin/psql -U sa -d imsa`

- `cdt` (password: “trend”)—Collect the following information:
  - Configuration information
  - Logs
  - Core dumps

- Other utilities:
  - `pstack`—shows the callstack of the process, including all threads
  - `ipcs`—lists all IPCs in the current system
  - `gdb`—the debugger
  - `tcpdump`—sniffs network packages
  - `netstat`—lists current network connection

Troubleshooting Issues

Table 9-1 shows common troubleshooting issues you might encounter with the configuration and administration of IMSA. Read through the solutions below. For troubleshooting and FAQ information pertaining to IMSA deployment, refer to the IMSA Deployment Guide.
<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Do any of the following:</td>
</tr>
<tr>
<td>Unable to access IMSA through a serial (RS232) connection to the Console port</td>
<td>• Press &lt;ENTER&gt; twice. If the HyperTerminal is sometimes inactive, if the &lt;ENTER&gt; key has not been pressed.</td>
</tr>
<tr>
<td></td>
<td>• Verify your HyperTerminal settings.</td>
</tr>
<tr>
<td></td>
<td>• Reset the device.</td>
</tr>
<tr>
<td>Unable to access IMSA through an SSH connection to the Data port</td>
<td>Do either of the following:</td>
</tr>
<tr>
<td></td>
<td>• Verify that SSH is enabled on IMSA. By default, SSH access to the Data port is disabled.</td>
</tr>
<tr>
<td></td>
<td>To enable SSH access:</td>
</tr>
<tr>
<td></td>
<td>1. Connect to the device’s Console (serial connection) or Management (SSH connection) port.</td>
</tr>
<tr>
<td></td>
<td>2. Enter your user name and password.</td>
</tr>
<tr>
<td></td>
<td>4. Select (6) Enable SSH access.</td>
</tr>
<tr>
<td></td>
<td>• Verify that the application on your computer is running SSH2, not SSH1. IMSA only supports SSH2.</td>
</tr>
<tr>
<td>Unable to activate products</td>
<td>If a proxy server is on your network, verify your proxy settings.</td>
</tr>
<tr>
<td></td>
<td>To activate NRS, IMSA needs to connect to Trend Micro. This process requires a DNS query. Therefore, if a DNS server is not available or has connection problems, activation will fail. Verify your DNS server settings.</td>
</tr>
<tr>
<td></td>
<td>To verify your DNS settings from the CLI:</td>
</tr>
<tr>
<td></td>
<td>1. Enter the command line interface through a serial or SSH connection.</td>
</tr>
<tr>
<td></td>
<td>2. Select (2) Network Settings.</td>
</tr>
<tr>
<td></td>
<td>3. Select (2) Change network settings.</td>
</tr>
<tr>
<td></td>
<td>4. Modify the IP address of your DNS server if necessary.</td>
</tr>
<tr>
<td></td>
<td>To verify your DNS settings from the Web console:</td>
</tr>
<tr>
<td></td>
<td>2. Modify the IP address of your DNS server if necessary.</td>
</tr>
</tbody>
</table>
Unable to update components

IMSA uses the HTTP protocol to connect to the update source (by default, the Trend Micro ActiveUpdate server). If a firewall is located between IMSA and the Internet and IMSA must use a proxy server, verify that your proxy settings are correct.

**To verify your proxy settings:**

1. On the Web console menu, choose one of the following:
   - Administration > Configuration Wizard > Update Source > Proxy Setting
   - Administration > Update > Components > Source > Proxy Settings
2. Modify the proxy server settings if necessary.

If you update the components manually and Unknown appears under Availability on the Update Now screen, IMSA is unable to connect to the update source.

Verify your network settings and connections and try again.

Email notifications do not display properly

If your computer is running a non-English operating system and the notification message was not written in English, it may appear distorted. Modify the character set through the Web console.

**To modify the character set:**

1. On the Web console menu, choose Administration > Notifications > Delivery Settings.
2. Next to Preferred Charset, select the language in which the messages will be written.

Unable to export configuration files

You will not be able to export configuration files if:

- Your computer is running Windows 2003 SP1 or Windows XP SP2
- Internet Explorer (IE) 6.0 or 7.0 has default security settings

You must change the default security settings on Internet Explorer.

**To change the IE security settings:**

1. On the Internet Explorer menu, choose Tools > Internet Options.
2. Click the Security tab.
3. Click Custom Level.
5. Click OK and save your settings.

---

**TABLE 9.1. Troubleshooting issues**
### Issue | Suggested Resolution
--- | ---
Cannot enable LDAP with Kerberos authentication | Synchronize the date/time for all IMSA devices.

When viewing detailed information for quarantined or archived email, attachment information is sometimes not available | IMSA records attachment information only when the scanning conditions for a policy is set to attachment. This issue occurs under the following circumstances:
1. When there is no attachment in the quarantined or archived email.
2. When attachment is not specified as a scanning condition.
3. Even when you have selected attachment as one of the scanning conditions, this issue will also occur if the number of attachments in the quarantined or archived email has exceeded the maximum number specified in the conditions.

Unable to access the Web console or other components. | The target port is not in the firewall approved list. Open the ports as shown in Table 9-2, “IMSA ports,” on page 9-9 in the firewall. If you are unable to access the Web console, do the following:
1. Start the database process, `dbctl.sh`, before starting the Central Controller process, `S99ADMINUI`.
2. If you are still unable to access the Web console, restart the Central Controller process, `S99ADMINUI`.

No access to the Web console | The Web console URL is not a trusted site in Internet Explorer. Add the URL to the trusted sites.

Cannot query message logs in IMSA. | IMSA scanner records the log with local time. To query message logs, synchronize the date/time for all machines with IMSA.

End-User Quarantine Issues

Unable to access the EUQ Web console | Do the following:
1. Verify that you are using the correct URL and port number.
2. To view the console from another computer on the network, go to `https://<target server IP address>:8447`.

