Legal Notice

Copyright © 2018 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our website at the following URL:

support.symantec.com

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

support.symantec.com

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
■ Operating system
■ Version and patch level
■ Network topology
■ Router, gateway, and IP address information
■ Problem description:
  ■ Error messages and log files
  ■ Troubleshooting that was performed before contacting Symantec
  ■ Recent software configuration changes and network changes

**Licensing and registration**

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:


**Customer service**

Customer service information is available at the following URL:


Customer Service is available to assist with non-technical questions, such as the following types of issues:

■ Questions regarding product licensing or serialization
■ Product registration updates, such as address or name changes
■ General product information (features, language availability, local dealers)
■ Latest information about product updates and upgrades
■ Information about upgrade assurance and support contracts
■ Information about the Symantec Buying Programs
■ Advice about Symantec's technical support options
■ Nontechnical presales questions
■ Issues that are related to CD-ROMs, DVDs, or manuals
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan  
customercare@symantec.com
Europe, Middle-East, and Africa  
semea@symantec.com
North America and Latin America  
supportsolutions@symantec.com
<table>
<thead>
<tr>
<th>Chapter 3</th>
<th>Activating licenses</th>
<th>53</th>
</tr>
</thead>
<tbody>
<tr>
<td>About licensing</td>
<td>53</td>
<td></td>
</tr>
<tr>
<td>About activating the Mail Security license</td>
<td>54</td>
<td></td>
</tr>
<tr>
<td>About the Mail Security license serial number</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>Obtaining a license file</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>Installing license files</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>About renewing the Mail Security license</td>
<td>57</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Managing your Exchange servers</th>
<th>59</th>
</tr>
</thead>
<tbody>
<tr>
<td>About managing your Exchange servers</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>Deploying settings and changes to a server or group</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>Managing servers and server groups</td>
<td>62</td>
<td></td>
</tr>
<tr>
<td>Logging onto servers</td>
<td>63</td>
<td></td>
</tr>
<tr>
<td>Configuring Symantec Mail Security for Exchange on DAG setup</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>Changing the password of the domain user account</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>Changing the service account used by Mail Security service</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>Modifying or viewing server or server group settings</td>
<td>66</td>
<td></td>
</tr>
<tr>
<td>Viewing the status of a server</td>
<td>67</td>
<td></td>
</tr>
<tr>
<td>Creating a user-defined server group</td>
<td>67</td>
<td></td>
</tr>
<tr>
<td>Adding servers to a group</td>
<td>68</td>
<td></td>
</tr>
<tr>
<td>Moving a server to another user-defined server group</td>
<td>69</td>
<td></td>
</tr>
<tr>
<td>Synchronizing group settings to a server</td>
<td>70</td>
<td></td>
</tr>
<tr>
<td>Restoring default settings to a server or group</td>
<td>70</td>
<td></td>
</tr>
<tr>
<td>Removing a server from group management</td>
<td>71</td>
<td></td>
</tr>
<tr>
<td>Removing a server group</td>
<td>71</td>
<td></td>
</tr>
<tr>
<td>Exporting and importing settings</td>
<td>72</td>
<td></td>
</tr>
<tr>
<td>Modifying the port and the communication properties of a server</td>
<td>73</td>
<td></td>
</tr>
<tr>
<td>Creating and assigning a custom throttling policy to the Mail Security service account user</td>
<td>73</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Quarantining messages and attachments</th>
<th>75</th>
</tr>
</thead>
<tbody>
<tr>
<td>About the quarantine</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>Forwarding quarantined items to the Quarantine Server</td>
<td>76</td>
<td></td>
</tr>
<tr>
<td>Establishing local quarantine thresholds</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>Viewing the contents of the local quarantine</td>
<td>78</td>
<td></td>
</tr>
<tr>
<td>Filtering the quarantined items</td>
<td>79</td>
<td></td>
</tr>
<tr>
<td>Specifying an action to take when a quarantine threshold is met</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>About releasing messages from the local quarantine</td>
<td>81</td>
<td></td>
</tr>
<tr>
<td>Releasing messages from the local quarantine by email</td>
<td>82</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 6  Protecting your server from risks ................................. 85
About Mail Security policies .................................................. 86
About protecting your server from risks ................................. 86
  How Mail Security detects risks ........................................... 87
Configuring a threat detection ............................................. 88
Configuring a security risk detection ..................................... 91
Configuring file scanning limits .......................................... 94
Configuring rules to address unscannable and encrypted files ... 95
Remediation overview ......................................................... 97
How remediation works ..................................................... 98
Configuring remediation options ......................................... 99
Types of Remediation .......................................................... 99
Remediation feed settings ................................................... 99
Creating an email remediation feed ................................. 100
Enabling authentication key ............................................... 102
Managing certificates ......................................................... 102
About file reputation .......................................................... 103

Chapter 7  Identifying spam ..................................................... 104
About spam detection ......................................................... 104
About reputation technology ............................................... 105
Configuring whitelists .......................................................... 105
How to detect spam using Symantec Premium AntiSpam .......... 106
  About registering Symantec Premium AntiSpam through an ISA
erver  .............................................................................. 106
  Configuring your proxy server to download spam definition
definition updates .............................................................. 107
  Configuring Symantec Premium AntiSpam to detect spam ...... 107
  Processing suspected spam messages .............................. 110
  Processing the suspected spam messages that exceed an SCL
  threshold ................................................................. 113
  Processing spam messages ........................................... 115
  About applying X-headers to messages for archiving .......... 118

Chapter 8  Filtering content ..................................................... 120
About content and file filtering ........................................... 120
  About file type filtering .................................................. 122
  About default content filtering rules ............................... 125
Introducing Symantec Mail Security for Microsoft Exchange

This chapter includes the following topics:

- About Symantec Mail Security for Microsoft Exchange
- What's new in Mail Security
- Components of Mail Security
- How Mail Security works
- What you can do with Mail Security
- Where to get more information about Mail Security

About Symantec Mail Security for Microsoft Exchange

Symantec™ Mail Security for Microsoft® Exchange (Mail Security) provides a complete, customizable, and scalable solution that scans the emails that transit or reside on the Microsoft Exchange Server.

Mail Security protects your Exchange server from the following:

- Threats (such as viruses, Trojan horses, worms, and denial-of-service attacks)
- Security risks (such as adware and spyware)
- Unwanted content
- Unwanted file attachments
Unsolicited email messages (spam)

Mail Security also lets you manage the protection of one or more Exchange servers from a single console.

The Exchange environment is only one avenue by which a threat or a security risk can penetrate a network. For complete protection, ensure that you protect every computer and workstation by an antivirus solution.

What's new in Mail Security

Table 1-1 lists the new and the enhanced features in Mail Security.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consolidated detailed reporting for server</td>
<td>Now, generate the consolidated detailed report for all the servers in the server group.</td>
</tr>
<tr>
<td>group</td>
<td>See “Managing reports” on page 219.</td>
</tr>
<tr>
<td>Quarantine search</td>
<td>User predefined filters to search the quarantined items for server and the server group.</td>
</tr>
<tr>
<td></td>
<td>See “Filtering the quarantined items” on page 79.</td>
</tr>
<tr>
<td>Remediation</td>
<td>Remediation feature lets you auto-remediate threats inside your mailboxes based on the email feeds.</td>
</tr>
<tr>
<td></td>
<td>See “How remediation works” on page 98.</td>
</tr>
</tbody>
</table>

Components of Mail Security

**Symantec Mail Security for Microsoft Exchange**

This software protects your Exchange servers from threats (such as viruses and denial-of-service attacks) and security risks (such as adware and spyware). It also detects spam email messages and unwanted email attachments.

**Location in the installation package:**

\SMSMSE\Install\LiveUpdate™ Administration Utility

This utility lets you configure one or more intranet FTP, HTTP, or LAN servers to act as internal LiveUpdate servers. LiveUpdate lets Symantec products download program and definition file updates directly from Symantec or from a LiveUpdate server.
For more information, see the LiveUpdate Administrator documentation on the Mail Security installation package in the following location:


**Symantec Central Quarantine**

This utility lets Mail Security forward infected messages and the messages that contain certain types of violations from the local quarantine to the Central Quarantine. This utility acts as a central repository.

For more information, see the *Symantec Central Quarantine Administrator's Guide* on the Mail Security installation package at the following location:

\DOCS\DIS\CentQuar.pdf

**Location in the installation package:** \ADMTOOLS\DIS

**Mail Security for Microsoft Exchange Management Pack**

This component lets you integrate Symantec Mail Security for Microsoft Exchange events with Microsoft System Center Operations Manager (SCOM) 2007 R2/2012.

Preconfigured Computer Groups, Rule Groups/Rules, and Providers are automatically created when you import the management pack. These rules monitor specific Symantec Mail Security for Microsoft Exchange events in the Windows Event Log and the Windows Performance Monitor.

For more information, see the *Symantec Mail Security for Microsoft Exchange Management Pack*.

**Location in the installation package:** \ADMTOOLS\Mgmt_Pack

# How Mail Security works

Mail Security can scan messages and their attachments to detect the following:

- **Risks**
  - Risks are comprised of threats and security risks
    - **Threats**
      - Threats include viruses, worms, and Trojan horses
      - See “Configuring a threat detection” on page 88.
    - **Security risks**
      - Security risks include adware, spyware, and malware
      - See “Configuring a security risk detection” on page 91.
  - See “About spam detection” on page 104.
Email attachment violations
See “About file type filtering” on page 122.
See “Blocking attachments by file name” on page 150.

Content filtering rule violations
See “About content and file filtering” on page 120.

Mail Security takes the actions that you specify in the respective policies when a violation is detected.
See “About Mail Security policies” on page 86.

Mail Security contains a decomposer that extracts container files so that they can be scanned. The decomposer continues to extract container files until it reaches the base file or until it reaches its extraction limit. If the decomposer reaches the set limit before the base file is reached, the scanning process stops. Mail Security then logs the violation to the specified logging destinations, and the file is handled according to Unscannable File Rule.
See “Configuring rules to address unscannable and encrypted files” on page 95.

What you can do with Mail Security

Table 1-2 lists the tasks that you can perform with Mail Security.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Manage your Exchange environment by using policies | You can configure Mail Security for Microsoft Exchange to scan email messages and their attachments for threats such as viruses, Trojan horses, adware, spyware, and spam. You can define policies to detect potential risks to your Microsoft Exchange email system and process email messages and attachments that contain threats.  
  See “About Mail Security policies” on page 86. |
| Scan your Exchange server for risks and violations | You can keep your server protected by performing any of the following types of scans:  
  - Auto-Protect scans  
  - Manual scans  
  - Scheduled scans  
  - Background scans (for Exchange Server 2010 only)  
  See “About the types of scanning that you can perform” on page 169. |
### Table 1-2 What you can do with Mail Security (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Protect against threats       | Symantec engineers track reported outbreaks of threats (such as viruses, Trojan horses, and worms) to identify new risks. After a threat is identified, information about the threat (a signature) is stored in a definition file. This file contains information to detect and eliminate the threat. When Mail Security scans for threats, it searches for these signatures. Definition files are downloaded using LiveUpdate or Rapid Release.  
See “About keeping your server protected” on page 230.  
Mail Security also uses Symantec Bloodhound heuristics technology to scan for threats for which no known definitions exist. Bloodhound heuristics technology scans for unusual behaviors such as self-replication to target potentially infected message bodies and attachments.  
See “Configuring a threat detection” on page 88. |
| Keep your protection up-to-date | Mail Security relies on up-to-date information to detect and eliminate risks. One of the most common reasons computers are vulnerable to attacks is that definition files are out-of-date. Symantec regularly supplies updated definition files.  
Using LiveUpdate, Mail Security connects to a Symantec server over the Internet and automatically determines if definitions need to be updated. If they do, the definition files are downloaded to the proper location and installed. If you need a quicker response for emerging threats, you can enable Rapid Release to get the most current definitions that are available.  
See “About keeping your server protected” on page 230.  
See “About using Mail Security with other antivirus products” on page 49.  
**Note:** You must have a valid license to update definitions.  
See “About licensing” on page 53. |
| Identify spam email           | Spam is unsolicited bulk email, which most often advertises messages for a product or service. It wastes productivity, time, and network bandwidth. Symantec Premium AntiSpam provides continuous updates to the premium antispam filters to ensures that your Exchange server has the most current spam detection filters.  
See “How to detect spam using Symantec Premium AntiSpam” on page 106.  
See “Configuring whitelists” on page 105.  
You must have a valid Symantec Premium AntiSpam license to enable Symantec Premium AntiSpam.  
See “About licensing” on page 53. |
### Table 1-2 What you can do with Mail Security (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter undesirable message content and attachments</td>
<td>Mail Security lets you create the filtering rules that you can use to filter email messages and attachments. Mail Security provides the predefined file name and file type filtering rules that you can use to enforce email attachment policies. Mail Security uses match lists to filter email messages and attachments for specific words, terms, and phrases. Mail Security also provides the predefined content filtering policy templates that help prevent data leakage. See “About content and file filtering” on page 120.</td>
</tr>
<tr>
<td>Apply X-headers to messages for archiving</td>
<td>Mail Security provides default X-headers that you can apply to the email messages that contain filtering rule violations or are spam or suspected spam. You can modify the default X-headers, or you can create your own. See “About applying X-headers to messages for archiving” on page 118.</td>
</tr>
</tbody>
</table>
| Manage outbreaks                          | An outbreak occurs when the number of threats to the Microsoft Exchange system that are detected over a period of time exceeds a specified limit. Mail Security lets you manage outbreaks quickly and effectively by setting outbreak rules and sending notifications when an outbreak is detected. You can also select an action to take when an outbreak is detected, such as the following:  
  - Delete the entire message.  
  - Delete the attachment or the message body.  
  - Quarantine entire message and replace with text.  
  - Quarantine the attachment or the message body.  
  - Log the event.  
  - Add Tag to the beginning of the subject line.  
You can set rules to define an outbreak based on event. For example, the same threat occurs a specified number of times within a specified time period. You can also configure Mail Security to send notifications and alerts in the case of an outbreak. See “About outbreak management” on page 193. |
Table 1-2 What you can do with Mail Security *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Quarantine infected message bodies and attachments | Mail Security for Microsoft Exchange includes a local quarantine that can store the infected message bodies and attachments that are detected during scans. You can configure Mail Security to quarantine threats and security risks, and file filtering violations in the local quarantine.  
  
  The quarantined items that contain threats can be forwarded to the Symantec Central Quarantine, if it is installed. The Symantec Central Quarantine program is available on the Mail Security installation package.  
  
  You can quarantine the entire message or by parts.  
  
  See “About the quarantine” on page 75. |
| Monitor Mail Security events       | Mail Security logs events to the Windows Application event log. You can view the events that are logged to the Windows Application event log from the console.  
  
  See “Viewing the Mail Security Event log” on page 204.  
  
  Mail Security logs extensive report data on threats, security risks, violations, spam, and server information to the reports database. You can use this data to generate summary or detailed reports based on different subsets of the data.  
  
  See “About logging events” on page 203.  
  
  See “Creating or modifying a Summary report template” on page 210.  
  
  See “Creating or modifying a Detailed report template” on page 215. |
| Generate reports                  | Mail Security collects scan data from your Exchange servers and generates reports.  
  
  Mail Security provides the preconfigured report templates that you can modify. You can also create your own report templates.  
  
  You can create the following types of report templates:  
  
  - Summary  
  - Detailed  
  
  See “About generating reports” on page 208. |
Table 1-2

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Send notifications when a threat or violation is detected            | Mail Security provides several options for notifying administrators, internal senders, and email recipients of threats and violations.  
Mail Security lets you define the conditions in which to send an alert. You can also customize the alert message text for each alert condition that you define.  
See "Configuring rules to address unscannable and encrypted files" on page 95.  
See "Configuring a threat detection" on page 88.  
See "Configuring notification settings for scan violations" on page 192. |
| Manage single and multiple Exchange servers                          | Mail Security can protect one or more Exchange servers. If your organization has multiple Exchange servers, you can manage all the servers from the same console that you use to manage a single server.  
By switching between the server view and group view, you can manage the following:  
■ Configuration settings for individual servers  
■ All servers in a specific location  
See "About managing your Exchange servers" on page 59. |
Provides the access to the Threat Explorer, which contains information about all known threats

www.symantec.com/enterprise/security_response/threatexplorer/azlisting.jsp
Installing Symantec Mail Security for Microsoft Exchange

This chapter includes the following topics:

- Before you install
- System requirements
- Installing Symantec Mail Security for Microsoft Exchange
- Post-installation tasks
- Uninstalling Symantec Mail Security for Microsoft Exchange

Before you install

Ensure that you meet all system requirements before you install Mail Security. Select the installation plan that best matches your organization's needs, and ensure that you have met the preinstallation requirements.

See “System requirements” on page 29.

See “Installing Symantec Mail Security for Microsoft Exchange” on page 32.

See "Uninstalling Symantec Mail Security for Microsoft Exchange" on page 52.
Note: Symantec Mail Security for Microsoft Exchange console only connects to the server of the same version.

You must uninstall and reinstall the product if you change the server role on which Mail Security is installed.

Do the following before you install the product:

- If you use the optional email tools feature of Symantec Endpoint Protection or Symantec AntiVirus Corporate Edition, you must uninstall the feature before you install Mail Security. These email tools are not compatible with Mail Security or Microsoft Exchange.
- If you have any antivirus software installed on the server, you must disable it before you install Mail Security.
  After installation but before you turn on the antivirus protection, configure your other antivirus programs to exclude certain folders from scanning.
- If you have any malware agent installed on the server (Exchange Server 2013/2016) on which you want to install Mail Security, you must disable it.

Note: The Mail Security installer disables the Microsoft Exchange malware agent during installation. If the installer fails to disable the malware agent, then make sure that you disable it manually after the installation. Mail Security may not function properly if any other malware agent is enabled. Therefore, make sure that you disable the malware agent before you use Mail Security.

- Log on as a Windows domain administrator to install Mail Security components correctly.
- Modify your screen resolution to a minimum of 1024 x 768. Mail Security does not support a resolution less than 1024 x 768.
- Configure the default receive connector for the Exchange Hub Transport server to permit connections from anonymous users.

While installing Symantec Mail Security on Exchange mailbox role, the installer needs a domain user account for installing Mail Security services. This domain account is used as a service account for running Mail Security services. Before running the installer, you must create a domain user account that fulfills following criteria.

- The domain account must have a mailbox.
- The domain account must not be member of domain administrator’s group.
- The user (domain account) must be a member of Organization Management group under the Microsoft Exchange Security Groups Organizational Unit.
By default, **Organization Management** group is a member of the local **Administrators** group on all the exchange servers in the organization. If not, then add the user to the local **Administrators** group.

You may use different user account for installations of Mail Security on other Exchange mailbox servers within that domain for better performance.

When the user updates the password, the same password must be provided to the Mail Security Service on all Exchange mailbox role servers.

---

**Note:** While installing Mail Security on local Exchange Mailbox server, in the **Logon Information** screen, specify the domain user credentials in the **User name** and **Password** fields. Mail Security provides this user account **Application Impersonation** and **Logon as service** rights.

Ensure that the following IIS Role Service components are installed when you install Mail Security on Windows Server 2008 for Exchange servers. This installation is applicable for both remote installation and local installation.

- Application Development - ASP.NET
- Security - Windows Authentication, Basic Authentication, Digest Authentication
- Management Tools - IIS management console, IIS 6 Scripting Tools

### Software component locations

**Table 2-1** lists the default locations in which Mail Security installs software components.

<table>
<thead>
<tr>
<th>Component</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Security program files</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server</td>
</tr>
</tbody>
</table>

---

Installing Symantec Mail Security for Microsoft Exchange

**Before you install**
<table>
<thead>
<tr>
<th>Component</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantined items in encrypted format</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server \Quarantine</td>
</tr>
<tr>
<td><strong>Note:</strong> Configure all antivirus file system scanners to exclude the quarantine directory from scanning. The system scanners might try to scan and delete the Mail Security files that are placed in the quarantine directory.</td>
<td></td>
</tr>
<tr>
<td>Reporting data</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server \Reports</td>
</tr>
<tr>
<td>Data files for the reports that are generated</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server \Reports&lt;report name&gt;</td>
</tr>
<tr>
<td>Report templates</td>
<td>C:\Program Files\Symantec\SMSMSE\7.0\Server \Reports\Templates</td>
</tr>
<tr>
<td>Match list files</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server \MatchLists</td>
</tr>
<tr>
<td>Allowed senders files and Symantec Premium AntiSpam configuration files</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server \SpamPrevention</td>
</tr>
<tr>
<td>Component</td>
<td>Location</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Location where Mail Security scans items</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server \Temp</td>
</tr>
<tr>
<td><strong>Note:</strong> Configure all antivirus products that scan files to exclude the Temp directory from scanning. The system scanners might try to scan and delete the Mail Security files that are placed in the Temp directory during the scanning process.</td>
<td></td>
</tr>
<tr>
<td>Dynamic-link libraries for Symantec Premium AntiSpam</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server \bin</td>
</tr>
<tr>
<td>Manual and scheduled scan mailbox configuration data</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server \Config</td>
</tr>
<tr>
<td>Configuration files for allowed and blocked senders for Symantec Premium AntiSpam</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server \etc</td>
</tr>
</tbody>
</table>
### About security and access permissions

Mail Security automatically creates the following user groups and assigns them access when you install the product:

---

**Table 2-1  Software component locations (continued)**

<table>
<thead>
<tr>
<th>Component</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component logs for Symantec Premium AntiSpam</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server \logs</td>
</tr>
<tr>
<td>Statistical information on the effectiveness of Symantec Premium AntiSpam rules</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server \stats</td>
</tr>
<tr>
<td>Console files</td>
<td>C:\Program Files\Symantec\CMaF\2.3</td>
</tr>
<tr>
<td>Definitions</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server\definitions\AntiVirus\</td>
</tr>
<tr>
<td>License files</td>
<td>C:\ProgramData\Symantec Shared\Licenses</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\Common Files\Symantec Shared\Licenses</td>
</tr>
<tr>
<td>Verity content extraction component</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server\Verity\bin</td>
</tr>
<tr>
<td>Mail Security Web service components</td>
<td>C:\Program Files\Symantec\CMaF\2.3\bin</td>
</tr>
<tr>
<td>Filtering rules</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server \Policies</td>
</tr>
<tr>
<td>Scan job configuration</td>
<td>C:\Program Files\Symantec\SMSMSE\7.9\Server \ScanJobs</td>
</tr>
</tbody>
</table>

See "Before you install" on page 22.

---
SMSMSE Admins

Permits read and write access to all Mail Security components and features.

Users in this group can change settings for Mail Security through the console.

The user who installs Mail Security is automatically added to the SMSMSE Admins group.

SMSMSE Viewers

Permits the read-only access to Mail Security components and features.

Users in this group cannot change settings for Mail Security. Users can view reports, event logs, and settings through console-only installations.

See “Installing the Mail Security console” on page 37.

The user groups are domain-wide for Active Directory. You can use the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in to change membership in the groups.

Users must be designated in one of the SMSMSE user groups to access the product. For example, administrators who are not in one of the SMSMSE user groups are not granted access to Mail Security. Adding a user to the SMSMSE Admins group does not automatically grant the user Windows Local Administrator, Windows Domain Administrator, or Exchange administrator rights.

Security is also set for the Mail Security registry key and file folders during the security set-up process. You must have administrator access to the local servers and domain administrator rights for the security set-up to proceed.

Reducing Mail Security installation time

If you do not have Internet connection on your system, then installing Mail Security may take a long time to complete. Verification of certificate revocation list (CRL) is performed for every digitally signed binary which gets installed using its digital certificate. When Mail Security is not connected to the Internet, each CRL request may timeout before the installation can continue and increases the installation time.

For more information see: http://www.symantec.com/business/support/index?page=content&id=TECH168751

To reduce Mail Security installation time

1. Start Internet Explorer.
2. On the Tools menu, click Internet Options.
3. Click the Advanced tab, and then locate the Security section.
4. Uncheck Check for publisher’s certificate revocation and then click OK.
5. After the installation is complete, check Check for publisher’s certificate revocation.

Note: The Check for publisher's certificate revocation option is set on a per-account basis.

See “Before you install” on page 22.
See “Installing Symantec Mail Security for Microsoft Exchange” on page 32.

System requirements

Ensure that you meet the appropriate system requirements for the type of installation that you want to perform.

See “Before you install” on page 22.
See “Server system requirements” on page 29.
See “Console system requirements” on page 30.
See “Port requirements” on page 31.

Mail Security supports various platforms of Microsoft Small Business Server. For the support matrix information, go to the following article:
http://www.symantec.com/business/support/index?page=content&id=TECH97861

Server system requirements

You must have domain administrator-level privileges to install Mail Security.

The server system requirements are as follows:

Exchange platform
- Exchange Server 2010 (Mailbox, Transport, Edge Role)
- Exchange Server 2013 (Mailbox, Edge Role)
- Exchange Server 2016 (Mailbox, Edge Role)
Minimum system requirements

- 2 GB of memory for Mail Security besides the minimum requirements for the operating system and Exchange. Approximately 4GB or more of memory is required.
- 4 GB disk space is required for Mail Security. This space does not include the disk space that is required for items such as quarantined messages and attachments, reports, and log data.
- Supported version of .NET Framework version is 3.5
- MDAC 2.8 or higher
- DirectX 9 or higher
- Microsoft Internet Information Services (IIS) Manager
- Microsoft .NET Framework 3.5 and Microsoft Windows PowerShell 2.0

Ensure that the components .NET Framework, MDAC, and DirectX are installed before you install Mail Security.

Adobe Acrobat Reader is not a requirement to install and run Mail Security. However, it is required to view the reports that are generated in .pdf format. You can download Adobe Acrobat Reader from www.adobe.com. You must also have Internet Explorer 8.0 or later to view the reports.

See “Installing Mail Security on a local server” on page 33.
See “Silently installing Mail Security using an automated installation tool” on page 42.
See “About installing Mail Security on remote servers” on page 39.

Console system requirements

You can install the Mail Security console on a computer on which Mail Security is not installed. Table 2-2 describes the Mail Security console system requirements.
### Table 2-2  Console system requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Mail Security supports the following operating systems:</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>- Windows 7</td>
</tr>
<tr>
<td></td>
<td>- Windows 8</td>
</tr>
<tr>
<td></td>
<td>- Windows 2012</td>
</tr>
<tr>
<td></td>
<td>- Windows 10</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2016 Standard or Datacenter</td>
</tr>
<tr>
<td></td>
<td>Mail Security Console supports 64-bit processors on all supported operating systems.</td>
</tr>
<tr>
<td>Memory</td>
<td>2 GB</td>
</tr>
<tr>
<td>Available disk space</td>
<td>2 GB</td>
</tr>
<tr>
<td></td>
<td>This requirement does not include the space that Mail Security requires for items such as quarantined messages and attachments, reports, and log data.</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>Version 3.5</td>
</tr>
<tr>
<td></td>
<td>Ensure that .NET Framework is installed before you install Mail Security.</td>
</tr>
</tbody>
</table>

Adobe Acrobat Reader is not a requirement to install and run the Mail Security console. However, it is required to view the reports that are generated in .pdf format. You can download Adobe Acrobat Reader from [www.adobe.com](http://www.adobe.com). You must also have Internet Explorer 8.0 or later to view the reports.

See “Installing the Mail Security console” on page 37.

### Port requirements

Symantec Mail Security for Microsoft Exchange scans the SMTP mail traffic that passes through Exchange servers on port 25. Mail Security does not interact with MAPI or any other mail protocols, such as POP3 on port 110 or IMAP on port 143.

Some Mail Security components require certain ports for communication. Table 2-3 lists the ports that Mail Security components use by default.
Table 2-3  Ports used by Mail Security components

<table>
<thead>
<tr>
<th>Mail Security component</th>
<th>Port</th>
<th>Process</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid Release Definitions</td>
<td>80</td>
<td>SAVFMSELive.exe</td>
<td>Frequent antivirus definition updates</td>
</tr>
<tr>
<td>Conduit</td>
<td>443</td>
<td>Conduit.exe</td>
<td>Continuous Premium AntiSpam updates</td>
</tr>
<tr>
<td>DEXL Service</td>
<td>8081</td>
<td>Process ID: 0 or 4 (System)</td>
<td>Console communications</td>
</tr>
<tr>
<td>CmafReportSrv</td>
<td>58081</td>
<td>CmafReportSrv.exe</td>
<td>Reporting database</td>
</tr>
</tbody>
</table>

**Note:** If Symantec Premium AntiSpam is enabled, ensure that you open port 443 on the firewall for bi-directional traffic to aztec.brightmail.com. If Symantec Premium AntiSpam is not licensed and enabled, Mail Security does not initiate activity on port 443. Similarly, if the optional Rapid Release feature is not enabled, Mail Security does not initiate activity on port 21.

The port that is used for communication with Mail Security Console can be configured during installation or at any time after the installation. You can see activity only on these ports when you use the console to administer a remote server.

**Note:** There are no port conflicts or incompatibility between Mail Security and Symantec Endpoint Protection 11.x or the Symantec Endpoint Protection Manager.

See “Console system requirements” on page 30.

See “Server system requirements” on page 29.

### Installing Symantec Mail Security for Microsoft Exchange

Use any of the following installation procedures based on the type of installation that you want to perform:

**Local server**
You can install or upgrade Mail Security on a local computer that is running the Microsoft Exchange Server.

See “Installing Mail Security on a local server” on page 33.
Remote server

You can install Mail Security on remote servers through the product console.
See “About installing Mail Security on remote servers” on page 39.

Console

You can install the product console on a computer that is not running Mail Security. This way you can manage your servers from any computer that has access to your Exchange servers.
See "Installing the Mail Security console" on page 37.

Silent/automated installation

You can install Mail Security using automated installation tools.
See "Silently installing Mail Security using an automated installation tool" on page 42.

Installing Mail Security on a local server

Ensure that you have met the system requirements before you begin the installation process.
See “System requirements” on page 29.

---

**Note**: Symantec automatically installs MSXML 6.0 during installation if the installer does not detect this component.

---

To install mail security, you must:

- Be logged on as a member of Administrator group on the local computer.
- Be logged on as a member of Exchange Organization Management group (this privilege is required to install the transport agents) on the local computer.
- Have domain administrator privileges on the computer on which you want to install Mail Security.

Computers must support 8dot3 formatted file names for all NTFS file systems.

To install Mail Security on a local server, do the following:
Begin the installation process  You can use the installation wizard to select the product installation folder location and the type of installation that you want to perform.

You can choose to retain existing settings or use the new default settings if you want to upgrade from a previous version of Mail Security.

When Mail Security detects a previous version of the product, it automatically uninstalls the previous version and then installs the new version.

Note: If you choose to retain your existing settings, then Mail Security saves the existing items in the quarantine at the following temporary directory:

```
C:\Program Files\Symantec\SMSMSEServerUpgradeTemp\Quarantine
```

This temporary directory is typically not configured as an exclusion for the virus scanning software. As a result, the virus scanning software detects and flags any viruses or security threats in the quarantine. To avoid this situation, configure your virus scanning software to exclude this temporary directory from scanning or delete all the items from the directory.

Configure additional setup options and confirm settings  You can specify whether you want to automatically restart the Exchange Transport Service after installation. You can also specify the Web service set-up values, designate an email notification address and SMTP server address, and review your setup configurations.

Install your licenses  You can install your licenses during installation.

See “About licensing” on page 53.

If you install a valid license, Mail Security lets you perform a LiveUpdate to obtain the most current definitions.

See “About keeping your server protected” on page 230.

To begin the installation process

1  Download and extract the Symantec Mail Security for Microsoft Exchange installation package.

2  Navigate to /SMSMSE/Install, and run Setup.exe.
3 Warning message appears that you may need to restart your computer after installation. Click OK.

4 Click Next until you reach the License Agreement panel.

5 In the License Agreement panel, click I accept the terms in the license agreement, and then click Next.

You must accept the terms of the license agreement for the installation to continue.

6 In the Existing Settings panel, select one of the following:

- Retain existing settings  Retains the existing settings that are supported for migration to the new version.
  This option is the default setting.

- Install with default settings  Installs the product with the default settings, as if you install Mail Security for the first time.

This panel appears only if you upgrade from a previous version of Mail Security.

7 In the Destination Folder panel, do one of the following:

- To install the product in the default location, click Next.
  The default directory is as follows:
  C:\Program Files\Symantec\

- To install the product in a different location, click Change, select the location of the installation folder, click OK, and then click Next.

  Mail Security does not support the directory names that contain multi-byte characters. If you intend to use the Symantec Premium AntiSpam, you cannot install the product to a directory whose name contains high ASCII characters.

8 In the Setup Type panel, click Complete, and then click Next.

9 In the Symantec Endpoint Protection or Symantec AntiVirus Corporate Edition Users warning dialog box, click OK.

To configure additional setup options

1 In the Exchange Transport Service Reset Options panel, click Next to accept the default setting to automatically restart the Exchange Transport Service after installation.

If you choose not to automatically restart the Exchange Transport Service after installation, you must do so manually. Otherwise, Mail Security does not function properly.

2 In the Web Service Setup panel, do one of the following:

- Click Next to accept the default values.
- Modify the following settings, and then click **Next**:

  **IP/Name**
  By default, the computer name resolves to the primary external network identification card (NIC). You can also use an IP address.
  The IP address validates the availability of the port.

  **Port #**
  By default, port 8081 is the port number for the Web service that Mail Security uses. A different default port number appears if another application is using port 8081.
  If you change the port number, ensure that another application is not using that. You should not use port 80. The default Web service uses port 80 and IIS hosts this port.

3. In the **Notification Email Address** panel, do one of the following to specify the email address from which email notifications are sent and to which notifications to the administrator are sent:

   - Click **Next** to accept the default value.
   - The default value is: Administrator

   - Modify the originator email address, and then click **Next**.

   You can modify the address after installation is complete.

   See “Configuring notification settings for scan violations” on page 192.

4. In the **SMTP Server Host** panel, specify the SMTP receive connector server address for sending email messages.

   The default server address is as follows: localhost.

5. In the **Service Account Information** panel, specify the user name and password of the domain user account.

   Do not specify the user name and password of the domain administrator account.

6. In the **Setup Summary** panel, review the information, and then click **Next**.

   If you need to make any modifications, click **Back** to return to the appropriate panel.

7. In the **Ready to Install the Program** panel, click **Install**.

   To install a license and the update definitions

1. In the **Install Content License File** panel, do one of the following:
To install a license file, do the following:

- Click Browse, locate the license file, and then click Open.
- Click Install, and in the confirmation dialog box, click OK.
- Click Next.

To install a license file later through the console, click Skip, and then click Next.

2 In the LiveUpdate panel, do one of the following:

- To perform a LiveUpdate: Click Yes, and then click Next.
  In the LiveUpdate Options window, click Start.
  When LiveUpdate is complete, click Close.

- To perform a LiveUpdate at a later time: Click No, and then click Next.

This panel appears only if you installed a valid license.

3 Click Finish.

Show the readme file is checked by default. The Readme file contains the information that is not available in the product documentation.

A Mail Security icon is placed on the computer desktop when installation is complete.

4 In the User Credential Refresh Required panel, click OK.

5 Log off and log on again.

See “Post-installation tasks” on page 43.

Installing the Mail Security console

The Mail Security console is a Windows application. The console lets you manage local and remote installations of Mail Security from a single computer. You can install and use the console on a computer on which Mail Security is not installed. This way you can manage Mail Security from a convenient location.

Ensure that you meet the system requirements before you install the console.

See “Console system requirements” on page 30.

A Mail Security icon is placed on the computer desktop when installation is complete.
Note: To ensure secured communication between the Mail Security console and server, it is recommended that you enable SSL.

To install the Mail Security console

1. Download and extract the Symantec Mail Security for Microsoft Exchange installation package.
2. Navigate to /SMSMSE/Install, and run Setup.exe.
3. Warning message appears that you may need to restart your computer after installation. Click OK.
4. Click Next until you reach the license agreement.
5. On the License Agreement screen, check I accept the terms in the license agreement, and then click Next.
6. On the Destination Folder screen, do one of the following:
   - To install the product in the default location, click Next.
     The default destination directory is as follows:
     C:\Program Files\Symantec\n   - To install the product in a different location, click Change, select the location of the installation folder, click OK, and then click Next.
     Mail Security does not support the directory names that contain multi-byte characters. If you intend to use the Symantec Premium AntiSpam service, you cannot install the product to a directory whose name contains high ASCII characters.
7. On Setup Type screen select Custom.
   If the installation program detects that no version of Exchange server is installed, the installation program proceeds with console-only installation by default.
8. If Exchange server is installed, select Custom on Setup Type and then click Next.
   On Custom Setup screen, select This feature will not be available under Symantec Mail Security for Microsoft Exchange Server.
9. Click Next until you reach the Notification Email Address panel.
10. On the Notification Email Address screen, do one of the following to specify the email address from which email notifications are sent. It is also used as the recipient of the notifications that are sent to the administrator.
    - Click Next to accept the default value.
      The default value is: Administrator
    - Modify the originator email address, and then click Next.
You can modify the address after installation is complete.

See “Configuring notification settings for scan violations” on page 192.

11 In the Setup Summary screen, review the information, and then click Next.

If you need to make any modifications, click Back to return to the appropriate screen.

12 On Ready to Install the Program page, click Install.

13 Click Finish.

Show the readme file is checked by default. The Readme file contains the information that is not available in the product documentation.

14 Log off and log on again.

See “Post-installation tasks ” on page 43.

About installing Mail Security on remote servers

After you install Mail Security on a local server or install the console, you can install the Mail Security server component on remote servers.

Review the preinstallation information and system requirements before you install the product on remote servers.

See “System requirements” on page 29.

To install Mail Security on remote servers, do the following:

- Customize installation settings, if needed.

  Remote servers are installed with default installation settings. If you want to customize the installation settings and apply them to a remote server, you can add the custom features to the vpremote.dat file.

  See “Customizing remote server installation settings” on page 39.

- Install Mail Security on remote servers.

  See “Installing Mail Security on a remote server” on page 42.

Customizing remote server installation settings

There may be cases in which you want to customize the installation of Mail Security on a remote Exchange server. For example, you might want to change the following settings:

- Installation location

- Default email address for notifications

- Stop/start of IIS

Table 2-4 lists the remote customization options that you can modify.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default value</th>
<th>Optional value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMAIL ADDRESS=</td>
<td>Serves as the address of the domain administrator for the &quot;Address of sender&quot; and &quot;Administrator and others to notify&quot; Notification/Alert settings.</td>
<td>N/A</td>
<td>(Email address of domain administrator)</td>
</tr>
<tr>
<td>EXISTING SETTING GROUP=</td>
<td>Controls whether to retain a previous version’s settings or apply the default settings of the new version.</td>
<td>Retain</td>
<td>Restore</td>
</tr>
<tr>
<td>IIS_RESET</td>
<td>Controls whether to stop and restart Microsoft Exchange Transport Service during installation. This setting is only available if the Exchange Transport Service is installed.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>INSTALLDIR=</td>
<td>Serves as the default product installation directory.</td>
<td>\Program Files\Symantec\</td>
<td>(Any valid path)</td>
</tr>
<tr>
<td>Note: If you install Mail Security in a non-default location and the path name contains spaces, then you must enclose the path name in quotation marks. For example, INSTALLDIR=&quot;E:\test vpremote&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PORTNUMBER=</td>
<td>Serves as the port that the product uses for Web services.</td>
<td>8081</td>
<td>(Any valid port)</td>
</tr>
<tr>
<td>SMSE_SMTP_SERVER_HOST=</td>
<td>Serves as the host through which notifications are sent using SMTP.</td>
<td>localhost</td>
<td>(Any valid host)</td>
</tr>
<tr>
<td>CONSOLE_ONLY</td>
<td>Specifies that installation should be for the console only.</td>
<td>0</td>
<td>Set to 1 to perform a console installation.</td>
</tr>
</tbody>
</table>
Table 2-4  Remote customization options (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default value</th>
<th>Optional value</th>
</tr>
</thead>
<tbody>
<tr>
<td>REINSTALLMODE</td>
<td>Controls the mechanism for reinstall.</td>
<td>N/A</td>
<td>Set to voums to perform a silent installation.</td>
</tr>
<tr>
<td>REINSTALL</td>
<td>Controls what features to install during reinstall.</td>
<td>ALL</td>
<td>Set to 1 to perform a silent installation.</td>
</tr>
</tbody>
</table>

Warning: The following entry should not be changed: \{setup.exe /s /v" NOT_FROM_ARP=1 REMOTEINSTALL=ALL REINSTALLMODE=voums REINSTALL=ALL\}. You can append the entry. For example, setup.exe /s /v" NOT_FROM_ARP=1 REMOTEINSTALL=1 REINSTALLMODE=voums REINSTALL=ALL PORTNUMBER=1010"

To customize remote server installation settings

1. Locate the folder that contains the Mail Security console files. The default location is as follows:
   \Program Files\Symantec\CMaF\2.3\bin\Products\SMSMSE\7.9\Remote Install Files\vpremote.dat

2. Open the following file by using WordPad or a similar tool:
   vpremote.dat

3. Insert one or more properties by doing the following:
   ■ Type a space after the previous or the existing entry inside the quotation marks.
   ■ Type the new property.
      The property portion of each entry is case-sensitive.
   ■ Type the value immediately after the = sign with no space.
      The values are not case-sensitive.

For example, to specify a silent installation, the entry would appear as follows:

\{setup.exe /s /v" NOT_FROM_ARP=1 REMOTEINSTALL=1 REINSTALLMODE=voums REINSTALL=1\}"

See “About installing Mail Security on remote servers” on page 39.
See “Installing Mail Security on a remote server” on page 42.
Installing Mail Security on a remote server

During remote installation, the Windows Login screen prompts you to provide administrator or domain user credentials. The domain user must fulfill all pre-requisites before the installation of Mail Security on a remote server.

When installation is complete, a Mail Security icon is placed on the computer desktop.

Note: The Mail Security installation may automatically restart your computer at the end of the installation. If you have selected the Send group settings option, you have to manually deploy the group settings on the remote server after the computer restarts.

To install Mail Security on a remote server

1. In the console on the toolbar, click Assets.
2. In the Asset Management window, in the sidebar under Tasks, click Install/Upgrade server(s).
3. In the Select Server(s) window, in the Servers and server groups list, highlight one or more servers and click the >> command icon.
4. Under Server options, check Keep installation files on server(s) to maintain the installation files on the server.
5. Check Send group settings to apply group settings.
   If unchecked, existing server settings are retained. Any future changes that you make to the server group are applied to the server.
6. Click OK.
7. In the Windows Login window, provide user name and password of a domain user who is a member of the Organization Management Exchange group and click OK.

Note: Remote install must be performed from the computer which is part of the same domain.

See “Post-installation tasks ” on page 43.

Silently installing Mail Security using an automated installation tool

Mail Security supports installing the product using automated installation tools, such as Microsoft Systems Management Server.

Ensure that you have met the system requirements before you perform a silent installation.

See "System requirements" on page 29.
You can modify certain installation properties to configure Mail Security installations. You can also provide command-line properties during manual or automated installation by using an automated installation tool

Modify the installation properties for Mail Security in the following file:

\Program Files \Symantec\CMaF\2.3\bin\Products\SMSMSE\7.9\Remote Install Files\vpremote.dat

See Table 2-4 on page 40.

---

**Note:** After the Mail Security silent installation, the **Symantec Mail Security Utility Service** and the **Symantec Mail Security for Microsoft Exchange** services do not start automatically. You must start these services manually.

---

**To silently install Mail Security using an automated installation tool on Exchange 2010 hub role**

1. Copy the installation media in its entirety to the location from which installation is launched.
   
   For example: `xcopy [Drive]::\*.* /s [Destination drive]`

2. Launch `setup.exe` using the following command to initiate a silent installation:
   
   `[Destination drive]\setup.exe /v"/lvx* "c:\smsmse_install.log" NOT_FROM_ARP=1 REMOTEINSTALL=1 REINSTALLMODE=voums REINSTALL=ALL" /s`

   Where "c:\smsmse_install.log" is the path of installation log file that gets generated during installation.

**To silently install Mail Security using an automated installation tool on mailbox role of Exchange**

1. Copy the installation media in its entirety to the location from which installation is launched.
   
   For example: `xcopy [Drive]::\*.* /s [Destination drive]`

2. Launch `setup.exe` using the following command to initiate a silent installation:
   
   `[Destination drive]\setup.exe /v"/lvx* "c:\smsmse_install.log" NOT_FROM_ARP=1 REMOTEINSTALL=1 REINSTALLMODE=voums REINSTALL=ALL SMSMSE_RBAC_USERNAME=<username> SMSMSE_RBAC_PASSWORD=<password>" /s`

   where "c:\smsmse_install.log" is the path of installation log file that is generated during installation.

---

**Post-installation tasks**

After you install Mail Security, you can perform the following post-installation tasks:

- Implement SSL communications.
Implementing SSL communications

You can configure Mail Security to use Secure Sockets Layer (SSL) communications by using a valid server certificate. You can create your own server certificate using Microsoft Certificate Services 2.0 or request one from a certificate authority.

After you implement SSL, you must enable SSL from the console and specify the SSL port for each server.

See “Modifying the port and the communication properties of a server” on page 73.

To install a server certificate

1. On the computer on which Mail Security is installed, click Start > Administrative Tools > Internet Information Services (IIS) Manager.
2. In the server list, expand the folder for the server that hosts Mail Security.
3. In the Web sites folder, right-click Symantec Mail Security for Microsoft Exchange, and then click Properties.
5. Follow the instructions in the Web server Certificate wizard to install the server certificate.
To implement SSL communications

1. Ensure that a valid server certificate is installed.
2. Under **Secure Communications**, click the **Directory Security** tab, and then click **Edit**.
3. In the **Secure Communications** dialog box, check **Require secure channel (SSL)**, and then click **OK**.
4. On the **Web Site** tab, under **Web site identification**, in the **IP Address** text box, type the IP address of the Mail Security server.
5. In the **SSL Port** text box, type the port to use for SSL communications.
6. Click **OK** to close the **Mail Security Properties** window.

To implement SSL communications on Windows 2008/2012/2016 Server

1. On the local computer, ensure that a valid server certificate is installed in **Trusted Root Certification Authorities**.
2. Click **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
3. In the **Websites** folder, right-click **Symantec Mail Security for Microsoft Exchange**, click **Edit Bindings** and select **Add**.
4. From the drop-down list, select **https** and **All Unassigned** for Type and IP addresses respectively.
5. In the **SSL Port** text box, type the port number.
   For example, type 8082 for SSL communications.
   To avoid port conflicts, ensure that you do not use the ports that Exchange server uses.
   For example, TCP port 80 and SSL port 443.
6. From the **SSL certificate**, select the certificate that you installed and restart the **Symantec Mail Security for Microsoft Exchange** website.
7. In the right pane, double-click **Authentication** and ensure that **Windows Authentication** and **ASP.NET Impersonation** are enabled.
8. From the **Web sites** folder, select **Symantec Mail Security for Microsoft Exchange**.
9. In the right pane, double-click **SSL Settings** and check **Require SSL** and **Require 128-bit SSL**.
10. Click **Apply** to apply the changes.

To implement SSL communications on client computer

1. Export the server certificate from the server and install it to the client computer where Mail Security console is installed in **Trusted Root Certification Authorities**.
2. Open **Certificate snap-in** and ensure that the certificate resides in **Trusted Root Certification Authorities**.
3 On the Mail Security console, click the Assets tab and click Add server(s) to add a server.
4 Right-click the server that you added and then click Properties.
5 Provide the SSL port number that is configured on the server.
6 Check Use SSL and click OK.

You can now connect to the server from the console by using the SSL connection.

Accessing the Mail Security console

You can access the Mail Security console from the Windows Start menu or from your desktop. You must have the appropriate administrator or viewer rights to open the console. If you do not have the required rights, the following error message appears:

"You either have insufficient permissions to access this application or your user credentials are not refreshed. Try logging off and logging on again to reload the user credentials. You either have insufficient permissions to access this application or your user credentials are not refreshed. Try logging off and logging on again to reload the user credentials."

You can only access the servers that run Mail Security 7.9 from the Mail Security console.

To access the Mail Security console

◆ Do one of the following:
  ■ On the desktop, double-click the SMSMSE 7.9 icon.

See “About the Mail Security console” on page 46.

About the Mail Security console

Figure 2-1 shows the Mail Security console.
Figure 2-1  Mail Security Server Home page view

Figure 2-2 shows additional console elements.
About the primary navigation bar

Management operations are grouped into the following categories on the primary navigation bar:

- **Home**  
  Lets you view server status, recent activities, and violations statistics

- **Policies**  
  Lets you create and configure the sets of rules that specific scans implement

- **Monitors**  
  Lets you configure notification addresses and quarantine settings and monitor quarantine data and events

- **Scans**  
  Lets you create, configure, schedule, and run scans

- **Reports**  
  Lets you view and print the data that Mail Security collects
Admin lets you update definitions, configure system settings, and install licenses

See “About the Mail Security console” on page 46.

**Refreshing the console**

You might periodically need to refresh the console to view changes or updated statuses.

To refresh the console

1. On any page in the console, click F5.
2. Click OK to log onto the current asset group.

This message only appears if you are not logged onto the current asset group.

See “Logging onto servers” on page 63.

**About using Mail Security with other antivirus products**

Configure your other antivirus programs to exclude certain folders from scanning. If another antivirus scans the Exchange directory structure or the Mail Security processing folder, it can cause false-positive threat detection. It also can cause unexpected behavior on the Exchange server, or damage to the Exchange databases.

For information about how to prevent Symantec Endpoint Protection or Symantec AntiVirus Corporate Edition from scanning the Exchange directory, go to the following article:


See “Components of Mail Security” on page 14.

If you have Symantec AntiVirus Corporate Edition or Symantec Endpoint Protection (SEP) 11.x installed on the same computer as Mail Security, configure Symantec AntiVirus Corporate Edition or SEP version 11.x to perform definition updates. You must also configure Mail Security to perform definition updates. You can also use LiveUpdate Administrator to perform definition updates for both the products.

See “About setting up your own LiveUpdate server” on page 231.

**Configuring Mail Security transport agents**

Mail Security automatically installs custom transport agents when you install the product on the Exchange servers. The Mail Security transport agents consist of an antispam transport agent and an antivirus transport agent.

Mail Security transport agents must act on email messages before any other spam or virus scanning transport agent. For example, Microsoft Exchange antispam agents such as follows:

- Connection Filtering Agent
By default, the Mail Security transport agents are installed with a lower priority than the Microsoft Exchange antispam agents. This means that the Microsoft Exchange antispam agents act on emails before Mail Security transport agents. As a result, Mail Security may not detect spam or viruses. Therefore, ensure that the Mail Security transport agents are set with a higher priority than any other spam filtering agents.

**To configure Mail Security transport agents**

1. Click **Start > Programs > Microsoft Exchange Server server version > Exchange Management Shell**.

2. Run the following command to check the transport agent priorities:

   ```
   Get-TransportAgent
   ```

   The following result appears, which shows that the Mail Security transport agents have a lower priority than the Exchange antispam transport agents:

<table>
<thead>
<tr>
<th>Identity Enabled</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Rule Agent</td>
<td>True 1</td>
</tr>
<tr>
<td>Journaling Agent</td>
<td>True 2</td>
</tr>
<tr>
<td>AD RMS Prelicensing Agent</td>
<td>False 3</td>
</tr>
<tr>
<td>Connection Filtering Agent</td>
<td>True 4</td>
</tr>
<tr>
<td>Content Filter Agent</td>
<td>True 5</td>
</tr>
<tr>
<td>Sender Id Agent</td>
<td>True 6</td>
</tr>
<tr>
<td>Sender Filter Agent</td>
<td>True 7</td>
</tr>
<tr>
<td>Recipient Filter Agent</td>
<td>True 8</td>
</tr>
<tr>
<td>SMSMSESMTPAgent</td>
<td>True 9</td>
</tr>
<tr>
<td>SMSMSESMTPAgent</td>
<td>True 10</td>
</tr>
<tr>
<td>Protocol Analysis Agent</td>
<td>True 11</td>
</tr>
</tbody>
</table>

3. Perform one of the following tasks:

   - Set the priority of the Mail Security transport agents higher than the Exchange antispam transport agents by running the following commands:

     ```
     Set-transportagent -identity "SMSMSESMTPAgent" -priority 4
     Set-transportagent -identity "SMSMSESMTPAgent" -priority 5
     ```

   - Disable Exchange transport agents by running the following commands:
disable-transportagent -identity "Connection Filtering Agent"
disable-transportagent -identity "Sender Id Agent"
disable-transportagent -identity "Sender Filter Agent"
disable-transportagent -identity "Recipient Filter Agent"
disable-transportagent -identity "Protocol Analysis Agent"
disable-transportagent -identity "Content Filter Agent"

You might encounter an error about not being able to edit the config file when running these commands. You can resolve the error by opening the Exchange Management Shell as an administrator and running the commands again.

4 Run the following command to restart the transport agent service:

```
restart-service -force MSExchangeTransport
```

### Setting scanning threads and number of scan processes

Mail Security lets you set the number of scan processes to control scanning speed and performance. The default is configured using the following formula: \((\text{number of processors}) \times 2 + 1\). Accept the default unless you have a compelling reason to do otherwise.

Mail Security considers a hyper-threaded processor as more than one processor. For example, if you have a dual hyper-threaded processor on your computer, Mail Security calculates the number of scanning processes as follows:

**Number of processors** \((4) \times 2 + 1 = 9\)

When the load is heavy, all nine scanning processes scan messages. Increasing the number of scan processes can consume a lot of memory if the server has few resources. This situation can severely affect the performance of your Exchange server.

Configure the number of scan processes based on the actual number of physical processors if you have a hyper-threaded processor on your computer. For example, if you have a dual hyper-thread processor, configure the number of scan processes as follows:

**Number of physical processors** \((1) \times 2 + 1 = 3\)

---

**Note:** If you use Intel Xeon processors, you must set this value using the formula based on the number of physical processors, instead of the number that is reported by the operating system.

---

1 In the console on the primary navigation bar, click **Admin**.

2 In the sidebar under **Views**, click **System Settings**.
3 In the **Number of VSAPI scanning threads** box, type the number of threads to use for VSAPI scanning.

The default value is 3.

**Note:** This step is applicable only for Exchange Server 2010.

4 In the **Number of scan processes** box, type the number of scan processes.

The default is configured during installation using the formula 2 times the number of processors plus 1.

5 On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

**Uninstalling Symantec Mail Security for Microsoft Exchange**

Stop Microsoft Internet Information Service (IIS) before you uninstall the product. This task ensures that all of the files that are installed with the product are removed.

**To stop Microsoft IIS**

1 On the Windows taskbar, click **Start > Administrative Tools > Services**.
2 In **Services** window, right-click **IIS Admin Service** and click **Stop**.
3 Close the **Stop Other Services** window.

**To uninstall Mail Security**

1 On the server on which Mail Security is installed, on the Windows taskbar, click **Start > Settings > Control Panel**.
2 In the **Control Panel** window, double-click **Add or Remove Programs**.
3 Click **Symantec Mail Security for Microsoft Exchange**, and then click **Remove**.
4 In the confirmation dialog box, click **Yes**.
5 In the **Information** dialog box, click **OK** to confirm that you have stopped IIS.
6 When the uninstallation is complete, click **OK**.

After you uninstall Mail Security, the users that you added and the groups to which you assigned them remain in the Active Directory. You can remove them manually from the Active Directory.
About licensing

Key features of Symantec Mail Security, which include definition updates and Symantec Premium AntiSpam, are activated by a license. When a license expires or no license is installed, limited functionality is available. To regain product functionality when your license expires, you must renew and reactivate your license subscription.

Table 3-1 describes the licenses that are required.

<table>
<thead>
<tr>
<th>License</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content license</td>
<td>A content license is required to update Symantec software with the latest associated content (such as new definitions) through LiveUpdate and Rapid Release. A valid content license enables your servers to stay protected.</td>
</tr>
<tr>
<td></td>
<td>When the content license is missing or invalid, you cannot download definition updates to keep protection current.</td>
</tr>
<tr>
<td></td>
<td>See “About keeping your server protected” on page 230.</td>
</tr>
</tbody>
</table>
Table 3-1  Symantec Mail Security Licenses (continued)

<table>
<thead>
<tr>
<th>License</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Premium AntiSpam license</td>
<td>This license is required to enable Symantec Premium AntiSpam. Symantec Premium AntiSpam is a subscription service that provides enhanced spam detection. Continuous updates to the premium antispam filters ensure that your Exchange server has the most current spam detection filters that are available. When the Symantec Premium AntiSpam license is missing or invalid, Symantec Premium AntiSpam does not function. See “How to detect spam using Symantec Premium AntiSpam” on page 106.</td>
</tr>
</tbody>
</table>

Definition updates and updates to Symantec Premium AntiSpam are limited to the period of time that the license specifies. The start and the end dates of the license period depend on the terms of your license agreement.

You must install one license file on each server that is running Symantec Mail Security. You cannot replicate license files.

You can view the status of your license on the Home page of the Mail Security console.

About activating the Mail Security license

Symantec issues a serial number when you purchase Mail Security. If you upgrade from a previous version and you have an active maintenance contract, Symantec issues an upgrade voucher with an alpha-numeric code. Register the serial number or upgrade code to receive a license key for the associated license file.

License keys are delivered in a Symantec license file (.slf). The serial number is provided on a license certificate, which is mailed separately and arrives in the same time frame as your software. For security reasons, the license certificate is not included in the Mail Security software distribution.

See “About renewing the Mail Security license” on page 57.

License activation involves the following process:

Obtain a license file from Symantec  To request a license file, you must have the license serial number or upgrade voucher code. After you complete the registration process, Symantec sends you the appropriate license file by email. See “Obtaining a license file” on page 55.
Install the license file on each server on which you run Mail Security. See “Installing license files” on page 56.

About the Mail Security license serial number

Your license certificate or upgrade voucher, which contains the license number, arrives within three to five business days of when you receive your software. Contact Symantec Customer Service at 800-721-3934 or your reseller to check the status of your order if you do not receive the license certificate or upgrade voucher. Contact Symantec License Administration if you have lost your license certificate or upgrade voucher.

See “Where to get more information about Mail Security” on page 20.

Obtaining a license file

You must have the serial number or upgrade voucher code to request a license file and to register for support.

See “About the Mail Security license serial number” on page 55.

The license file that you receive from Symantec is contained within a .zip file. The .slf file that is contained within the .zip file is the actual license file. Ensure that your inbound email environment permits .zip email message attachments.

If you purchased multiple types of licenses but registered them separately, Symantec sends you a separate license file for each license. You must install each license file separately. If you registered multiple licenses at the same time, Symantec sends you a single license file that contains all of your licenses.

Warning: License files are digitally signed. When you try to edit a license file, it corrupts the file and renders it invalid.
To obtain a license file

1 In a web browser, type the following address:

   https://licensing.symantec.com

   Your web browser must use 128-bit encryption to view the site.

2 If the **Security Alert** dialog box appears, click **OK**.

3 Follow the procedures on the Symantec Licensing website to register your license and request your license file.

   Symantec sends you an email message that contains the license file in an attachment. If the email message does not arrive within two hours, an error might have occurred. Try again to obtain the license file through the Symantec website. If the problem continues, contact Symantec Technical Support.

   See “Where to get more information about Mail Security” on page 20.

Installing license files

Install the license file on each server on which Mail Security is installed.

You can install your license file during product installation or in the console. Mail Security issues periodic messages in the event log to notify you that your license is invalid or expired until a valid license is installed. You can view the status of your license on the Home page of the console.

The procedures for installing license files vary for a local server installation and a remote server or server group.

To install license files to a local server

1 In the console on the primary navigation bar, click **Admin**.

2 In the sidebar under **Views**, click **Licensing**.

3 In the content area, do one of the following:

   ■ In **Step 3**, under **Enter path to the license file**, type the fully qualified path to the license file.

      You can specify a mapped drive or Universal Naming Convention path to the file if the license file does not reside on the same computer.

   ■ Click **Browse**, select the license file, and then click **Open**.

      You can locate the file using My Network Places if the license file does not reside on the same computer.

4 Click **Install**.
To install license files to a remote server or server group

1 In the console on the toolbar, click Change.
2 In the Select Asset window, select a server or server group from the menu.
3 Click Select.
4 On the primary navigation bar, click Admin.
5 In the sidebar under Views, click Licensing.
6 In the content area, do one of the following:
   - In Step 3, under Enter path to the license file, type the fully qualified path to the license file.
     You can specify a mapped drive or UNC path to the file if the license file does not reside on the same computer.
   - Click Browse, select the license file, and then click Open.
     You can locate the file using My Network Places if the license file does not reside on the same computer.
7 Click Install.

If a server within a server group is already licensed, the license file is reapplied. The license file with the latest expiration date is applied.

About renewing the Mail Security license

Content updates and spam definition updates are not applied when a server has an expired license or when the license is missing or invalid. A missing or an invalid license can leave your server vulnerable to attacks. Renew your maintenance agreement to receive content updates when your license expires.

The process for license renewal is specific to how you purchased your software. The license renewal process is as follows:

If you purchased Mail Security through the Symantec Value or Elite Enterprise Licensing programs

Contact your administrator, reseller, or Symantec account manager to determine whether your maintenance agreement has been renewed and if new licenses are available.

After your maintenance agreement is renewed, you receive the new serial numbers that you can register to obtain your new license files.

If you purchased Mail Security Small Business Edition

To find more information about license renewal on the Internet, go to the following URL:

See “Obtaining a license file” on page 55.
Managing your Exchange servers

This chapter includes the following topics:

- About managing your Exchange servers
- Deploying settings and changes to a server or group
- Managing servers and server groups

About managing your Exchange servers

Mail Security can simplify the management of one or more Microsoft Exchange Servers across your organization. You can create the server groups that have a common purpose and, therefore, require the same protection. By grouping servers, you can apply a common set of protection settings once, rather than repeatedly to each server. The reduction in configuration time and maintenance costs can be considerable in a large network with multiple servers that perform similar roles.

Symantec Mail Security for Microsoft Exchange primarily consists of two components, server and console. With this console, you can manage your Mail Security from a single computer. When you open this console, mail security automatically logs onto all of your managed servers. The console logs onto a server to check status or apply settings to it. Several settings like remote install and upgrade can be done with the console. As per your requirement you can create the various server groups that serve a similar purpose. You can also deploy settings to all you managed servers in the group from the console. By grouping servers, you can apply a set of security rules or policies settings once, rather than repeatedly to each server.

You can configure settings for each server individually. You can use the following groups to configure and manage multiple servers:
The Global Group consists of all of the servers that you manage through the Mail Security console. The changes are propagated to all servers in all groups when you configure and apply Global Group settings. Changes that are made at the Global Group level overwrite all individual server and user-defined server group settings.

Mail Security provides the following Global Groups:

- **Global Group - Exchange 2010**
  All Exchange 2010 servers belong to the Global Group - Exchange 2010. No other exchange server group other than Exchange 2010 Server is supported in this group.

- **Global Group - Exchange 2013**
  All Exchange 2013 servers belong to the Global Group - Exchange 2013. No other exchange server group other than Exchange 2013 Server is supported in this group.

- **Global Group - Exchange 2016**
  All Exchange 2016 servers belong to the Global Group - Exchange 2016. No other exchange server group other than Exchange 2016 Server is supported in this group.

Global Groups include the servers that are added to user-defined groups. They also include the servers that are added to multi-server management control but are not assigned to a specific server group.

You cannot create or delete Global Groups.

A user-defined server group is a grouping of servers that have common roles and, therefore, require similar configurations. You can create a user-defined server group and configure settings for the group to simplify server management. For example, a server group can be the mail servers that are used by department such as marketing or the physical location of servers such as third floor of Building A).

A managed server can only belong to one user-defined group.

See “Moving a server to another user-defined server group” on page 69.

See “Viewing the status of a server” on page 67.

Server stores the settings for that individual server. Mail Security saves the settings for groups in the following default file location:

\Program Files\Symantec\CMaF\2.3\Settings\Groups

The associated files are automatically deleted when you delete a group.

**Deploying settings and changes to a server or group**

Mail Security lets you make changes to multiple pages before you apply those settings. When the **Deploy changes** icon on the toolbar is active, it indicates that you have made the changes that you need to apply.

You can manage change deployment by using the following toolbar icons:
**Deploys your changes.**
Deploys your changes to the server if you are in the server view.
Deploys your changes to each server in the group and to the group settings if you are in the group view.
See “To deploy pending changes to a server or group” on page 61.

**Discard changes**
Cancels the pending changes.
When you cancel pending changes, settings are returned to their configuration as of the last time changes were successfully deployed.
See “To cancel pending changes” on page 61.

**Deploy all settings**
Applies the pending changes to the group settings, and then pushes out the group settings to all the servers in the group.
Pushes out the group settings to all of the servers in the group if there are no pending changes.
**Note:** Any configuration settings that were made to an individual server within the group are overwritten.
This option is only available in the group view.
See “To apply pending changes (if any) and deploy group settings to each server in the group” on page 61.

After you deploy your changes, the **Operation Status** window indicates whether changes were successfully applied.

**To deploy pending changes to a server or group**
1 In the console on the toolbar, click **Deploy changes**.
2 In the **Pending changes** window, click **Deploy changes**.
3 In the **Operation Status** window, click **Close** when the operation is complete.

**To apply pending changes (if any) and deploy group settings to each server in the group**
1 In the console on the toolbar, click **Deploy all settings**.
   The **Deploy all settings** icon is only enabled in the group view.
2 In the **Deploy all settings** dialog box, click **OK**.
3 In the **Operation Status** window, click **Close** when the operation is complete.

**To cancel pending changes**
1 In the console on the toolbar, click **Discard changes**.
2 In the **Discard changes** dialog box, click **OK**.
Managing servers and server groups

You can manage servers and server groups by performing the following tasks:

- Logon to the servers.
  See “Logging onto servers” on page 63.

- Modify or view server or server group settings.
  See “Modifying or viewing server or server group settings” on page 66.

- View the status of a server.
  See “Viewing the status of a server” on page 67.

- Create a user-defined server group.
  See “Creating a user-defined server group” on page 67.

- Add servers to a group.
  See “Adding servers to a group” on page 68.

- Move a server to another user-defined server group.
  See “Moving a server to another user-defined server group” on page 69.

- Synchronize group settings to a server.
  See “Synchronizing group settings to a server” on page 70.

- Restore default settings to a server or group.
  See “Restoring default settings to a server or group” on page 70.

- Remove a server from group management.
  See “Removing a server from group management” on page 71.

- Remove a server group.
  See “Removing a server group” on page 71.

- Export and import the settings.
  See “Exporting and importing settings” on page 72.

- Modify the port and the communication properties of a server.
  See “Modifying the port and the communication properties of a server” on page 73.

- Create and assign a custom throttling policy to the Mail Security service account user.
  See “Creating and assigning a custom throttling policy to the Mail Security service account user” on page 73.
Logging onto servers

Mail security consists of two components, server and console. The console logs onto a server to check status or apply settings to it. Console logs onto all of your managed servers when you open (start) the console.

You might experience a delay when you open the console while Mail Security logs onto the managed servers. The length of the delay depends on the number of managed servers that you have. If you frequently open the console to view settings or to make changes without applying them, you can disable the automatic logon feature. When you disable the automatic logon feature, the console opens more quickly.

If you disable the automatic logon feature, Mail Security logs onto your servers in the following ways:

<table>
<thead>
<tr>
<th>Single server</th>
<th>Mail Security logs onto a single server when you do any of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ Open the console when a single server is the current asset.</td>
</tr>
<tr>
<td></td>
<td>■ Select a single server as the current asset.</td>
</tr>
<tr>
<td></td>
<td>See &quot;Modifying or viewing server or server group settings&quot; on page 66.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server group (user-defined server groups and Global Groups)</th>
<th>Mail Security logs onto all of the servers in the current asset list when you do any of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ Manually refresh the console. See &quot;Refreshing the console&quot; on page 49.</td>
</tr>
<tr>
<td></td>
<td>■ Apply settings to a server group.</td>
</tr>
</tbody>
</table>

Mail Security logs onto all of the servers in a group when you apply settings to that group. If you apply settings to a user-defined server group, Mail Security logs onto all of the servers in the user-defined group. If you apply settings to a Global Group, Mail Security logs onto all of the servers in the Global Group. Mail Security also logs onto all of the servers in the user-defined groups within that Global Group.

For example, assume that you have Global Group - Exchange - 2010 and Global Group - Exchange - 2013. Within Global Group - Exchange - 2010, you have user-defined groups named ServersEast and ServersWest.


Another example assumes that you apply settings to the ServersEast group. Mail Security logs onto all of the servers in the ServersEast group. But Mail Security does not log onto any of the servers in the ServersWest group.

See "Deploying settings and changes to a server or group" on page 60.
See "About managing your Exchange servers" on page 59.
To log onto servers when you open the console
1. In the console on the toolbar, click **Assets**.
2. In the **Asset Management** window in the **Assets** box, check **Automatically connect to the servers in the current group on startup**.
   
   Mail Security logs onto all of the servers that you have listed in the **Assets** box every time you open the console.
   
   This option is enabled by default.
3. Click **Close**.

To log onto servers when you apply settings or refresh the console
1. In the console on the toolbar, click **Assets**.
2. In the **Asset Management** window in the **Assets** box, uncheck **Automatically connect to the servers in the current group on startup**.
   
   Mail Security only logs onto a server when you apply settings to that server or when you view or modify the settings of that server.
3. Click **Close**.

Configuring Symantec Mail Security for Exchange on DAG setup

You must follow the configurations that are recommended for Exchange Server on Database Availability Group (DAG) setup.

To configure Symantec Mail Security for Exchange on DAG setup
1. In the console on the toolbar, click **Assets**.
2. In the **Asset Management** window, under **Tasks**, click **New group**.
   
   Create a new group for exchange DAG servers.
   
   Create separate groups for each DAG if there are multiple DAG groups. Set up a quarantine server on each DAG group from the console so that the quarantine data is available if any DAG server is unavailable.
3. Click **Add server(s)** and add all DAG member servers to the new group.
4. Create and apply the same security policies to every server in the group. This ensures that all the mailboxes have the same Mail Security settings if a database failover occurs.
   
   See “Forwarding quarantined items to the Quarantine Server” on page 76.

Changing the password of the domain user account

For every installation of Mail Security on Exchange 2010 in the mailbox role, the user credentials must be updated whenever the password of the domain user account is changed.
To change password of the domain user account

1. From the Windows taskbar, click **Start > Programs > Administrative Tools > Services.**
2. Right-click **Symantec Mail Security for Microsoft Exchange** and click **Stop** to stop the Mail Security service.
3. Click **Start > Programs > Administrative Tools > Services.**
4. Right-click **Symantec Mail Security for Microsoft Exchange** and click **Properties.**
5. On the **Log On** tab, enter new password and click **Apply** to change the password.

See “Changing the service account used by Mail Security service” on page 65.

Changing the service account used by Mail Security service

If you want to change the service account for the Mail Security service, perform the following steps:

To remove service account from the Mail Security service

1. From the Windows taskbar, click **Start > Programs > Administrative Tools > Services.**
2. Right-click **Symantec Mail Security for Microsoft Exchange** and click **Stop** to stop the Mail Security service.
3. Click **Start > Programs > Microsoft Exchange Server (version) > Exchange Management Shell.**
4. Remove the RBAC right by typing the following command from the Exchange Management Shell.

   `remove-ManagementRoleAssignment SMSMSE_RBAC_domainname\username`

5. Click **Start > Programs > Administrative Tools > Active Directory Users and Computers.**
6. In the **Active Directory Users and Computers** window in the left pane, click **Microsoft Exchange Security Groups.**
7. In the right pane, right-click **Organization Management** and then click **Properties.**
8. On the **Members** tab, select the user that you want to remove and click **Remove.**
9. Click **Start > Programs > Administrative Tools > Local Security Policy.**
10. In the **Local Security Policy** window in the left pane, click **Local Policies.**
11 In the right pane, double-click **User Rights Assignment**.

12 In the right pane, right-click **Log on as a Service** and then click **Properties**.

13 Select the user that you want to remove and click **Remove**.

**To assign new service account to the Mail Security service**

1 Assign the RBAC right to the new user by typing the following command from the same Exchange Management Shell:

```
new-ManagementRoleAssignment -name SMSMSE_RBAC_domainname\username -role ApplicationImpersonation -user <username>
```

2 Click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

3 In the **Active Directory Users and Computers** window in the left pane, click **Microsoft Exchange Security Groups**.

4 In the right pane, right-click **Organization Management** and then click **Properties**.

5 On the **Members** tab, select the user that you want to add and click **Add**.

You must ensure that the user is a member of the Local Administrators Group.

6 Click **Start > Programs > Administrative Tools > Local Security Policy**.

7 In the **Local Security Policy** window in the left pane, click **Local Policies**.

8 In the right pane, double-click **User Rights Assignment**.

9 In the right pane, right-click **Log on as a Service** and then click **Properties**.

10 Select the user that you want to add and click **Add**.

11 From the Windows taskbar, click **Start > Programs > Administrative Tools > Services**.

12 Right-click **Symantec Mail Security for Microsoft Exchange** and click **Properties**.

13 On the **Log On** tab, enter the new user's credentials and click **Apply** to apply the settings.

14 Start the Mail Security service.

See “Changing the password of the domain user account” on page 64.

**Modifying or viewing server or server group settings**

Mail Security lets you manage one or more servers from a single console. The **Server/group** box on the toolbar indicates the server or group that is currently selected. The settings that you make and deploy are applied to that server or group.

See “Deploying settings and changes to a server or group” on page 60.

You can view and modify the settings of a different server or group by selecting the server or group in the **Select Asset** window.
To modify or view server or server group settings

1. In the console on the toolbar, click Change.

2. In the Select Asset window, select the server or group whose settings you want to modify or view.

3. Click Select.

Viewing the status of a server

Mail Security provides server status information on the Home page of the Mail Security console. You can view more detailed information about the status of a server by accessing Monitors > Server Status.

The server status details appear in the Server Status preview pane. If you are in a group view, the Server Status list contains all of the servers in the group. The first time that you access the Server Status in a group view, you must refresh the page to view the list of servers. If you are in a single-server view, the Server Status list contains the server that you selected.

To view the status of a server

1. In the console on the primary navigation bar, click Monitors.

2. In the sidebar under Views, click Server Status.

3. In the Server Status table, select the server whose status you want to view.

   If you are in a server view, the server is already selected.

4. Press F5 to refresh the list.

   Refreshing the list might take several minutes for a large group.

See “Modifying or viewing server or server group settings” on page 66.

Creating a user-defined server group

If your network contains a large number of Exchange servers, create user-defined groups. Add servers to your user-defined groups that have a common purpose and, therefore, require the same protection. This lets you administer all of your servers that run Mail Security on a group basis.

To create a user-defined server group

1. In the console on the toolbar, click Assets.

2. In the Asset Management window, in the sidebar under Tasks, click New group.

3. In the New Group window, in the Group Name box, type a name for the user-defined server group.
4 In the **Global Group** list, select the appropriate group, and then click **OK**.

5 Click **Close**.

See “Modifying or viewing server or server group settings” on page 66.