**TABLE 9-1. Troubleshooting issues**
Users are unable to log on to the EUQ Web console  

Do the following:  
1. On the LDAP server, verify that the user accounts are in the correct group. Only user accounts in the approved group can access EUQ.  
2. Verify LDAP and End-User Access settings from the IMSA Web console:  
   - Choose Administration > IMSA Configuration > Connections > LDAP  
   - Verify all the settings, especially the LDAP type and server information  
   - Choose Administration > End-User Quarantine -> User Quarantine Access  
   - Select the Enable access check box  
   - Verify that the correct LDAP groups appear under Selected Groups  
3. Verify that your users are using the correct login name and password.

The EUQ Web digest does not display quarantined email information correctly

Do the following:  
1. Choose Administration > Notifications > Delivery Settings.  
2. Next to Preferred charset, choose the character set that will display the digest information properly.

Some quarantined emails are not appearing on the EUQ Web console

You can only access emails that IMSA identifies as spam or phishing attempts from the EUQ Web console, but not view quarantined emails that violated other rules, such as the antivirus rule.

The IP profiler did not block IP addresses that were just added to the blocked list

Wait for one (1) minute as the changes require about one (1) minute to take effect.

The imssps daemon is running but refusing connections

If the imssps daemon is running, the policy service is working. Check the connection between the policy service and scanner service, then verify your LDAP settings.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users are unable to log on to the EUQ Web console</td>
<td>Do the following:</td>
</tr>
<tr>
<td>The EUQ Web digest does not display quarantined email information</td>
<td>correct information</td>
</tr>
<tr>
<td>Some quarantined emails are not appearing on the EUQ Web console</td>
<td>You can only access emails that IMSA identifies as spam or phishing attempts from</td>
</tr>
<tr>
<td>The IP profiler did not block IP addresses that were just added to</td>
<td>the EUQ Web console, but not view quarantined emails that violated other rules, such</td>
</tr>
<tr>
<td>The imssps daemon is running but refusing connections</td>
<td>as the antivirus rule.</td>
</tr>
</tbody>
</table>

TABLE 9-1. Troubleshooting issues
### Troubleshooting, FAQ, and Support

**IP Filtering Issues**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>FoxProxy cannot start up</td>
<td>There are several reasons why FoxProxy might not start. To find out the reason, view the IP Profiler logs.</td>
</tr>
<tr>
<td></td>
<td><strong>To view IP Profiler logs:</strong></td>
</tr>
<tr>
<td></td>
<td>1. Go to the directory where IP Profiler is installed (by default: /opt/trend).</td>
</tr>
<tr>
<td></td>
<td>2. Open foxproxy.ini.</td>
</tr>
<tr>
<td></td>
<td>3. Change the value for log_level to 4.</td>
</tr>
<tr>
<td></td>
<td>4. Restart FoxProxy by typing the following:</td>
</tr>
<tr>
<td></td>
<td>/opt/trend/ipprofiler/script/foxprofy restart</td>
</tr>
<tr>
<td></td>
<td>5. Open the log file by typing the following:</td>
</tr>
<tr>
<td></td>
<td>/opt/trend/ipprofiler/logs/foxproxy-general.****</td>
</tr>
<tr>
<td>Unable to connect to FoxProxy</td>
<td>Verify that FoxProxy is running and that it is binding on port 25.</td>
</tr>
<tr>
<td>FoxProxy processes email messages slowly</td>
<td>When FoxProxy receives email, it performs a DNS query on FoxDNS. If Bind is not running, FoxProxy continues to wait until the DNS query times out.</td>
</tr>
<tr>
<td></td>
<td><strong>Verify that the bind service is running on the parent device:</strong></td>
</tr>
<tr>
<td></td>
<td>1. Type the following command:</td>
</tr>
<tr>
<td></td>
<td>ps –ef</td>
</tr>
<tr>
<td></td>
<td>2. Start the service if it is not running.</td>
</tr>
<tr>
<td>Unable to view connections that FoxProxy is blocking</td>
<td>Every five (5) minutes, FoxProxy sends information about blocked connections to the IMSA server. Wait for at least five minutes before viewing the connection information.</td>
</tr>
<tr>
<td></td>
<td><strong>To change this time value:</strong></td>
</tr>
<tr>
<td></td>
<td>1. Open foxproxy.ini.</td>
</tr>
<tr>
<td></td>
<td>2. Modify the value for report_send_interval.</td>
</tr>
</tbody>
</table>

**TABLE 9-1. Troubleshooting issues**


No IP Profiler log information exists

Verify that the log files exist:

1. Go to the log directory on the where IMSA is installed (by default: /opt/trend/imss/log/).
2. If the files are not present, use the following command to check if imssmgr is running:
   ```bash
   ps -ef | grep imssmgr
   ```
3. Check if FoxProxy is running:
   ```bash
   ps -ef | grep foxproxy
   ```
4. Verify that IP Profiler is enabled. In table 't_foxhuntersetting', the following should exist:
   ```sql
   record: 'Type' = 1 and 'enable' = TRUE
   ```

NRS does not work after being enabled from the Web console.

NRS may not work due to the following reasons:

- Spam Prevention Solution (SPS) was not activated. NRS shares the same AC code with SPS. If SPS has not been activated, please activate SPS and then activate NRS.
- The computer on which the scanning service is deployed cannot access the Internet. MTA cannot get a response for the DNS query for AC validation. Please confirm that the computer where the scanner service is deployed has access to the Internet.
- Please activate SPS and confirm that the computer with SPS deployed can access the Internet.