## Adding servers to a group

You can add servers to the Global Group or to a user-defined server group within a Global Group. Group servers together that have a common purpose and, therefore, require the same protection. By adding a server to a group, you can apply a common set of protection settings once, rather than repeatedly to each server. In a large network with multiple servers that perform similar roles, the reduction in configuration time and maintenance costs can be considerable.

Mail Security automatically detects the Exchange servers that are within your domain. Identify servers outside of your domain by their name or IP address.

You can install Mail Security on the servers that you add to a server group. All servers must be running the version same as Mail Security to be managed from the console.

**Note:** The Global Groups have version association with the Exchange Servers. For example, Exchange 2013 Global Group can have Exchange 2013 Servers only.

### To add servers to a group

1 In the console on the toolbar, click **Assets**.

2 In the **Asset Management** window, in the sidebar under **Tasks**, click **Add server(s)**.

3 In the **Add Server(s)** window, under **Management group**, do one of the following:

   - To select an existing group Click **Select group**, select the existing group in which you want to add the server, and then click **OK**.
   - To create a new group In the Group box, type the name of the new server group that you want to create.

4 Under **Servers to add**, do one of the following:

   - In the **Available servers** list, select one or more servers, and then click the `>` command icon.
   - In the **Server name or IP** box, type the server name or IP address of the server that you want to add, and then click the `>` command icon.
5 Under Server options, in the TCP port number box, type the TCP port number for the
server or group of servers that you want to add.

The default port number is 8081. The port number must be the same for all servers that
you want to add. The port number and SSL setting must be identical for the console to
communicate with the server.

See “Modifying the port and the communication properties of a server” on page 73.

6 Check Send group settings to apply group settings to the newly added server.

If unchecked, existing server settings are retained, and the future changes that are made
to the server group are applied to the server.

7 Check Install SMSMSE to install Mail Security to the newly added server.

8 Check Keep installation files on server(s) to maintain the installation files on the server.

9 Click OK, and then click Close.

Moving a server to another user-defined server group

You can move a server from one user-defined group to another user-defined group. You can
choose to retain the server's settings or apply the settings of the new group.

If you have already created the user-defined group to which you want to move the server and
you do not want to apply the group's settings, you can move the server by dragging it to the
group.

Use the Move Server window to create a new user-defined group, move multiple servers, or
apply group settings to the newly added server.

To drag a server to another user-defined server group

1 In the console on the toolbar, click Assets.

2 In the Asset Management window, in the Assets list, expand the group that contains the
server that you want to move and the group you want to move the server to, if necessary.

3 Select the server that you want to move and drag it into the new server group.

4 In the confirmation dialog box, click OK.

5 Click Close.

To move a server to another user-defined server group using the Move Server window

1 In the console on the toolbar, click Assets.

2 In the Asset Management window, in the Assets list, expand the group that contains the
server that you want to move and the group you want to move the server to, if necessary.

3 Do one of the following:
   - Select the server that you want to move and under Tasks, click Move server.
Right-click on the server that you want to move, and then click Move server.

4 In the Move Server window, do one of the following:

■ Select the user-defined server group to which you want to add the server.

■ In the Select a group or add a new group box, type the name of a new user-defined server group.

5 Check Send group settings to server to apply the settings of the targeted user-defined server group to the server.

6 Click OK, and then click Close.

See “Synchronizing group settings to a server” on page 70.

**Synchronizing group settings to a server**

Settings on a particular server might not be synchronized with its server group settings. This situation can occur if a server is configured in the server view.

To synchronize group settings to a server

1 In the console on the toolbar, click Assets.

2 In the Asset Management window, under Assets, select the server to which you want to apply group settings.

3 In the sidebar under Tasks, click Send group settings to server.

   This step applies the settings of the server group to the selected server.

4 In the Operation Status window, click Close when the operation is complete.

5 In the Asset Management window, click Close.

See “Modifying or viewing server or server group settings” on page 66.

**Restoring default settings to a server or group**

You can restore all of the settings for a server or group to their initial, default settings. Restoring default settings also deletes any custom content filtering rules, file type filtering rules, match lists, report templates, and scheduled scans that you have created. It does not delete existing reports.

Close and reopen the Mail Security console to see the updated settings.

To restore default settings to a server or group

1 In the console on the toolbar, click Assets.

2 In the Asset Management window, under Assets, select the server in which you want to restore the Mail Security default settings.
3. In the sidebar under **Tasks**, click **Reset to factory defaults**.

4. In the **Reset to factory defaults** confirmation dialog box, click **OK**.

5. In the **Operation Status** window, click **Close** when the operation is complete.

6. In the **Asset Management** window, click **Close**.

See “Modifying or viewing server or server group settings” on page 66.

### Removing a server from group management

Removing a server from group management does not uninstall Mail Security from the server. Mail Security continues to provide protection. However, you can no longer manage a server through the Mail Security console when you remove it from the Global Group.

**To remove a server from group management**

1. In the console on the toolbar, click **Assets**.

2. In the **Asset Management** window, under **Assets**, in the Global Group - Exchange Server list, select one or more servers that you want to remove.

3. In the sidebar under **Tasks**, click **Remove server**.

4. In the confirmation dialog box, click **OK**.

5. Click **Close**.

See “Removing a server group” on page 71.

### Removing a server group

Remove a server group when it is no longer needed. The server group settings are retained on the servers that are in the group until new settings are applied.

If you remove a user-defined server group, the servers that belong to the group can be managed through the Global Group.

---

**Note**: Global Groups cannot be removed.

---

**To remove a server group**

1. In the console on the toolbar, click **Assets**.

2. In the **Asset Management** window, under **Assets**, select the group that you want to remove.

3. In the sidebar under **Tasks**, click **Remove group**.
4 In the confirmation dialog box, click **OK**.

5 Click **Close**.

See “Removing a server from group management” on page 71.

---

**Exporting and importing settings**

Mail Security provides a feature that lets you export the settings for a server or group to .xml file. This feature lets you save the settings as a backup file or import the settings to another computer.

You can view the setting configurations in the console when you import settings. However, the settings are not applied until you deploy them. You can only deploy settings for Symantec Premium AntiSpam if the computer on which you import the settings has a valid Symantec Premium AntiSpam license.

You can only export setting configurations, not data such as items in the event log. Deploy pending changes before you export settings.

---

**Note:** Importing settings file exported from version 7.5 into version 7.9 is not supported.

---

**To export settings**

1 In the console on the toolbar, click **File > Export**.

2 In the confirmation dialog box, click **OK**.

3 In the **Select the file to save exported settings** window, choose the location where you want to save the file.

4 In the **File name** box, type the file name.

5 Click **Save**.

6 In the **Operation Status** window, click **Close** when the operation is complete.

**To import settings**

1 In the console on the toolbar, click **File > Import**.

2 In the confirmation dialog box, click **OK**.

3 In the **Select an SMSE settings file** window, locate the file that you want to import.
To modify the port and the communication properties of a server

1. In the console on the toolbar, click **Assets**.
2. In the **Asset Management** window, under **Assets**, select a server.
3. In the sidebar under **Tasks**, click **Server properties**.
4. In the **Properties** window, in the **Port number** box, type the new port number. The default port number is 8081.
5. Check **Use SSL** to use SSL for communication between the console and server.
6. Click **OK**, and then click **Close**.

Creating and assigning a custom throttling policy to the Mail Security service account user

Microsoft Exchange Server uses client throttling policies to manage the performance of your Exchange organization. Exchange Server tracks the resources that each user consumes and enforces connection bandwidth limits, as necessary.

The Mail Security service account has a default Client Access Server (CAS) throttling policy. However, the bandwidth that is allocated to the default policy parameters is not sufficient in the case of multithreaded manual scanning. You may see degradation in the performance of a manual scan if you use the default throttling policy. Therefore, you must create a custom throttling policy and assign it to the Mail Security service account user.

See “About manual scans” on page 180.
To create and assign a custom throttling policy to the Mail Security service account user

1. Click **Start > Programs > Microsoft Exchange Server server version > Exchange Management Shell**.

2. Type the following command to create the throttling policy and then press **Enter**:

   `New-ThrottlingPolicy -Name <PolicyName> -EWSPercentTimeInAD $null -EWSPercentTimeInMailboxRPC $null -EWSMaxConcurrency $null -EWSMaxSubscriptions $null -EWSPercentTimeInCAS $null`

3. Type the following command to assign the throttling policy to the Mail Security service account user and then press **Enter**:

   `Set-ThrottlingPolicyAssociation -Identity Service Account User Name -ThrottlingPolicy Throttling Policy Name`
Quarantining messages and attachments

This chapter includes the following topics:

- About the quarantine
- Forwarding quarantined items to the Quarantine Server
- Establishing local quarantine thresholds
- Viewing the contents of the local quarantine
- Filtering the quarantined items
- Specifying an action to take when a quarantine threshold is met
- About releasing messages from the local quarantine
- Deleting items from the local quarantine

About the quarantine

Mail Security provides the following options for quarantining messages:

Local quarantine

You can choose to send infected messages and attachments to the local quarantine when you configure Mail Security policies. You can also configure policies to quarantine the messages that trigger violations.

See “Establishing local quarantine thresholds” on page 77.

See “Viewing the contents of the local quarantine” on page 78.

See “Deleting items from the local quarantine” on page 84.
You can forward the infected files that are in the local quarantine to the Symantec Quarantine Server, if it is set up on your network. Mail Security forwards infected files to the Quarantine Server at 60-minute intervals.

Files that are sent to the Quarantine Server are then forwarded to Symantec for analysis in real-time using HTTPS communications. Symantec automatically distributes updated definitions to the Quarantine Server when they are available.

The Quarantine Server is a component of Symantec AntiVirus Central Quarantine. Mail Security supports version 3.4 or later of the Symantec AntiVirus Central Quarantine Server. Version 3.4 is provided with the Mail Security installation package at the following location and must be installed separately:

\ADMTOOLS\DIS

See the Symantec Central Quarantine Administrator's Guide for more information about the Symantec AntiVirus Central Quarantine, which is provided with the installation package at the following location:

\DOCS\DIS\CentQuar.pdf

Note: Files that contain non-viral threats, are unscannable, or violate filtering rules are not forwarded to the Quarantine Server.

Forwarding quarantined items to the Quarantine Server

You can configure Mail Security to forward local quarantine events to the Quarantine Server, if you have the Quarantine Server installed.

You can only forward the events that contain threats to the Quarantine Server.

To forward quarantined items to the Quarantine Server

1. In the console on the primary navigation bar, click Monitors.
2. In the sidebar under Views, click Quarantine Settings.
3. In the content area under Quarantine Server, check Send quarantined items to Quarantine Server.
4. Check Delete local quarantined items after forwarding to Quarantine Server to remove items from the local quarantine.
5. In the Server Address box, type the IP address of the Quarantine Server.
6. In the Server Port box, type the port number for the Quarantine Server.
In the Network Protocol list, click the drop-down menu and select the appropriate network protocol.

On the toolbar, click Deploy changes to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

Establishing local quarantine thresholds

You can specify the thresholds for the local quarantine and how you want Mail Security to respond when a threshold is met.

See “Specifying an action to take when a quarantine threshold is met” on page 80.

When you establish the quarantine thresholds for the local quarantine, you can specify the following limits:

- Maximum number of items
- Maximum size of quarantine
- Retain items in quarantine

To establish local quarantine thresholds

1. In the console on the primary navigation bar, click Monitors.
2. In the sidebar under Views, click Quarantine Settings.
3. In the content area, under Quarantine Thresholds, check Maximum number of items, and then type the maximum number of messages or attachments to retain in the quarantine.
4. To limit the maximum size of the quarantine, do the following:
   - Check Maximum size of quarantine.
     - This item is checked by default.
   - Type the maximum size of the quarantine.
     - The default value is 500.
   - Click the drop-down menu and select MB or GB.
     - The default value is MB.
5. Check Retain items in quarantine to limit how long an item is quarantined, and then type the number of days.
Viewing the contents of the local quarantine

You can view the contents of the local quarantine for a server and server group. For a server group view, quarantined items are consolidated and displayed for last seven days for all the servers.

See “Modifying or viewing server or server group settings” on page 66.

Table 5-1 lists the information that is found in the Quarantine list pane.

### Table 5-1 Quarantined file summary information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time encrypted</td>
<td>The date and time when Mail Security intercepted and encrypted the file.</td>
</tr>
<tr>
<td>Recipient</td>
<td>Intended recipient(s) of the message.</td>
</tr>
<tr>
<td>Sender</td>
<td>Address of the sender of the message.</td>
</tr>
<tr>
<td>Message part</td>
<td>Part of the message that was sent to the quarantine.</td>
</tr>
<tr>
<td>Location</td>
<td>Location where the file was intercepted.</td>
</tr>
<tr>
<td>Rule violated</td>
<td>The policy or the rule that was violated.</td>
</tr>
<tr>
<td>Quarantine Id</td>
<td>The Alpha-numeric identifier that Mail Security assigns to the quarantined file.</td>
</tr>
<tr>
<td>Sent to QServer</td>
<td>Whether the file was sent to the Quarantine Server.</td>
</tr>
</tbody>
</table>

When you select an item in the Quarantine, details about the message (and attachments, if any) appear in the preview pane.

Table 5-2 lists the detailed information that is shown in the preview pane.

### Table 5-2 Quarantined file detailed information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time encrypted</td>
<td>The date and time when Mail Security intercepted and encrypted the file.</td>
</tr>
<tr>
<td>Attachment Name</td>
<td>Name of the attachment that triggered the violation.</td>
</tr>
<tr>
<td></td>
<td>If the message body triggered the violation, this entry is: Message Body.</td>
</tr>
<tr>
<td>Rule violated</td>
<td>The policy or the rule that was violated.</td>
</tr>
<tr>
<td>Location</td>
<td>Location where the file was intercepted.</td>
</tr>
<tr>
<td>Sender</td>
<td>Address of the sender of the message.</td>
</tr>
</tbody>
</table>
Table 5-2  Quarantined file detailed information (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipient(s)</td>
<td>Intended recipient(s) of the message.</td>
</tr>
<tr>
<td>Sent to QServer</td>
<td>Whether the file was sent to the Quarantine Server.</td>
</tr>
<tr>
<td>Virus Name</td>
<td>Name of the virus, if a virus was detected.</td>
</tr>
</tbody>
</table>

To view the contents of the local quarantine

1. In the console on the primary navigation bar, click **Monitors**.
2. In the sidebar under **Views**, click **Quarantine**.
3. In the **list** pane, click an item to view the item’s details.
   The data appears in the **preview** pane.
4. Press **F5** to refresh the display.

**Filtering the quarantined items**

You can view the quarantined items in the group as well as server view. For a sever group view, quarantined items are consolidated and displayed for last seven days for all the servers.
You can use the following filters to filter the items. Use one or multiple filters to narrow down your search.

- Quarantine ID
- Violated rule
- Attachment name
- Item encryption time

To filter the quarantined items

1. In the console on the primary navigation bar, click **Monitors**.
2. In the sidebar under **Views**, click **Quarantine**.
3. In the sidebar under **Tasks**, click **Search Item**.

In the Search Criteria for Quarantine window, use the following filters:

- **Quarantine ID**: Filter the items based on the Quarantine ID.
- **Rule violated**: Type the name of the violated rule to filter the items that are quarantined for the specific rule violation.
- **Message part (Attachment name)**: Filter the items based on the attachment name.
- **Time encrypted**: Select the option and specify the date range to filter the items that are quarantined (encrypted) during the specified period.

**Note**: You can type the complete filter name or part of the filter name (literal string) to filter the items. Regular expression and wildcard expression search is not supported.

To clear the search results on the page, in the sidebar under Tasks, click Clear Search.

### Specifying an action to take when a quarantine threshold is met

You can define thresholds for the local quarantine and specify the actions that you want Mail Security to take when a quarantine threshold is met.

See “Establishing local quarantine thresholds” on page 77.

You can specify any of the following actions:

- **Notify Administrator**: Sends a notification message to the administrator when a threshold is met. This item is checked by default.
- **Notify others**: Sends a notification to the other recipients that you specify when a threshold is met.
- **Delete oldest items**: Removes the oldest items in the local quarantine when a threshold is met.

To specify an action to take when a quarantine threshold is met

1. In the console on the primary navigation bar, click Monitors
2. In the sidebar under Views, click Quarantine Settings
3 Under **When a threshold is met**, check **Notify Administrator** to send notification messages to the administrator.

See “Configuring notification settings for scan violations” on page 192.

4 Check **Notify others** to send notification messages to additional people.

5 In the **Notify others** box, type the email addresses of the people to whom you want Mail Security to send notifications.

Separate email addresses with commas.

6 Check **Delete oldest items** to remove the items that reach a threshold.

This option is not enabled by default.

If **Delete oldest items** is not checked and a quarantine size threshold is reached, the event is logged. Mail Security sends a notification to the recipients that are specified on the **Quarantine Settings** page.

7 Under **Administrator Notification**, in the **Subject Line** box, type your subject line text.

The default text is: Administrator Alert: The Symantec Mail Security Quarantine has exceeded a set limit.

8 In the **Message Body** box, type the administrator notification message body.

The default text is: You should manage the Quarantine to remove files or change the Quarantine settings. Details: %details%.

You can use variables in the message body.

See “Alert and notification variables” on page 238.

9 On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

---

**About releasing messages from the local quarantine**

You can release messages from the local quarantine in the following ways:

- Release messages by email
  See “Releasing messages from the local quarantine by email” on page 82.

- Release messages to a file
  See “Releasing messages from the local quarantine to a file” on page 83.
Note: By default, Mail Security version 7.5 and later do not re-scan the items that are quarantined due to antivirus and file filtering violations, once they are released. However, if the items are quarantined due to content filtering violations, Mail Security scans these items only for virus policies and file filtering conditions. This behavior is configurable through registry.

Messages that are released from the quarantine are not filtered for spam and filtering rules.

Releasing messages from the local quarantine by email

You can send quarantined files to specified destinations by email. When you release a file from the quarantine by email, you remove it from the quarantine.

The released email is then sent with revised sender information to the recipients that are specified in the to box. Rather than being sent from the original sender's email address, it is sent from the email account that you specify on the Notification Settings page. The email is not delivered to the recipients that are specified in the cc or bc boxes.

If Mail Security releases an email by taking the Quarantine entire message and replace with text action, then the email contains the original message in the .msg format as an attachment.

See "Configuring notification settings for scan violations" on page 192.

To release messages from the local quarantine by email

1 In the console on the primary navigation bar, click Monitors.

2 In the sidebar under Views, click Quarantine.

   This option is not available in the group view.

3 Do one of the following:
   ■ In the sidebar under Tasks, click Select all to select all of the items in the quarantine.
   ■ In the list pane under Quarantine, select the items that you want to release.

   To select multiple items, press CTRL and select the items that you want to release.

   To unselect all of the selected items, in the sidebar under Tasks, click Deselect all.

4 In the sidebar under Tasks, click Release by mail.
5 In the **Releasing item(s) by mail** window, select from the mail options that Mail Security provides.

Mail Security provides the following mail options:

- **Send to original intended recipient(s)**
  Sends the message to the original intended recipient(s).

- **Send to administrators**
  Sends the message to administrators.
  List administrators' email addresses in the Administrators box. Separate multiple email addresses with commas.

- **Send to the following**
  Sends the message to alternate recipients.
  List recipients' email addresses one per line in the Alternate recipients box.

6 Click **OK**.

7 In the **Operation Status** window, click **Close** when the operation is complete.

---

**Releasing messages from the local quarantine to a file**

You can move quarantined messages to a folder for review or analysis. The folder is in the following location:

\Program Files\Symantec\SMSMSE\7.9\Server\Quarantine\Release

The file location cannot be modified.

Messages that Mail Security quarantines by taking the **Quarantine entire message and replace with text** action are saved at this location in the .msg format.

See “Releasing messages from the local quarantine by email” on page 82.

**To release messages from the local quarantine to a file**

1 In the console on the primary navigation bar, click **Monitors**.

2 Under **Views**, click **Quarantine**.
   
   This option is not available in group view.

3 Do one of the following:
   - In the sidebar under **Tasks**, click **Select all** to select all of the items in the quarantine.
   - In the **list** pane under **Quarantine**, select the items that you want to release.

   To select multiple items, press **CTRL** and select the items that you want to release.
   To unselect all of the selected items, in the sidebar under **Tasks**, click **Deselect all**.
In the sidebar under **Tasks**, click **Release to file (Save)**.

In the **Releasing to file and delete** dialog box, select one of the following options:

- **Yes** Removes the item from the quarantine after it has been saved to the Release folder
- **No** Keeps the item in the quarantine after it has been saved to the Release folder
- **Cancel** Cancels the file release operation

In the **confirmation** dialog box, click **OK**.

In the **Operation Status** window, click **Close** when the operation is complete.

## Deleting items from the local quarantine

You can delete one or more items from the quarantine at a time.

See “About releasing messages from the local quarantine” on page 81.

**To delete items from the local quarantine**

1. In the console on the primary navigation bar, click **Monitors**.
2. In the sidebar under **Views**, click **Quarantine**.
3. Do one of the following:
   - In the sidebar under **Tasks**, click **Select all** to select all of the items in the quarantine.
   - In the list pane under **Quarantine**, select the items that you want to remove.
     To select multiple items, press **CTRL** and select the items that you want to delete. To unselect all of the selected items, in the sidebar under **Tasks**, click **Deselect all**.
4. In the sidebar under **Tasks**, click **Delete**.
Protecting your server from risks

This chapter includes the following topics:

- About Mail Security policies
- About protecting your server from risks
- Configuring a threat detection
- Configuring a security risk detection
- Configuring file scanning limits
- Configuring rules to address unscannable and encrypted files
- Remediation overview
- How remediation works
- Configuring remediation options
- Types of Remediation
- Remediation feed settings
- Creating an email remediation feed
- Enabling authentication key
- Managing certificates
- About file reputation
About Mail Security policies

Mail Security scans email messages and their attachments for violations to policies. A policy is a set of rules that are designed to detect potential risks to your Microsoft Exchange mail system.

Mail Security contains the following policies:

- **General**: Contains the rules controlling scanning limits, exceptions, and outbreak management.
- **Antivirus**: Contains the rules for detecting threats in messages and attachments with viruses, virus-like characteristics, or security risks, such as adware or spyware.
- **Antispam**: Contains the rules for the following:
  - Detect spam.
  - Allow specified senders to bypass antispam scanning.
  - Specify the recipients whose email messages are not scanned for spam.
- **Content Enforcement**: Contains the rules to filter inappropriate content in message bodies and attachments. Also contains file filtering rules and match the lists that let you detect and block messages by file name and file type.

See “About protecting your server from risks” on page 86.


About protecting your server from risks

Mail Security can detect risks in all major file types (for example, Windows®, DOS, Microsoft® Office Word, and Microsoft® Office Excel files).

Table 6-1 describes the risks against which Mail Security protects your Exchange server.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats</td>
<td>Mail Security detects viruses, worms, and Trojan horses in all major file types.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring a threat detection” on page 88.</td>
</tr>
</tbody>
</table>
Table 6-1  Risks that can threaten your Exchange server (continued)

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mass-mailer worms</td>
<td>Mail Security detects that an email message is a mass-mailer worm. It automatically deletes the infected email message and any attachments.</td>
</tr>
<tr>
<td>Denial-of-service attacks</td>
<td>Mail Security protects your network from the file attachments that can overload the system and cause denial-of-service attacks. The attachments include the container files that are overly large. They contain large numbers of embedded, compressed files or are designed to maliciously use resources and degrade performance. You can impose limits to control how Mail Security handles container files to reduce your exposure to denial-of-service threats. See &quot;Configuring file scanning limits&quot; on page 94.</td>
</tr>
<tr>
<td>Security risks</td>
<td>Mail Security detects security risks, such as adware, dialers, hacking tools, joke programs, remote access programs, spyware, and trackware.</td>
</tr>
<tr>
<td></td>
<td>See &quot;Configuring a security risk detection&quot; on page 91.</td>
</tr>
</tbody>
</table>

Mail Security also helps you detect and block other potential risks from entering your network, such as unscannable and encrypted container files.

See "Configuring rules to address unscannable and encrypted files" on page 95.

When a risk is detected, the incident is logged to the locations that you specify. You can also configure Mail Security to issue alerts when risks are detected or when an outbreak occurs.

See “About logging events” on page 203.

See "About outbreak management" on page 193.

How Mail Security detects risks

Mail Security uses the following tools to detect risks:

Definitions  Symantec engineers track reported outbreaks of threats (such as viruses, Trojan horses, worms) to identify new threats. After a threat is identified, information about the threat (a signature) is stored in a definition file. This file contains information to detect and eliminate the threat. Mail Security searches for these signatures when it scans for threats.
Mail Security uses Symantec Bloodhound heuristics technology to scan for threats for which no known definitions exist. Bloodhound heuristics technology scans for unusual behavior such as self-replication to target potentially infected message bodies and attachments. Bloodhound technology is capable of detecting upwards of 80 percent of new and unknown executable file threats.

Bloodhound-Macro technology detects and repairs over 90 percent of new and unknown macro viruses. Bloodhound requires minimal overhead since it examines only message bodies and the attachments that meet stringent prerequisites. In most cases, Bloodhound can determine in microseconds whether a message or attachment is likely to be infected. If it determines that a file is not likely to be infected, it moves to the next file.

Mail Security contains a decomposer that extracts container files so that they can be scanned for risks. The decomposer attempts to extract container files until it reaches the base file or until it reaches its extraction limit. If the decomposer reaches the set limit before the base file is reached, the scanning process stops. Mail Security then logs the violation to the specified logging destinations, and the file is handled according to the Unscannable File Rule.

See “About protecting your server from risks” on page 86.

Configuring a threat detection

To configure threat detection, do the following:

Enable threat detection scanning  
Mail Security detects viruses, worms, and Trojan horses in all major file types. Antivirus scanning must be enabled for Mail Security to detect threats. Threat detection scanning applies to all types of scans. See “About the types of scanning that you can perform” on page 169.

Set the Bloodhound Detection level  
Mail Security uses Bloodhound technology to supplement the detection of threats by signature.

You can customize your level of protection against new threats, from zero protection to a high level of protection. A high level of protection increases protection of your network; however, server performance might be affected. At lower levels of protection, an unknown threat might escape detection, but the trade-off with server performance decreases. In most cases, the default (Medium) setting is appropriate.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable mass-mailer</td>
<td>Mail Security detects that an email message is a mass-mailer worm or virus when this feature is enabled. If Mail Security detects that an email message is a mass-mailer worm or virus, it deletes the infected email message and any attachments. Mail Security does not send notifications after deleting a mass-mailer worm or virus message and any attachments. When the mass-mailer detection feature is not enabled, an infected mass-mailer email message is treated the same as an infected message.</td>
</tr>
<tr>
<td>worm-infected message</td>
<td></td>
</tr>
<tr>
<td>detection</td>
<td></td>
</tr>
<tr>
<td>Enable advanced heuristics</td>
<td>Mail Security provides a better antivirus protection if you enable the <strong>Advanced heuristics detection</strong> check box.</td>
</tr>
<tr>
<td>detection</td>
<td></td>
</tr>
<tr>
<td>Modify default threat</td>
<td>Mail Security provides default antivirus rules, which are always enabled. You can modify these rules.</td>
</tr>
<tr>
<td>detection rules, as needed</td>
<td></td>
</tr>
</tbody>
</table>

**To configure a threat detection**

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Antivirus**, click **Antivirus Settings**.
3. In the content area under **Antivirus Settings**, check **Enable virus scanning**. Virus scanning is enabled by default.
4. In the **Bloodhound Detection** list, select one of the following using the drop-down menu:
   - **Off** Disables the Bloodhound Detection.
   - **Low** Optimizes the server performance, but might not detect potential threats.
   - **Medium** Provides a balance between threat detection and server performance. The default setting is Medium.
   - **High** Increases the detection of threats, but might affect server performance.
5. Check **Delete mass-mailer worm-infected messages (no notifications)** to automatically delete mass-mailer messages. This feature is enabled by default.
6 In the **Rules** table, select any of the following rules to view or modify them in the preview pane:

- **Basic Virus Rule**: Applies to the messages or the attachments that contain repairable threats.
  - This option is always enabled.

- **Unrepairable Virus Rule**: Applies to the messages or the attachments that contain the threats that cannot be repaired.
  - This option is always enabled.

- **Security Risk Rule**: Applies to messages that contain security risks, such as adware or spyware.
  - See “Configuring a security risk detection” on page 91.
  - This option is enabled by default.

The settings for the rule that you select appear in the preview pane.

7 In the preview pane, in the **Action to take** list, select the action to take when a threat is detected using the drop-down menu.

8 In the **Replacement text** box, type your customized message if you want to replace the message or the attachment body with a text message.

   The default text is: Symantec Mail Security replaced %attachment% with this text message.
   The original file contained %violation% and was %action%.

   You can use variables in your customized text.

   See “Alert and notification variables” on page 238.

9 Check one or more of the following to send email notifications about the detection:

- **Notify administrators**.
  - Click the down arrow and type your customized text in the **Subject line** box and the **Message body** box. The default Subject line and Message body text is as follows:
  - Default subject line text: Administrator Alert: Symantec Mail Security detected %violation%
  - Default message body text: Location of the infected item: %location% Sender of the infected item: %sender% Subject of the message: %subject% The attachment(s) "%attachment%" was %action% for the following reasons: %information% This was done due to the following Symantec Mail Security settings: Scan: %scan% Rule: %rule%

- **Notify internal sender**.
Click the down arrow and type your customized text in the **Subject line** box and the **Message body** box. The default Subject line and Message body text is as follows:

- Default subject line text: Symantec Mail Security detected %violation% in a message that is sent from your address
- Default message body text: %subject% Recipient of the message: %recipient%
- Notify external sender.

Click the down arrow and type your customized text in the **Subject line** box and the **Message body** box. The default Subject line and Message body text is as follows:

- Default subject line text: Symantec Mail Security detected %violation% in a message that is sent from your address
- Default message body text: Subject of the message: %subject% Recipient of the message: %recipient%

10  On the toolbar, click **Deploy changes** to apply your changes.

See "Deploying settings and changes to a server or group" on page 60.

### Configuring a security risk detection

Mail Security can detect security risks. Security risks are the programs that do any of the following:

- Provide unauthorized access to computer
- Compromise data integrity, privacy, confidentiality, or security
- Present some type of disruption or nuisance

These programs can put your employees and your organization at risk for the following:

- Identity theft or fraud by logging keystrokes
- Capture of email and instant messaging traffic
- Theft of personal information such as passwords and logon identifications

Security risks can be introduced into your computer unknowingly. This risk can occur when users visit a website, download shareware, or freeware software programs, click links or attachments in email messages, or through instant messaging clients. A program can also be installed after or as a by-product of accepting an End User License Agreement from another software program that is related to the security risk.

Enable **Security Risk Rule** for Mail Security to detect security risks.

**Table 6-2** lists the categories of security risks that Mail Security detects.
### Table 6-2 Security risk categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware</td>
<td>The standalone or appended programs that gather personal information through the Internet and relay it back to a remote computer without the user's knowledge. Adware might monitor browsing habits for advertising purposes. It can also deliver the advertising content.</td>
</tr>
<tr>
<td>Hack tools</td>
<td>Programs that are used to gain unauthorized access to a user's computer. For example, a keystroke logger tracks and records individual keystrokes and sends this information to a remote computer. The remote user can perform port scans or vulnerability scans. Hack tools might also be used to create viruses.</td>
</tr>
<tr>
<td>Dialers</td>
<td>Programs that use a computer, without the user's permission or knowledge, to dial through the Internet to a 900 number or FTP site. Dialers typically to accrue charges.</td>
</tr>
<tr>
<td>Joke programs</td>
<td>Programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or bothersome. For example, a joke program might move the Recycling Bin away from the mouse when the user tries to click on it.</td>
</tr>
<tr>
<td>Remote access programs</td>
<td>Programs that let a remote user gain access to a computer over the Internet to gain information from, attack, or alter the host computer.</td>
</tr>
<tr>
<td>Spyware</td>
<td>The standalone programs that can secretly monitor computer activity and detect passwords and other confidential information. Spyware can then relay the information back to a remote computer.</td>
</tr>
<tr>
<td>Trackware</td>
<td>The standalone or appended applications that trace a user's path on the Internet and relay the information to a remote computer.</td>
</tr>
</tbody>
</table>

**To configure a security risk detection**

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Antivirus**, click **Antivirus Settings**.
3. In the content area, in the **Rules** table, on the **Security Risk Rule** row, click the box under the **Status** column. Then select **Enabled** from the drop-down menu.
   This rule is enabled by default.
4. In the preview pane, in the **Action to take** list, use the drop-down menu to select the action to take when a security risk is detected.
5 In the **Replacement text** box, type your customized message if you want to replace the message or the attachment body with a text message.

The default text is: Symantec Mail Security replaced %attachment% with this text message. The original file contained %violation% and was %action%.

You can use variables in your customized text.

See “Alert and notification variables” on page 238.

6 Check one or more of the following to send email notifications about the detection:

- **Notify administrators.**
  
  Click the down arrow and type your customized text in the **Subject line** box and the **Message body** box. The default Subject line and Message body text is as follows:

  - Default subject line text: Administrator Alert: Symantec Mail Security detected %violation%
  
  - Default message body text: Location of the infected item: %location% Sender of the infected item: %sender% Subject of the message: %subject% The attachment(s) "%attachment%" was %action% for the following reasons: %information% This was done due to the following Symantec Mail Security settings: Scan: %scan% Rule: %rule%

- **Notify internal sender.**
  
  Click the down arrow and type your customized text in the **Subject line** box and the **Message body** box. The default Subject line and Message body text is as follows:

  - Default subject line text: Symantec Mail Security detected %violation% in a message that is sent from your address
  
  - Default message body text: %subject% Recipient of the message: %recipient%

- **Notify external sender.**
  
  Click the down arrow and type your customized text in the **Subject line** box and the **Message body** box. The default Subject line and Message body text is as follows:

  - Default subject line text: Symantec Mail Security detected %violation% in a message that is sent from your address
  
  - Default message body text: Subject of the message: %subject% Recipient of the message: %recipient%

7 On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.
Configuring file scanning limits

Mail Security imposes limits on file extraction. These limits protect against denial-of-service attacks that are associated with the overly large or the complex container files that take a long time to decompose. These limits also enhance scanning performance.

Mail Security contains a decomposer that extracts container files so that they can be scanned for risks. The decomposer continues to extract container files until it reaches the base file. When a container file reaches a set limit, the scanning process stops. The violation is logged to the specified logging destinations, and the file is handled according to Unscannable File Rule.

See “Configuring rules to address unscannable and encrypted files” on page 95.

To configure file scanning limits

1. In the console on the primary navigation bar, click Policies.

2. In the sidebar under General, click Scanning Limits.

3. In the content area, in the Maximum scan time (in seconds) box, type the maximum time that Mail Security can spend extracting a single container file.

   You can enter a value from 20 to 500000. The default value is 300.

4. In the Maximum archive scan depth (number of levels) box, type the maximum number of nested levels of files that are decomposed within a container file.

   You can enter a value from 1 to 50. The default value is 10.

5. In the Maximum size of one extracted file (in MB) box, type the maximum file size, in megabytes, for individual files in a container file.

   You can enter a value from 1 to 1024. The default value is 100.

6. In the Maximum total size of all extracted files (in MB) box, type the maximum size, in megabytes, of all extracted files.

   You can enter a value from 1 to 1024. The default value is 200.

7. In the Maximum number of files extracted box, type the maximum allowable number of files to be extracted.

   You can enter a value from 1 to 1000000. The default value is 5000.

8. On the toolbar, click Deploy changes to apply your changes.

   See “Deploying settings and changes to a server or group” on page 60.
## Configuring rules to address unscannable and encrypted files

A file that cannot be scanned can put your network at risk if it contains a threat. Mail Security provides the following default rules to address unscannable and encrypted files:

### UFR - Scanning Limits (Unscannable File Rule for Scanning Limits)
This rule gets triggered when any of the scanning limits are violated. You can set the scanning limits under the Policies > Scanning Limits workspace.

The default action for the Unscannable File Rule for Scanning Limits is Quarantine entire message and replace with text (By part for Store).

### UFR - Malformed Files (Unscannable File Rule for Malformed Files)
This rule gets triggered when Mail Security does not recognize the file format of a specific file and is unable to scan it. In such cases, the file is treated as Malformed.

The default action for the Unscannable File Rule for Malformed Files is Quarantine entire message and replace with text (By part for Store).

### Encrypted File Rule
Infected files can be intentionally encrypted. Encrypted files cannot be decrypted and scanned without the appropriate decryption tool. You can configure how you want Mail Security to process encrypted container files to protect your network from threats.

The default setting for the Encrypted File Rule is to log the violation only.

These rules are always enabled.

### To configure rules to address unscannable and encrypted files

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **General**, click **Exceptions**.
3. In the **Exceptions** table, select one of the following rules that you want to view or modify:
   - UFR - Scanning Limits
   - UFR - Malformed Files
   - Encrypted File Rule
4. In the preview pane, in the **Action to take** list, use the drop-down menu to select the action to take when a violation is detected.
5 In the **Replacement text** box, type your customized message if you want to replace the message or the attachment body with a text message.

The default text is: Symantec Mail Security replaced %attachment% with this text message. The original file was unscannable and was %action%.

You can use variables in your customized text.

See “Alert and notification variables” on page 238.

6 Check the option **Enable list of trusted domains or users** if you want to enter a list of domains or email addresses.

For each of the three rules, you can enter a list of trusted domains or users. You can set different actions for these trusted domains or users.

7 From the **Action to take** drop-down menu, select an action that you want to take on the list of trusted domains or users.

8 In the **Replacement text** box, type your customized message if you want to replace the message or the attachment body with a text message.

The default text is: Symantec Mail Security replaced %attachment% with this text message. The original file was unscannable and was %action%.

9 Check one or more of the following to send email notifications about the detection:

- Notify administrators.
  
  Click the down arrow and then type your customized text in the **Subject line** box and the **Message body** box. The default Subject line and Message body text is as follows:

  - Default subject line text: Administrator Alert: Symantec Mail Security detected a message with an unscannable attachment or body
  
  - Default message body text: Location of the message: %location% Sender of the message: %sender% Subject of the message %subject% The attachment(s) "%attachment%" was %action%. This action was done due to the following Symantec Mail Security settings: Scan: %scan% Rule: %rule%

- Notify Trusted Domain: Send the email notification to administrator. When the checkbox is cleared, the email notification is not sent. By default, this is enabled.

- Notify internal sender.
  
  Click the down arrow and then type your customized text in the **Subject line** box and the **Message body** box. The default Subject line and Message body text is as follows:

  - Default subject line text: Symantec Mail Security detected unscannable content in a message that is sent from your address
  
  - Default message body text: Subject of the message: %subject% Recipient of the message %recipient%
Notify Trusted Domain: Send the email notification to sender. By default, this is enabled.
When the checkbox is cleared, the email notification is not sent.

- Notify external sender.
  Click the down arrow and then type your customized text in the Subject line box and the Message body box. The default Subject line and Message body text is as follows:
  
  ■ Default subject line text: Symantec Mail Security detected unscannable content in a message that is sent from your address
  
  ■ Default message body text: Subject of the message: %subject% Recipient of the message %recipient%

- Notify Trusted Domain: Send the email notification to sender. By default, this is enabled.
  When the checkbox is cleared, the email notification is not sent.

10 On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

Registry keys can be used to bypass actions on unscannable malformed files. For more information refer the Mail Security Knowledge Base.

**Remediation overview**

Symantec Mail Security for Microsoft Exchange has been enriched with a new fully-automated remediation feature to protect exchange mailboxes against known email threats. This feature lets you auto-remEDIATE threats inside your mailboxes based on the email feeds. The email feeds contain information about the location of the email threat and the action to be taken. Mail Security enables Symantec or third-party products to automatically initiate remediation over secure, email-based communication channel. On the Remediation settings page, you can specify detailed configuration, such as the remediation mode – Sent items folder or Deep discovery and clean-up.

Following are the remediation categories:

- In **Internal Remediation**, the Mail security generates the email feeds.

- In **External Remediation**, other Symantec products or third-party products generate the email feeds.

---

**Note:** This feature is not supported on the Edge Transport role.

Once the remediation feature is configured and enabled, Mail Security handles the remediation requests automatically for the whole organization.
Remediation aims to address the following issues by searching for threats in one or more mailboxes of your organization and sanitize them.

- Copies of email threats residing in the sent items folder.
- Delayed detection and remediation of malware poses risk.
- Day zero threats which can quickly proliferate making it difficult to remediate.

See “How remediation works” on page 98.

See “Configuring remediation options” on page 99.

See “Types of Remediation” on page 99.

**How remediation works**

Mail Security remediation requires a dedicated mailbox to be configured to receive remediation email feeds (remediation requests). Mail security now hosts a new component that is called the Remediation handler which continuously monitors the configured mailbox for the remediation feeds. The email feeds for remediation can be issued by Mail Security, other Symantec products, or third-party products. The email feeds are in well-defined format and can be **Message ID** based or **File Hash** based. On receiving the email feed, the remediation handler validates the feed settings and remediates the threats inside mailbox and quarantines the email or file immediately.

**Note:** Remediation search scope does not include public folders in your mailbox.

See “Remediation overview” on page 97.
Configuring remediation options

To configure remediation options
1. Go to Monitors > Remediation Settings.
2. Check Enable Remediation.
3. Select a feed validation setting. See “Remediation feed settings” on page 99.
4. Select the action to be taken after receiving a remediation request.
5. Press Deploy Changes.

See “Types of Remediation” on page 99.

Types of Remediation

You can remediate threats present in a single mailbox or all the mailboxes across organization and clean all possible threat trails. Mail Security searches data in the mailbox for last 24 hours.

- **Sent Items Remediation Only**
  In this mode, only the Sent Items folder of the sender’s mailbox is searched for email threats.
  For example, If email with malicious attachment is sent, Mail Security scans and cleans the email and forwards the email to the intended recipient. But, a copy of the sent email is saved in the sent items folder containing the malicious attachment. The sent items are never scanned and can pose a risk which can proliferate across other mailboxes. In this scenario, you might want to use the sent items remediation to sanitize the sent items folder.

- **Deep discovery and Clean-up**
  The scope of Sent Item remediation is limited only to the sender’s mailbox. But, if you want to remediate threats across the organization, this remediation type is useful. In deep discovery and clean-up, the threat is searched with the attachment hash and all the emails for which the hash matches are quarantined. The deep discovery and clean-up remediation type generate multiple quarantine entries.
  See “Viewing the contents of the local quarantine” on page 78.

See “Configuring remediation options” on page 99.

See “Remediation feed settings” on page 99.

Remediation feed settings

- **Manually move feeds to mailbox folder**
  This option requires you to configure a separate folder at the root level which is parallel to the Inbox folder in your mailbox. The email feeds arrives in the Inbox folder. The
administrator has to select and move the email feeds from the Inbox folder to the newly configured folder for remediation. Once the remediation feed arrives, the remediation handler picks up the feed and starts processing it.

If you want to create your own remediation email feed, See “Creating an email remediation feed” on page 100.

- **Certificate based auto validation** (Symantec Recommended)
  This option provides the highest level of security by verifying and authenticating the validity of the sender. It requires you to install digital certificate on all the servers where Mail Security is installed. You can also use self-signed certificate for validation purpose.
  Once you have installed the certificate, you must specify the **Certificate Subject (CN=)** and **Certificate Serial Number** in **Remediation Setting > Feed Validation Settings > Certificate based auto validation**.
  After certificate validation, the email feed is consumed for processing else the email feed is ignored.
  See “Managing certificates” on page 102.

- **Custom auto Validation** (Default option)
  Use this option to create a list of valid senders of the feeds. Any email that arrives apart from the configured list of senders is discarded.
  For an additional layer of secure connection, you can enable the auth key. Once you enable the authentication key, both sender email ID and auth key is used for validation purpose.
  To enable auth key, See “Enabling authentication key” on page 102.

See “Configuring remediation options” on page 99.

### Creating an email remediation feed

You can create your own email remediation feed if you want to remediate a known threat.

- Create an email in the plain-text format.

- In the email body, create remediation feed entries in the following format:
  - For file hash-based remediation feed: `<Parameters> = <File Hash Remediation Request>`
  - For message ID-based remediation feed: `<Parameters> = <Message ID Hash Remediation Request>`

Use the following table to refer to the parameters.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
<th>File Hash Remediation Request values</th>
<th>Message ID Remediation Request values</th>
</tr>
</thead>
<tbody>
<tr>
<td>rem_requesttype</td>
<td>Mandatory</td>
<td>[value=file_hash]</td>
<td>[value=message_id]</td>
</tr>
<tr>
<td>rem_key</td>
<td>Mandatory</td>
<td>[value=base64 encoded SHA2]</td>
<td>[value=Internet Message ID]</td>
</tr>
<tr>
<td>rem_scope_mailboxes</td>
<td>Optional, Default All Mailboxes</td>
<td>[value=mailbox1;mailbox2]</td>
<td>[value=mailbox1;mailbox2]</td>
</tr>
<tr>
<td>rem_scope_last_n_hours</td>
<td>Optional, Default last 24 hrs</td>
<td>[value=N]</td>
<td>[value=N]</td>
</tr>
</tbody>
</table>

Supported request types are: file_hash and message_id. A remediation request can either be file_hash or message_id based.

To narrow down search, the scope parameter is used. If you want to search multiple mailboxes, you can specify multiple mailboxes that are separated by a semicolon.

For example,
```
rem_scope_mailboxes=user1@xyz.com;user2@xyz.com
```

Remediation search scope for the emails that arrived in last N hours.

For example,
```
rem_scope_last_n_hours=24
```

**Sample file hash remediation request**
```
rem_requesttype=file_hash
rem_key=iz8ZGBmTHR8s73KJI5tfd8ALB5hHucJjblaFTR5e/3E=
rem_scope_last_n_hours=24
```

**Sample message ID remediation request**
```
rem_requesttype=message_id
rem_key=<1518536193415.4087@smsauto.lab >
rem_scope_mailboxes=user.test1@smsauto.lab;user.test2@smsauto.lab
rem_scope_last_n_hours=24
```

See "Remediation feed settings" on page 99.
Enabling authentication key

You can enable the auth key to enable enhanced security for the Custom Validation feed setting.

To enable auth key

1. If Console-Server SSL mode is not enabled, you must enable the default security key. You can create your own passkey to modify the default security key that is used by Mail Security.

To create your own passkey

Run the Passkey tool. Make sure that you run the passkey tool on all the servers where Mail security is installed and specify the same passkey.

You can find the Passkey tool in the Mail Security installation directory:

- **For Server-based Installation:** C:\Program Files\Symantec\SMSMSE\7.9\Server\Config
- **For Console Only Installation:** C:\Program Files\Symantec\CMaF\7.9\bin\Products\SMSMSE\7.9

2. Enable Auth key.

3. Specify a new passkey. The new passkey overrides the default encryption key that is used by the Mail security.

See “Remediation feed settings” on page 99.

Managing certificates

For certificate-based validation feed setting, you must install a self-signed certificate or a third-party certificate. The certificate must be installed in the local machine store and the current user store.

You can create a self-signed certificate by using the Visual Studio tools command line.

For example, to create a 'emailsinging.pfx' certificate, use the following commands:

```
C:\Program Files (x86)\Microsoft Visual Studio 11.0\VC>makecert -r -pe -n "CN=emailsinging" -sky exchange "emailsinging.cer" -sv "emailsinging.pvk"
```

```
C:\Program Files (x86)\Microsoft Visual Studio 11.0\VC>pvk2pfx -pvk "emailsinging.pvk" -spc "emailsinging.cer" -pfx "emailsinging.pfx" -pi Password123
```
To install certificate in the local machine store and current user store

1. Install certificate in the user personal store: Certificates- Current user > Personal > Certificate.

2. Install certificate in local machine store: Certificates (Local Computer) > Personal > Certificate. While installing the certificate, make sure to enable Mark this key as exportable. Also, give full permissions to the Network Service in the certificate. To do this, select the certificate, All Tasks > Manage Private keys....

3. Repeat steps 1 and 2 on all the servers where Mail Security is installed.

4. After installing the certificate, specify the certificate serial number and subject in the Remediation Setting > Feed Settings > Certificate based validation.

You can configure additional validation for certificates where you want to assign certain certificate for remediation feature. This may be required in case multiple certificates are installed on different exchange servers. Instead of validating the certificate generically from certificate store, you can add extra validation by providing certificate information. In this case, if certificate is not found in the list, the validation fails.

If the list is configured and certificate is found in the list, the validation process validates the certificate from the store. If the file RemediationTrustedCert.txt does not exist or empty, the certificate validation happens from the certificate store.

To configure the certificate list

1. Go to the installation directory.

2. Create a text file RemediationTrustedCert.txt in the etc folder.

   <InstallDir>\SMSMSE\7.9\Server\etc\RemediationTrustedCert.txt

3. Type issuer name that is followed by comma and the serial number. Type one entry per line if you have multiple certificates.

   For example, CN=Remediation, f00000087974e880405f414e8x4fxx7

See "Remediation feed settings" on page 99.

About file reputation

File reputation is a file-based detection technology that classifies files as good or bad by examining properties, usage patterns, or users of a given file rather than scanning it. Insight-based security puts files in context, using their age, frequency, location, and more to expose threats otherwise missed.

File reputation provides reputation information for only Portable Executable (PE) files.
Identifying spam

This chapter includes the following topics:

- About spam detection
- About reputation technology
- Configuring whitelists
- How to detect spam using Symantec Premium AntiSpam

About spam detection

Mail Security protects your servers from unwanted email messages, such as spam. Spam is usually defined as junk or unsolicited email from a third party. The spam message sender has no discernible relationship with all or some of the message recipients. Often, the message headers are forged or altered to conceal the origination point of the sender. Spam is not only an annoyance to users and administrators, it is also a serious security concern. Spam can be used to deliver viruses, Trojan horses, and in phishing attempts. High volume of spam can create denial-of-service conditions in which mail servers are so overloaded that legitimate email and network traffic cannot get through. Mail Security can detect if an incoming email message is spam with a high level of accuracy.

You can adjust antispam detection by specifying the domains that are automatically permitted to bypass antispam scanning.

See “Configuring whitelists” on page 105.

Spam detection is only available on Mail Security when it is installed on Exchange server 2010 transport role, Exchange 2013 Mailbox role and above, and on Edge role of all Exchange versions.

You must have a valid Symantec Premium AntiSpam license to enable Symantec Premium AntiSpam.

See “About licensing” on page 53.
About reputation technology

Symantec monitors number of email sources to determine how much email is sent from these addresses is legitimate and how much is spam. By evaluating the sender according to dimensions such as mail volume, the percentage of spam sent, and a variety of vulnerabilities, the Sender IP reputation service and DNS IP reputation service creates a reputation profile for a given IP address. Email from these email sources can then be blocked or allowed based on the reputation value of the source that Symantec determines.

Configuring whitelists

You can enable and populate the following whitelists to minimize false positives:

- **Allowed Senders**: Lets you list the sender domains that are permitted to bypass antispam scanning
- **Unfiltered Recipients**: Lets you list the email addresses to which inbound emails are permitted to bypass antispam scanning

If the Allowed Senders and Unfiltered Recipients lists are both enabled, Mail Security processes the Allowed Senders list first.

Email messages that are permitted to bypass antispam scanning are still scanned for risks and file filtering violations.

To configure whitelists

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Antispam**, click **Whitelist**.
3. In the content area, under **Allowed Senders**, check **Bypass spam detection for messages sent from the following**.
4. In the **Email and domain addresses** box, type the domains and email addresses (one per line) that are permitted to bypass spam detection.
   
   Domain names must begin with either @ (at symbol) or an asterisk before the at symbol (for example, @mail.com or *@mail.com).
   
   You can use DOS wildcard characters.
   
   See "About DOS wildcard style expressions" on page 159.
5. Under **Unfiltered Recipients List**, check **Bypass spam detection for messages sent to the following**.
6. In the **Fully qualified email addresses** box, type the fully qualified email addresses (one per line) to which email messages are permitted to bypass spam detection. You can list up to 50 email addresses.

7. On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

How to detect spam using Symantec Premium AntiSpam

Symantec Premium AntiSpam provides continuous updates to the premium antispam filters to ensure that your Exchange server has the most current spam detection filters. Updates to the premium antispam service are handled automatically through the Symantec Premium AntiSpam service and not through LiveUpdate.

You must have an active Internet connection and permit outbound secure HTTP traffic through your firewall (port 443). Manually register the service if your connection uses an HTTP proxy. After Symantec Premium AntiSpam is registered and enabled, spam rules are continually downloaded from Symantec. Mail Security checks for updates every minute and receives new rule sets every 10 - 15 minutes.

See “About registering Symantec Premium AntiSpam through an ISA server” on page 106.

See “Configuring your proxy server to download spam definition updates” on page 107.

About registering Symantec Premium AntiSpam through an ISA server

Symantec Premium AntiSpam requires the ability to communicate by HTTPS (Port 443). If your connection uses an HTTP proxy, manually register the service so that spam rules can be automatically downloaded from Symantec. To register Symantec Premium AntiSpam through an ISA server that filters traffic for your Exchange server, do one of the following:

- If the ISA server is installed on the same computer as the Exchange server, create a Host-based protocol rule. This rule allows “Any Request” for the HTTPS protocol and HTTPS server protocols.

- If the ISA server is installed on a different computer from the Exchange server, create a Host-based protocol rule. This rule specifically allows traffic for the IP address of the Exchange server for the HTTPS protocol and HTTPS server protocols.

See “About spam detection” on page 104.

See "How to detect spam using Symantec Premium AntiSpam" on page 106.
Configuring your proxy server to download spam definition updates

Mail Security checks for updates to antispam filters every minute and receives new rule sets every 10 - 15 minutes. You can configure your proxy server to permit updates.

To configure your proxy server to download spam definition updates

1. On the Start menu, click Programs > Accessories > Command Prompt to open command prompt window.

2. At the command prompt, change directories to the Mail Security installation directory. The default directory is: \Program Files\Symantec\SMSMSE\7.9\Server

3. Type the following:

   register -c SpamPrevention\bmiconfig.xml -l SpamPrevention\SPAlicense.slf -p <proxyserver:proxyport>

   where <proxyserver:proxyport> is the IP address of your proxy server and the port.

   Symantec Premium AntiSpam licenses are placed in the SpamPrevention folder.

4. On the Start menu, click Run.

5. In the Run dialog box, type the following:

   regedit

6. Click OK.

7. In the Registry Editor window, in the left pane, browse and locate the following folder:

   HKEY-LOCAL_MACHINE\SOFTWARE\Symantec\SMSMSE\<version>\Licensing\n
8. Do one of the following:

   - If the file SPARunRegister does not exist
     In the right pane, right-click on any blank space, and select New > DWORD Value. In the name box, type:

       SPARunRegister

   - If the file SPARunRegister exists
     In the right pane, right-click on the file, and select Modify. In the Edit DWORD Value dialog box, in the Value data box, change the value to 0, and then click OK.

9. Save the file and close the Registry Editor window.

Configuring Symantec Premium AntiSpam to detect spam

Before you configure Symantec Premium AntiSpam, ensure that you have done the following:

- If you have an ISA server, register Symantec Premium AntiSpam through the ISA server.
See “About registering Symantec Premium AntiSpam through an ISA server” on page 106.

- Configure your proxy server to permit downloads for Symantec Premium AntiSpam.
  See “Configuring your proxy server to download spam definition updates” on page 107.

- Install the Symantec Premium AntiSpam license.
  See “About licensing” on page 53.

Configure the following settings to detect and handle spam:

**Reputation service**: Symantec monitors email sources to determine how much of the email messages that are sent from those sources is legitimate. Email from those sources can then be blocked or allowed based on the source's reputation value as determined by Symantec.

| Enable Ruleset based sender IP reputation | The Rule Based Reputation Service is the name for a set of downloadable IP address lists. You can use this list to block SMTP connections from known spam IP addresses or allow SMTP connections from known reputable IP addresses.
| --- | --- |
|  | The Rule Based Reputation Service currently includes the following classification lists of IP addresses, which are continuously compiled and updated:
|  | - Open proxy list:
|  |   Enables the open proxy list service.
|  |   The open proxy list contains the IP addresses that are open proxies, which spammers and ‘zombie’ computers use.
|  | - Safe List:
|  |   Enables the safe list service.
|  |   The safe list contains IP addresses from which no outgoing email is spam.
|  | - Suspect List
|  |   Contains the IP addresses from which all of the outgoing email is spam. This list is always enabled.
|  | - Fast Pass
|  |   The Fast Pass feature conserves resources by providing a temporary exemption from spam scanning for senders with a demonstrated history of sending no spam messages. Thus senders with the best local reputation are exempted from spam scanning.
|  | - Marketing mail
|  |   Emails that contain commercial or fund-raising messages, requested by the user. When the policy detects these messages it takes the action that is configured under **Suspected Spam**.
|  | - Newsletter
|  |   Emails that include content on specific topics for a known period, often weekly, or monthly. The user may have requested to receive these publications. When the policy detects these messages it takes the action that is configured under **Suspected Spam**.
Suspicious URL  Suspicious URLs include free hosting sites, URL shortening services, and URL redirecting the services that can potentially be abused to deliver spam or malware payloads. SMSMSE can filter against the email messages that contain one or more suspicious URLs. When the policy detects the messages it takes the action that is configured under **Suspected Spam**.

**DNS IP Reputation:**

**Note:** DNS IP reputation feature is disabled by default during a fresh install.

**Note:** DNS IP reputation feature is disabled by default for all upgrade scenarios.

Enable DNS IP Reputation  DNS-based IP (DNS IP) reputation allows the delivery of the Symantec Global Bad Senders list, which is the largest Symantec IP reputation list. When an inbound email arrives in your organization and the DNS IP reputation feature is enabled, the IP address of this inbound email is sent to the Symantec DNS reputation server. If this IP address in the Symantec DNS reputation server is recorded as bad, the verdict is provided back to the Symantec Mail Security for Microsoft Exchange.  

**Note:** We recommend either enable DNS-based IP Reputation feature or Rule Based Reputation feature. Enabling both of them at the same time leads to heavy utilization of network resources.

**Spam Scoring**

Flag messages as suspected spam  Flags the messages as suspected spam when their scores reach the suspected spam threshold.

Lower spam threshold  Indicates the minimum threshold for suspected spam.  

You can enter a value between 25 and 89. The default value is 72.

You must have a valid Symantec Premium AntiSpam license to enable Symantec Premium AntiSpam.
To configure Symantec Premium AntiSpam to detect spam

1. In the console on the primary navigation bar, click **Policies**.

2. In the sidebar under Antispam, click **Premium AntiSpam Settings**.

3. In the content area, under **Symantec Premium AntiSpam Settings**, check **Enable Symantec Premium AntiSpam**.

4. Under **Reputation Services**, check **Enable Ruleset based sender IP reputation** and then select any of the following that you want to use:
   - Open proxy list
   - Safe list

5. Check **Suspect list** which contains the emails sources that primarily send spam. This option is selected by default and cannot be changed.

6. To bypass antispam filtering of email messages from verified senders check **Fast Pass**.

7. Under **DNS IP reputation**, check the **Enable DNS IP Reputation** option. This DNS-based IP (DNS IP) reputation allows the delivery of the Symantec Global Bad Senders list, which is the largest Symantec IP reputation list.

   **Note:** Symantec recommends using either Enable Ruleset based sender IP or DNS IP reputation services to avoid heavy network bandwidth consumption.

8. Under **Spam Scoring**, check **Flag messages as suspected spam** if you want the messages that are flagged as suspected spam. In the **Lower spam threshold** box, type the suspected spam threshold level if you choose to identify suspected spam.

9. On the toolbar, click **Deploy changes** to apply your changes.

   See “Deploying settings and changes to a server or group” on page 60.

### Processing suspected spam messages

You can configure Mail Security to reject or accept suspected spam messages. You can log all spam events to the specified logging destinations.

See “About logging events” on page 203.

If you configure Mail Security to accept suspected spam messages, you can specify the following message delivery options:

- Prevent the message from being sent to the intended recipient.
- Deliver the spam message to an alternate recipient.
- Add your customized subject line text to the message.
Add one or more X-headers to the message.

See “About applying X-headers to messages for archiving” on page 118.

Re-assign the SCL value of the message.

To reject suspected spam messages
1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Antispam, click Premium AntiSpam Actions.
3. Under Suspected Spam from If message is Suspected Spam, select Reject the message.
4. Check Log to log spam messages to the specified logging destinations.
5. On the toolbar, click Deploy changes to apply your changes.

To accept suspected spam messages
1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Antispam, click Premium AntiSpam Actions.
3. Under Suspected Spam from If message is Suspected Spam, select Accept the message.
4. Check Prevent delivery to original recipient(s) to prevent the intended recipients from receiving suspected spam messages.
5. Check Deliver to alternate recipient to send suspected spam messages to a different recipient, and type the address to which suspected spam messages are delivered.

You can only specify one recipient.

6. Check Add to subject line to prepend the subject line of suspected spam messages, and in the subject line box, type your customized text.

The default text is Spam.

7. Check Add X-header(s) to add one or more X-headers to messages that trigger the violation, and then do any of the following:
<table>
<thead>
<tr>
<th>Add an existing X-header</th>
<th>Do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Click <strong>Add X-header</strong>.</td>
<td>■ In the X-header name column, use the drop-down menu to select the X-header that you want to use. You can modify the existing X-header by clicking on the text and typing the new content.</td>
</tr>
<tr>
<td>■ In the X-header value column, type the X-header value. You can type up to 127 characters. The following characters are not supported in X-header values: ~</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create a new X-header</th>
<th>Do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Click <strong>Add X-header</strong>.</td>
<td>■ In the X-header box, type the name of the X-header. You can type up to 127 characters. The name must begin with &quot;x-&quot; or X-&quot;. The following characters are not supported in X-header names: , . ; &lt; &gt; : ? / ( ) [ ] @</td>
</tr>
<tr>
<td>■ In the X-header box, type the X-header value. You can type up to 127 characters. The following characters are not supported in X-header values: ~</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remove an existing X-header</th>
<th>Do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Select the X-header that you want to remove by clicking to the left of the X-header name column.</td>
<td>■ Click <strong>Delete X-header(s)</strong>.</td>
</tr>
</tbody>
</table>

**8** Check **Assign SCL value to message** to reassign the SCL value, and in the drop-down list, select the threshold value. You can choose a value from 1 to 9. The default value is 6.
9 Check **Log** to log suspected spam messages to the specified logging destinations.

   Suspected spam messages are identified in the Windows Event Log as information or events.

10 On the toolbar, click **Deploy changes** to apply your changes.

**Processing the suspected spam messages that exceed an SCL threshold**

If you use a mail screening tool, you can configure Mail Security to reject or accept the suspected spam messages that exceed an SCL threshold. Assign the SCL threshold for which the suspected spam and SCL settings apply.

You can log all spam events to the specified logging destinations.

See “About logging events” on page 203.

You can specify how you want Mail Security to process the messages that are identified as suspected spam and exceed the SCL threshold that you specify.

If you configure Mail Security to accept the suspected spam messages that exceed the threshold, you can configure the following message delivery options:

■ Prevent the message from being sent to the intended recipient.

■ Deliver the spam message to an alternate recipient.

■ Add your customized subject line text to the message.

■ Add one or more X-headers to the message.
   
   See “About applying X-headers to messages for archiving” on page 118.

■ Re-assign the SCL value of the message.

To **reject the suspected spam messages that exceed an SCL threshold**

1 In the console on the primary navigation bar, click **Policies**.

2 In the sidebar under Antispam, click **Premium AntiSpam Actions**.

3 Under **Suspected Spam and SCL** from the **If message is Suspected Spam and SCL is** list, select the SCL value threshold.

   You can choose a value from 0 to 8. The default value is 5.

4 Check **Reject the message**.

5 Check **Log** to log suspected spam messages to the specified logging destinations.

6 On the toolbar, click **Deploy changes** to apply your changes.

   See “Deploying settings and changes to a server or group” on page 60.
To accept the suspected spam messages that exceed an SCL threshold

1. In the console on the primary navigation bar, click *Policies*.
2. In the sidebar under Antispam, click *Premium AntiSpam Actions*.
3. Under *Suspected Spam and SCL* from the *If message is Suspected Spam and SCL is* list, select the SCL value threshold.
   
   You can choose a value from 0 to 8. The default value is 5.
4. Check *Accept the message*.
5. Check *Prevent delivery to original recipient(s)* to prevent the intended recipients from receiving suspected spam messages.
6. Check *Deliver to alternate recipient* to send suspected spam messages to a different recipient, and type the address to which suspected spam messages are delivered.
   
   You can only specify one recipient.
7. Check *Add to subject line* to prepend the subject line of suspected spam messages, and in the subject line box, type your customized text.
   
   The default text is *Spam*.
8. Check *Add X-header(s)* to add one or more X-headers to messages that trigger the violation, and then do any of the following:

   Add an existing X-header

   Do the following:

   - Click *Add X-header*.
   - In the X-header name column, use the drop-down menu to select the X-header that you want to use.
     
     You can modify the existing X-header by clicking on the text and typing the new content.
   - In the X-header value column, type the X-header value.
     
     You can type up to 127 characters. The following characters are not supported in X-header values:

     ~ |
**Create a new X-header**

Do the following:

- Click **Add X-header**.
- In the X-header box, type the name of the X-header.
  
  You can type up to 127 characters. The name must begin with "x-" or X-". The following characters are not supported in X-header names:
  
  `:, .; < > : ? / = ( ) [ ] @ | ;~`

- In the X-header box, type the X-header value.
  
  You can type up to 127 characters. The following characters are not supported in X-header values:
  
  `~ |`

**Remove an existing X-header**

Do the following:

- Select the X-header that you want to remove by clicking to the left of the X-header name column.
- Click **Delete X-header(s)**.

**Processing spam messages**

You can configure Mail Security to reject or accept spam messages. You can also configure whether you want Mail Security to log spam events to the specified logging destinations.

See "About logging events" on page 203.

If you configure Mail Security to accept spam messages, you can specify the following message delivery options:

- Prevent the message from being sent to the intended recipient.
- Deliver the spam message to an alternate recipient.
- Add your customized subject line text to the message.
Add one or more X-headers to the message.

See “About applying X-headers to messages for archiving” on page 118.

Assign an SCL value to the message.

To reject spam messages

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Antispam, click Premium AntiSpam Actions.
3. In the content area, under Spam Messages, under If message is Spam, check Reject the message.
4. Check Log to log spam messages to the specified logging destinations.
5. On the toolbar, click Deploy changes to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

To accept spam messages

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Antispam, click Premium AntiSpam Actions.
3. In the content area, under Spam Messages, under If message is Spam, check Accept the message.
4. Check Prevent delivery to original recipient(s) to prevent the intended recipients from receiving spam messages.
5. Check Deliver to alternate recipient to send spam messages to a different recipient, and type the address to which spam messages are delivered.

You can enter only one address.
6. Check Add to subject line to prepend the subject line of spam messages, and in the subject line box, type your customized text.

The default text is Spam.
7. Check Add X-header(s) to add one or more X-headers to messages that trigger the violation, and then do any of the following:
Add an existing X-header

Do the following:

- Click Add X-header.
- In the X-header name column, use the drop-down menu to select the X-header that you want to use.
  
  You can modify the existing X-header by clicking on the text and typing the new content.
- In the X-header value column, type the X-header value.
  
  You can type up to 127 characters. The following characters are not supported in X-header values:
  ~ | 

Create a new X-header

Do the following:

- Click Add X-header.
- In the X-header box, type the name of the X-header.
  
  You can type up to 127 characters. The name must begin with “x-” or X-“. The following characters are not supported in X-header names:
  , . ; < > : ? / = ( ) [ ] @ | ; ~
- In the X-header box, type the X-header value.
  
  You can type up to 127 characters. The following characters are not supported in X-header values:
  ~ | 

Remove an existing X-header

Do the following:

- Select the X-header that you want to remove by clicking to the left of the X-header name column.
- Click Delete X-header(s).

8 Check Assign SCL value to message to assign an SCL value to spam messages, and in the drop-down list, select the threshold value.

You can choose a value from 1 to 9. The default value is 9.
Check Log to log spam messages to the specified logging destinations. Spam messages are identified in the Windows Event Log as information or events.

On the toolbar, click **Deploy changes** to apply your changes.

### About applying X-headers to messages for archiving

Mail Security lets you apply X-headers to the email messages that contain filtering rule violations or are spam or suspected spam. Symantec Enterprise Vault uses the X-headers to search for and retrieve the messages that are archived in the vault. Enterprise Vault is a data warehouse that provides secure, centralized archiving and retrieval of information.

**Note:** X-headers can only be applied to SMTP transported email messages. X-headers cannot be applied to messages that are scanned in the message store.

Mail Security provides default X-headers that Enterprise Vault uses. You can modify the default X-headers, or you can create your own. You can apply up to 25 X-headers for a single violation.

When a message triggers one or more violations and the disposition for any of the violations is to delete the message, no X-headers are applied. For example, a message is identified as spam, and the disposition is to reject the message. No X-header is applied to the message.

**Table 7-1** describes how Mail Security handles multiple filtering violations based on where the violations occur within the message.

**Table 7-1**  How X-headers are applied for multiple violations

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Which X-headers are applied</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Multiple violations in different parts of a message | Mail Security applies X-headers for each rule that is violated for each message part. Message parts include:  
  - Message body  
  - Subject  
  - Sender  
  - Attachment name  
  - Attachment content | A single message violates a filtering rule for message body and a separate content filtering rule for subject. Mail Security applies the X-headers that you specify for the message body rule and the X-headers that you specify for the subject rule.  
In this example, the message can have up to 50 X-headers applied to it. You can apply up to 25 X-headers for the message body violation and up to 25 X-headers for the subject violation. |
### Table 7-1  How X-headers are applied for multiple violations (continued)

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Which X-headers are applied</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Multiple violations for the same message part | When a message triggers multiple violations for the same message part, Mail Security applies only the X-headers that you specify for the first rule that is triggered. | A message triggers violations for two different attachment filtering rules. Mail Security only applies the X-headers for the first rule that was violated.  
**Note:** X-headers are applied to the message even when the disposition is to delete the attachment but not the message body. |

See “Processing spam messages” on page 115.

See “About creating the filtering rules” on page 126.
Filtering content

This chapter includes the following topics:

- About content and file filtering
- About creating the filtering rules
- What you can do with the filtering rules
- About enforcing email attachment policies
- About match lists
- About content filtering policy templates

About content and file filtering

Mail Security can filter messages and their attachments using the following features:

<table>
<thead>
<tr>
<th>Content filtering rules</th>
<th>Content filtering rules filter messages and their attachments for the specific content that you specify (for example, offensive language or sensitive information).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mail Security lets you create the content filtering rules that apply to SMTP inbound and SMTP outbound mail and the Exchange Information Store.</td>
</tr>
<tr>
<td></td>
<td>Mail Security can scan for content within the following message parts: message body, subject, sender, attachment name, and attachment content.</td>
</tr>
<tr>
<td></td>
<td>You can use the default content filtering rules that Mail Security provides or you can create your own rules. You can individually enable and disable each rule. Mail Security takes the action that you specify in the rule when it detects a violation.</td>
</tr>
<tr>
<td></td>
<td>See “About creating the filtering rules” on page 126.</td>
</tr>
<tr>
<td></td>
<td>See “About default content filtering rules” on page 125.</td>
</tr>
</tbody>
</table>
Mail Security lets you use file filtering rules to filter messages based on attached file names or file types such as video or document files.

Mail Security uses file filtering rules to enforce email attachment policies.

Mail Security provides the following predefined file name filtering rule:

- **File Name Rule**
  
  Blocks the attachments based on the file name that you specify

You can customize the file name rule by associating it with a match list to block attachments with specific names included in the match list.

Mail Security provides the following predefined file type filtering rules:

- **Compressed File Rule**
- **Documents File Rule**
- **Executable File Rule**
- **Image File Rule**
- **Multimedia File Rule**

Mail Security handles filtering violations according to the action that you configure for the rule. Mail Security can notify administrator and senders (internal and external) of file filtering violations. You can customize the notification message.

See “About file type filtering” on page 122.

See “About default file type filtering rules” on page 126.

See “About enforcing email attachment policies” on page 150.

Mail Security uses match lists to filter email messages and attachments for specific words and phrases. To implement a match list, you must associate it with a content or file filtering rule. When the rule is enabled, Mail Security scans for the criteria that you specify in the rule. The criteria includes the words and phrases that are in the associated match list.

Mail Security provides the match lists for use with the File Name Rule or with content filtering rules. You can create new match lists and delete or edit words in an existing match list. Match lists support literal strings, DOS wildcard-style expressions, or regular expressions.

See “About match lists” on page 154.

See “About regular expressions” on page 160.

See “About DOS wildcard style expressions” on page 159.

You can also use match lists to help manage outbreaks. You can configure Mail Security to automatically add the names of outbreak-triggered attachments and outbreak-triggered subject text to match lists. Mail Security uses these match lists with content or file filtering rules to automatically block suspicious file attachments or subjects.

See “About outbreak management” on page 193.
You can specify the action that you want Mail Security to take when it detects a filtering rule violation. You can also configure Mail Security to notify the administrator and senders (internal and external) of a violation with a message that you can customize.

**About file type filtering**

You might want to prohibit users from receiving the email messages that contain certain type of a file as an attachment. You can use the file type filtering feature of Mail security to filter the message attachment based on its true type.

When you enable the file type filtering and the rules, Mail Security detects the supported file types and takes the actions that you specify.

Mail Security can determine if a file is a true file by analyzing the file attributes, rather than looking at the file name extension. Blocking file attachments not only helps your organization enforce content policies, it also conserves scanning and file storage resources.