Blocked IP address does not display in the Overview page

The Overview page displays the top 10 blocked IP addresses by type for the last 24 complete hours. For example, at 16:12 today the Overview page displays data from 16:00 yesterday to 16:00 today. Please view the Overview page after an hour.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>No IP Profiler log information exists</td>
<td>The following IP Profiler-related log files are in the IMSA admin database: • foxmsg.**** • foxnullmsg.**** • foxreport.**** Verify that the log files exist: 1. Go to the log directory on the where IMSA is installed (by default: /opt/trend/imss/log/). 2. If the files are not present, use the following command to check if imssmgr is running: `ps -ef</td>
</tr>
<tr>
<td>NRS does not work after being enabled from the Web console.</td>
<td>NRS may not work due to the following reasons: • Spam Prevention Solution (SPS) was not activated. NRS shares the same AC code with SPS. If SPS has not been activated, please activate SPS and then activate NRS. • The computer on which the scanning service is deployed cannot access the Internet. MTA cannot get a response for the DNS query for AC validation. Please confirm that the computer where the scanner service is deployed has access to the Internet. Please activate SPS and confirm that the computer with SPS deployed can access the Internet.</td>
</tr>
<tr>
<td>Blocked IP address does not display in the Overview page</td>
<td>The Overview page displays the top 10 blocked IP addresses by type for the last 24 complete hours. For example, at 16:12 today the Overview page displays data from 16:00 yesterday to 16:00 today. Please view the Overview page after an hour.</td>
</tr>
</tbody>
</table>

TABLE 9-1. Troubleshooting issues
Table 9-2 lists the ports that IMSA uses.

<table>
<thead>
<tr>
<th>Port</th>
<th>Services Using the Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5060</td>
<td>Policy service</td>
<td></td>
</tr>
<tr>
<td>15505</td>
<td>IMSA control service</td>
<td>The IMSA Manager.</td>
</tr>
<tr>
<td>53</td>
<td>IP Profiler</td>
<td>IP Profiler uses this port to check whether an IP address should be blocked.</td>
</tr>
<tr>
<td>53 UDP/TCP</td>
<td>IP Profiler</td>
<td></td>
</tr>
<tr>
<td>5432</td>
<td>Database service</td>
<td></td>
</tr>
<tr>
<td>8009</td>
<td>EUQ Internal service</td>
<td></td>
</tr>
<tr>
<td>10024</td>
<td>Scan daemon</td>
<td>Used internally by the scan daemon.</td>
</tr>
<tr>
<td>10025</td>
<td>Scan daemon</td>
<td>Receives mail from MTA.</td>
</tr>
<tr>
<td>10026</td>
<td>MTA</td>
<td>Receives scanned mail from daemon.</td>
</tr>
<tr>
<td></td>
<td>Ports for services that require outside access to the device</td>
<td></td>
</tr>
<tr>
<td>8445</td>
<td>HTTPS</td>
<td>Web console remote access.</td>
</tr>
<tr>
<td>8446, 8447</td>
<td>EUQ</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>POP3</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>SSHD</td>
<td>Secure shell remote access.</td>
</tr>
<tr>
<td></td>
<td>Ports for services that depend on IMSA</td>
<td></td>
</tr>
<tr>
<td>123</td>
<td>NTPD</td>
<td>If network time is enabled, this port must be accessible.</td>
</tr>
<tr>
<td>389</td>
<td>LDAP</td>
<td>If IP Profiler is enabled, access must be available on all devices. Otherwise, only devices running LDAP require access on this port.</td>
</tr>
<tr>
<td></td>
<td>User defined</td>
<td>Web proxy</td>
</tr>
<tr>
<td></td>
<td>User defined</td>
<td>Only the parent device uses this port to access the Trend Micro ActiveUpdate server (for component updates) and the product registration server.</td>
</tr>
<tr>
<td></td>
<td>TMCM console</td>
<td>Access required if TMCM agent is enabled.</td>
</tr>
</tbody>
</table>

**TABLE 9-2. IMSA ports**
Frequently Asked Questions

Postfix MTA Settings

How can I change my MTA settings without using the Web console?

You can modify the IMSA configuration file and add the following key.

1. Open `imss.ini`.
2. Make the following modification:

   ```
   detach_key_postfix=smtpd_use_tls:queue_directory:{Parameter1:{Parameter2}:…::{Parameter n}
   ```

   The parameters above will not be overwritten by any settings that you configure through the Web console. You can modify `main.cf` manually.

   **Note:** “{Parameter1:{Parameter2}:…::{Parameter n}” means you can use one or more parameters by separating them using colons.

   **WARNING!** Use extreme caution when modifying the configuration file.

IP Profiler

How does IP Profiler process email?

IMSA records and calculates each email that has been identified as virus-infected email, spam, DHA attack or bounced email. When an IP address that sends any of these emails matches the criteria specified in the IP filtering rule, the IP address will be blocked temporarily or permanently.

Is the LDAP service mandatory for analyzing whether an incoming traffic is a form of DHA attack?

Technically, LDAP service is a must-have for IMSA. Without LDAP, the IMSA MTA or scanner is unable to detect if the message is sent to an existing recipient or not. The DHA rule only works when LDAP is enabled.
Why is the domain name of an IP address that was added to the blocked/approved list always N/A?

IMSA does not determine the domain name of an IP address that was added to the blocked/approved list. It does, however, resolve the IP address of an added domain name.

Why does the IP Filtering Suspicious IP/Domain screen also display the connection information of blocked IP addresses?

The IP Filtering > Suspicious IP/Domain screen shows all information for successful connections. Therefore, although an IP address is now in the blocked list, the previous connections for this IP address, which have not been blocked, are shown.

Mail Areas and Queues

Can I use special characters to perform queries?

Yes, you can use the following special characters to perform queries:

- **Asterisk (•)** — Used as a wildcard character to search for zero or more characters. You can use asterisk (*) to search for email addresses or file names.

  **To search for email addresses, see the following examples:**
  
  * — Valid representation of all email addresses.
  
  *@domain.tld, name*.*.tld — Valid representation of the whole name or the domain (not the top level domain (TLD)).
  
  *@*.tld — Valid representation of both the name and the domain (not the TLD).

  **To search for file names, see the following examples:**
  
  *.* — Valid representation of all files.
  
  *.extension — Valid representation of all files of a certain extension.
  
  name.* — Valid representation of files with a specific name but of any extension.

- **Semicolon (;)** — Used as a separator when searching for multiple recipients or attachments.
Importing and Exporting

**Will all IMSA 1.0 or IMSS 5.7 settings be retained during migration?**
No. Due to architectural changes in IMSA 7.0, some settings will not be retained. After migration has completed successfully, a report containing the "Migrated Settings" and "Settings Not Migrated" information will be displayed. All settings that are not retained and policies that are not migrated can be found in the "Settings Not Migrated" section.