All the file types that Mail Security supports are categorized into the following:

- Application & Executables
- Documents
- Images
- Videos
- Sounds
- Compressed files

Table 8-1 lists the application and executable file types that Mail Security supports

<table>
<thead>
<tr>
<th>File type</th>
<th>File extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS-DOS/Windows Executables</td>
<td>.exe, .dll, .vxd, .com, .sys, .bin, .dat</td>
</tr>
<tr>
<td>Windows Installer Package</td>
<td>.msi</td>
</tr>
<tr>
<td>MS-DOS/Windows Object Library</td>
<td>.lib</td>
</tr>
<tr>
<td>MS-DOS Batch File</td>
<td>.bat</td>
</tr>
<tr>
<td>ISO</td>
<td>.iso</td>
</tr>
</tbody>
</table>

Table 8-2 lists the documents file types that Mail Security supports
Table 8-2  Supported documents file types

<table>
<thead>
<tr>
<th>File type</th>
<th>File extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Portable Document Format</td>
<td>.pdf</td>
</tr>
<tr>
<td>Compiled HTML Help</td>
<td>.chm</td>
</tr>
<tr>
<td>Microsoft Access</td>
<td>.mdb, .accdb</td>
</tr>
<tr>
<td>Microsoft Excel</td>
<td>.xls, .xlt, .xla, .xlsx, .xltx</td>
</tr>
<tr>
<td>Microsoft Word</td>
<td>.doc, .dot, .docx, .dotx</td>
</tr>
<tr>
<td>Microsoft PowerPoint</td>
<td>.pps, .ppt, .pot, .pptx, .potx, .ppsx</td>
</tr>
<tr>
<td>Macro-Microsoft Excel 2007 and later</td>
<td>.xslm, .xltm, .xslb, .xlam</td>
</tr>
<tr>
<td>Macro-Microsoft Word 2007 and later</td>
<td>.docm, .dotm</td>
</tr>
<tr>
<td>Macro-Microsoft PowerPoint 2007 and later</td>
<td>.pptm, .potm, .ppam, .ppsm</td>
</tr>
<tr>
<td>Microsoft Project</td>
<td>.mpp</td>
</tr>
<tr>
<td>Microsoft Rich Text Format</td>
<td>.rtf</td>
</tr>
<tr>
<td>Microsoft Help</td>
<td>.hlp</td>
</tr>
<tr>
<td>Microsoft Outlook File</td>
<td>.pst</td>
</tr>
<tr>
<td>Open Documents Formats</td>
<td>.odg, .odt, .ods, .odp</td>
</tr>
<tr>
<td>Markup Language</td>
<td>.htm</td>
</tr>
</tbody>
</table>

Table 8-3 lists the image file types that Mail Security supports

Table 8-3  Supported image file types

<table>
<thead>
<tr>
<th>File type</th>
<th>File extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompuServe GIF</td>
<td>.gif</td>
</tr>
<tr>
<td>JPEG image</td>
<td>.jpg, .jpeg, .jpe</td>
</tr>
<tr>
<td>Portable Network Graphics</td>
<td>.png</td>
</tr>
<tr>
<td>Tagged image format</td>
<td>.tiff</td>
</tr>
<tr>
<td>Windows/OS/2 Bitmap</td>
<td>.bmp</td>
</tr>
<tr>
<td>RBG Bitmap</td>
<td>.rgb</td>
</tr>
</tbody>
</table>
Table 8-3  
Supported image file types (continued)

<table>
<thead>
<tr>
<th>File type</th>
<th>File extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>X Windows Pixmap</td>
<td>.xpm</td>
</tr>
<tr>
<td>Icons on Windows</td>
<td>.ico</td>
</tr>
</tbody>
</table>

Table 8-4 lists the video file types that Mail Security supports

Table 8-4  
Supported video file types

<table>
<thead>
<tr>
<th>File type</th>
<th>File extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Streaming Format</td>
<td>.asf, .wmv</td>
</tr>
<tr>
<td>Macromedia Flash</td>
<td>.wsf</td>
</tr>
<tr>
<td>Audio Video Interleave File Format</td>
<td>.avi</td>
</tr>
<tr>
<td>Movie Files</td>
<td>.mpg, .mpeg, .mp3, .mov, .qt</td>
</tr>
<tr>
<td>RealMedia Streaming Media</td>
<td>.rm, .ra</td>
</tr>
<tr>
<td>OGG Vorbis Codec Compressed WAV File</td>
<td>.ogg</td>
</tr>
<tr>
<td>Dolby Lab</td>
<td>.ac3</td>
</tr>
</tbody>
</table>

Table 8-5 lists the sounds file types that Mail Security supports

Table 8-5  
Supported sounds file types

<table>
<thead>
<tr>
<th>File type</th>
<th>File extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Musical Instrument Digital Interface</td>
<td>.mid</td>
</tr>
<tr>
<td>MPEG Audio Layer 3</td>
<td>.mp3</td>
</tr>
<tr>
<td>Waveform Audio Format</td>
<td>.wav</td>
</tr>
<tr>
<td>Amiga MOD</td>
<td>.mod</td>
</tr>
<tr>
<td>Audio Interchange File</td>
<td>.aiff, aifc, aif</td>
</tr>
<tr>
<td>Sun MicroSystems Audio Format</td>
<td>.au</td>
</tr>
<tr>
<td>Apple m4a</td>
<td>.m4a</td>
</tr>
</tbody>
</table>
Table 8-6 lists the compressed file types that Mail Security supports

<table>
<thead>
<tr>
<th>File type</th>
<th>File extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive created by LHA</td>
<td>.lzh, .lha</td>
</tr>
<tr>
<td>Java Archive, Pkzip</td>
<td>.zip, .jar</td>
</tr>
<tr>
<td>Archive created by RAR</td>
<td>.rar</td>
</tr>
<tr>
<td>Archive created by Tar</td>
<td>.tar</td>
</tr>
<tr>
<td>BINHEX</td>
<td>.hqx</td>
</tr>
<tr>
<td>GNU Zip</td>
<td>.gz, .gzip</td>
</tr>
<tr>
<td>Microsoft Cabinet</td>
<td>.cab</td>
</tr>
<tr>
<td>MIME</td>
<td>.eml, .tnf, .tnef, .mht</td>
</tr>
<tr>
<td>Unix BZ2 Bzip compressed file</td>
<td>.bz2, .tbz</td>
</tr>
<tr>
<td>UUEncode</td>
<td>.uu</td>
</tr>
<tr>
<td>MacBinary</td>
<td>.bin</td>
</tr>
<tr>
<td>UNIX Compress</td>
<td>.z</td>
</tr>
<tr>
<td>7 Zip</td>
<td>.7z</td>
</tr>
</tbody>
</table>

See "About default file type filtering rules" on page 126.
See "Creating a file type filtering rule" on page 128.

About default content filtering rules

Table 8-7 describes the preconfigured content filtering rules that Mail Security provides.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blank Subject and Sender</td>
<td>Detects and filters messages with blank subject line and blank sender line</td>
</tr>
<tr>
<td>Quarantine Triggered Attachment Names</td>
<td>Detects and filters the files whose attachment name matches a list of outbreak-triggered attachment names</td>
</tr>
<tr>
<td></td>
<td>See &quot;About match lists&quot; on page 154.</td>
</tr>
</tbody>
</table>
Table 8-7

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine Triggered Subjects</td>
<td>Detects and filters the messages whose subject matches a list of outbreak-triggered subjects</td>
</tr>
<tr>
<td>Sample Executable File</td>
<td>Detects and filters executable files based on the Sample Attachment Name match list</td>
</tr>
</tbody>
</table>

Enable the default content filtering rules that you want to use. You can modify the rules as needed.

About default file type filtering rules

Table 8-8 describes the preconfigured file type filtering rules that Mail Security provides.

Table 8-8

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compressed File Rule</td>
<td>Detects and filters messages with an attachment of compressed file based on its true file type.</td>
</tr>
<tr>
<td>Documents File Rule</td>
<td>Detects and filters messages with an attachment of document file based on its true file type.</td>
</tr>
<tr>
<td>Executable File Rule</td>
<td>Detects and filters messages with an attachment of executable file based on its true file type.</td>
</tr>
<tr>
<td>Image File Rule</td>
<td>Detects and filters messages with an attachment of image file based on its true file type.</td>
</tr>
<tr>
<td>Multimedia File Rule</td>
<td>Detects and filters messages with an attachment of multimedia file based on its true file type.</td>
</tr>
</tbody>
</table>

Enable the default file type filtering rules that you want to use. You can modify the rules as needed.

See "About file type filtering " on page 122.

See "Creating a file type filtering rule" on page 128.

About creating the filtering rules

Creating a content filtering rule involves the following process:

■ Configuring the conditions of a content filtering rule
Specifying the users and groups in a filtering rule
Specifying whom to notify if a filtering rule is violated
Configuring rule actions

Creating a file type filtering rule involves the following process:

- Creating a file type filtering rule
- Specifying the users and groups in a filtering rule
- Specifying whom to notify if a filtering rule is violated
- Configuring rule actions

Configuring the conditions of a content filtering rule

A content filtering rule consists of one or more conditions that you define. For example, a condition might be that an email subject line contains one or more words from a subject line match list. A rule can optionally contain one or more exceptions.

Mail Security uses OR (Match any term) and AND (Match all terms) conditions to create a framework in which to evaluate email messages or email messages and their attachments. By default, content filtering rules are set to Match any term for the entries in the Content list. This means that the rule triggers a violation if any of the entries are present and all of the other criteria that you configured are met. If you select Match all terms, then the rule only triggers a violation if all the items in the Content list are present and all other rule criteria that you configure are met. "Match any terms" is the only condition available for the entries in the Unless list.

To configure the conditions of a content filtering rule

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Content Enforcement, click Content Filtering Rules.
3. Do one of the following:
   - Create a rule In the sidebar under Tasks, click New rule.
   - Modify an existing rule In the content area, double-click the rule that you want to edit.

4. On the Rule tab, define the conditions for the content filtering rule.
   See “Elements of a content filtering rule” on page 141.
5. Do any of the following:
   - Configure the remaining components of the content filtering rule.
     See “Specifying the users and groups in a filtering rule” on page 128.
Creating a file type filtering rule

A file type filtering rule consist of the file types that you can configure to filter email messages with those attachments. When you enable the file type filtering and the rules, Mail Security detects the supported file and types and takes the actions that you specify.

To create a file type filtering rule

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Content Enforcement, click File Type Filtering Rules.
3. In the sidebar under Tasks, click New rule.
4. On the Rule tab, type the name and description for the file type filtering rule.
5. Under Rule Content, select the file types for the rule.
6. Click OK.
7. On the toolbar, click Deploy changes to apply your changes.

Specifying the users and groups in a filtering rule

Mail Security lets you specify the users and groups to which the rule applies. You can also specify which users and groups are exceptions to the rule.

Note: This feature is not available for the Edge Server role.

You can select groups from Active Directory. You can also add users based on SMTP addresses.

Table 8-9 shows the SMTP address formats that Mail Security supports.

<table>
<thead>
<tr>
<th>Address</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>@&lt;domain name&gt;</td>
<td>@symantecdomain.com</td>
</tr>
</tbody>
</table>
Table 8-9  Supported SMTP address formats (continued)

<table>
<thead>
<tr>
<th>Address</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>*@&lt;domain name&gt;</td>
<td>*@symantecdomain.com</td>
</tr>
<tr>
<td>&lt;name&gt;@&lt;domain name&gt;</td>
<td><a href="mailto:joe@symantecdomain.com">joe@symantecdomain.com</a></td>
</tr>
<tr>
<td>&lt;name&gt;@&lt;subdomain.domain name&gt;</td>
<td><a href="mailto:joe@security.symantecdomain.com">joe@security.symantecdomain.com</a></td>
</tr>
</tbody>
</table>

Note: Using regular expressions for SMTP addresses is not supported.

When you use the address formats from the table above, sub-domains are automatically supported. For example, when you use the address format <name>@<domain name>, Mail Security will support joe@symantec.com, as well as joe@security.symantec.com.

If you do not specify users, the rule applies to all senders and recipients.

If you want to specify a user or group whose domain is not in the Exchange server domain, specify the domain name in the Internal Domains list.

See “Specifying inbound SMTP domains” on page 149.

Note: You can select any Active Directory group except the Users group. Adding the Users group to Active Directory Groups list results in unintended behavior. For the filtering rules based on Active Directory group, you must add SMSMSE service account user (RBAC user) to the SMSMSE Admin's Active Directory group.

To specify the users and groups in a filtering rule

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under Content Enforcement, click **Content Filtering Rules** or **File Type Filtering Rules**.
3. Do one of the following:
   
   Create a rule  
   In the sidebar under Tasks, click **New rule**.

   Modify an existing rule  
   In the content area, double-click the rule that you want to edit.

4. Click the **Users** tab.
5. Under Sender/Recipient Selection, do one of the following:
To apply the rule based on the sender
Click **Sender**, and then select one of the following options from the drop-down list:
- Apply if the sender of the message is in the list
- Apply if the sender of the message is NOT in the list

To apply the rule based on the recipient
Click **Recipient**, and then select one of the following options from the drop-down list:
- Apply if ANY of the recipients of the message are in the list
- Apply if ANY of the recipients of the message are NOT in the list
- Apply if ALL of the recipients of the message are in the list
- Apply if ALL of the recipients of the message are NOT in the list

6 Under **List of Users or Groups**, in the SMTP addresses box, do one of the following:
- Type the addresses of the users that you want to include or exclude.
  - Type one address per line.
- To add a preconfigured match list that contains user addresses, click **Add Match List** and select a match list.
  
  You can only insert one match list. You can combine a match list with typed addresses. See “About match lists” on page 154.

7 Under the **Active Directory groups** list, to select groups from Active Directory, click **Add**.

8 In the **Active Directory domains and groups** window, under **Available** groups, select the group that you want to add and click the >> command icon.

   The group that you select appears in the **Selected groups** list. To deselect a group in the **Selected groups** list, click on the group entry, and then click the << command icon.

9 Do any of the following:
- Configure the remaining components of the content filtering rule.
- Click **OK** and then click **Deploy Changes**.
  
  See “Deploying settings and changes to a server or group” on page 60.

**Specifying whom to notify if a filtering rule is violated**

Mail Security lets you specify whom you want to notify when a rule is violated.

**To specify whom to notify if a filtering rule is violated**

1 In the console on the primary navigation bar, click **Policies**.

2 In the sidebar under Content Enforcement, click **Content Filtering Rules/File Type Filtering Rule**.
3  Do one of the following:

- Create a rule  In the sidebar under Tasks, click **New rule**.
- Modify an existing rule  In the content area, double-click the rule that you want to edit.

4  Click the **Notifications** tab.

5  Check any of the following:

- **Notify administrators**
  - Click the down arrow, and then type your customized text in the Subject line box and the Message body box. The default Subject line and Message body text is as follows:
    - Default Subject line text: Administrator Alert: Symantec Mail Security detected a message containing prohibited content
    - Default Message body text: Location of the message:%location%n%Sender of the message:%sender%n%Subject of the message: %subject%n%The message was %action%n%This was done due to the following Symantec Mail Security settings: %n%Scan: %scan%n%Rule: %rule%nViolating term(s): %violatingterm%

- **Notify internal sender**
  - Click the down arrow, and then type your customized text in the Subject line box and the Message body box. The default Subject line and Message body texts are as follows:
    - Default Subject line text: Symantec Mail Security detected prohibited content in a message sent from your address
    - Default Message body text: Subject of the message: %subject%n%Recipient of the message: %recipient%

- **Notify external sender**
  - Click the down arrow, and then type your customized text in the Subject line box and the Message body box. The default Subject line and Message body texts are as follows:
    - Default Subject line text: Symantec Mail Security detected prohibited content in a message sent from your address
    - Default Message body text: Subject of the message: %subject%n%Recipient of the message: %recipient%

See “Alert and notification variables” on page 238.

6  Click **OK**.

7  On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.
Configuring rule actions

You can specify the action that you want Mail Security to take when a violation occurs. Mail Security provides the following options for processing the messages that trigger the filtering rule violations:

- Delete entire message
- Delete attachment/message body and replace with text
  You can customize the replacement text.
- Quarantine entire message and replace with text
  You can customize the replacement text.
- Quarantine attachment/message body and replace with text
  You can customize the replacement text.
- Add tag to beginning of subject line
  You can customize the text that you want to prepend the subject line. This rule action is not available if you apply the rule to the internal messages (store).
- Log only
  See “About logging events” on page 203.

You can also configure Mail Security to add one or more X-headers to messages that violate the filtering rule. Mail Security provides five default X-headers from which you can choose. Mail Security also lets you create your own X-headers. You can specify up to 25 X-headers for each violation.

See “About applying X-headers to messages for archiving” on page 118.

To configure rule actions to delete the message

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Content Enforcement, click Content Filtering Rules/File Type Filtering Rules.
3. Do one of the following:

   Create a rule
   In the sidebar under Tasks, click New rule.

   Modify an existing rule
   In the content area, double-click the rule that you want to edit.
4 On the **Actions** tab, in the **When a violation occurs** box, use the drop-down menu to select **Delete entire message**.

The default setting is: Quarantine entire message and replace with text.

5 Do any of the following:

- Configure the remaining components of the content filtering or file type filtering rule.
  - See “Creating a file type filtering rule” on page 128.
  - See “Specifying whom to notify if a filtering rule is violated” on page 130.

- Click **OK** and then click **Deploy Changes**.

To configure rule actions to delete the attachment and message body and replace with text

1 In the console on the primary navigation bar, click **Policies**.

2 In the sidebar under **Content Enforcement**, click **Content Filtering Rules/File Type Filtering Rules**.

3 Do one of the following:

   Create a rule    In the sidebar under **Tasks**, click **New rule**.

   Modify an existing rule    In the content area, double-click the rule that you want to edit.

4 On the **Actions** tab, in the **When a violation occurs** box, use the drop-down menu to select **Delete attachment/message body and replace with text**.

The default setting is: Quarantine entire message and replace with text.

5 In the **Replacement text** box, type your customized text.

   The default text is: Symantec Mail Security replaced %attachment% with this text message.

   The original attachment content type was not allowed and was %action%.

   See “Alert and notification variables” on page 238.

6 Check **Add X-header(s)** to add one or more X-headers to messages that trigger the violation, and then do any of the following:
Add an existing X-header

Do the following:

- Click Add X-header.
- In the X-header name column, use the drop-down menu to select the X-header that you want to use.
  You can modify the existing X-header by clicking on the text and typing the new content.
- In the X-header value column, type the X-header value.
  You can type up to 127 characters. The following characters are not supported in X-header values:
  ~ | 

Create a new X-header

Do the following:

- Click Add X-header.
- In the X-header name box, type the name of the X-header.
  You can type up to 127 characters. The name must begin with "x-" or X-". The following characters are not supported in X-header names:
  , . ; < > : ? / = ( ) [ ] @ | ;~
- In the X-header value box, type the X-header value.
  You can type up to 127 characters. The following characters are not supported in X-header values:
  ~ | 

Remove an existing X-header

Do the following:

- Select the X-header that you want to remove by clicking to the left of the X-header name column.
- Click Delete X-header(s).

7 Do any of the following:

- Configure the remaining components of the content filtering or file type filtering rule. See “Creating a file type filtering rule” on page 128.
- Click OK and then click Deploy Changes.
To configure rule actions to quarantine entire message and replace with text

1 In the console on the primary navigation bar, click Policies.

2 In the sidebar under Content Enforcement, click Content Filtering Rules/File Type Filtering Rules.

3 Do one of the following:

   Create a rule  In the sidebar under Tasks, click New rule.

   Modify an existing rule  In the content area, double-click the rule that you want to edit.

4 On the Actions tab, in the When a violation occurs box, ensure that Quarantine entire message and replace with text is selected.

   This option is selected by default.

5 In the Replacement text box, type your customized text.

   The default text is: Symantec Mail Security replaced %attachment% with this text message.
   The original attachment content type was not allowed and was %action%.

6 Check Add X-header(s) to add one or more X-headers to messages that trigger the violation, and then do any of the following:

   Add an existing X-header

   Do the following:

   • Click Add X-header.

   • In the X-header name column, use the drop-down menu to select the X-header that you want to use.
     You can modify the existing X-header by clicking on the text and typing the new content.

   • In the X-header value column, type the X-header value.
     You can type up to 127 characters. The following characters are not supported in X-header values:
     ~ |
Create a new X-header

Do the following:

- Click **Add X-header**.
- In the **X-header name** box, type the name of the X-header.
  You can type up to 127 characters. The name must begin with "x-" or X-". The following characters are not supported in X-header names:
  , . ; < > : ? / = ( ) [ ] @ | ;~
- In the **X-header value** box, type the X-header value.
  You can type up to 127 characters. The following characters are not supported in X-header values:
  ~ |.

Remove an existing X-header

Do the following:

- Select the X-header that you want to remove by clicking to the left of the **X-header name** column.
- Click **Delete X-header(s)**.

7 Do any of the following:

- Configure the remaining components of the content filtering or file type filtering rule.
  See “Configuring the conditions of a content filtering rule” on page 127.
  See “Creating a file type filtering rule” on page 128.
  See “Specifying the users and groups in a filtering rule” on page 128.
  See “Specifying whom to notify if a filtering rule is violated” on page 130.
- Click **OK** and then click **Deploy Changes**.
  See “Deploying settings and changes to a server or group” on page 60.

To configure rule actions to quarantine the attachment and message and replace with text

1 In the console on the primary navigation bar, click **Policies**.

2 In the sidebar under **Content Enforcement**, click **Content Filtering Rules/File Type Filtering Rules**.

3 Do one of the following:

Create a rule In the sidebar under **Tasks**, click **New rule**.

Modify an existing rule In the content area, double-click the rule that you want to edit.
4 On the Actions tab, in the When a violation occurs box, select Quarantine attachment/message body and replace with text. The default setting is: Quarantine entire message and replace with text.

5 In the Replacement text box, type your customized text. The default text is: Symantec Mail Security replaced %attachment% with this text message. The original attachment content type was not allowed and was %action%.

6 Check Add X-header(s) to add one or more X-headers to messages that trigger the violation, and then do any of the following:

Add an existing X-header

Do the following:

- Click Add X-header.
- In the X-header name column, use the drop-down menu to select the X-header that you want to use. You can modify the existing X-header by clicking on the text and typing the new content.
- In the X-header value column, type the X-header value. You can type up to 127 characters. The following characters are not supported in X-header values:
  ~ | 

Create a new X-header

Do the following:

- Click Add X-header.
- In the X-header name box, type the name of the X-header. You can type up to 127 characters. The name must begin with "x-" or X-. The following characters are not supported in X-header names:
  , . ; < > : ? / = ( )[] @ | ;~
- In the X-header value box, type the X-header value. You can type up to 127 characters. The following characters are not supported in X-header values:
  ~ |
Remove an existing X-header

Do the following:
- Select the X-header that you want to remove by clicking to the left of the X-header name column.
- Click Delete X-header(s).

7 Do any of the following:
- Configure the remaining components of the content filtering or file type filtering rule. See “Creating a file type filtering rule” on page 128.
- Click OK and then click Deploy Changes.

To configure rule actions to prepend the subject line

1 In the console on the primary navigation bar, click Policies.
2 In the sidebar under Content Enforcement, click Content Filtering Rules/File Type Filtering Rules.
3 Do one of the following:
   - Create a rule In the sidebar under Tasks, click New rule.
   - Modify an existing rule In the content area, double-click the rule that you want to edit.

4 On the Actions tab, in the When a violation occurs box, use the drop-down menu to select Add tag to beginning of subject line.
   - The default setting is: Quarantine entire message and replace with text.
   - This rule action is not available if you apply the rule to the internal messages (store).

5 In the Subject line tag box, type the customized text that you want to prepend to the subject line.
   - The default text is: Content Violation:

6 Check Add X-header(s) to add one or more X-headers to messages that trigger the violation, and then do any of the following:
Add an existing X-header

Do the following:

- Click **Add X-header**.
- In the **X-header name** column, use the drop-down menu to select the X-header that you want to use.
  You can modify the existing X-header by clicking on the text and typing the new content.
- In the **X-header value** column, type the X-header value.
  You can type up to 127 characters. The following characters are not supported in X-header values:
  ~ |

Create a new X-header

Do the following:

- Click **Add X-header**.
- In the **X-header name** box, type the name of the X-header.
  You can type up to 127 characters. The name must begin with "x-" or X-". The following characters are not supported in X-header names:
  , . < > ? /= ( ) [ ] @ | ;~
- In the **X-header value** box, type the X-header value.
  You can type up to 127 characters. The following characters are not supported in X-header values:
  ~ |

Remove an existing X-header

Do the following:

- Select the X-header that you want to remove by clicking to the left of the **X-header name** column.
- Click **Delete X-header(s)**.

7 Do any of the following:

- Configure the remaining components of the content filtering or file type filtering rule.
  See “Creating a file type filtering rule” on page 128.
- Click **OK** and then click **Deploy Changes**.
To configure rule actions to only log the event

1 In the console on the primary navigation bar, click **Policies**.

2 In the sidebar under **Content Enforcement**, click **Content Filtering Rules/File Type Filtering Rules**.

3 Do one of the following:

   - **Create a rule** In the sidebar under **Tasks**, click **New rule**.
   - **Modify an existing rule** In the content area, double-click the rule that you want to edit.

4 On the **Actions** tab, in the **When a violation occurs** box, use the drop-down menu to select **Log only**.

   The default setting is: Quarantine entire message and replace with text.

5 Check **Add X-header(s)** to add one or more X-headers to messages that trigger the violation, and then do any of the following:

   - **Add an existing X-header**
   - **Do the following:**

     - Click **Add X-header**.
     - In the **X-header name** column, use the drop-down menu to select the X-header that you want to use.
       You can modify the existing X-header by clicking on the text and typing the new content.
     - In the **X-header value** column, type the X-header value.
       You can type up to 127 characters. The following characters are not supported in X-header values:
       ~ |
Create a new X-header

Do the following:

- Click **Add X-header**.
- In the **X-header name** box, type the name of the X-header.
  You can type up to 127 characters. The name must begin with "x-" or X-". The following characters are not supported in X-header names:
  , . ; < > : ? / = ( ) [] @ | ;~
- In the **X-header value** box, type the X-header value.
  You can type up to 127 characters. The following characters are not supported in X-header values:
  ~ |

Remove an existing X-header

Do the following:

- Select the X-header that you want to remove by clicking to the left of the **X-header name** column.
- Click **Delete X-header(s)**.

6 Do any of the following:

- Configure the remaining components of the content filtering or file type filtering rule. See “Creating a file type filtering rule” on page 128.
- Click **OK** and then click **Deploy Changes**.

Elements of a content filtering rule

**Table 8-10** describes the rule elements that you can configure on the content filtering rule tab.

<table>
<thead>
<tr>
<th>Rule condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Lets you provide a unique name for the content filtering rule that you can easily identify in the list of rules and in reports in the event log.</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you provide a unique description for the content filtering rule. The description should provide enough detail to remind you what the rule is configured to detect.</td>
</tr>
<tr>
<td>Rule condition</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Message part to scan</td>
<td>Lets you specify the part of the email message that you want Mail Security to scan for violations. Use the <strong>Message part to scan</strong> drop-down list to choose from the following message parts:</td>
</tr>
<tr>
<td></td>
<td>▪ Message Body</td>
</tr>
<tr>
<td></td>
<td>▪ Subject</td>
</tr>
<tr>
<td></td>
<td>▪ Sender</td>
</tr>
<tr>
<td></td>
<td>▪ Attachment Name</td>
</tr>
<tr>
<td></td>
<td>▪ Attachment Content</td>
</tr>
<tr>
<td></td>
<td>▪ Any Part</td>
</tr>
<tr>
<td></td>
<td>When the message part to scan is Attachment Name, Mail Security scans the attachment name and all the file names inside the container. You can bypass the scanning of the container files. Select the <strong>Bypass scanning of container file(s)</strong> box, and Mail Security will not evaluate the file names that are inside a container file. For example, the compressed files in a .zip file.</td>
</tr>
<tr>
<td></td>
<td>See “About outbreak management” on page 193.</td>
</tr>
<tr>
<td></td>
<td>See “What you can do with the filtering rules” on page 146.</td>
</tr>
<tr>
<td></td>
<td>See “About creating the filtering rules” on page 126.</td>
</tr>
<tr>
<td>Apply rule to</td>
<td>Lets you specify the messages to which you want the rule to apply. You can choose to apply the rule to any combination of inbound, outbound, or internal messages. You must select at least one of these options.</td>
</tr>
<tr>
<td></td>
<td>The default setting is Internal messages.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> To allow content filtering of internal messages, you must select Inbound messages option along with Internal messages.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Apply rule to</strong> element only applies to Auto-Protect scanning. Manual and scheduled scans automatically scan internal messages.</td>
</tr>
<tr>
<td></td>
<td>See “Specifying inbound SMTP domains ” on page 149.</td>
</tr>
</tbody>
</table>
Table 8-10  Elements of a content filtering rule (continued)

<table>
<thead>
<tr>
<th>Rule condition</th>
<th>Description</th>
</tr>
</thead>
</table>
| Match type     | Lets you determine how words and phrases in the Content list and Unless list are interpreted.  
**Note:** The content filtering rule **Match type** element does not determine how the match lists that you use in the **Content** list and **Unless** list are interpreted. A match list can have a different match type than the content filtering rule.  
See “About match lists” on page 154.  
The **Match Type** options are as follows:  
- Literal string: Matches the exact text in the **Content** and **Unless** lists  
- Regular expression: Matches the patterns of text using symbols and syntactic elements  
  See “About regular expressions” on page 160.  
- Wild cards: Specifies the file names using wild card-style expressions  
  See “About DOS wildcard style expressions” on page 159. |
| Options        | Lets you select from the following match options:  
- Whole term: Applies the rule only if the exact term in the **Content** list and **Unless** list or match list is found.  
- Case: Applies the rule only if the exact term is in the same case as in the **Content** list and **Unless** list or in the match list. For example, if you type ACME in the **Content** list, a message that contains the word Acme does not trigger a violation. |
| Content Pane   | Lets you specify the Contains condition for a content filtering rule.  
The Contains conditions are as follows:  
- Contains: The message part to scan contains the terms in the **Content** list.  
- Does not contain: The message part to scan does not contain the terms in the **Content** list.  
- Equals: The message part to scan equals the terms in the **Content** list.  
- Does not equal: The message part to scan does not equal the terms in the **Content** list.  
The Equals and Does not equal options only apply to the Subject, Sender, and Attachment Name message parts. |
Table 8-10  Elements of a content filtering rule (continued)

<table>
<thead>
<tr>
<th>Rule condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add match list</td>
<td>Lets you specify a match list to use in your content filtering rule. You can also create a new match list or edit an existing match list.</td>
</tr>
<tr>
<td></td>
<td>Using a match list in content filtering rule is optional.</td>
</tr>
<tr>
<td></td>
<td>See “About match lists” on page 154.</td>
</tr>
<tr>
<td>Match any term</td>
<td>Lets you evaluate the specified message part for any term that is contained in the <strong>Content</strong> list.</td>
</tr>
<tr>
<td></td>
<td>For example, assume that the <strong>Content</strong> list contains the terms: free, confidential, and money. If Mail Security detects any one of these terms</td>
</tr>
<tr>
<td></td>
<td>in the specified message part, it triggers a violation.</td>
</tr>
<tr>
<td>Match all terms</td>
<td>Lets you evaluate the specified message part for all of the terms that are contained in the <strong>Content</strong> list.</td>
</tr>
<tr>
<td></td>
<td>The Match all terms option is only available to use with the terms in the <strong>Content</strong> list.</td>
</tr>
<tr>
<td></td>
<td>For example, assume that the <strong>Content</strong> list contains the terms: free, confidential, and money. Mail Security must detect all of these terms</td>
</tr>
<tr>
<td></td>
<td>in the specified message part to trigger a violation.</td>
</tr>
<tr>
<td></td>
<td>The Match all terms option is not available when the message part to scan is Any Part.</td>
</tr>
<tr>
<td>Template</td>
<td>Lets you add a template to your content filtering rule. You can edit an existing template but cannot create a new template or delete an existing</td>
</tr>
<tr>
<td></td>
<td>one. You can add a single template to a content filtering rule.</td>
</tr>
<tr>
<td></td>
<td>Using a template in a content filtering rule is optional.</td>
</tr>
<tr>
<td></td>
<td>See “About content filtering policy templates” on page 163.</td>
</tr>
<tr>
<td>Content list</td>
<td>Lets you specify the words or phrases for which you want to evaluate the specified message parts.</td>
</tr>
<tr>
<td></td>
<td>The format of the terms that you type in the <strong>Content</strong> list should mirror that of the match type that you select. For example, if you select</td>
</tr>
<tr>
<td></td>
<td>literal string from the match type list, format your Content list entries as literal strings.</td>
</tr>
</tbody>
</table>
Table 8-10  Elements of a content filtering rule (continued)

<table>
<thead>
<tr>
<th>Rule condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment size is</td>
<td>Lets you specify Attachment size is as a condition of the content filtering rule. The Attachment size is option can be applied to all message parts to scan, except message body. You can also use Attachment size is by itself if you want Mail Security to detect attachments of a certain size. When you select the sender or subject message parts and the Match any term or Match all terms conditions, the rule action is applied to the message or the attachment based on the violation that is detected. For example, assume that you have specified Sender, chosen the Match any term condition, and specified the Attachment size is as = 2MB. Since Mail Security scans messages in parts, if there is a Sender match, dispositions are applied to the message body and the attachment. If the attachment size is the only match, the disposition only applies to the attachment. Assume for the same example that you change the condition to Match all terms. Mail Security applies a disposition to the attachment only if it detects all of the terms in the Content list AND the specified attachment size.</td>
</tr>
<tr>
<td>Unless Pane</td>
<td></td>
</tr>
<tr>
<td>Contains</td>
<td>Lets you specify the Contains condition for a content filtering rule. The Contains conditions are as follows: Contains: The message part to scan contains the terms in the Unless list. Does not contain: The message part to scan does not contain the terms in the Unless list. Equals: The message part to scan equals the terms in the Unless list. Does not equal: The message part to scan does not equal the terms in the Unless list. The Equals and Does not equal options apply only to the Subject, Sender, and Attachment Name message parts.</td>
</tr>
<tr>
<td>Add match list</td>
<td>Lets you specify a match list to use in your content filtering rule Unless condition. You can also create a new match list or edit an existing match list. Using a match list is optional.</td>
</tr>
</tbody>
</table>
### Table 8-10  Elements of a content filtering rule (continued)

<table>
<thead>
<tr>
<th>Rule condition</th>
<th>Description</th>
</tr>
</thead>
</table>
| Unless list          | Lets you create exceptions to content filtering rules. You can add words and phrases to the Unless list which Mail Security evaluates as exceptions to the content filtering rule.  

All entries in the Unless list are automatically designated with the **Match any term** (OR condition) option.  

The format of the terms that you type in the Unless list should mirror that of the match type that you select. For example, if you select Literal string from the Match Type menu, you should format your Unless list entries as literal strings. |
| Or attachment size   | Lets you specify **Attachment size is** as a condition of the content filtering rule. The **Attachment size is** option can be applied to all message parts to scan, except message body. You can also use **Attachment size is** by itself if you want Mail Security to detect attachments of a certain size.  

When you select the sender or subject message parts, the rule action is applied to the message or the attachment based on the violation that is detected. (All Unless conditions are applied as OR conditions between the message part and the attachment.) And the **Match any term** condition always applies to all Unless conditions.  

For example, assume that you have specified Sender and specified the **Attachment size is** as = 2MB. Since Mail Security scans messages in parts, if there is a Sender match, dispositions are applied to the message body and the attachment because "Match any term" makes this rule an OR condition. However, if the attachment size is the only match, the disposition only applies to the attachment. |

---

### What you can do with the filtering rules

The following describes the tasks that you can perform with the filtering rules:

- Enabling or disabling the filtering for Auto-Protect scanning
- Prioritizing the filtering rules
- Deleting a filtering rule
- Specifying inbound SMTP domains
- Refreshing the Active Directory group cache
Enabling or disabling the filtering for Auto-Protect scanning

You can enable or disable content filtering or file type filtering for Auto-Protect scanning. You can enable or disable content filtering and file type filtering for manual and scheduled scans when you configure those scans.


See “About scheduling a scan” on page 186.

To enable or disable content filtering for Auto-Protect scanning

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Content Enforcement, click Content Filtering Rules.
3. In the content area under Content Filtering Rules, do one of the following:
   - Check Enable content filtering to enable content filtering for Auto-Protect scanning.
   - Uncheck Enable content filtering to disable content filtering for Auto-Protect scanning.
4. On the toolbar, click Deploy changes to apply your changes.

To enable or disable file type filtering for Auto-Protect scanning

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Content Enforcement, click File Type Filtering Rules.
3. In the content area under File Type Filtering Rules, do one of the following:
   - Check Enable file type filtering to enable file type filtering for Auto-Protect scanning.
   - Uncheck Enable file type filtering to disable file type filtering for Auto-Protect scanning.
   - On the toolbar, click Deploy changes to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

Prioritizing the filtering rules

Mail Security evaluates messages using all of the filtering rules that you enable. By default, Mail Security applies rules in the order in which you enable them. For example, if you enable the Sample Executable File rule and then enable the Quarantined Triggered Subjects rule, Mail Security priorities the Sample Executable File rule first. However, you can specify the order in which you want Mail Security to apply the rules.

If a message violates more than one rule, Mail Security applies the most severe disposition of the rules that were violated. This ensures that your environment maintains the highest level of protection.

The severity levels, from most severe to least severe, are as follows:

- Delete entire message
- Delete attachment/message body and replace with text
- Quarantine entire message and replace with text
- Quarantine attachment/message body and replace with text
- Add tag to beginning of subject line
- Log only

For example, assume that you have two filtering rules enabled: Rule A and Rule B. Rule A is the higher priority, and the rule action is “Log only.” Rule B is the lower priority, and the rule action is to “Delete entire message.” A message that violates both rules is deleted.

If the message violates more than one rule and all of the rules have the same disposition, Mail Security uses the prioritization categorization to determine which rule action to apply.

For example, assume that you have two filtering rules enabled: Rule C and Rule D. Rule C is the higher priority, the rule action is “Add tag to the beginning of subject line,” and your customized text is "Spam." Rule D is the lower priority, the rule action is “Add tag to the beginning of subject line,” and your customized text is "Prohibited content." A message that violates both rules will have the subject line prepended with "Spam."

The rule order does not change in the Content filtering rules table. You can only view and modify rule prioritization in the Rule prioritization window.

To prioritize the filtering rules

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Content Enforcement, click Content Filtering Rules/File Type Filtering Rules.
3. In the sidebar under Tasks, click Prioritize rules.
   More than one rule must be enabled to prioritize rules.
4. In the Rule prioritization window, click a rule to select it.
5. Click Move up or Move down until the rule is at the priority that you want.
   Rules are prioritized from top to bottom, with the top being the highest priority.
6. Click OK.
7. On the toolbar, click Deploy changes to apply your changes.
   See “Deploying settings and changes to a server or group” on page 60.