**What is the mapping relationship between IMSA 1.0 or IMSS 5.7 policies and IMSA 7.0 rules?**
After the migration has completed successfully, a report containing the "Migrated Settings" and "Settings Not Migrated" information will be displayed. The mapping relationship is described in the "Migrated Settings" section.

**How are filters and policies mapped during migration?**
The architectures of IMSA 1.0 or IMSS 5.7 and IMSA 7.0 are very different. Therefore, the migration module maps all IMSA 1.0 or IMSS 5.7 filters to related rules in IMSA 7.0 in the following ways:

- **Virus filter(s)** — There is only one virus rule for both incoming and outgoing traffic directions after migration (regardless of the number of virus filters in IMSS 5.7).
  - The status of virus rules will be "Enable" if one of the virus filters is "active" in IMSS 5.7
  - Otherwise, the status of the virus rule will be "Disable" after migration.

- **SPS filter(s)** — The migration module maps each SPS filter into one SPS rule after migration or several SPS rules depending on the Routes and Filter Actions. There will normally be one SPS rule after migration. The following are exceptions when there will be several SPS rules:
  - **If there are multiple routes with different "To" or "From" addresses.**
    For example: SPS filter with the routes (a->b; c->d; e->b) will be migrated to two SPS rules with the routes (a,e->b; c->d)
  - **If three filter actions are different.**
    For example, SPS filter with the following filter actions will be migrated to two SPS rules named "Spam Filter (SPS) BlackWhiteList"
And Phish->Global Policy" and "Spam Filter (SPS) Spam->Global Policy"

- "Tag and Deliver" for "Blocked senders"
- "Tag and Deliver" for "Phishing emails"
- "Quarantine" for "Spam"

**eManager filter**

- There will be several rules for one eManager filter after migration if there are multiple routes with different "To" or "From" addresses.
  
  For example: eManager filter with the routes (a->b; c->d; e->b) will be migrated to two eManager rules with the routes (a,e->b; c->d)

- There will be two rules for one eManager filter after migration if it was "active" in IMSA 1.0 or IMSS 5.7 for both SMTP and POP3 traffic.

- There will be only one rule for one eManager filter after migration if it is "inactive" in IMSA 1.0 or IMSS 5.7 for both SMTP and POP3 traffic.
  
  The rule direction is for "Both incoming and outgoing directions". You can add the related rule for the POP3 rule direction in IMSA 7.0 if necessary.

**What is the source of internal addresses during migration?**

To retain IMSA 1.0 or IMSS 5.7 internal domains, IMSA 7.0 extracts all domains from the following fields:

- Domains in the "To" field of incoming policy routes
- Domains in the "From" field of outgoing policy routes

**Note:** If there are address groups in the two fields above, all domains in the address group are extracted.

**How do I upgrade multiple IMSA 1.0 devices into a IMSA7.0 group?**

To upgrade from multiple IMSA 1.0 devices:

- Export settings from the IMSA 1.0 device with the desired settings
- Upgrade all IMSA 1.0 devices to IMSA7.0
- Import the settings into one of the IMSA 7.0 parent device
- Register all other IMSA 7.0 devices to that parent device
Is a smooth rollback to IMSA 1.0 possible after upgrade?
Yes, you can rollback to IMSA 1.0 after upgrade by doing one of the following:

**If you want to replace 250GB hard disks with the original IMSA 1.0 80GB hard disks**
- Shutdown the IMSA device and unplug the hard disks from the disk bays
- Rescue IMSA 1.0 .R package
- Rescue IMSA 1.0 .B package
- Shutdown the device and plug the old hard disks into the disk bays
- Enter CLI and configure the system setting

**If you want to keep the hard disks, you should store the IMSA 1.0 application GM build in an ftp server**
- Rescue IMSA 7.0 .G package
- Rescue IMSA 1.0 .R package
- Rescue IMSA 1.0 .B package
- Enter CLI and configure the system setting
- Enter shell, run the command:
  ```bash
  mount /dev/sda6 /mnt/backup
  ```
- Download the IMSA 1.0 application build from the ftp server and save it into the directory `/mnt/backup`, that is, store this application build into `/dev/sda6`
- Return to CLI, enter the Maintenance menu to rescue IMSA application
- Restore IMSA 1.0 application level configurations into the IMSA device.

**End-User Quarantine**
If I installed Exchange Server, and have set multiple mail addresses for each user, how do I enable EUQ to check multiple mail addresses for one user?
If you installed one Exchange Server together with the Active Directory, you can do the following:

a. Open the table `tb_global_setting` in IMSA administrator database and replace the value of `LDAP--->mail_attr` from "mail" to "proxyAddresses".
b. Restart all IMSA services.

What user logon name formats does IMSA support for Active Directory?
Active Directory supports the following logon name formats:

- Example 1: bob@domain.com

  Note: The logon name is not email address (though it appears as one).

- Example 2 (pre-Windows 2000): domain\bob

  Note: The pre-Windows 2000 format is not supported by Kerberos authentication.

If I am using Kerberos, why can't users log into the EUQ console with a short
name: "domain\user_name"?
Kerberos servers cannot accept user names in the format
domain\user_name.

Kerberos requires the format user_name@domain.xxx

How can I speed up my LDAP access if the LDAP server is Active Directory?
There are two methods to speed up your access. The method you use depends on
the port number, which is port 389 or port 3268.

Active Directory uses 3268 for the Global Catalog. LDAP queries that are
directed to the Global Catalog are faster because they do not involve referrals to
different domain controllers.

Tip: Trend Micro recommends using port 3268 for LDAP queries.

Active Directory uses 389 for LDAP queries. If one item cannot be queried in
one domain controller, it uses the LDAP referral mechanism to query another
domain controller. Use port 389 if your company has only one domain or port
3268 is unavailable for use.
To use port 3268 or 389 for LDAP queries:

- Click **Administration > IMSA Configuration > Connections**. The **Connections** screen appears.
- Click the **LDAP** tab.
- Configure the LDAP listening port.
  - To use port 3268, configure the LDAP listening port as 3268.
  - To use port 389, configure the LDAP listening port as 389.

**Transport Layer Security (TLS)**

**What do I have to do to use Transport Layer Security (TLS)?**

Upload the certificate for TLS and enable it on the **Administration > IMSA Configuration > SMTP Routing > Connections** screen. IMSA 7.0 uses the Postfix TLS function. All settings are written to the configuration file **main.cf**. For more information, see **Transport Layer Security** on page C-1.

**Spam Protection Service**

**How is the spam catch rate determined?**

Specify a threshold value between 3.0 and 10.0 for IMSA classification of an email message as spam. A high threshold value means that a message must be very "spam-like" to be classified as spam (this decreases the spam catch rate but reduces the likelihood of false positives). A lower threshold value means that a message only needs to be slightly "spam-like" to be classified as spam (this increases the spam catch rate and may lead to more false positives).
How do I simplify SPS rules after migration?
In order to retain all SPS filter settings for all policies of IMSA 1.0 or IMSS 5.7, IMSA 7.0 migrates each SPS filter to one SPS rule (or several SPS rules depending on the Routes and Filter Actions). If you want to reduce the number of SPS rules after migration, do the following:

- Create a new SPS rule after migration.
- Delete all migrated SPS rules.

ActiveUpdate

How do I roll back a pattern file?
Click the Rollback button on the Summary page.

Others

How does IMSA process a partial email?
IMSA rejects partial email as a malformed message if
BypassMessagePartial=no in the imss.ini file (default setting).

If the key is set to yes, IMSA will bypass the partial mails. Trend Micro does not recommend changing the item "BypassMessagePartial" to yes as this may cause virus leak.

Why can’t newly created administrator accounts access the User Quarantine Access, Admin Accounts and Product License pages?
Only the default IMSA admin account has the permission to access the User Quarantine Access, Admin Accounts and Product License pages. Delegated admin accounts cannot access these pages.

Why are changes to the IMSA configuration settings not effective immediately?
There is a lapse between the time you modify the configuration settings from the Web management console and the time modifications are actually updated on the IMSA server.
Policy settings will be reloaded in no longer than three (3) minutes. If you want the settings to load faster, please modify the
policy_server=>dbChangePollIntervalInSecs setting in the
tb_global_setting table of the IMSA administrator database as desired.
For other general settings, imssmgr will take no longer than one (1) minute to reload the new settings modified from the Web management console.

Trend Micro recommends that you do not send mail to IMSA immediately after modifying the configuration settings from the Web management console.

Is there any limit on the maximum number of the following items?

- Senders and recipients for each rule
- Mail addresses in one address group
- Approved/Block Senders for SPS rule

Technically, there is one limitation on the total size of each rule, which is 640kb. The total size includes the rule route (senders/recipients), rule filter (scanning condition), and rule action. Assuming that each email address/LDAP account consists of 20 characters, IMSA can support at least 10,000 senders/recipients for the rule route.

The maximum number of mail addresses for one address group is 10,000.

The maximum number of Approved/Block Senders for SPS rule is 5000.

Mails from some senders are always received as attachments. The mail body is also replaced by the disclaimer or stamp. Why is that so?

When the charset of the stamp is different from the charset of the mail content, IMSA will encounter issues inserting the stamp into the mail body after scanning the mail. In this situation, IMSA will create a new mail, insert the stamp into the mail body and attach the original message. The mail content, however, will not be changed.

How can I specify a keyword expression to represent a blank header for matching fields such as “from”, “to”, or “subject” when creating rules with content filter?

If you are going to use a regular keyword expression to represent a blank header, Trend Micro recommends that you use “^\s*" (without the quotation marks).

The expression “^\s*" (without the quotation marks) represents a blank header or whitespace characters.

For example, if you want to check if a mail’s “from” header is blank, you can edit a rule’s scanning condition as follows:


b. Click the link for an existing rule to edit the rule.
c. Click **And scanning conditions match**.

d. Click **Header keyword expressions** under the **Content** section.

e. Click **Add** to create a new keyword expression.

f. Add the content as “^ \( \backslash b \) * $” (without the quotation marks).
Using the Knowledge Base

The Trend Micro Knowledge Base, maintained at the Trend Micro Web site, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:

http://esupport.trendmicro.com

The contents of the Knowledge Base are updated continuously, and new solutions are added daily. If you are unable to find an answer, however, you can describe the problem in email and send it directly to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

Contacting Support

Trend Micro provides technical support, virus pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

Trend Micro Incorporated provides worldwide support to all of our registered users. Get a list of the worldwide support offices:

http://www.trendmicro.com/support

Get the latest Trend Micro product documentation:

http://www.trendmicro.com/download

In the United States, you can reach the Trend Micro representatives via phone, fax, or email:

Trend Micro, Inc.
10101 North De Anza Blvd.
Cupertino, CA 95014
Toll free: +1 (800) 228-5651 (sales)
Voice: +1 (408) 257-1500 (main)
Fax: +1 (408) 257-2003
Web address: www.trendmicro.com
Email address: support@trendmicro.com
IMSA Scripts

This appendix provides you with a list of IMSA scripts and their respective parameters that you can invoke from the command line.

Topics include:

• Invoking IMSA Scripts on page A-2
**Invoking IMSA Scripts**

IMSA scripts provide a convenient and alternative means of performing administrative tasks from the command line.

See Table A-1 for a list of the scripts, their respective parameters and the functions they perform.

---

**Note:** All scripts listed in the table are located in `/opt/trend/imss/script`, except `foxproxyd`, which is located in `/opt/trend/imss/ipprofiler/script`.