Deleting a filtering rule

You can delete a content filtering or file type filtering rule when it is no longer needed.
To delete a filtering rule

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Content Enforcement**, click **Content Filtering Rules/File Type Filtering Rules**.
3. In the content area, select the rule that you want to delete.
4. In the sidebar under **Tasks**, click **Delete rule**.
5. In the confirmation dialog box, click **OK**.
6. On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

### Specifying inbound SMTP domains

By default, content filtering rules for inbound SMTP messages apply to messages that have at least one recipient who has a mailbox in the Exchange organization. Rules for outbound SMTP messages apply to messages that have at least one recipient that does not have a mailbox in the Exchange organization.

You can modify these settings by specifying the domains that your organization considers local. By adding a domain to the domain list, emails with recipients for that domain are considered local, even if they do not have local mailboxes.

**Note:** A single message can be considered both inbound and outbound. In this case, both inbound and outbound rules are applied to the message.

To specify inbound SMTP domains

1. In the console on the primary navigation bar, click **Admin**.
2. In the sidebar under **Views**, click **System Settings**.
3. In the content area, under **System Settings**, check **Enable list of internal domains**.
4. In the **List of internal domains** box, type the domain or domains that define which email message domains are inbound.
   Type only one domain per line.
5. On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.
Refreshing the Active Directory group cache

Mail Security does not refresh the Active Directory group cache when you create or edit a filtering rule. Mail Security automatically updates the cache upon startup and at 1:00 A.M. in the time zone to which your computer clock is set. You should manually update the cache if you modify the users in an Active Directory group that is used in a filtering rule. You should also manually update the cache if you create a filtering rule that applies to the Active Directory group Executives.

Note: This feature is not available for the Edge Server role.

For example, you create a filtering rule that applies to the Active Directory group Executives and deploy your changes. Then you add a user to the Executives group. After you deploy your changes, you must update the Active Directory group cache so that the rule applies to the user that you added to the group.

You must have access to Active Directory or be logged onto a client in the Active Directory domain to update the Active Directory group cache.

To refresh the Active Directory group cache

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Content Enforcement, click Content Filtering Rules/File Type Filtering Rules.
3. In the sidebar under Tasks, click Update Active Directory groups cache now.
4. In the Operation Status window, click Close when the operation is complete.

See "What you can do with the filtering rules" on page 146.

About enforcing email attachment policies

Mail Security contains the following default rule that enforces email attachment policies:

File Name Rule  Lets you filter attachments by file name

See “Blocking attachments by file name” on page 150.

Blocking attachments by file name

You can filter attachments by file name to protect your network during an outbreak. For example, in the case of a new email-borne threat, if you know the file name of the infected attachment, you can use this information to block any infected email messages.
You can configure Mail Security to match words and phrases that are in a match list against the names of files. Names of both non-container files (individual files without embedded files) and container files (files with embedded files) are examined.

The prohibited file is blocked if Mail Security detects a match. The entire container file is blocked if the prohibited file is within a container file.

For example, if an incoming .zip file named sample.zip contains three executable files (a.exe, b.doc, and c.bat), sample.zip is blocked if any of the following occurs:

- The match list contains one of the literal strings: sample.zip, a.exe, b.doc, or c.bat
- The match list contains one of the DOS wildcard expressions: *.zip, *.exe, *.doc, or *.bat
- The match list contains one of the regular expressions: sample\w*, a\w*, b\w*, or c\w*

See “About match lists” on page 154.

To block attachments by file name, do the following:

- Enable the File Name Rule.
- Select the match list that contains the file name attachments that you want detected. You can create or modify match lists when you modify the File Name Rule.
  
  You can only select one match list.
- Specify the action to take if a violation is detected, who to notify of the violation, and the notification message text.

To enable the File Name Rule

1. In the console, on the primary navigation bar, click **Policies**.
2. In the sidebar, under Content Enforcement, click **File Filtering Rules**.
3. In the content area, in the File Filtering Rules table, on the File Name Rule row, click the box under the Status column, and then click **Enabled** from the drop-down menu.

This rule is disabled by default.

To bypass scanning of container files

1. In the console, on the primary navigation bar, click **Policies**.
2. In the sidebar, under Content Enforcement, click **File Filtering Rules**.
3. In the content area, in the File Name Rule, select the **Bypass scanning of container file(s)** check box to bypass contents of container files without scanning. However, other filtering rules and AV scanning are applicable to the contents of the container.

This option is not selected by default.
To select an existing match list that does not need to be modified

1. In the console, on the primary navigation bar, click Policies.
2. In the sidebar under Content Enforcement, click File Filtering Rules.
3. In the File Filtering Rules table, select the rule that you want to modify.
4. In the File Filtering Rules preview pane, beside Match list for prohibited file names, click Select.
5. In the Select a match list window, in the Name table, select the match list, and then click Select.

To create a match list or modify an existing match list

1. In the File Filtering Rules table, select the rule that you want to modify.
2. In the console, on the primary navigation bar, click Policies.
3. In the sidebar under Content Enforcement, click File Filtering Rules.
4. In the File Filtering Rules table, select the rule that you want to modify.
5. In the File Filtering Rules preview pane, beside Match list for prohibited file names, click Select.
6. In the Select a match list window, do one of the following:
   - To modify an existing match list, select the match list, and on the toolbar, click Edit match list.
   - To create a new match list, on the toolbar, click New match list.
7. Under Filter, type the file attachment names, one per line, that you want to add to the match list.
8. Click OK.
9. In the Select a match list window, click Select to select the match list that you just created or modified.

To specify the action to take if a file filtering rule violation is detected

1. In the console, on the primary navigation bar, click Policies.
2. In the sidebar under Content Enforcement, click File Filtering Rules.
3. In the File Filtering Rules table, select the rule that you want to modify.
4. In the File Filtering Rules preview pane, in the Action to take list, use the drop-down menu to select one of the following:
   - Delete entire message
   - Delete attachment/message body and replace with text
- Quarantine entire message and replace with text
- Quarantine attachment/message body and replace with text
- Log only

The default setting is: Quarantine entire message and replace with text.

5 In the Replacement text box, type your customized message if you are replacing the message or attachment body with a text message.

The default text is: Symantec Mail Security replaced %attachment% with this text message. The original file contained %violation% and was %action%.

6 Check one or more of the following to send email notifications about the detection:

- Notify administrators
  Click the down arrow, and then type your customized text in the Subject line box and the Message body box.
  The default Subject line and Message body text is as follows:
  
  - Default Subject line text: Administrator Alert: Symantec Mail Security detected a message containing prohibited attachment
  - Default Message body text: Location of the message: %location% Sender of the message: %sender% Subject of the message: %subject% The attachment(s) "%attachment%" and/or the message was %action%. This was done due to the following Symantec Mail Security settings: Scan: %scan% Rule: %rule%

- Notify internal sender
  Click the down arrow, and then type your customized text in the Subject line box and the Message body box. The default Subject line and Message body text is as follows:
  
  - Default Subject line text: Symantec Mail Security detected a prohibited attachment in a message sent from your address
  - Default Message body text: Subject of the message: %subject% Recipient of the message: %recipient%

- Notify external sender
  Click the down arrow, and then type your customized text in the Subject line box and the Message body box. The default Subject line and Message body text is as follows:
  
  - Default Subject line text: Symantec Mail Security detected a prohibited attachment in a message sent from your address
  - Default Message body text: Subject of the message: %subject% Recipient of the message: %recipient%

7 On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.
About match lists

Mail Security uses match lists to filter email messages and attachments for specific words, terms, and phrases. To implement a match list, you must associate it with a content filtering rule or file filtering rule. When the rule is applied to scan messages, it also scans for the terms in the match list.

Note: The preconfigured match lists are designed to be used with content filtering rules. However, you can modify and use the preconfigured match lists with the File Name Rule file filtering rule.

Table 8-11 lists the preconfigured match lists that Mail Security provides.

Table 8-11 Preconfigured match lists

<table>
<thead>
<tr>
<th>Match list name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbreak Triggered Attachment Names</td>
<td>When you enable outbreak management, Mail Security adds the names of outbreak-triggered attachments to the Outbreak Triggered Attachment Names match list. You can use this match list with the Quarantine Triggered Attachment Names content filtering rule. This rule lets you automatically quarantine files with the attachment names that are found in the Outbreak Triggered Attachment Names match list. You can edit the rule description and the text in the Filter box. Leave the match type as wild cards. Note: The preconfigured match lists are designed to be used with content filtering rules. However, you can modify and use the preconfigured match lists with the File Name Rule file filtering rule. See &quot;Configuring outbreak triggers&quot; on page 197.</td>
</tr>
</tbody>
</table>
### Table 8-11 Preconfigured match lists (continued)

<table>
<thead>
<tr>
<th>Match list name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbreak Triggered Subject Lines</td>
<td>When you enable outbreak management, Mail Security adds the names of outbreak-triggered subject lines to the Outbreak Triggered Subject Lines match list.</td>
</tr>
<tr>
<td></td>
<td>You can use this match list with the Quarantine Triggered Subjects content filtering rule. This rule lets you automatically quarantine files with the subject line text that is found in the Outbreak Triggered Subject Lines match list.</td>
</tr>
<tr>
<td></td>
<td>You can edit the rule description and the text in the Filter box. Leave the match type as literal.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The preconfigured match lists are designed to use with content filtering rules. However, you can modify and use the preconfigured match lists with the File Name Rule file filtering rule.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring outbreak triggers” on page 197.</td>
</tr>
<tr>
<td>Sample Attachment Name</td>
<td>This match list contains a list of attachment file names or extensions that might contain malicious code.</td>
</tr>
<tr>
<td></td>
<td>You can edit the rule description and add or remove file extensions in the Filter box. Leave the match type as wild cards.</td>
</tr>
<tr>
<td>Sample Executable File Names</td>
<td>This list contains the file names or extensions that can potentially execute malicious code.</td>
</tr>
<tr>
<td></td>
<td>Leave the match type as wild cards.</td>
</tr>
<tr>
<td>Sample Message Body Words</td>
<td>This list contains keywords and phrases typically found in the bodies of spam email messages.</td>
</tr>
<tr>
<td></td>
<td>You can edit the rule description, add, or remove keywords and phrases in the Filter box, and modify the match type. The default match type is literal.</td>
</tr>
<tr>
<td>Sample Multimedia File Names</td>
<td>This list contains file names or extensions of multimedia files.</td>
</tr>
<tr>
<td></td>
<td>Leave the match type as wild cards.</td>
</tr>
<tr>
<td>Sample Subject Line</td>
<td>This list contains keywords and phrases typically found in spam email message subject lines.</td>
</tr>
<tr>
<td></td>
<td>You can edit the rule description, add, or remove keywords and phrases in the Filter box, and modify the match type. The default match type is literal.</td>
</tr>
<tr>
<td>Match list name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Canadian Social Insurance Keywords</strong></td>
<td>This match list contains the keywords that indicate a Canadian social insurance number. The default match type is literal. You can add or remove keywords in the <strong>Filter</strong> box.</td>
</tr>
<tr>
<td><strong>Canadian Social Insurance Numbers</strong></td>
<td>This match list contains a pattern that indicates a Canadian social insurance number. The default match type is regular expression.</td>
</tr>
<tr>
<td><strong>Credit Card Number Keywords</strong></td>
<td>This match list contains the keywords that are associated with a credit card number. The default match type is literal. You can add or remove keywords in the <strong>Filter</strong> box.</td>
</tr>
<tr>
<td><strong>Credit Card Number Pattern</strong></td>
<td>This match list contains a pattern that indicates a credit card number. The default match type is regular expression.</td>
</tr>
<tr>
<td><strong>M and A Project Code Names</strong></td>
<td>This match list contains the keywords that can help you identify information or communication about upcoming merger and acquisition activity. For example, <strong>MergerProjectName</strong>. The default match type is literal. You can add or remove keywords in the <strong>Filter</strong> box.</td>
</tr>
<tr>
<td><strong>Sensitive Project Code Names</strong></td>
<td>This match list contains sensitive project code names. The default match type is literal. You can add or remove keywords in the <strong>Filter</strong> box.</td>
</tr>
<tr>
<td><strong>SWIFT Code Keywords</strong></td>
<td>This match list contains the keywords that are associated with Society for Worldwide Interbank Financial Telecommunication (SWIFT) codes. The default match type is literal. You can add or remove keywords in the <strong>Filter</strong> box.</td>
</tr>
<tr>
<td><strong>SWIFT Code Regex</strong></td>
<td>This match list contains a pattern that indicates a SWIFT Code. The default match type is regular expression.</td>
</tr>
<tr>
<td><strong>UK Drivers License Numbers Pattern1</strong></td>
<td>This match list contains a pattern that indicates a UK drivers license number. The default match type is regular expression.</td>
</tr>
<tr>
<td><strong>UK Drivers License Numbers Pattern2</strong></td>
<td>This match list contains another pattern that indicates a UK drivers license number. The default match type is regular expression.</td>
</tr>
<tr>
<td>Match list name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>UK Electoral Roll Numbers Keywords</td>
<td>This match list contains the keywords that indicate a UK electoral roll number. The default match type is literal. You can add or remove keywords in the Filter box.</td>
</tr>
<tr>
<td>UK Electoral Roll Numbers Pattern</td>
<td>This match list contains a pattern that indicates a UK electoral roll number. The default match type is regular expression.</td>
</tr>
<tr>
<td>UK Keywords</td>
<td>This match list contains the keywords that indicate UK-related information. The default match type is literal. You can add or remove keywords in the Filter box.</td>
</tr>
<tr>
<td>UK NIN Keywords</td>
<td>This match list contains the keywords that indicate a UK national insurance number. The default match type is wild cards. You can add or remove keywords in the Filter box.</td>
</tr>
<tr>
<td>UK NIN Pattern</td>
<td>This match list contains a pattern that indicates a UK national insurance number. The default match type is regular expression.</td>
</tr>
<tr>
<td>UK Passport Keywords</td>
<td>This match list contains the keywords that indicate a UK passport number. The default match type is wild cards. You can add or remove keywords in the Filter box.</td>
</tr>
<tr>
<td>UK Passport Pattern (New)</td>
<td>This match list contains a pattern that indicates a UK passport number. The default match type is regular expression.</td>
</tr>
<tr>
<td>UK Passport Pattern (Old)</td>
<td>This match list contains another pattern that indicates a UK passport number. The default match type is regular expression.</td>
</tr>
<tr>
<td>UK Tax ID Number Keywords</td>
<td>This match list contains the keywords that indicate a UK tax ID number. The default match type is literal. You can add or remove keywords in the Filter box.</td>
</tr>
<tr>
<td>UK Tax ID Number Pattern</td>
<td>This match list contains another pattern that indicates a UK tax ID number. The default match type is regular expression.</td>
</tr>
<tr>
<td>US ITIN Keywords</td>
<td>This match list contains the keywords that indicate a US individual taxpayer identification number (ITIN). The default match type is literal. You can add or remove keywords in the Filter box.</td>
</tr>
</tbody>
</table>
### Preconfigured match lists (continued)

<table>
<thead>
<tr>
<th>Match list name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>US ITIN Pattern</td>
<td>This match list contains a pattern that indicates a US individual taxpayer identification number. The default match type is regular expression.</td>
</tr>
<tr>
<td>IP Address Pattern</td>
<td>This match list contains a pattern that indicates an IP address. The default match type is regular expression.</td>
</tr>
<tr>
<td>US SSN Keywords</td>
<td>This match list contains the keywords that indicate a US individual social security number (SSN). The default match type is literal. You can add or remove keywords in the Filter box.</td>
</tr>
<tr>
<td>US SSN Patterns</td>
<td>This match list contains another pattern that indicates a US individual social security number. The default match type is regular expression.</td>
</tr>
</tbody>
</table>

See “Creating or editing a match list” on page 158.

See "Deleting a match list" on page 159.

## Creating or editing a match list

Mail Security provides some preconfigured match lists that you can use with content filtering rules and the File Name Rule file filtering rule. You can also create your own match list or modify an existing match list. Match lists support literal strings, DOS wildcard-style expressions, or regular expressions.

See “About match lists” on page 154.

**To create or edit a match list**

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **Content Enforcement**, click **Match Lists**.
3. Do one of the following:
   - **Create a match list** In the sidebar under **Tasks**, click **New match list**.
   - **Edit an existing match list** In the content area under **Match Lists**, select the list that you want to edit, and then in the sidebar under **Tasks**, click **Edit match list**.
4. In the **New Match List** window, in the **Title** box, type a name for the match list.
   - You can only configure the title when you create a new match list.
5. In the **Description** box, type a description for the match list.
In the Match Type box, select one of the following:

- Literal string
- Regular expression
- Wild cards

The match type you select is specific for a match list. The match type that you choose when you add or edit a rule does not affect a match list.

In the Filter box, type a literal string, regular expression, or DOS wildcard-style expression. Enter one expression per line. You can link several regular expressions to form a larger one to match certain content in email.

Click OK.

On the toolbar, click Deploy changes to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

Deleting a match list

You can delete only those match lists that are not used in any content filtering or file filtering rules or any content filtering policy templates.

See “About match lists” on page 154.

To delete a match list

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Content Enforcement, click Match Lists.
3. In the content area, under Match Lists, select the match list that you want to delete.
4. In the sidebar under Tasks, click Delete match list.
5. In the confirmation dialog box, click OK.
6. On the toolbar, click Deploy changes to apply your changes.

About DOS wildcard style expressions

DOS wildcard style expressions ("**", ".", and "?") provide a convenient way to specify file names, similar to the way in which DOS wildcard characters are used. For example, match lists of type DOS wildcard are typically used with the Attachment Name Attribute to specify file names such as *.exe. In addition, a DOS wildcard expression lets you easily specify files without extensions.

Table 8-12 describes the DOS wildcard style expressions.
### Table 8-12 DOS wildcard expressions

<table>
<thead>
<tr>
<th>DOS wildcard expression</th>
<th>Equivalent regular expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>.*</td>
<td>Zero or more of any character</td>
</tr>
<tr>
<td>?</td>
<td>[^.]?</td>
<td>Any one character except the period (.)</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
<td>Literal period character</td>
</tr>
<tr>
<td>*.</td>
<td>[^.]+.?</td>
<td>Does not contain a period, but can end with one</td>
</tr>
</tbody>
</table>

See “About regular expressions” on page 160.

### About regular expressions

A regular expression is a set of symbols and syntactic elements that Mail Security uses to match patterns of text. Mail Security matches regular expressions on a line-by-line basis. It does not evaluate the line feed (newline) character at the end of each input expression phrase.

You can build regular expressions using a combination of normal alphanumeric characters and metacharacters. For example, some email messages contain a trailing number at the end of the subject line text. Trailing numbers often indicate that a message is spam. Consider the following sample subject line:

Here’s a hot stock pick!43234

To write a rule to match email subject lines that have trailing numbers, compare the subject against the following regular expression:

`^.+![0-9]+$`

This regular expression contains the normal alphanumeric characters 0-9 and the following metacharacters: circumflex (^), period (.), plus (+), and open and close brackets ([, ]). By using the subject attribute, the = operator, and the regular expression as the value, you can build a content filtering rule to catch any email messages whose subject lines end with a trailing number.

See “Regular expressions” on page 160.

### Regular expressions

You can combine alphanumeric characters and metacharacters to create match patterns for rules that will block messages and attachments specifically designed to bypass file filtering rules.
Table 8-13 lists examples of regular expressions that show how pattern matching is accomplished with the use of metacharacters and alphanumerical characters.

<table>
<thead>
<tr>
<th>Regular expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>abc</td>
<td>Matches any line of text that contains the three letters abc in that order. Your results may differ depending on the comparison that you use to create the rule. For example, if you build a rule to match the word Free and use the Contains condition, then the filtering engine detects all words that contain the word Free instead of an exact match (for example, Freedom). However, if you use the Equal condition, then the filtering engine detects only exact matches of the word Free with no other surrounding text. If you use the Contains condition with Whole words only, then the filtering engine detects Free as a stand-alone word, even if there are other words present in the text that is being searched.</td>
</tr>
<tr>
<td>a.c</td>
<td>Matches any string that begins with the letter a, followed by any character, followed by the letter c.</td>
</tr>
<tr>
<td>^.$</td>
<td>Matches any line that contains exactly one character. (The newline character is not counted.)</td>
</tr>
<tr>
<td>a(b*</td>
<td>c*)d</td>
</tr>
</tbody>
</table>
| .+\...\....      | Matches any file name that has two, three-letter extensions (for example, Filename.gif.exe). This regular expression is helpful in blocking email attachments with double extensions. For example:  
If Attachment Name + .+\...\.... |
| [0-9a-zA-Z]+<!--.*-->[0-0a-zA-Z]+ | Matches an embedded comment in the middle of meaningful HTML text. Embedding comments within HTML text is a trick that spam senders use to bypass some pattern-matching software. |
| \s*               | Matches a white space character zero or more times. |

See “About regular expressions” on page 160.

See “About DOS wildcard style expressions” on page 159.

About metacharacters

Table 8-14 lists the metacharacters that you can use in regular expressions to build filtering rules.
Some characters are not considered special unless you use them in combination with other characters.

**Note:** You can use metacharacters in regular expressions to search for both single-byte and multi-byte character patterns.

<table>
<thead>
<tr>
<th>Metacharacter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>Period: Matches any single character of the input sequence.</td>
</tr>
<tr>
<td>^</td>
<td>Circumflex: Represents the beginning of the input line. For example, ^A is a regular expression that matches the letter A at the beginning of a line. The ^ character is only a special character at the beginning of a regular expression, or after the [ or</td>
</tr>
<tr>
<td>$</td>
<td>Dollar sign: Represents the end of the input line. For example, A$ is a regular expression that matches the letter A at the end of a line. The $ character is only special character at the end of a regular expression or before the ) or</td>
</tr>
<tr>
<td>*</td>
<td>Asterisk: Matches zero or more instances of the string to the immediate left of the asterisk. For example, A* matches A, AA, AAA, and so on. It also matches the null string (zero occurrences of A).</td>
</tr>
<tr>
<td>?</td>
<td>Question mark: Matches zero or one instance of the string to the immediate left of the question mark.</td>
</tr>
<tr>
<td>+</td>
<td>Plus sign: Matches one or more instances of the string to the immediate left of the plus sign.</td>
</tr>
<tr>
<td>\</td>
<td>Escape: Turns on or off the special meaning of metacharacters. For example, . only matches a dot character. $ matches a literal dollar sign character. Note that \ matches a literal \ character.</td>
</tr>
<tr>
<td></td>
<td>Pipe: Matches either expression on either side of the pipe. For example, exe</td>
</tr>
</tbody>
</table>
Table 8-14  Metacharacter descriptions (continued)

<table>
<thead>
<tr>
<th>Metacharacter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[string]</td>
<td>Brackets: Inside the brackets, matches a single character or collating element, as in a list. Characters within brackets are not case-sensitive. The string inside the brackets is evaluated literally, as if an escape character () were placed before each character in the string. If the initial character in the bracket is a circumflex (^), then the expression matches any character or collating element except those inside the bracket expression. If the first character after any potential circumflex (^) is a dash (-) or a closing bracket (]), then that character matches only a literal dash or closing bracket.</td>
</tr>
<tr>
<td>(string) (\text{string})</td>
<td>Parentheses: Groups parts of regular expressions, which gives the string inside the parentheses precedence over the rest.</td>
</tr>
</tbody>
</table>

The order in which metacharacters are evaluated, from highest to lowest precedence, is as follows:

- Escape \ \n- List [ ]
- Precedence override ( )
- Single character *
- +
- ?
- Start with ^
- $
- Alternation |

See “About regular expressions” on page 160.

**About content filtering policy templates**

Content filtering policy templates let you create an enhanced content filtering rules that help prevent data leakage.

These templates are a combination of match lists. Each match list in a template is associated with a frequency. The frequency specifies the number of matches from the match list.
You can edit an existing template but cannot create a new template or delete an existing one. See “Editing a content filtering policy template” on page 167.

Table 8-15 lists the preconfigured templates that Mail Security provides.

### Table 8-15  Preconfigured content filtering policy templates

<table>
<thead>
<tr>
<th>Template name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Canadian Social Insurance Number                  | You can use this template in a rule to detect the patterns that indicate Canadian Social Insurance Numbers that are at a risk of exposure. This template is a combination of the following match lists:  
  - Canadian Social Insurance Numbers  
  - Canadian Social Insurance Keywords |
| Credit Card Numbers                               | You can use this template in a rule to detect the patterns that indicate credit card numbers at a risk of exposure. This template is a combination of the following match lists:  
  - Credit Card Number Keywords  
  - Credit Card Number Pattern |
| Individual Taxpayer Identification Number (ITIN)  | An Individual Taxpayer Identification Number (ITIN) is a tax processing number issued by the US Internal Revenue Service (IRS). The IRS issues ITINs to track individuals who are not eligible to obtain a social security number (SSN).  
  You can use this template in a rule to detect individual taxpayer identification numbers. This template is a combination of the following match lists:  
  - US ITIN Keywords  
  - US ITIN Pattern |
| Mergers and Acquisitions Data                     | You can use this template in a rule to detect information and communication about upcoming merger and acquisition activity.  
  Before you use this template in a rule, you must specify company-specific code words in the M and A Project Code Names match list to detect specific deals. |
### Table 8-15  Preconfigured content filtering policy templates (continued)

<table>
<thead>
<tr>
<th>Template name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Data</td>
<td>You can use this template in a rule to identify the sensitive project code names that are at a risk of exposure. Before you use this template in a rule, you must specify sensitive project code name in the <strong>Sensitive Project Code Names</strong> match list.</td>
</tr>
</tbody>
</table>
| UK Tax ID Numbers      | You can use this template in a rule to detect UK Tax ID numbers. This template helps you detect UK Tax ID numbers by using the official specification of the UK Government Standards of the UK Cabinet Office. This template is a combination of the following match lists:  
  ■ UK Tax ID Number Keywords  
  ■ UK Tax ID Number Pattern |
| SWIFT Codes            | The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a cooperative organization under Belgian law and its member financial institutions own it. The SWIFT code is also known as a Bank Identifier Code (BIC) or ISO 9362. The SWIFT code has a standard format to identify a bank, location, and the branch involved. These codes are used to transfer money between banks, particularly across international borders. You can use this template in a rule to detect valid SWIFT codes. This template is a combination of the following match lists:  
  ■ SWIFT Code Keywords  
  ■ SWIFT Code Regex |
<table>
<thead>
<tr>
<th>Template name</th>
<th>Description</th>
</tr>
</thead>
</table>
| UK Drivers License Numbers | This policy template helps you detect UK drivers license numbers by using the official specification of the UK Government Standards of the UK Cabinet Office. This template is a combination of the following match lists:  
  - UK Keywords  
  - UK Drivers License Numbers Pattern1  
  - UK Drivers License Numbers Pattern2  |
| UK Passport Numbers        | This policy template helps you detect valid UK passports by using the official specification of the UK Government Standards of the UK Cabinet Office. This template is a combination of the following match lists:  
  - UK Passport Keywords  
  - UK Passport Pattern (New)  
  - UK Passport Pattern (Old)  |
| UK National Insurance Numbers | UK Department for Work and Pensions and Inland Revenue (DWP/IR) issues the national insurance numbers to individuals to administer the national insurance system. You can use this template in a rule to identify valid UK national insurance numbers. This template is a combination of the following match lists:  
  - UK NIN Keywords  
  - UK NIN Pattern  |
| UK Electoral Roll Numbers  | You can use this template in a rule to detect UK electoral roll numbers. This template is a combination of the following match lists:  
  - UK Keywords  
  - UK Electoral Roll Numbers Pattern  
  - UK Electoral Roll Numbers Keywords |
Table 8-15 Preconfigured content filtering policy templates (continued)

<table>
<thead>
<tr>
<th>Template name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>US SSN Numbers</td>
<td>This policy template detects US SSN Numbers, which is a personal identification number issued by the Social Security Administration of the United States government. You can use this template in a rule to identify valid US individual social security numbers. This template is a combination of the following match lists: ■ US SSN Keywords ■ US SSN Patterns</td>
</tr>
</tbody>
</table>

Editing a content filtering policy template

You can edit a content filtering policy template by using any of the following options:

- Enable or disable the conditions that are used in a template.
- Edit the frequency that is specified for match lists in a template.
- Edit the match lists that are used in a template.

See “Creating or editing a match list” on page 158.

You can customize the default templates based on your requirements. For example, every organization has sensitive information regarding to their projects. You can use the Sensitive Project Code Names match list to feed project code names. The Project Data template uses the Sensitive Project Code Names match list to identify the project code names that are at a risk of exposure.

When you edit a template, the changes are reflected in all the content filtering rules that use the template.

See “About content filtering policy templates” on page 163.

To edit a content filtering policy template

1. In the console on the primary navigation bar, click Policies.
2. In the sidebar under Content Enforcement, click Content Filtering Rules.
3. In the content area, double-click a rule.
4. On the Rule tab under Content pane, click Template.
5 In the Select a template window, select the template that you want to edit and click Edit template. Alternatively you can double-click the template that you want to edit.

6 Edit the description for the template.

7 Edit the frequency that is specified for match lists in the template.

8 Uncheck the box beside the match list name to disable it.

   If you disable the parent condition, the child conditions are no longer applicable.

9 Click OK and then click Close.

10 Click OK.

11 On the toolbar, click Deploy changes to apply your changes.
Scanning your Exchange servers for threats and violations

This chapter includes the following topics:

- About the types of scanning that you can perform
- How Mail Security scans messages
- Configuring Auto-Protect scanning
- Configuring background scanning for Exchange Server 2010 mailbox role
- Configuring advanced scanning options for Auto-Protect and background (Exchange Server 2010 only) scanning
- About manual scans
- About scheduling a scan
- Configuring notification settings for scan violations

About the types of scanning that you can perform

You can perform the following types of scans to detect risks, spam, and violations:
<table>
<thead>
<tr>
<th>Scanning Type</th>
<th>Description</th>
<th>Relevant Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Protect scans</td>
<td>When Auto-Protect is enabled, it runs constantly and detects threats and violations in real-time to everything that is on or passes through your Exchange server. Auto-Protect scanning applies to all policies, except for antispam detection. Antispam scanning occurs continuously, in real-time as email traffic flows through your Exchange server.</td>
<td>See “Configuring Auto-Protect scanning” on page 175.</td>
</tr>
<tr>
<td>Manual scans</td>
<td>Manual scans run on-demand and scan public folders and mailboxes. All policies apply to manual scans, except antispam. Antispam scanning continuously occurs in real-time as email traffic flows through your Exchange server. You can specify which file folders and mailboxes to scan during a manual scan. You can also specify the filtering rules that you want to enable for the manual scan.</td>
<td>See “About manual scans” on page 180.</td>
</tr>
<tr>
<td>Scheduled scans</td>
<td>Scheduled scans run unattended, usually at off-peak periods. All policies apply to scheduled scans, except antispam. Antispam scanning continuously occurs in real-time as email traffic flows through your Exchange server. You can specify which file folders and mailboxes to scan during a scheduled scan. You can also specify the filtering rules that you want to enable for the scheduled scan.</td>
<td>See “About scheduling a scan” on page 186.</td>
</tr>
<tr>
<td>Background scanning</td>
<td>Background scanning is a scan of the message store on Exchange Server 2010 Mailbox role. You can perform scans of the message store during off-peak periods to enhance performance.</td>
<td>See &quot;Configuring background scanning for Exchange Server 2010 mailbox role&quot; on page 176.</td>
</tr>
</tbody>
</table>

When Mail Security detects a security risk or a violation during a scan, it takes the action that you specify for that policy. For example, when a threat is detected, Mail Security takes the action that you specify in the Antivirus Settings policy.

Mail Security does not support the **Quarantine entire message and replace with text** action for Auto-Protect, Manual, Scheduled, or Background scanning. If a violation is detected during these scans, Mail Security quarantines the message by parts although you specify the action as **Quarantine entire message and replace with text** for a policy.

**Excluding Journal database from On Access and Background scanning**

SMSMSE has an additional option to exclude Journal database from On Access and Background scanning.
To configure this option

1. Create a REG_DWORD registry named `BypassVsapiDbScan` at location `HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\SMSMSE\7.9\Server` and set it to 1.

2. Create a file named `vsapi.xmb` at the location `...\Server\Config`.

   Enter the Journal database names that you want to exclude from scanning and save the file.

   **Note:** Ensure that each Journal database name is entered on a new line.

3. Set the registry `ReloadNow` to 1 and wait for this value to set back to 0 for changes to take effect.

   This registry is located at `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSExchangeIS\VirusScan`.

4. Whenever the file `vsapi.xmb` is updated further with new database entries or the database entries are removed, perform step 3 for the changes to take effect.

   See “About the types of scanning that you can perform” on page 169.

---

**How Mail Security scans messages**

When Auto-Protect scanning is enabled, Mail Security applies a stamp to messages it scans at the Edge Transport or Hub Transport servers. The stamp indicates the version of definitions that were used for the scan. Each time Mail Security scans the message, it also scans for file filtering rule violations.

See “Configuring Auto-Protect scanning” on page 175.

Mail Security searches for this stamp each time the message is routed through the mail flow to another server. Mail Security determines if the message has been scanned and if the message was scanned with the most current definitions. When the server in which the mail is routed contains more current definitions than those indicated in the stamp, the message is rescanned with the newer definitions.

**Note:** Messages that have been stamped are not rescanned for file filtering and content filtering rules.

The message is disposed of based on the settings that you configure when Mail Security detects a violation. No stamp is applied to the message, even if the message is repaired. If the message is routed to another server role, Mail Security detects that there is no stamp and rescans the message.
Figure 9-1 shows how an incoming email message is scanned as it enters your Exchange Server 2010 environment.

**Figure 9-1**  How incoming email messages are scanned

![Diagram of email message scanning process](image)

- **Internet**
  - The message is scanned
  - **No virus or violation is detected**
    - The message is stamped
      - Definitions in stamp are compared to Hub definitions
      - Hub definitions are the same as or older than those used at the Edge
      - The message is rescanned
      - Mailbox definitions are the same as or older than those used in stamp
      - The message is delivered to the recipient's mailbox
  - **A virus or violation is detected**
    - The message is disposed of (no stamp is applied)
      - Quarantine
      - Repair
      - Delete attachment
      - Message body
      - Log only
      - The message is rescanned
      - Mailbox definitions are more current
      - The message is delivered to the recipient's mailbox
      - The message is delivered to the recipient's mailbox
      - The message is disposed of
        - Delete entire message
      - The message is delivered to the recipient's mailbox
      - The message is rescanned on access
      - No virus or violation is detected
        - The message is stamped
          - Definitions in stamp are compared to Mailbox definitions
          - Hub definitions are the same as or older than those used in stamp
          - The message is delivered to the recipient's mailbox
          - The message is delivered to the recipient's mailbox
          - The message is delivered to the recipient's mailbox
          - The message is disposed of
            - Delete entire message
      - A virus or violation is detected
        - The message is disposed of (no stamp is applied)
          - Quarantine
          - Repair
          - Delete attachment
          - Message body
          - Log only
          - The message is rescanned
          - Mailbox definitions are more current
          - The message is delivered to the recipient's mailbox
          - The message is delivered to the recipient's mailbox
          - The message is disposed of
            - Delete entire message

Figure 9-2 shows how an outgoing email message is scanned as it leaves your Exchange Server 2010 environment.
Figure 9-2 shows how outgoing email messages are scanned.

The outgoing message is routed to the Hub Transport server. By default, the message is not scanned nor stamped.

The message is scanned.

No virus or violation is detected.

A virus or violation is detected.

The message is stamped.

Definitions in stamp are compared to Edge definitions.

(edge definitions are the same or older than the Hub definitions)

(edge definitions are more current)

The message is rescanned.

A virus or violation is detected.

The message is disposed of (no stamp is applied)

Quarantine
Repair
Delete attachment/message body
Log only

Delete entire message

The message is disposed of

Quarantine
Repair
Delete attachment/message body
Log only

Delete entire message

Definitions in stamp are compared to Edge definitions.

Outgoing message is routed to the Hub Transport server.

By default, the message is not scanned nor stamped.

Figure 9-3 shows how an internally routed email message is scanned.
How Mail Security offloads Mailbox server scanning for Exchange Server 2010

Mail Security lets you offload Mailbox server scanning to enhance server performance. Most of the scanning is performed on the Hub Transport and Edge Transport servers.
Mail Security scans email messages at the Mailbox only when the following occurs:

- An incoming email message does not have a stamp that indicates that it has already been scanned.
- The Mailbox server has more current definitions than those used to scan the message at the Hub Transport or Edge Transport servers.
- You schedule background scanning.
  See “Configuring background scanning for Exchange Server 2010 mailbox role” on page 176.
- You disable the "Exclude outbound scanning on mailbox server" setting.
  This option is enabled by default.
  See “Configuring advanced scanning options for Auto-Protect and background (Exchange Server 2010 only) scanning” on page 179.
- You send an Outlook Web Access message.

How Mail Security optimizes scanning performance for Exchange Server 2010

Mail Security is integrated with Exchange Server 2010 to enhance scanning performance. Scanning performance is enhanced by reducing the amount of scanning that takes place as mail is routed through your Exchange environment across the various roles and by offloading Mailbox server scanning.


Note: Install and configure Mail Security on all of the server roles in your Exchange environment using the same parameters. This ensures optimum scanning performance and violation and threat detection.

See “How Mail Security scans messages ” on page 171.

Configuring Auto-Protect scanning

Auto-Protect scanning provides continuous risk and violation detection. When you enable Auto-Protect scanning, Mail Security scans email messages as they pass through the Exchange server. Infected message bodies and attachments and rule violations are detected on a real-time basis, based on the settings that you enable and configure.

You must enable Auto-Protect scanning to perform background scanning.