<table>
<thead>
<tr>
<th>Scripts</th>
<th>Parameters</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>foxproxyd</td>
<td>start / stop / restart</td>
<td>IP Profiler service</td>
</tr>
<tr>
<td>dbctl.sh</td>
<td>start / stop / restart</td>
<td>Postgres database service</td>
</tr>
<tr>
<td>imssctl.sh</td>
<td>start / stop / restart</td>
<td>All IMSA services</td>
</tr>
<tr>
<td>postfixctl.sh</td>
<td>start / stop / reload / restart</td>
<td>Postfix daemon</td>
</tr>
<tr>
<td>regippro.sh</td>
<td>reg / unreg</td>
<td>Register or unregister IP Profiler to or from the admin database.</td>
</tr>
<tr>
<td>S99ADMINUI</td>
<td>start / stop / restart</td>
<td>Central Controller</td>
</tr>
<tr>
<td>S99CLEANEUQ</td>
<td></td>
<td>Removes expired quarantined data from the EUQ databases as configured under the Administration &gt; User Quarantine Access area of the Web management console.</td>
</tr>
<tr>
<td>S99CLEANEXPIRE</td>
<td></td>
<td>Removes expired quarantined and archived data from the EUQ and admin databases as configured under the Quarantine &amp; Archive &gt; Settings area of the Web management console.</td>
</tr>
<tr>
<td>S99CMAGENT</td>
<td>start / stop / restart</td>
<td>CMAgent service</td>
</tr>
<tr>
<td>S99DIGEST</td>
<td></td>
<td>Sends the EUQ digest message</td>
</tr>
<tr>
<td>S99EUQ</td>
<td>start / stop / restart</td>
<td>EUQ service</td>
</tr>
<tr>
<td>S99FOXDNS</td>
<td>start / stop / restart</td>
<td>Foxdns service</td>
</tr>
</tbody>
</table>

**TABLE A-1. IMSA scripts**
<table>
<thead>
<tr>
<th>Scripts</th>
<th>Parameters</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>S99IMSS</td>
<td>start / stop / restart</td>
<td>IMSA scanner service</td>
</tr>
<tr>
<td>S99MANAGER</td>
<td>start / stop / restart</td>
<td>Manager service</td>
</tr>
<tr>
<td>S99MONITOR</td>
<td>start / stop / restart</td>
<td>Manager monitor service</td>
</tr>
<tr>
<td>S99POLICY</td>
<td>start / stop / restart</td>
<td>Policy service</td>
</tr>
<tr>
<td>S99REPORT</td>
<td>[option] start / stop / restart [option]:</td>
<td>Used by S99SCHEDULED to generate related reports.</td>
</tr>
<tr>
<td></td>
<td>-s—generates centralized reports (covers all one-time and scheduled reports configured on the Web management console)</td>
<td>Note: Do not run this script on its own.</td>
</tr>
<tr>
<td></td>
<td>-h—generates hourly individual traffic data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-t—generates hourly traffic data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-d—performs database log maintenance</td>
<td></td>
</tr>
<tr>
<td>S99UPDATE</td>
<td>start / stop</td>
<td>Used by S99SCHEDULED to run the scheduled update.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Do not run this script on its own.</td>
</tr>
<tr>
<td>S99SCHEDULED</td>
<td>start / stop</td>
<td>Starts the scheduled task.</td>
</tr>
<tr>
<td>forceUpdate.sh</td>
<td>DBDSN username password</td>
<td>Notifies the policy server to reload the policy settings</td>
</tr>
<tr>
<td>euqtrans</td>
<td></td>
<td>Transfers EUQ database data</td>
</tr>
</tbody>
</table>

**TABLE A-1. IMSA scripts**
Default Directory Locations

This appendix provides information on the default directory locations that IMSA uses for mail processing.

Topics include:

- Default Mail Queues on page B-2
- eManager, Virus and Program Logs on page B-3
- Temporary Folder on page B-3
- Notification Pickup Folder on page B-3
Default Mail Queues

Table B-1 shows the various mail directories that store the mail messages managed by IMSA.

<table>
<thead>
<tr>
<th>Queues for Regular Mails</th>
<th>Queues for Large Mails</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>queue_malform=/opt/trend/imss/queue/malform</td>
<td></td>
<td>Stores malformed messages.</td>
</tr>
<tr>
<td>queue_archive=/opt/trend/imss/queue/archive</td>
<td></td>
<td>Stores archived messages.</td>
</tr>
<tr>
<td>queue_quarantine=/opt/trend/imss/queue/quarantine</td>
<td></td>
<td>Stores quarantined messages.</td>
</tr>
<tr>
<td>queue_notify=/opt/trend/imss/queue/notify</td>
<td>queue_notify_big=/opt/trend/imss/queue/notifybig</td>
<td>Stores notification messages.</td>
</tr>
<tr>
<td>queue_postpone=/opt/trend/imss/queue/postpone</td>
<td>queue_postpone_big=/opt/trend/imss/queue/postponebig</td>
<td>Stores postponed messages.</td>
</tr>
<tr>
<td>queue_deliver=/opt/trend/imss/queue/deliver</td>
<td>queue_deliver_big=/opt/trend/imss/queue/deliverbig</td>
<td>Stores messages for final delivery.</td>
</tr>
<tr>
<td>queue_reprocess=/opt/trend/imss/queue/reprocess</td>
<td>queue_reprocess_big=/opt/trend/imss/queue/reprocessbig</td>
<td>Stores messages pending reprocessing.</td>
</tr>
<tr>
<td>queue_handoff=/opt/trend/imss/queue/handoff</td>
<td>queue_handoff_big=/opt/trend/imss/queue/handoffbig</td>
<td>Stores messages pending handoff.</td>
</tr>
<tr>
<td>queue_undeliverable=/opt/trend/imss/queue/undeliverable</td>
<td></td>
<td>Stores undeliverable messages.</td>
</tr>
<tr>
<td>queue_unnotify=/opt/trend/imss/queue/unnotify</td>
<td></td>
<td>Stores undeliverable notification messages.</td>
</tr>
<tr>
<td>/var/spool/postfix/incoming</td>
<td></td>
<td>Stores incoming mail from the network, or from the /var/spool/postfix/maildrop directory.</td>
</tr>
</tbody>
</table>

**TABLE B-1.** Default IMSA Mail Locations
eManager, Virus and Program Logs

Many modules in IMSA write log information for troubleshooting purposes to the following folders:

```
/opt/trend/imss/log and
/var/log
```

Temporary Folder

IMSA stores all application-generated temporary files in the following temporary folders:

```
/opt/trend/imss/temp and
/tmp
```