See “Configuring background scanning for Exchange Server 2010 mailbox role” on page 176.
To configure Auto-Protect scanning

1. In the console on the primary navigation bar, click **Scans**.
2. In the sidebar under **Views**, click **Auto-Protect**.
3. In the content area, under **Auto-Protect Settings**, check **Enable Auto-protect**.
4. On the toolbar, click **Deploy changes** to apply your changes.

**Note:** If the Auto-Protect status on the SMSMSE UI is seen as “Started (VSAPI is still down)”, the transport scan functionality works seamlessly but the On Access scan and Background scanning functionality may not function.

See “Deploying settings and changes to a server or group” on page 60.

## Configuring background scanning for Exchange Server 2010 mailbox role

When Mail Security is installed on a Microsoft Exchange Mailbox server and background scanning is enabled, Microsoft Exchange creates a background thread for each message database in the Exchange store. These threads run at a lower priority to minimize the impact on other Exchange server actions. As each thread reads through the messages in the database, it detects the messages that have not been scanned by the latest definitions and scans them. This is useful if you have updated your definitions and need to re-scan the entire store with new definitions.

You can also scan the email messages that have attachments and specify which messages to scan based on the message date.

**Note:** Mail Security enables the Exchange VSAPI background scanning feature. Based on the load and Microsoft Exchange’s algorithms, Microsoft might interrupt the background scanning process.

See “Configuring advanced scanning options for Auto-Protect and background (Exchange Server 2010 only) scanning” on page 179.

See “About enhancing performance when you update definitions on Exchange 2010 mailbox server” on page 235.
To configure background scanning

1. In the console on the primary navigation bar, click **Scans**.
2. In the sidebar under Views, click **Auto-Protect**.
3. In the content area, under **Background Scanning Options**, check **Enable background scanning**.
   
   You can select this option only when **Enable Auto-Protect** option is checked.

   See “Configuring Auto-Protect scanning” on page 175.

4. Do one of the following:
   - In the schedule matrix, click the boxes for the days and hours during which you want background scanning to occur.
   - Under the schedule matrix, click the drop-down list and select the day that you want background scanning to occur, the time that you want scanning to start, the time that you want scanning to finish, and then click **Select**.
   - Click **Select All** to select all day and time ranges.

   The boxes in the schedule matrix are blackened to indicate the time frames that background scanning will occur.

   Click **Clear All** to clear all of the options that you selected.

   You must indicate a time range for background scanning to run.

5. Check **Scan messages with attachments only** to scan email messages and their attachments that are in the mailbox store.

   Mail Security only scans the messages that have attachments when you select this option.

6. Under **Choose messages to scan**, select one of the following options:

   - **Scan all messages in the store**
     - Scans all messages in the store.
   - **Scan all messages from the past number of days**
     - Scans all messages from the past number of days.
     - Type the number of days.
     - The default setting is 2 days.
Scan all messages from the past number of hours

Scans all messages from the past number of hours.

Type the number of hours.

The time is measured from the time at which the scan starts. For example, at 12:05 PM a user schedules a background scan to start at 8:00 P.M. The user enables the "Scan all messages from the past number of hours" and selects a value of 10. The time frame for the messages to be scanned would be 10 hours before 8:00 PM.

Scan all messages from the start date

If you select this option, do the following:

- Click the drop-down arrow and specify the start date.
- Select one of the following options:
  - To the date of the scan
    Performs the scan as of the start date that you specify to the current date.
  - To the following date
    Performs the scan as of the start date that you specify to the date that you specify in the drop-down list.

7 On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

**Background scan log status for Exchange Server 2010 mailbox role**

Mail Security version 6.5.5 provides improved logs with status of the background scan. An event is generated when background scan is either halted or is completed. This event also provides the count of the number of items that were scanned so far during the background scan. Another event is generated when background scan is completed. This event provides the total time that is taken for completing the scan. See “Configuring background scanning for Exchange Server 2010 mailbox role” on page 176.

**Stopping background scanning on Exchange Server 2010 mailbox role**

You can stop Mail Security from running a background scan at any time.
To stop a background scan

1. In the console on the primary navigation bar, click **Scans**.
2. In the sidebar under **Views**, click **Auto-Protect**.
3. In the content area, under **Background Scanning Options**, uncheck **Enable background scanning**.
4. On the toolbar, click **Deploy changes**.

See “Configuring background scanning for Exchange Server 2010 mailbox role” on page 176.

---

**Configuring advanced scanning options for Auto-Protect and background (Exchange Server 2010 only) scanning**

You can configure the additional scanning options that apply to Auto-Protect and background scanning for Exchange Server 2010 mailbox role.

To configure advanced scanning options for Auto-Protect and background scanning

1. In the console on the primary navigation bar, click **Scans**.
2. In the sidebar under **Views**, click **Auto-Protect**.
3 Under **Advanced Scanning Options**, check any of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan message bodies (applies to AV only)</td>
<td>Detects the risks in message bodies. The option is disabled by default.</td>
</tr>
<tr>
<td>Exclude outbound scanning on mailbox server</td>
<td>Prevents the scanning of outbound messages so that they can be scanned at the Hub Transport. This option is enabled by default.</td>
</tr>
<tr>
<td>On virus definition update, force rescan before allowing access to Information Store</td>
<td>Performs a scan each time definitions are updated and a user attempts to access a message. Microsoft Exchange does not allow access to any messages in the store until Mail Security re-scans the message with the latest definitions when a user attempts to access a file. As the definitions are delivered frequently, the scan might not complete before new definitions are available. This can affect overall mail throughput. This option is disabled by default. <strong>Note:</strong> If this option is selected, background scanning of the store restarts after every virus definition update. Ensure that you do not select this option if you want to complete background scanning of the entire store. See &quot;About keeping your server protected&quot; on page 230.</td>
</tr>
</tbody>
</table>

4 Under **Advanced Scanning Options**, check **Scan message bodies (applies to AV only)**.

5 On the toolbar, click **Deploy changes** to apply your changes.

   See “Deploying settings and changes to a server or group” on page 60.

### About manual scans

You can perform manual scans when you want to scan messages for specific purposes. For example, you can create a content filtering rule to detect a particular category of subject-line violations that are associated with a new threat, and then run the scan immediately.
To perform a manual scan, do the following:

■ Configure the manual scan parameters.

You can configure basic scanning options and specify the mailboxes, archive mailboxes, and public folders that you want to scan. You can also enable filtering and enable the filtering rules that you want to apply to the scan.

**Note:** Ensure that the public folders that you want to scan have owners assigned to them. Mail Security does not perform a manual scan on the public folders that do not have owners assigned to them.

See “Configuring the manual scan parameters” on page 181.

■ Run the manual scan.

**Note:** Before you run the manual scan, ensure that you create a custom throttling policy and assign it to the Symantec Mail Security for Microsoft Exchange service account user.

See “Creating and assigning a custom throttling policy to the Mail Security service account user” on page 73.

See “Performing a manual scan” on page 185.

■ View the manual scan results.

See “Viewing manual scan results” on page 185.

You can stop running a manual scan at any time.

**Configuring the manual scan parameters**

Before you run a manual scan, configure the parameters for the scan. After you deploy your changes, the parameters remain the same until you change them.

Mail Security lets you specify the following parameters for a manual scan:
### Scan Options

You can choose from the following basic scanning options:

- **Stop scanning after ___ minutes. Next scan will restart where it stopped**
  
  Select this option if you want to specify a duration for the scan. Type the number of minutes you want the scan to run in the box next to the option.

- **Scan only the items modified since last rescan**
  
  Select this option to scan only the items that have been modified since the last scan. Scanning only the items that have been modified decreases overall scanning time.

- **Scan message bodies (Applies to AV only)**
  
  Select this option to scan only the message bodies. Scanning message bodies increases the overall scanning time.

### Scan location

You can specify the mailboxes, archive mailboxes, and public folders that you want included or excluded from the scan.

You can select one of the following options:

- **Exclude archive**: You can specify to exclude archive mailbox scanning, and scan mailboxes only.

- **Archive with mailboxes**: You can specify this option to scan both mailboxes and its associated archive mailbox.

- **Archive Only**: You can specify to scan only archive mailboxes as per selection of mailboxes in the list.

**Note:** When you select *All mailboxes* or *Specific Mailboxes*, the associated archive mailbox is selected or excluded based on the options selected: Exclude archive, Archive with mailboxes, Archive only.

The **Scan location** option is available if you are in a server view only.

### Content filtering rules

You can enable or disable content filtering scanning. If content filtering is enabled, enable the rules that you want to apply to the scan.

Content filtering is enabled by default.

### File type filtering rules

You can enable or disable file type filtering. If file type filtering is enabled, enable the rules that you want to apply to the scan.

### To configure basic scanning options

1. In the console on the primary navigation bar, click **Scans**.
2. In the sidebar under **Views**, click **Manual Scan**.
3. Under **Tasks**, click **Edit manual scan**.
4. In the Manual Scan Wizard, under **Scan Options**, check one or more of the following:
   - **Stop scanning after ___ minutes**

   If you select this option, type the number of minutes you want the scan to run.
The default value is 120.

- Only scan the items modified since last scan
- Scan message bodies (applies to AV only)

5 Under **Choose messages to scan**, select one of the following options:

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan all messages in the store</td>
<td>This is the default setting.</td>
</tr>
<tr>
<td>Scan all messages from the past number of days</td>
<td>Scans all messages from the past number of days.</td>
</tr>
<tr>
<td></td>
<td>Type the number of days in the box to the right.</td>
</tr>
<tr>
<td>Scan all messages from the past number of hours</td>
<td>Scans all messages from the past number of hours.</td>
</tr>
<tr>
<td></td>
<td>Type the number of hours in the box to the right.</td>
</tr>
<tr>
<td>Scan all messages from the start date</td>
<td>If you select this option, do the following:</td>
</tr>
<tr>
<td></td>
<td>■ Use the drop-down menu to specify the start date.</td>
</tr>
<tr>
<td></td>
<td>■ Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>■ To the date of the scan</td>
</tr>
<tr>
<td></td>
<td>Performs the scan as of the start date that you specify to the current date</td>
</tr>
<tr>
<td></td>
<td>■ To the following date</td>
</tr>
<tr>
<td></td>
<td>Performs the scan as of the start date that you specify to the date that you specify in the drop-down list</td>
</tr>
</tbody>
</table>

6 Click **Next**.
To configure the scan location

1. Under **Scan Location**, to specify mailboxes to scan, select one of the following:
   - **All mailboxes** — Scans all mailboxes.
     - This option is enabled by default.
   - **Exclude mailboxes** — Scans no mailboxes.
   - **Specific mailboxes** — Scans only the mailboxes that you specify in the list box.
     - This option is available in the single-server view only.

2. To specify public folders to scan, select one of the following:
   - **All public folders** — Scans all public folders.
     - This option is enabled by default.
   - **Exclude public folders** — Scans no public folders.
   - **Specific public folders** — Scans only the public folders that you specify in the list box.
     - This option is available in the single-server view only.

3. Click **Next**.

To disable content and file type filtering

1. Uncheck **Enable content filtering**/**Enable file type filtering**.
   - This option is enabled by default.

2. Click **Finish**.

3. On the toolbar, click **Deploy changes** to apply your changes.

   See “Deploying settings and changes to a server or group” on page 60.

To enable content and file type filtering

1. Check **Enable content filtering**/**Enable file type filtering**.
   - This option is enabled by default.

2. Do any of the following:
   - To add a new filtering rule, on the toolbar, click **Add new**.
   - To modify an existing filtering rule, on the toolbar, click **Edit rule**.
   - To delete an existing filtering rule, click **Delete rule**.

   See “About creating the filtering rules” on page 126.
3 Click the box under the Enable column and select Enable to enable the rules that you want to apply to the scan.
4 Click Finish.
5 On the toolbar, click Deploy changes to apply your changes.

Performing a manual scan
After you configure the manual scan parameters, you can perform the manual scan.
See “Viewing manual scan results” on page 185.

To perform a manual scan
1 In the console on the primary navigation bar, click Scans.
2 In the sidebar under Views, click Manual Scan.
3 Under Tasks, click Run now.
   To stop the scan before it finishes, in sidebar under Tasks, click Stop.
4 In the Operation Status window, click Close when the operation is complete.

Stopping a manual scan
You can stop Mail Security from finishing a manual scan at any time.

To stop a manual scan
1 In the console on the primary navigation bar, click Scans.
2 In the sidebar under Views, click Manual Scan.
3 Under Tasks, click Stop.
See “Performing a manual scan” on page 185.

Viewing manual scan results
The Manual Scan page shows the results of the most recent manual scan.

To view manual scan results
1 In the console on the primary navigation bar, click Scans.
2 In the sidebar under Views, select Manual Scan.
3 Press F5 to refresh the page.
   This process might take several minutes for large server groups.
About scheduling a scan

In addition to Auto-Protect scanning and manual scanning, you can schedule scans to look for different types of policy violations.

See “Creating a scheduled scan” on page 186.
See “Editing a scheduled scan” on page 186.
See “Configuring scheduled scan options” on page 187.
See “Enabling a scheduled scan” on page 191.
See “Deleting a scheduled scan” on page 191.

Note: From the Mail Security console, you cannot stop scheduled scans once they are started.

Creating a scheduled scan

You can create as many scheduled scans as you need. When you create a scheduled scan, it is disabled by default. Enable the scan so that it runs according to the schedule.

See “Enabling a scheduled scan” on page 191.

To create a scheduled scan
1. In the console on the primary navigation bar, click **Scans**.
2. In the sidebar under Views, select **Scheduled Scans**.
3. Under **Tasks**, click **New scan**.
4. Configure the schedule scan options.
   See “Configuring scheduled scan options” on page 187.
5. On the toolbar, click **Deploy changes** to apply your changes.
   See “Deploying settings and changes to a server or group” on page 60.

Editing a scheduled scan

You can modify an existing scheduled scan as needed. Enable the scan so that it runs according to the schedule that you specify.

See “Enabling a scheduled scan” on page 191.

To edit a scheduled scan
1. In the console on the primary navigation bar, click **Scans**.
2. In the sidebar under **Views**, select **Scheduled Scans**.
3 In the content pane, do one of the following:
   ■ Select the scheduled scan that you want to modify, and in the sidebar under Tasks, click **Edit scan**.
   ■ Under the Name column, double-click the scheduled scan that you want to modify.

4 Modify the schedule scan options as needed.
   See “Configuring scheduled scan options” on page 187.

5 On the toolbar, click **Deploy changes** to apply your changes.
   See “Deploying settings and changes to a server or group” on page 60.

### Configuring scheduled scan options

Mail Security provides a wizard that guides you through the process of configuring a scheduled scan.

After you configure the scheduled scan options, enable the scan so that it runs according to the schedule.

See "Enabling a scheduled scan" on page 191.

You can configure the following scheduled scan options:

- Name of the scan and the basic scan options
- Mailboxes and the public folders that you want to scan
- Filtering rules that you want to apply to the scan
- Scan schedule

**To configure basic scanning options**

1 In the console on the primary navigation bar, click **Scans**.

2 In the sidebar under Views, select **Scheduled Scans**.

3 Do one of the following:

   Create a new scan In the sidebar under Tasks, click **New scan**.
   Modify an existing scan In the content area, under the Name column, double-click the scan that you want to modify.

4 In the Scan name box, type the name for the scan.
   Mail Security lets you enter a maximum of 128 SBCS (single-byte character set) characters (64 double-byte character set characters) in the Scan name box.
   This option is available only when you create a new scheduled scan.
5 Under **Scan Options**, check **Stop after scanning ___ minutes** to limit the amount of
time for the scan, and then type the maximum scanning time in minutes.
The default value is 120 minutes.
If Mail Security reaches this limit, it stops scanning. The next scheduled scan starts where
the previous scan stopped.
6 Check **Only scan items modified since last scan** to exclude the items that have not
changed since the last scan.
7 Check **Scan message bodies** to scan message bodies.
8 Under **Choose messages to scan**, select one of the following options:

- Scan all messages in the store.

- Scan all messages from the past number of days.

- Scan all messages from the past number of hours.

- Scan all messages from the start date.

9 Click **Next**.

To select what to scan

1 In second panel of the schedule scan wizard, under **Scan Location**, to specify mailboxes
to scan, select one of the following:
All mailboxes: Scans all mailboxes. This option is enabled by default.

Exclude mailboxes: Scans no mailboxes.

Specific mailboxes: Scans only the mailboxes that you specify in the list box.

You can select one of the following options:

- Exclude archive: You can specify to exclude archive mailbox scanning, and scan mailboxes only.
- Archive with mailboxes: You can specify this option to scan both mailboxes and its associated archive mailbox.
- Archive Only: You can specify to scan only archive mailboxes as per selection of mailboxes in the list.

**Note:** When you select All mailboxes or Specific Mailboxes, the associated archive mailbox is selected or excluded based on the options selected: Exclude archive, Archive with mailboxes, Archive only.

This option is available in the single-server view only.

2 To specify public folders to scan, select one of the following:

All public folders: Scans all public folders. This option is enabled by default.

Exclude public folders: Scans no public folders.

Specific public folders: Scans only the public folders that you specify in the list box. This option is available in the single-server view only.

3 Click Next.

**To scan for the filtering rules**

1 In the third panel of the scheduled scan wizard, click **Enable content filtering** to enable content filtering rule scanning for the scheduled scan.

2 In the next pane, click **Enable file type filtering rules** to enable file type filtering rule scanning for the scheduled scan.

3 Do any of the following:

- To add a new filtering rule, on the toolbar, click **New rule**.
- To modify an existing filtering rule, on the toolbar, click **Edit rule**.
- To delete an existing filtering rule, click **Delete rule**.
See “About creating the filtering rules” on page 126.

4 Click the box under the Enable column and select Enable to enable the rules that you want to apply to the scan.

5 Click Next.

To specify the scanning schedule

1 In the final panel of the scheduled scan wizard, in the Time of day to run box, select the time of day that you want Mail Security to perform the scan (in 24-hour format).

2 Under Days to run on, check the days of the week that you want the scan to run.

3 Under Dates of the month to run on, select any of the following:

   1st        The scan runs on the first day of each month.
   15th       The scan runs on the 15th day of each month.
   End of the month  The scan runs on the 28th day of each month.

4 Check Run scan at service start to perform a scan when the service starts.

5 Check Run scan when virus definitions change to perform a scan when new definitions are received.

   Enabling Run scan when virus definitions change in conjunction with Rapid release definitions can significantly affect performance. Leave this feature disabled if you update definitions at frequent intervals. If this option is enabled, the scheduled scan runs each time definitions are updated. Because definitions are delivered frequently, the scan might not complete before new definitions are available. This can affect overall scanning performance.

   See “Scheduling definition updates” on page 234.

6 Click Finish.

7 On the toolbar, click Deploy changes to apply your changes.

   See “Deploying settings and changes to a server or group” on page 60.

Stopping scheduled scans

You can stop Mail Security from running a scheduled scan at any time using registry settings.

To stop a scheduled scan

1 Close the Mail Security console.

2 On the Windows menu, click Start > Run.
In the Run box, type the following command:

regedit

Click OK.

In the registry editor window, in the left pane, browse and locate the following folder:
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\SMSMSE\7.x\Server\ScanJobs\<name of scheduled scan>

In the right pane, double-click ProgressStateDword.

In the Value data box, type the binary value 0, and then click Ok.

Close the registry editor window.

On the Windows menu, click Start > Programs > Administrative Tools > Services.

Restart the Symantec Mail Security for Exchange service.

See “Configuring scheduled scan options” on page 187.

### Enabling a scheduled scan

You must enable a scan so that it runs according to the schedule that you specify. Scheduled scans are disabled by default.

To enable a scheduled scan

1. In the console on the primary navigation bar, click Scans.
2. In the sidebar under Views, select Scheduled Scans.
3. In the content pane, select the scheduled scan that you want to enable.
4. Click the box under the Status column, and then click Enabled from the options in the drop-down menu.
5. On the toolbar, click Deploy changes to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

### Deleting a scheduled scan

You can delete a scheduled scan when it is no longer needed.

To delete a scheduled scan

1. In the console on the primary navigation bar, click Scans.
2. In the sidebar under Views, click Scheduled Scans.
3. Select the scan that you want to delete.
4 In the sidebar under Tasks, click **Delete scan**.
5 On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

### Configuring notification settings for scan violations

You can specify the administrators, users, or computers that should receive email notifications about scan violations. Restrict the issuing of alerts to a small list of interested administrators to avoid unnecessary interruptions.

Email notifications can be issued when a Mail Security scan detects a policy violation or an outbreak. An alert can also be sent to notify an administrator when a server experiences a critical service failure.

You can also customize the subject line and message text for each type of notification message when you configure policies and rules.

---

**Note:** Email notifications are sent only to the names and addresses that can be resolved against Active Directory. If you install Mail Security on the Edge server role, type a fully qualified email address (for example, user@mycompany.com).

---

To configure notification settings for scan violations

1 In the console on the primary navigation bar, click **Monitors**.
2 In the sidebar under Views, click **Notification Settings**.
3 In the content area, in the **Address of sender to use in email notification** box, type the email address of the sender that you want to use for email notifications.
4 In the **Administrators or others to notify** box, type the email addresses of administrators and users to notify.

Separate each entry by commas. If you include an email address that is not within your domain, type the fully qualified email address (for example, user@mycompany.com).
5 On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.
Managing outbreaks

This chapter includes the following topics:

- About outbreak management
- Enabling outbreak management
- Configuring outbreak triggers
- Configuring outbreak notifications
- Clearing outbreak notifications

About outbreak management

An outbreak situation occurs when an excessive number of threats or events that exhibit virus-like behavior occur on a network. When an outbreak occurs, prompt identification of the situation and notification of administrative staff is critical.

Outbreak management lets you configure Mail Security to send alerts. Alerts are sent when a certain threshold of duplicate messages, which are sent within a period of time, is reached. In some instances, a large number of duplicate messages can indicate an active virus outbreak or a problem within your Exchange server. You can monitor different type of conditions and receive timely alerts as they occur. An outbreak condition does not necessarily indicate that there is a problem. Sometimes the duplicate messages threshold meets the normal email flow. This threshold depends on your settings and the amount of email flow passing through the Exchange server.

When you configure outbreak settings, it is recommended that you consider the following:

- Threat potential of the event category that is monitored
- Amount of the email that is typically processed
- Size of your mail system
- Stringency with which you want to define an outbreak
As your outbreak triggers are tested, you can fine-tune the values that you use.

Mail Security lets you manage outbreaks with the following options:

- **Enable Outbreak Management.**
  See “Enabling outbreak management” on page 197.

- **Specify the criteria for an outbreak.**
  The criteria consist of the number of times that an event must occur during a specified time interval.
  See “About the criteria that defines an outbreak” on page 194.
  See “About outbreak triggers” on page 196.
  See “Configuring outbreak triggers” on page 197.

- **Define the email notifications to send to the administrator when an outbreak is detected.**
  See “Configuring outbreak notifications” on page 199.

- **End the outbreak event after the situation is managed.**
  See “Clearing outbreak notifications” on page 202.

### About the criteria that defines an outbreak

You can specify the number of occurrences of an event that must occur within a specified time frame to define an outbreak. Although there are no standard numbers to use when specifying frequencies, take into consideration the following:

- Threat potential of the event category that is monitored
- Size of your mail system
- Amount of the email that is typically processed
- Stringency with which you want to define an outbreak

Mail Security monitors your server at regular intervals to detect outbreaks (the default setting is every 2 minutes). When Mail Security checks your server for outbreaks, it checks the events that occurred within the specified period of time. The default setting is 20 minutes. Mail Security issues an outbreak notification when it detects an outbreak.

For example, if you enable outbreak management, configure Mail Security to monitor for outbreaks every 2 minutes, and enable the “Same virus” outbreak trigger using the default configuration.

*Figure 10-1* provides an explanation of the events. For example, Mail Security detects 50 messages that contain the EICAR virus at 1:05 P.M. and 50 messages that contain the EICAR virus at 1:19 P.M.
Figure 10-1  Example of an outbreak event

At 1:20, checks the prior 20 minutes and detects an outbreak. An outbreak notification is sent.

At 1:22, checks the prior 20 minutes and detects an outbreak still exists. A subsequent notification is sent.

At 1:24, checks the prior 20 minutes and detects an outbreak still exists. A subsequent notification is sent.

At 1:26, checks the prior 20 minutes. Does not detect outbreak conditions. No notification is sent.

Time at which 50 messages with ‘Free Offer’ subject line are received

See “About outbreak management” on page 193.
See “About outbreak triggers” on page 196.

About outbreak triggers

The set of defining criteria for an outbreak is called an outbreak trigger. Each outbreak trigger only monitors one type of event and defines an outbreak as the frequency of the specified event within a given time period.

For example, one outbreak trigger can be defined as the occurrence of 50 or more unscannable files within 1 hour. Another outbreak trigger can be defined as 30 or more filtering rule violations within 15 minutes.

If you enable multiple outbreak triggers and a message is received that violates more than one, Mail Security goes into outbreak mode. Mail Security stops looking for additional outbreaks. Only one outbreak rule is triggered.

Message bodies typically do not contain threats or security risks. To conserve processing resources, Mail Security installs with the default settings that do not scan message bodies. (Message attachments are always scanned.) You can modify the settings to scan message bodies.

If Mail Security does not scan the message body (which includes the subject line), the Same subject outbreak cannot be triggered. Outbreak is triggered when the message contains an attachment.

To activate the Same subject outbreak trigger for the messages that do not contain attachments, you can do any of the following:

■ Enable message body scanning.
  See “Configuring advanced scanning options for Auto-Protect and background (Exchange Server 2010 only) scanning” on page 179.

■ Enable at least one content filtering rule.
  Content filtering rules require message body scanning, regardless of whether the message contains an attachment. The content filtering rule can be any of the default rules or a rule that you create.

Outbreak triggers apply to Auto-Protect scans only.

See “Configuring outbreak triggers” on page 197.

Best practices for managing outbreak conditions on Exchange 2010 mailbox server

Do the following to improve security during an outbreak:

■ Run Rapid Release to update virus definitions.
  See “Updating definitions on demand” on page 234.
Enabling outbreak management

Outbreak management is enabled by default. You can specify the interval during which you want Mail Security to check for outbreaks. By default, the interval is set to every two minutes.

At least one outbreak trigger must be enabled for outbreak management to work.

See “Configuring outbreak triggers” on page 197.

To enable outbreak management

1. In the console on the primary navigation bar, click **Policies**.
2. In the sidebar under **General**, click **Outbreak**.
3. In the content area under **Outbreak**, check **Enable Outbreak Management**.
   
   This option is enabled by default.
4. In the **Check for Outbreaks every ___ minutes** box, type the interval in minutes that you want Mail Security to monitor your server for outbreaks.
   
   The default value is 2 minutes.
5. On the toolbar, click **Deploy changes** to apply your changes.
   
   See “Deploying settings and changes to a server or group” on page 60.

Configuring outbreak triggers

Mail Security provides the following outbreak triggers:

- Same attachment name
- Same subject
- Same virus
• Unrepairable viruses
• Unscannable files
• Filtering violations
• Total viruses

You can enable or disable the triggers. You can also modify the number of occurrences for a violation and the span of time in which the events must occur to constitute an outbreak. You can specify whether to notify an administrator when an outbreak occurs.

See “Configuring outbreak notifications” on page 199.

When you enable outbreak management, you can also configure Mail Security to automatically add the names of attachments that triggered an outbreak. The names of the attachments are added to the Outbreak Triggered Attachment Names match list and outbreak triggered subject text to the Outbreak Triggered Subject Lines match list. Mail Security uses these match lists for the preconfigured content filtering rules that automatically block suspicious file attachments or subjects. You can also use these match lists to create your own content filtering rules.

To configure outbreak triggers

1 In the console on the primary navigation bar, click Policies.
2 In the sidebar under General, click Outbreak.
3 In the content area, in the table, select the trigger that you want to modify.
   The trigger that you select is highlighted in blue.
4 In the Status column, use the drop-down menu to select Enabled or Disabled.
5 In the Occurrences column, type the number of instances that must occur to constitute an outbreak.
   The default value is 100.
6 In the Time column, type the span of time in which the instances must occur to constitute an outbreak.
   The default value is 20.
7 In the Units column, click the drop-down menu, and select one of the following:
   • Minutes
     This setting is the default setting.
   • Hours
   • Days
8 In the **Notify Administrator** column, check the box if you want to notify an administrator of the outbreak.

9 In the **Update Match List** column, check the box if you want to automatically add the attachment name or subject to the **Outbreak Triggered Names** match list or **Outbreak Triggered Subjects** match list. The trigger must be activated.

   See “About match lists” on page 154.

10 In the Rule column, click **View Rule** to view or modify the associated content filtering rule.

   This option is available only for the Same attachment name and Same subject triggers.

   Note that Mail Security disables content filtering on the server if you uncheck **Enable content filtering** in the **Content Enforcement Rule** window.

11 On the toolbar, click **Deploy changes** to apply your changes.

   See “Deploying settings and changes to a server or group” on page 60.

### Configuring outbreak notifications

When you configure outbreak management settings, you can customize the notification subject line and message text that is sent to the administrator. You can use variables to customize your text.

   See “About the criteria that defines an outbreak” on page 194.

   See “Alert and notification variables” on page 238.

To configure outbreak notifications

1 In the console on the primary navigation bar, click **Policies**.

2 In the sidebar under **General**, click **Outbreak**.
3 In the content area, in the preview pane, under **Initial Notification**, in the **Subject Line** box, type your customized subject line text.

The default text is as follows:

**Initial notification**

Rules **Initial notification**

Same attachment name Symantec Mail Security has started noticing possible email outbreak conditions. The “%outbreak_rule%” rule was violated %outbreak_count% times.

Same subject Symantec Mail Security has started noticing possible email outbreak conditions. The “%outbreak_rule%” rule was violated %outbreak_count% times.

Filtering violations Symantec Mail Security has started noticing possible email outbreak conditions. The “%outbreak_rule%” rule was violated %outbreak_count% times.

Same virus Symantec Mail Security has started noticing possible conditions of outbreak of emails with viruses. The “%outbreak_rule%” rule was violated %outbreak_count% times.

Unrepairable viruses Symantec Mail Security has started noticing possible conditions of outbreak of emails with viruses. The “%outbreak_rule%” rule was violated %outbreak_count% times.

Total viruses Symantec Mail Security has started noticing possible conditions of outbreak of emails with viruses. The “%outbreak_rule%” rule was violated %outbreak_count% times.

Unscannable files Symantec Mail Security has started noticing possible conditions of outbreak of emails with unscannable files. The “%outbreak_rule%” rule was violated %outbreak_count% times.

4 In the **Message Body** box, type your customized message body text.

The default text is as follows:

Outbreak Trigger Information: %trigger%

Threshold is set at: %threshold%

Current count for configured time period: %count%

Server name: %server%

Outbreak triggers at: %outbreak_count% times
5 Under **Subsequent Notifications**, in the **Subject Line** box, type your customized subject line text.

The default text is as follows:

Subsequent notification

<table>
<thead>
<tr>
<th>Rules</th>
<th>Subsequent notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same attachment name</td>
<td>Symantec Mail Security continues to observe possible email outbreak conditions. The rule “%outbreak_rule%” was violated %outbreak_count% times.</td>
</tr>
<tr>
<td>Same subject</td>
<td>Symantec Mail Security continues to observe possible email outbreak conditions. The rule “%outbreak_rule%” was violated %outbreak_count% times.</td>
</tr>
<tr>
<td>Filtering violations</td>
<td>Symantec Mail Security continues to observe possible email outbreak conditions. The rule “%outbreak_rule%” was violated %outbreak_count% times.</td>
</tr>
<tr>
<td>Same virus</td>
<td>Symantec Mail Security continues to observe possible conditions of outbreak of emails with viruses. The rule “%outbreak_rule%” was violated %outbreak_count% times.</td>
</tr>
<tr>
<td>Unrepairable viruses</td>
<td>Symantec Mail Security continues to observe possible conditions of outbreak of emails with viruses. The rule “%outbreak_rule%” was violated %outbreak_count% times.</td>
</tr>
<tr>
<td>Total viruses</td>
<td>Symantec Mail Security continues to observe possible conditions of outbreak of emails with viruses. The rule “%outbreak_rule%” was violated %outbreak_count% times.</td>
</tr>
<tr>
<td>Unscannable files</td>
<td>Symantec Mail Security continues to observe possible conditions of outbreak of emails with unscanable files. The rule “%outbreak_rule%” was violated %outbreak_count% times.</td>
</tr>
</tbody>
</table>
6 In the **Message Body** box, type your customized message body text.

   The default text is as follows:
   Outbreak Trigger Information: %trigger%
   Threshold is set at: %threshold%
   Current count for configured time period: %count%
   Server name: %server%
   Outbreak triggers at: %outbreak_count% times

7 On the toolbar, click **Deploy changes** to apply your changes.

   See “Deploying settings and changes to a server or group” on page 60.

---

**Clearing outbreak notifications**

   During an outbreak, subsequent notifications are sent based on the Time and Units interval that you specify until the outbreak is no longer in effect. You can end subsequent outbreak notifications by clearing the current outbreak.

   See “Configuring outbreak triggers” on page 197.

   See “Configuring outbreak notifications” on page 199.

   **To clear outbreak notifications**

   1 In the console on the primary navigation bar, click **Policies**.

   2 In the sidebar under **General**, click **Outbreak**.

   3 Under **Tasks**, click **Clear current outbreak**.
This chapter includes the following topics:

- About logging events
- About generating reports
- About report templates
- Managing reports

About logging events

Mail Security logs performance counters and events to the following locations:

Windows Application Event Log

Server events and policy violations are reported in the Windows Application Event Log. The Mail Security console provides an event log page. This page lets you view Windows Application event log entries in chronological order with the most current event at the top. The event log page displays information, warning, and error events.

See “Viewing the Mail Security Event log” on page 204.
Mail Security Reports database

Mail Security logs extensive report data on threats, security risks, violations, spam, and server information to a reports database. You can use this data to generate summary or detailed reports based on different subsets of the data. When you define a report, you specify criteria. For example, the time span of the collected data, whether to show specific violations or all violations, and the output format of the report.

See “About report templates” on page 209.

You can specify how long Mail Security maintains data in the Reports database. You can also purge the database at any time.

See “Specifying the duration for storing data in the Reports database” on page 206.

See “Purging the Reports database” on page 207.

Microsoft Management Console (MMC) Performance console

The MMC Performance console shows system performance. You can add Mail Security performance counters to the MMC view.

See “About logging performance counters to the MMC Performance console” on page 207.

Viewing the Mail Security Event log

Mail Security reports server events and policy violations (such as threat detections and filtering violations) to the Windows Application event log. You can access the Windows Application Event Log on the computer on which Mail Security is installed. For more information about how to access and use the Windows Application Event Log, see the documentation for your Exchange server.

The Mail Security event log lets you view and then sort the event data that Mail Security generates and writes to the Windows Application event log. You can view the Mail Security event log from the console. You can filter event data by categories. You can also select a start date from which to begin displaying event data. When you select an event in the event log table, detail about the event appear in the preview pane.

The Mail Security event log displays the 5000 most recent Mail Security events from the Windows Application event log, per server. For example, if your group contains five servers, the event log can display up to 25,000 events.

The event log displays the following information:

Server Name of the server on which the event occurred
Timestamp Date and time the event occurred
Severity categories are as follows:
- Warning
- Information
- Error

Category categories are as follows:
- Auto-Protect
- Content Filtering Engine
- Content Filtering Rules
- Encrypted
- Error
- Licensing
- LiveUpdate/Rapid Release
- Manual and Scheduled Scanning
- Outbreak Management
- Quarantine
- Scanning
- Service
- Premium AntiSpam
- Threat/Security Risk
- Unscannable
- VSAPI (for Exchange Server 2010)

Manually refresh the page if it is blank or to refresh the page to view the most recent events. In a large group, refreshing the page might take several minutes.

**To view the Mail Security event log**

1. In the console on the primary navigation bar, click **Monitors**.
2. In the sidebar under **Views**, click **Event Log**.
3. Click the column headers to sort the list data by different criteria.

**To populate and refresh the Mail Security event log**

- Press **F5**.
To filter the Mail Security event log

1. Under the event log table, in the **Number of items per page** list, select a number of items that you want to view per page using the drop-down menu.
   The default value is 10.

2. In the **List** box, select a category on which to filter the event data using the drop-down menu.

3. In the entries since list, select a start date from which to begin displaying event data using the drop-down menu.

Specifying the duration for storing data in the Reports database

Mail Security stores data on threat detection, definitions, spam, policy violations, scanning, and server events in a Reports database. You can use this data to generate the reports that include subsets of this data.

You can configure Mail Security to retain this data for the period of time that you specify. Once the data is removed, it cannot be used in reports. For example, assume that you configure Mail Security to retain data for 6 months. If you generate a report for the past year, only the data for most recent 6 months appears in the report.

Mail Security provides a separate option to include spam data in reports. Selecting this option increases the time that is required to generate reports, which can affect performance. Consider using this option short term (for example, a few weeks) to evaluate spam-related issues.

See “Resetting statistics” on page 228.

To specify the duration for storing data in the Reports database

1. In the console on the primary navigation bar, click **Reports**.

2. In the sidebar under Views, click **Report Settings**.
In the content area, select one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store all data</td>
<td>Keeps all data indefinitely.</td>
</tr>
<tr>
<td>Store no data</td>
<td>No violation data is retained.</td>
</tr>
<tr>
<td>Store data for ___ months</td>
<td>The data is cleared after the specified time period.</td>
</tr>
<tr>
<td></td>
<td>If you select this option, type the number of months of data to store. Only summary spam data is stored</td>
</tr>
<tr>
<td></td>
<td>unless you check the &quot;Include spam data&quot; option.</td>
</tr>
<tr>
<td></td>
<td>The default value is 12.</td>
</tr>
</tbody>
</table>

Check **Include spam data** to include all spam-related events.