**Note:** This directory is not configurable.

Notification Pickup Folder

IMSA stores all notification messages and picks them up from the following folders, then delivers them to a specified SMTP notification server:

<table>
<thead>
<tr>
<th>Queues for Regular Mails</th>
<th>Queues for Large Mails</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/spool/postfix/active</td>
<td></td>
<td>Stores messages that the queue manager has opened for delivery.</td>
</tr>
<tr>
<td>/var/spool/postfix/deferred</td>
<td></td>
<td>Stores messages that could not be delivered on the first attempt.</td>
</tr>
<tr>
<td>/var/spool/postfix/corrupt</td>
<td></td>
<td>Unreadable or damaged queue files are moved here for inspection.</td>
</tr>
<tr>
<td>/var/spool/postfix/hold</td>
<td></td>
<td>Stores messages that are kept &quot;on hold&quot; until someone releases them.</td>
</tr>
</tbody>
</table>

**TABLE B-1. Default IMSA Mail Locations**
/opt/trend/imss/queue/notify/ and
/opt/trend/imss/queue/notifybig

To configure the SMTP notification server:
Choose Administration > Notifications > Delivery Settings from the menu.

Note: The queue_notify_big queue is for large mail messages.
Transport Layer Security

This appendix provides you with an introduction to Transport Layer Security (TLS), and includes additional information on configuring TLS settings.

Topics include:

• How Transport Layer Security Works on page C-2
• Transport Layer Security Related Terms on page C-2
• Prerequisites to Using Transport Layer Security with IMSA on page C-3
• Configuring Transport Layer Security Settings on page C-4
How Transport Layer Security Works

Transport Layer Security (TLS) provides a secure communication channel between client and server applications over the internet, ensuring the privacy and integrity of the data during transmission.

A client and server establish a TLS connection through a handshaking procedure as described below:

1. The handshake begins when the client requests a secure connection with the server by sending a list of ciphers.
2. The server then selects one cipher presented by the client and replies with its digital certificate that may have been signed by a Certificate Authority (CA).
3. The client verifies the server’s identity with the trusted CA certificate. If the verification fails, the client may choose to stop the TLS handshake.
4. Upon verifying the server’s identity, the client proceeds to generate the session keys by encrypting a message using the server’s public key.
5. This message can only be decrypted using the corresponding private key. The server’s identity is thus authenticated when the server is able to decrypt the message successfully using the private key.
6. The handshake completes and the secure connection is established after the client and server have created the material required for encryption and decryption.

Transport Layer Security Related Terms

- **TLS handshake**—The process by which the client and server applications establish the TLS secure connection.
- **Certificate Authority (CA)**—A CA is an entity that issues digital certificates to applicants after verifying the applicants’ credentials. A CA acts as a trusted third-party and attests that the public key contained in the certificate belongs to the party specified in the certificate.
- **Certificate**—A digital certificate owned by a client or server that is used to verify the client or server’s identity. A valid certificate is signed by a trusted CA that verifies the party specified in the certificate is indeed the owner of the public key contained therein.
- **Public key**—A recipient’s public key used to encrypt a message.
- **Private key**—The only key that can decrypt a message encrypted using the recipient’s public key.

---

**Prerequisites to Using Transport Layer Security with IMSA**

Check the following before you configure a TLS connection in IMSA:

- **Obtain a digital certificate**
  You may obtain a digital certificate through one of the following methods:
  - Generate the certificate and public/private key pairs using some certificate generator or key generator tools, then request a certificate authority to sign the certificate.
  - Apply for the certificate and public/private key pairs from a certificate authority.

- **Ensure that the certificate format is valid**
  - IMSA only supports `.pem` certificate format.
  - Ensure that the signed certificate contains both the private key and certificate information.

- **Upload the certificate**
  - Click **Administration > IMSA Configuration > SMTP Routing** on the menu.
  - Click the **Connections** tab.
  - Under **Transport Layer Security Setting**, click the **Browse** button next to **CA certificate**.
  - Select the signed certificate.
  - Click **Upload**.
Configuring Transport Layer Security Settings

You can enable global Transport Layer Security (TLS) settings for incoming and outgoing messages using the Web management console. When implementing TLS with IMSA acting as the server, you enable incoming TLS, but when implementing TLS with IMSA acting as the client, enable outgoing TLS.

While the Web management console provides a convenient means to enable global TLS settings, it does not provide the option to configure specific TLS settings per site. To configure site-specific TLS settings, refer to the scenario below.

Scenario on Configuring Site-Specific TLS Settings

This example is based on the assumptions that you would like to:

• disable incoming TLS globally
• enforce TLS and set the TLS level to verify for messages received from 192.168.1.1
• disable outgoing TLS globally
• enforce TLS and set the TLS level to verify for messages sent to example.com. It is assumed that you have configured the relay method through domain-based delivery with the next hop set to 192.168.2.2, port 25.
• enforce TLS and set the TLS level to encrypt for messages sent to example1.com (relay by querying DNS server).

To configure site-specific TLS settings for the above scenario, do the following:

1. Edit /opt/trend/imss/config/imss.ini as follows:
   detach_key_postfix=smtpd_use_tls:smtpd_enforce_tls:smtpd_tls_CAfile:smtpd_tls_cert_file:smtpd_tls_key_file:smtp_use_tls

2. Restart imssmgr using the command /opt/trend/imss/script/S99MANAGER restart.

3. Copy the CA certificate file, public key file and private key file to the /opt/trend/imss/postfix/etc/postfix folder.

4. Add the following in /opt/trend/imss/postfix/etc/postfix/main.cf:
   smtpd_tls_security_level = none
   smtpd_tls_CAfile = /opt/trend/imss/postfix/etc/postfix/ca.pem
smtpd_tls_cert_file = 
/opt/trend/imss/postfix/etc/postfix/public.pem
smtpd_tls_key_file = 
/opt/trend/imss/postfix/etc/postfix/private.pem
smtpd_tls_policy_maps = 
hash:/opt/trend/imss/postfix/etc/postfix/smtpd_tls_policy
smtpd_tls_policy:
192.168.1.1 verify
smtp_tls_security_level = none
smtp_tls_CAfile = /opt/trend/imss/postfix/etc/postfix/ca1.key
smtp_tls_cert_file = 
/opt/trend/imss/postfix/etc/postfix/public1.key
smtp_tls_key_file = 
/opt/trend/imss/postfix/etc/postfix/private1.key
smtp_tls_policy_maps = 
hash:/opt/trend/imss/postfix/etc/postfix/smtp_tls_policy
smtp_tls_policy:
[192.168.2.2]:25 verify
example1.com encrypt

5. Create two files smtpd_tls_policy and smtp_tls_policy under the folder
   /opt/trend/imss/postfix/etc/postfix.

   **Content of smtpd_tls_policy:**
   192.168.1.1 verify

   **Content of smtp_tls_policy:**
   [192.168.2.2]:25 verify
   example1.com encrypt

6. Generate the database files using the commands:
   postmap smtpd_tls_policy
   postmap smtp_tls_policy

7. Reload Postfix using the command postfix reload.
Incoming Transport Layer Security Levels

The `smtpd_tls_security_level` parameter controls the global TLS settings for incoming messages. To configure specific incoming TLS settings per site, you need to define the security levels for each site by editing the `smtpd_tls_policy_maps` and `smtpd_tls_policy` parameters in `main.cf`.

Table C-1 lists the incoming TLS security levels in order of increasing security. For more information on each security level, visit http://www.postfix.org/TLS_README.html#server_tls

<table>
<thead>
<tr>
<th>Security Levels</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>No TLS.</td>
</tr>
<tr>
<td>may</td>
<td>Opportunistic TLS.</td>
</tr>
<tr>
<td>encrypt</td>
<td>Mandatory TLS encryption.</td>
</tr>
<tr>
<td>verify</td>
<td>Mandatory TLS verification.</td>
</tr>
</tbody>
</table>

**TABLE C-1. Incoming TLS levels**

Scenario on Configuring Incoming Transport Layer Security Settings

Assuming that you would like to disable TLS globally but apply TLS settings only to specific IP addresses, for example, 10.28.148.1, configure `main.cf` as follows:

```plaintext
smtpd_tls_security_level=none
smtpd_tls_policy_maps=
    hash:/opt/trend/imss/postfix/etc/postfix/smtpd_tls_policy
smtpd_tls_policy:
    10.28.148.1 may
```

Client whose IP address is not in the `smtpd_tls_policy` list will communicate with the Postfix server without TLS.

You can change the security level from 'may' to 'encrypt' or 'verify' if desired.
Outgoing Transport Layer Security Levels

The `smtp_tls_security_level` parameter controls the global TLS settings for outgoing messages. To configure specific outgoing TLS settings per site, you need to define the security levels for each site by editing the `smtp_tls_policy_maps` and `smtp_tls_policy` parameters in `main.cf`.

Table C-2 lists the outgoing TLS security levels in order of increasing security. For more information on each security level, visit http://www.postfix.org/TLS_README.html#client_tls

<table>
<thead>
<tr>
<th>Security Levels</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>No TLS</td>
</tr>
<tr>
<td>may</td>
<td>Opportunistic TLS</td>
</tr>
<tr>
<td>encrypt</td>
<td>Mandatory TLS encryption</td>
</tr>
<tr>
<td>verify</td>
<td>Mandatory TLS verification</td>
</tr>
<tr>
<td>secure</td>
<td>Secure-channel TLS</td>
</tr>
</tbody>
</table>

TABLE C-2. Outgoing TLS levels

Scenario on Configuring Outgoing Transport Layer Security Settings

Assuming that you would like to disable TLS globally but apply TLS settings only to specific outgoing connections, for example, 10.28.148.1, configure `main.cf` as follows:

```plaintext
smtp_tls_security_level=none
smtp_tls_policy_maps=
hash:/opt/trend/imss/postfix/etc/postfix/smtp_tls_policy
smtp_tls_policy:
[10.28.148.1]:25 may
```

Server whose ip is not in the `smtp_tls_policy` list will communicate with Postfix client without TLS.

You can change the security level from 'may' to 'encrypt' or 'verify' if desired.
Index

A
address groups
  examples of 2-23
APOP 2-19
application
  rescuing 8-6
audience viii

B
backup IMSA settings 3-1

C
command line interface
  accessing 6-2
  configuring network settings 6-7
  enabling and disabling Web access and SSH 6-11
  entering the shell environment 6-10
  navigation 6-5
  network information and status 6-6
  overview 6-4
  shutting down the device 6-11
  using 6-2
commands A-2
connections 2-12
contact support 9-20

D
device
  rescuing 8-4
    application 8-6
    entering rescue mode 8-5
    operating system 8-6
    restarting services 6-10
    shutting down 6-11
Documentation viii
domain-based delivery 2-15

E
EUQ
  Web console 5-10

F
FAQ
  EUQ 9-14
  IP Profiler 9-10
  postfix 9-10
filters
  examples of 2-23

H
Hardware Maintenance Sheet viii
hostname formats 6-8

I
IMSA ports 9-9

K
Knowledge Base 9-20

M
maintenance 4-1
MTA
  with NRS 2-3

N
network information and status 6-6
network settings 6-7-6-8
NRS
  Activation Code 2-2
  Administration Console 2-4
  MTA settings 2-3
  using 2-2

O
Online Help viii
operating system
rescuing 8-6

P
permitted senders 2-15

Q
Quick Start Guide viii

R
Readme File viii
remote device management 6-11
rescue mode 8-4-8-5
rescuing the application 8-6
rescuing the device 8-4-8-5
rescuing the operating system 8-6
restarting
IMSA services 6-10

S
scanning conditions 2-34
shell environment 6-10
shutting down 6-11

SMTP routing 2-11
Spam Prevention Solution (SPS)
  Activation Code 2-2
SSH access 6-11
SSL
  viewing console using SSL 1-3
SSL certificate 1-3
support 9-20

T
third-party license agreements viii
time and date settings 6-10
transport layer 2-13
Trend Micro Knowledge Base 9-20
troubleshooting 9-2
  IP Filtering 9-7

W
Web access 6-11
Works C-2