This option is disabled by default.

On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

### Purging the Reports database

In addition to configuring the period of time that you want Mail Security to store data in the Reports database, you can purge the Reports database at any time. When you purge the Reports database, all data is removed.

**To purge the Reports database**

1. In the console on the primary navigation bar, click **Reports**.
2. In the sidebar under Views, click **Report Settings**.
3. Under **Tasks**, click **Reset database statistics**.
4. In the **Operation Status** window, click **Close**.

### About logging performance counters to the MMC Performance console

Add the Mail Security 7.9 performance object to the Microsoft System Monitor to view Mail Security performance data in the MMC Performance console. You can view all of the Mail Security counters or select specific counters.

The Mail Security for Microsoft Exchange Management Pack is located in the installation package at the following location:
ADMTOOLS\MOM

See the MMC documentation for more information about how to add the Mail Security performance object.

Table 11-1 lists the Mail Security counters that are available.

Table 11-1  Performance counters

<table>
<thead>
<tr>
<th>Performance counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes Scanned</td>
<td>Number of bytes scanned</td>
</tr>
<tr>
<td>Bytes Scanned/Sec</td>
<td>Number of bytes scanned per second</td>
</tr>
<tr>
<td>Total Scans</td>
<td>Number of the scans that are performed on messages and attachments</td>
</tr>
<tr>
<td>Total Scans/Sec</td>
<td>Number of the scans that are performed on messages and attachments per second</td>
</tr>
<tr>
<td>Threats and Risks Found</td>
<td>Number of software threats detected</td>
</tr>
<tr>
<td>Threats and Risks Found/Sec</td>
<td>Number of the software threats detected per second</td>
</tr>
<tr>
<td>Content Filtering Found</td>
<td>Number of the content violations detected</td>
</tr>
<tr>
<td>Content Filtering Found /Sec</td>
<td>Number of the content violations detected per second</td>
</tr>
<tr>
<td>Spam Violations Found</td>
<td>Number of spam violations detected</td>
</tr>
<tr>
<td>Spam Violations Found/Sec</td>
<td>Number of spam the violations detected per second</td>
</tr>
</tbody>
</table>

**Note:** Mail Security lets you configure performance counters for logging. By default, this counter is enabled. To improve a scanning performance, these performance counters for logging can be turned off by adding the following registry key and setting its value to 1:

HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\SMSMSE\7.9\Server\TurnOffPerfCounters.

Restart the Mail Security service after setting this registry key.

---

About generating reports

Mail Security collects and saves scan data on your Exchange servers. You can create reports from the data, which gives you a history of risk detection activity and filtering violations. You
can create a report for an individual server. You can also create a single Summary report that consolidates data for all the servers in a server group.

See “Configuring the initial setup of the report consolidation feature” on page 219.

Report templates let you define a subset of the raw report data that Mail Security collects for a single server. Report templates can include different categories or combinations of security-related statistics.

You can create different report templates to describe different subsets of the raw report data. After you create a report template, you use it to generate reports.

Mail Security provides two preconfigured report templates that you can modify. You can also create your own report templates. When you create or modify a report template, Mail Security provides a wizard to guide you through the configuration process.

The types of report templates that you can create are as follows:

- **Summary**
  - See “Creating or modifying a Summary report template” on page 210.

- **Detailed**
  - See “Creating or modifying a Detailed report template” on page 215.

### About report templates

Report templates let you define a subset of the raw report data that Mail Security collects for a single server. The goal of creating a template is to describe a set of data that summarizes threats, security risks, filtering violations, spam, and server information. The information, which can be saved and used to generate on-demand or scheduled reports. Report templates can include different categories or combinations of security-related statistics.

You can create different report templates to describe different subsets of the raw report data. After you create a report template, you can use it to generate reports.

**Note:** Reports cannot be generated with a new or an updated report template until you deploy your changes.

Mail Security provides two preconfigured report templates that you can modify. You can also create your own report templates. When you create or modify a report template, Mail Security provides a wizard to guide you through the configuration process.

The types of report templates that you can create are as follows:

- **Summary**
  - See “Creating or modifying a Summary report template” on page 210.

- **Detailed**
See “Creating or modifying a Detailed report template” on page 215.

About report output formats

The format options that are available for a Summary report are HTML and PDF. You can configure Mail Security to send copies of the report to the people that you specify. The recipients’ email client must support and permit HTML-based or PDF-based attachments.

If you use Outlook Express and you intend to use the HTML format, you need to modify the following settings in Outlook Express:

- On the **Security** tab, deselect the option “Do not allow attachments to be saved or opened that can potentially be a virus.”
- On the **Read** tab, deselect the option “Read all messages in plain text.”

When you generate a Detailed report, Mail Security can save the report in HTML format, PDF format, or comma-separated value (.csv) format.

Generating a report in .csv format lets you do the following:

- You can view or print the complete report data in an application, such as Microsoft Excel.
  
  If you have Microsoft Excel on your computer, a .csv file opens automatically as an Excel spreadsheet.

- You can import the data into a third-party reporting application to generate custom charts and reports.
  
  See “Accessing a report” on page 224.

Creating or modifying a Summary report template

You can customize the Summary report template to contain the information that you want to include in a report. You can generate a Summary report for an individual server or for an entire server group.

The Summary report template that you create appears in the Report Templates table. You can modify the template at any time.

If you configure the template to create reports on demand, you can generate the report from the **Reports > Report Templates** page. If you configure the template to generate a scheduled report, Mail Security automatically generates the report based on the schedule that you specify.

See “Generating a report on demand” on page 224.

---

**Note:** Mail Security supports emailing the reports that are 5 MB or smaller only. You can view the reports that are larger than 5 MB on the Reports page. Mail Security logs the generation of reports that are larger than 5 MB to the Windows Application event log.
Mail Security provides a wizard that helps you configure your report template.

To identify the report to be created or modified
1 Select the server or server group for which you want to generate a report.
   See “Modifying or viewing server or server group settings” on page 66.
2 In the console on the primary navigation bar, click Reports.
3 In the sidebar under Views, click Report Templates.
4 Do one of the following:
   - Create a new executive summary report template
   - Modify an existing report template

To configure the report template options
1 Under Report Template Options, in the Template name box, type a name for the report template.
   This option is available only when you create a new report template.
2 In the Description box, type a description for the template.
3 Under Report type, click Executive summary.
   This option is checked by default.
4 Under Report format, select the format in which you want Mail Security to generate the report.
   The default setting is PDF.
5 Check Email report to the following recipients and type one or more addresses to which the report should be delivered.
   Separate entries with semicolons.
6 Click Next.

To configure on-demand report generation
1 Under Report Generation Option, click On demand.
2 Click Next.

To specify the report time range
1 Click the drop-down arrow in the Time Range box and select one of the following:
- Past Day
  This setting is the default setting.
- Past Week
- Past Month
- Past Year
- Customized

2. If you select the Customized time range, in the customize time range boxes, click the drop-down arrows and select the start and the end dates for the data that you want included in your report.

**To configure scheduled report generation**

1. Under **Report Generation Option**, click **Scheduled**.
2. In the **Generate report at** list, select the time of day to generate the report.
3. Click **Daily**, **Weekly**, or **Monthly**.
   - If you select Weekly, check the day(s) of the week to generate the report.
   - If you select Monthly, use the drop-down menu to select the day of the month to generate the report.
   - If you select Monthly, also ensure that you select a day that exists in each month. Otherwise, a report is not generated for that month. If you select the 31st day of every month, reports are not generated for any month that has 30 days or less. For example, February, April, June, September, and November.
4. Click **Next**.

**To configure the report chart options**

1. Under **Report Chart Options**, select any of the following:
   - Total violations chart
   - Threats and security risks chart
     - Also select the chart granularity using the drop-down menu.
     - The default setting is Week.
   - Content violation chart
     - Also select the chart granularity using the drop-down menu.
     - The default setting is Week.
   - Spam pie chart
2. Click **Next**.
To configure report content

1. **Under Executive Summary Template Options**, select the options that you want to appear in the Summary report.

Data selections are as follows:

- **Show scan summary**

<table>
<thead>
<tr>
<th>Description</th>
<th>Total number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total items scanned</td>
<td>Total number of the files that were processed during the reporting period</td>
</tr>
<tr>
<td>Items that are scanned by Auto-Protect</td>
<td>Total number of the files that were scanned with Auto-Protect scanning during the reporting period</td>
</tr>
<tr>
<td>Items that are scanned by background scan (applicable to Exchange 2010 mailbox server only)</td>
<td>Total number of the files that were scanned with background scanning during the reporting period</td>
</tr>
<tr>
<td>Items that are scanned by Manual scan</td>
<td>Total number of the files that were scanned with manual scanning during the reporting period</td>
</tr>
<tr>
<td>Items that are scanned by scheduled scan(s)</td>
<td>Total number of the files that were scanned with a scheduled scan during the reporting period</td>
</tr>
<tr>
<td>Items that are scanned by antispam scan</td>
<td>Total number of the files that were scanned with a spam scan during the reporting period</td>
</tr>
</tbody>
</table>

- **Show violation summary**

<table>
<thead>
<tr>
<th>Description</th>
<th>Total number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total violations</td>
<td>Total number of the violations that were detected during the reporting period</td>
</tr>
<tr>
<td>Virus violations</td>
<td>Total number of virus violations</td>
</tr>
<tr>
<td>Content violations</td>
<td>Total number of filtering violations</td>
</tr>
<tr>
<td>Antispam violations</td>
<td>Total number of antispam violations</td>
</tr>
</tbody>
</table>

- **Show threats and security risks**

<table>
<thead>
<tr>
<th>Description</th>
<th>Total number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total threats</td>
<td>Total number of the threats that were detected during the reporting period</td>
</tr>
</tbody>
</table>
### Table of the top threats that were detected during the reporting period

<table>
<thead>
<tr>
<th>Top threats table</th>
<th>Number of threats to include in the Top Threats Table</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of items to include</strong></td>
<td><strong>Total number of the unrepairable threats that were detected during the reporting period</strong></td>
</tr>
<tr>
<td><strong>Unrepairable threats</strong></td>
<td><strong>Number of the security risks that were detected during the reporting period</strong></td>
</tr>
<tr>
<td><strong>Total security risks</strong></td>
<td><strong>Number of messages in which mass-mailer threats were detected during the reporting period</strong></td>
</tr>
<tr>
<td><strong>Mass-mailer threats</strong></td>
<td><strong>Number of the threats that were repaired during the reporting period</strong></td>
</tr>
<tr>
<td><strong>Infection disposition</strong></td>
<td><strong>Number of the threats that were deleted during the reporting period</strong></td>
</tr>
<tr>
<td><strong>Threats repaired</strong></td>
<td><strong>Number of the threats that were quarantined during the reporting period</strong></td>
</tr>
<tr>
<td><strong>Threats deleted</strong></td>
<td><strong>Number of the threats that were recovered during the reporting period</strong></td>
</tr>
<tr>
<td><strong>Threats quarantined</strong></td>
<td><strong>Number of the threats that were blocked during the reporting period</strong></td>
</tr>
</tbody>
</table>

2 Click Next.

3 Under **Executive Summary Template Options**, select the data that you want to appear in the executive summary report.

Data selections are as follows:

- **Show content violations**

| Total content violations | Total number of the content violations that were detected during the reporting period |
| Table of top content violations | Table of the top content violations that were detected during the reporting period |
| No. of items to include | Number of items to include in the Table of Top Content Violations |
| Total attachments blocked | Total number of the attachments that were blocked during the reporting period |
Total file type violations

Total number of the file type violations that were detected during the reporting period.

Total encrypted attachments blocked

Total number of the encrypted attachments that were blocked during the current reporting period.

Table of top attachments blocked

Table of the top attachments that were blocked during the reporting period.

No. of items to include

Number of items to include in the Table of Top Attachments Blocked.

Unscannable items

Total number of the unscannable items that were blocked during the reporting period.

Spam options

Spam by category

The total number of spam messages in each spam category that the product identifies during the reporting period.

You must check the "Include spam data" box on the Reports Settings page to view data about spam in the Summary report.

See “Specifying the duration for storing data in the Reports database” on page 206.

4 Click Next.

5 Under Executive Summary Template Options, check Show server information.

6 Select the data that you do want to appear in the executive summary report.

7 Click Finish.

8 On the toolbar, click Deploy changes to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

Creating or modifying a Detailed report template

The Detailed report templates that you create appear in the Report Templates table. You can modify the template at any time.

If you configure the template to create reports on demand, you can generate the report from the Reports > Report Templates page. If you configure the template to generate a scheduled report, Mail Security automatically generates the report based on the schedule that you specify.
See “Generating a report on demand” on page 224.

**Note:** Consider limiting the date range to less than 30 days. Generating a detailed report over 30 days might consume large amounts of computer memory. This report depends on the number of violations that are in the report database.

**Note:** Mail Security supports emailing the reports that are 5 MB or smaller only. You can view the reports that are larger than 5 MB on the Reports page. Mail Security logs the generation of reports that are larger than 5 MB to the Windows Application event log.

Mail Security provides a wizard that helps you configure your report template.

**To identify the report to be created or modified**

1. Select the server or server group for which you want to generate a report.
   - See “Modifying or viewing server or server group settings” on page 66.
2. In the console on the primary navigation bar, click **Reports**.
3. In the sidebar under **Views**, click **Report Templates**.
4. Do one of the following:
   - Create a new Detailed report template. In the sidebar under Tasks, click **New template**.
   - Modify an existing report template. In the content pane, in the Report Templates table, double-click the template that you want to modify.

**To configure the report template options**

1. In the **Report Template Options** panel, in the **Template name** box, type a name for the report template.
   - This option is available only when you are create a new template.
2. In the Description box, type a description for the template.
3. Under **Report type**, click **Detailed**.
4. Under **Report format**, select the format in which you want Mail Security to generate the report.
   - The default setting is PDF.
Check **Email report to the following recipients** and type one or more addresses to which the report should be delivered.
Separate entries with semicolons.

6 Click **Next**.

**To specify the report time range**

1 Click the drop-down arrow in the Time Range box and select one of the following:
   - Past Day
     This setting is the default setting.
   - Past Week
   - Past Month
   - Past Year
   - Customized

2 If you select the Customized time range, in the customize time range boxes, click the drop-down arrows. Select the start and the end dates for the data that you want included in your report.

**To configure on-demand report generation**

1 Under **Report Generation Option**, click **On demand**.
2 Click **Next**.

**To configure scheduled report generation**

1 Under **Report Generation Option**, click **Scheduled**.
2 In the **Generate report at** list, select the time of day to generate the report.
3 Click **Daily**, **Weekly**, or **Monthly**.
   If you select Weekly, check the day(s) of the week to generate the report.
   If you select Monthly, use the drop-down menu to select the day of the month to generate the report.
   If you select Monthly, also ensure that you select a day that exists in each month. Otherwise, a report is not generated for that month. If you select the 31st day of every month, reports are not generated for any month that has 30 days or less. For example, February, April, June, September, and November.
4 Click **Next**.
To configure report content

1 Under Detailed Template Options, in the Type of violation list, use the drop-down menu to select the type of violation that you want to appear in the report.

2 In the Sender filter box, type an identifying characteristic of the sender whose messages appear in the report.

This entry can be the domain name or address of the sender, or a name or word, or a wildcard expression.

If the sender is a member of your Active Directory group, use the user name instead of the full email ID. For example, you would use John_Doe instead of John_Doe.symantecsecurity.com.

3 In the Violation filter list, do one of the following:

   To select a predefined violation filter

   Click the drop-down menu and select a predefined violation filter.

   The list consists of the default rules (for example, Basic Virus Rule) that are provided when you install the product. Filter selections vary based on the type of violation that you choose.

   To select a user-defined content filtering rule

   (This option is only available if you select the violation types “All” or “Content Enforcement.”)

   Click the drop-down menu and select User Defined Rule.

   Click the drop-down menu in the Rule name box and select one of the content filtering rules that you created.

4 Select the columns that you want to appear in the detailed report.

5 Click Finish.

6 On the toolbar, click Deploy changes to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

Deleting a report template

You can delete a report template when it is no longer needed.

To delete a report template

1 In the console on the primary navigation bar, click Reports.

2 In the sidebar under Views, click Report Templates.

3 In the content area, select the template that you want to delete.
4 In the sidebar under Tasks, click **Delete template**.
5 In the confirmation dialog box, click **OK**.
6 On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

## Managing reports

The following lists the tasks that you can do to reports:

- Configuring the initial setup of the report consolidation feature
- Generating a consolidated report
- Scheduling a consolidated report
- Generating a report on demand
- Accessing a report
- Printing a report
- Saving report data
- Deleting a report

### Configuring the initial setup of the report consolidation feature

Mail Security supports generating a consolidated summary report and detailed report for all the servers in a server group. Mail Security stores report information on each server in the location that you specify. When you generate a consolidated report, Mail Security pulls the report information for each of the servers to create the consolidated report.

To use the report consolation feature, perform the following initial setup tasks:

- **Specify the shared location to store reports**
  - Mail Security lets you specify where you want each server to store the reports for consolidation. The location must be the same for each server in the group.
  - You must ensure that the full directory path exists on each server. For example, if you specify a directory path of `\Program Files\Symantec\7.9\My Reports`, ensure that each server contains this full directory path. You must also ensure that the path location has permission to allow read and write access.
Grant access for the Symantec Mail Security Utility service to access the shared storage location. The Symantec Mail Security Utility service must be able to access the shared storage location. Configure the service to run in an account that is a member of the local system administrators and domain users groups. The account must also have access to the shared storage location.

To specify the shared location to store reports

1. Select the server or server group that you want to modify.
   See “Modifying or viewing server or server group settings” on page 66.
2. In the console on the primary navigation bar, click Reports.
3. In the sidebar under Views, click Report Settings.
4. Under Report Consolidation, type the name of a valid UNC path. For example:
   `\<serverip>\<location>`
   The path must be fewer than 256 characters. The following characters are not supported in the path name:
   `~!@#$%^&*()+=|?;:"[]{}`
5. On the toolbar, click Deploy changes to apply your changes.
   See “Deploying settings and changes to a server or group” on page 60.

To grant access for the Symantec Mail Security Utility service to access the shared storage location

1. In the Services MMC snap-in, select the Symantec Mail Security Utility service.
2. Right-click and select Properties.
3. Click on the Log On tab.
4. Under Log on as, select This account.
5. Type the user name and password (and confirm the password) of a valid account that is configured to be a member of the local system administrators and domain users groups. The account must have access to the shared storage location.
6. Click OK.
7. Right-click and select Restart to restart the Symantec Mail Security Utility service.

Generating a consolidated report

When you are in a group view, you can generate a consolidated report of all of the servers in the group. You must do an initial set-up for the report consolidation settings before you generate a consolidated report. Consolidated reports can be generated for on-demand reports and
scheduled reports. For on-demand reports, a single consolidated report is generated. But if a consolidated report is scheduled, then separate reports for each and every server in the group are generated.

See “Configuring the initial setup of the report consolidation feature” on page 219.

To generate a consolidated report

1. In the console on the primary navigation bar, click Reports.
2. In the sidebar under Views, click Report Templates.
3. In the Report Templates table, select the report that you want to generate.
4. In the sidebar under Tasks, click Generate consolidated report.
   You must be in a group view to generate a consolidated report.
5. In the Operation Status window, click Close when the operation is complete.

Scheduling a consolidated report

When you are in a group view, you can schedule the generation of consolidated reports on a daily, weekly, or monthly basis. You must do an initial setting of the parameters that are required to schedule a consolidated report generation.

Before you schedule a consolidated report, under Server/group, click Change and select a global group or sub group, if not already selected. Reports can be scheduled only on global groups or sub groups of exchange servers.
To ensure that scheduling consolidated report works in a multi-domain environment

1. Launch the **Server Manager** from the **Administrative Tools** and browse to **Roles > Active Directory Domain Services > Active Directory Users and Computers > <server_name> > Users**.

2. Double-click **SMSMSE Admins** properties panel and make the **SMSMSE Admins** group as a **Universal** security group, as illustrated.

3. Save the setting and let the Active Directory replication complete.

4. Under the **Members** tab of the **SMSMSE Admins Properties** panel, add the domain user to the **SMSMSE Admins** group.

   The user who schedules the consolidated report is the domain user.

---

**Note:** Repeat steps 1 through 4 for every domain where SMSMSE is installed in the forest. SMSMSE Admins group from each domain must be changed to Universal security Group. The user account that is used for generating the reports must be added to SMSMSE Admins group.
The user account or the group (SMSMSE Admins) that is used for generating reports must have the **Log on as a batch job** permission on the SMSMSE console computer. To perform this action, go to **Start > Run** and type `secpol.msc` to launch the **Local Security Policy** console. Browse to **Local Policies > User Rights Assignment > Log on as a batch job** properties panel, as illustrated and add the user or the group SMSMSE Admins.

To schedule a consolidated report

1. In the Mail Security console, go to **Reports > Tasks > Schedule consolidated report**.
2. In the **Schedule consolidated report** panel, select **Enable Scheduling**.

   The default option select is **Disable Scheduling**.
3. Select a time in **hh–mm** format under the **Generate report at** box.
4. Select either **Daily**, **Weekly**, or **Monthly** option to schedule a consolidated report.
   - Daily - A report is generated daily, at the time that you set in step 3
   - Weekly - Select one or more day(s) of a week to schedule a consolidated report.
Monthly - Select the day of the month from the Day drop-down list on which you want to schedule generation of a consolidated report.

5 Enter a password in the Please Enter Logged-in User Password input box.

You must provide the logged on user password to schedule the task in Task Scheduler with the property Run whether user is logged on or not.

6 Click Ok to save the settings.

The SMSMSE report consolidation process needs to wait till the request gets routed to each server in the group. The default wait time can be changed. For more information refer the Mail Security Knowledge Base.

Generating a report on demand

After you create a report template, you can use it to generate reports of policy violation information. Mail Security automatically appends the current date and time to the name of your report template when it names the report. This mechanism lets you run the same report on different dates and compare the data.

See “Configuring the initial setup of the report consolidation feature” on page 219.

See “Accessing a report” on page 224.

To generate a report on demand

1 In the console on the primary navigation bar, click Reports.

2 In the sidebar under Views, click Report Templates.

3 In the Report Templates table, select the report that you want to generate.

4 In the sidebar under Tasks, click Generate report if you are in a server view or Generate consolidated report if you are in a group view.

5 In the Operation Status window, click Close when the operation is complete.

Accessing a report

You can view a report from the console or from the Mail Security Reports folder. If you view a report from the console, you must be in a server view.

The Reports page in the console displays the following information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Indicates the name of the report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Indicates the type of report (Detailed or Summary)</td>
</tr>
<tr>
<td>Date Created</td>
<td>Indicates the date and time that the report was generated</td>
</tr>
</tbody>
</table>
A generated report (scheduled or on demand) is also automatically saved in its own folder in the Mail Security Reports folder. You can browse to the folder location and view the report file.

The file is automatically deleted from the Mail Security Reports folder when you delete a report in the console.

See "Deleting a report" on page 227.

To access a report from the console

1. In the console on the primary navigation bar, click Reports.
2. In the sidebar under Views, click Reports.
3. In the content pane in the Reports table, do one of the following:
   - Select the report that you want to view, and in the sidebar under Tasks, click View report if you are in a server view. Click View consolidated report if you are in a group view.
   - Double-click the report.

See “Printing a report” on page 226.

To access a report from the Mail Security Reports folder

1. Right-click on the Start menu and select Explore.
2. Browse to the Mail Security Reports folder.

The default location is as follows:

\Program Files\Symantec\SMSMSE\7.9\Server\Reports
3 Double-click the report folder that contains the report that you want to view.

4 Do one of the following:

   For a report in .html format  Double-click the file to view it. The report appears the same as if it were accessed from the console.

   For a report in .pdf format  Double-click the file to view it. You must have Adobe Acrobat Reader installed to view reports generated in .pdf format.

   For a report in .csv format  Open the .csv file in a program such as Microsoft Excel to view it. Files that are created in .csv format contain raw data and must be viewed in a program that can interpret the data.


Printing a report

You can print a report if your printer is properly configured. Mail Security provides the features that let you configure the page set-up and preview the report. Print reports in landscape mode to prevent the data from being cut off at the right margin.

To print a report

1 In the console on the primary navigation bar, click Reports.

2 In the sidebar under Views, click Reports.

3 In the content pane in the Reports table, do one of the following:
   - Select the report that you want to view, and in the sidebar under Tasks, click View report if you are in a server view. Click View consolidated report if you are in a group view.
   - Double-click the report.

4 On the toolbar, do any of the following:

   Configure printer options  Click Page Setup.

   Preview the report  Click Print Preview.
   You can print the report from the Print Preview window.

   Print the report  Click Print.

5 Click OK.
Saving report data

You can save reports to the destination of your choice. This action lets you manage and maintain your reports. It also lets you email reports or lets users access the reports that they want to view.

To save report data
1. In the console on the primary navigation bar, click Reports.
2. In the sidebar under Views, click Reports.
3. In the content pane in the Reports table, do one of the following:
   - Select the report that you want to view, and in the sidebar under Tasks, click View report if you are in a server view. Click View consolidated report if you are in a group view.
   - Double-click the report.
4. On the toolbar, click Save.
5. In the Save window, do the following:
   - In the File name box, type the name of the file.
   - In the Save as type box, select the file type.
   - In the Encoding box, select the encoding that you want to use.
     The default value is Unicode.
     This option only appears if you save the file in .htm or .html format.
6. Click Save.

Deleting a report

You can delete a report when it is no longer needed or after you have saved the report to a file location. This action lets you manage the volume of reports on the Reports page.

See “Saving report data” on page 227.

When you delete a report in the console, the file is automatically deleted from the Mail Security Reports folder.

See “Accessing a report” on page 224.

To delete a report
1. In the console on the primary navigation bar, click Reports.
2. In the sidebar under Views, click Reports.
3 In the content pane in the Reports table, select the report that you want to delete.

4 In the sidebar under Tasks, click **Delete report** if you are in a server view or **Delete consolidated report** if you are in a group view.

### Resetting statistics

You can reset statistics for reporting purposes. Resetting statistics also resets the Activity Summary information on the Home page.

#### To reset statistics

1 In the console on the primary navigation bar, click **Reports**.

2 In the sidebar under Views, click **Report Settings**.

3 Under **Tasks**, select one of the following:
   - Reset database statistics
     Purges all data from the Reports database.
     See “Purging the Reports database” on page 207.
   - Reset Home page statistics
     Resets the Home page statistics for Recent Activity, Total Violations, and Activity Summary data.
   - Reset all statistics
     Resets the Home page statistics and database statistics

4 In the **Operation Status** window, click **Close**.
Keeping your product up to date

This chapter includes the following topics:

■ Monitoring your version support status
■ About keeping your server protected
■ Updating definitions
■ About enhancing performance when you update definitions on Exchange 2010 mailbox server
■ About alert notifications for out-of-date virus definitions

Monitoring your version support status

Mail Security provides version support status information so that you know the support life cycle for the version of Mail Security that you are use. It also keeps you informed when a newer version of the product is available.

The version support status information is updated through LiveUpdate. You obtain updated version support status information automatically when you run a manual or scheduled LiveUpdate on a computer. The computer must have the product and the console installed. (You might have to refresh the console to see the updated version support status information after a manual or scheduled LiveUpdate runs.)

You can also manually update the version support information from the Home page. Manually update your version support information from the Home page if you are on a computer that only has the Mail Security console installed. You must also manually update your version if you update definitions through Symantec Endpoint Protection or Symantec AntiVirus Corporate Edition.
The version support status information is stored, and the console applies the information to all the servers that the console manages. You only need to update the version support status in any view. The version support information is automatically updated for all of the servers that are managed in the server group. The version support information appears on the console for all of the servers in the group. The information does not appear on the console for the individual server.

To monitor your version support status in a server view

- In the console on the primary navigation bar, click **Home**.

  The version status information appears in the **Status** pane.

To monitor your version support status in a group view

1. In the console on the primary navigation bar, click **Home**.
2. In the **Status** pane, in the **Server** list, select the server for which you want to view version status information.

   The version status information appears below the server list.

To manually update the version status information

1. In the console on the primary navigation bar, click **Home**.
2. In the **Status** pane, click **Refresh Version Details...**
3. In the **LiveUpdate** dialog box, click **Next**.

   This LiveUpdate session only searches for updates to your product. It does not search for or download updates to your definitions.
4. In the **LiveUpdate** dialog box, click **Finish** when LiveUpdate is complete.

To refresh the version status information on the Home page

1. In the console on the primary navigation bar, click **Home**.
2. Press F5.

**About keeping your server protected**

Mail Security relies on up-to-date information to detect and eliminate risks. One of the most common reasons that problems occur is that definition files are not up-to-date. Symantec regularly supplies the updated definition files that contain the necessary information about all newly discovered risks. Regular updates of that information maximize security and guard your organization's Exchange mail server against infections and the downtime that is associated with an outbreak.

Mail Security lets you update your protection from threats and security risks using the following tools:
LiveUpdate downloads and installs available definitions from the Symantec LiveUpdate server. LiveUpdate certified definitions undergo stringent testing and are updated daily. LiveUpdate is enabled by default with a recommended daily schedule. However, you can modify the schedule.

See “Scheduling definition updates” on page 234.

Rapid Release definitions provide the fastest response to emerging threats and are updated approximately every hour. HTTP delivers the Rapid Release definitions and provides reliable first-line protection.

Rapid Release definitions are created when a new threat is discovered. Rapid Release definitions undergo quality assurance testing by Symantec Security Response. Rapid Release definitions do not undergo the intense testing that is required for a LiveUpdate release. Symantec updates Rapid Release definitions as needed to respond to high-level outbreaks and might be made available before the LiveUpdate definitions quality assurance process is complete. Rapid Release definitions provide a quick response to new threats and security risks and can be augmented later on by more robust detection capabilities in certified definitions.

Rapid Release definitions can be retrieved manually on demand.

See “Updating definitions on demand” on page 234.

Both methods let you update definitions on demand and automatically, based on the schedule that you specify. You can run Rapid Release definition updates instead of or in addition to LiveUpdate updates. For example, you can schedule daily LiveUpdate and then manually run Rapid Release when a new threat emerges.

---

Note: Mail Security relies on the definition update process to keep the version support information current. Configure Mail Security to perform definition updates if you have multiple Symantec AntiVirus products on the same computer.

You must have a valid content license to update definition files. A content license is a grant by Symantec Corporation for you to update Symantec corporate software with the latest associated content, such as new definitions. When you do not have a content license or your license expires, your product does not receive the most current definitions. This results in servers vulnerable to risks.

See "About licensing" on page 53.

---

About setting up your own LiveUpdate server

The LiveUpdate Administration Utility lets you set up an intranet HTTP server. This mechanism lets you handle LiveUpdate operations for your network.

The LiveUpdate Administration Utility is available at the following location:
If you set up your own LiveUpdate server, you must edit the LiveUpdate configuration for Mail Security to point to the local LiveUpdate server.

To set up your own LiveUpdate server

1. Navigate to the installation directory and run PassKeyTool.exe.
   
   \<InstallDir>\SMSMSE\7.9\Server\Config\PassKeyTool.exe

2. Type the passkey and click **Submit**.

3. Open proxy configuration tool.
   
   \<InstallDir>\SMSMSE\7.9\Server\Config\ConfigureProxy.exe

4. In the **Configure Live Update Settings** dialog box, specify the protocol as HTTP.

5. In the **Server** box, type the IP address of LiveUpdate server.

6. In the **Port** box, type the port number.
   
   Port number is 7070 by default.

7. Specify the path that is configured on Distribution Center page of the LiveUpdate Administrator.
   
   Default path is `clu-prod`.

8. Type the user name and password if it is configured in the Distribution Center.

9. Click **Submit**.

For more information, contact Symantec service and support.

See “Where to get more information about Mail Security” on page 20.

---

**Note:** If you use LiveUpdate Administrator to push definitions to Mail Security Servers, include the product **Symantec Mail Security for Microsoft Exchange 7.9** to your product list in the LiveUpdate Administrator.

---

**Configuring a proxy server to permit LiveUpdate definitions**

Some organizations use proxy servers to control connections to the Internet. To use LiveUpdate, you might need to specify the address and port of the proxy server as well as a user name and password. You can modify the proxy server configuration settings through LiveUpdate.
To configure HTTP settings for LiveUpdate

1. Navigate to the installation directory and run PassKeyTool.exe.
   
   `<InstallDir>\SMSMSE\7.9\Server\Config\PassKeyTool.exe`

2. Type the passkey and click **Submit**.

3. Open proxy configuration tool.
   
   `<InstallDir>\SMSMSE\7.9\Server\Config\ConfigureProxy.exe`

4. In the **Configure Live Update Settings** dialog box, specify the protocol as HTTP.

5. In the **Server** box, type `liveupdate.symantec.com`.

6. In the **Port** box, type the port number.
   
   Typically, the port number for HTTP is 80.

7. Select **Enable Proxy Settings**.

8. In the **URL** box, type the IP address of the HTTP proxy server.

9. In the **Port** box, type the port number of proxy server.

10. If user authentication is enabled for proxy server, provide user name and password.

11. Click **Submit**.

### Configuring a proxy server to permit rapid release definitions

To configure a server to permit rapid release definitions

1. Navigate to the installation directory and run PassKeyTool.exe.
   
   `<InstallDir>\SMSMSE\7.9\Server\Config\PassKeyTool.exe`

2. Type the passkey and click **Submit**.

3. Navigate to the installation directory and open proxy configuration tool.
   
   `<InstallDir>\SMSMSE\7.9\Server\Config\ConfigureProxy.exe`

4. Select **Enable Proxy Settings**.

5. In the **URL** box, type the IP address of the HTTP proxy server.

6. In the **Port** box, type the port number of proxy server.

7. If user authentication is enabled for proxy server, provide user name and password.

8. Click **Submit**.
Updating definitions

You can update definitions using any of the following methods:

- Perform updates on demand.
  See “Updating definitions on demand” on page 234.
- Schedule automatic updates.
  See “Scheduling definition updates” on page 234.

Updating definitions on demand

If you are in a single-server view, you can use LiveUpdate or Rapid Release to download the most current definitions on demand.

If you are in a group view, you can use LiveUpdate to download the most current definitions. After you update the definitions, distribute the updated definitions to the servers in your group.

To update definitions on demand for a single server

1. In the console on the primary navigation bar, click Admin.
2. In the sidebar under Views, click LiveUpdate/Rapid Release Status.
3. Under Tasks, select one of the following:
   - Run LiveUpdate Certified Definitions
   - Run Rapid Release Definitions (by HTTP)
4. In the Operation Status window, click Close when the operation is complete.

Scheduling definition updates

You can schedule Mail Security to perform definition updates automatically. If you have multiple servers that you want to perform their own updates using the same settings, you can configure the settings in the Global Group view or a user-defined group view. When you deploy your changes, the settings are deployed to all of the servers in the group. If you configure LiveUpdate to run on a schedule and deploy the changes to a group, it runs at the specified time in the local time zone of each server.

See “About enhancing performance when you update definitions on Exchange 2010 mailbox server” on page 235.

To schedule definition updates

1. In the console on the primary navigation bar, click Admin.
2. In the sidebar under Views, click LiveUpdate/Rapid Release Schedule.
3 In the content pane, under LiveUpdate/Rapid Release Schedule, check **Enable automatic virus definitions updates**.

This option is enabled by default.

4 Select one of the following:

- **Use Rapid Release definitions**
- **Use Certified LiveUpdate definitions**

This option is enabled by default.

5 Under **Schedule**, select one of the following:

- **Run every [ ]**, and then use drop-down menu, select the interval in hours that you want to run LiveUpdate or Rapid Release.

  The default value is 1 hour.

- **Run at a specific time**, and then type the time of day (in 24-hour format). Check the day or days of the week that you want LiveUpdate to run.

  The default setting for LiveUpdate is to run at 10:56 A.M. every day of the week.

  This option is not available for Rapid Release.

6 On the toolbar, click **Deploy changes** to apply your changes.

See “Deploying settings and changes to a server or group” on page 60.

**About enhancing performance when you update definitions on Exchange 2010 mailbox server**

If Auto-Protect scanning is enabled and you update definitions at hourly intervals or less (using Rapid Release or LiveUpdate), disable at least one of the following Auto-Protect features on the servers that have a message store:

- **Scans > Auto-Protect: Enable Background Scanning**

- **Scans > Auto-Protect: On virus definitions update, force rescan before allowing access to the Information Store**

When both of these options are enabled, the message store is rescanned each time definitions are updated. Overall mail throughput is affected if you update definitions at hourly intervals or less.

See “Configuring Auto-Protect scanning” on page 175.
About alert notifications for out-of-date virus definitions

Mail Security provides the following methods for notifying administrators when virus definitions are older than the configured number of days.

- An alert notification email is sent to the administrator.
- An event is logged on the system’s event log with event ID 404.

Mail Security checks at least once a day whether the current virus definitions are latest or out of date. If virus definitions are found outdated, then Mail Security sends an email notification to the administrator. Mail Security continues to send periodic notifications until it gets a new definition set.

Administrator can specify the frequency of sending notifications when an old definition is found. By default, an email notification is sent to the administrator after every 6 hours. Administrator can set the frequency of sending notifications at an hour-level granularity.

Administrator can configure the number of days an outdated virus definition can remain on the system after which an alert notification is sent. This configuration is done by specifying values for the registry keys `DefsMonitorDaysThreshold` and `DefsMonitorResendIntervalInHr`.

The path for these registry keys for 64-bit platform is:
`HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\SMSMSE\ 7.9\Server\ Components\LiveupdateConfig`

Table 12-1 lists the registry keys for this feature, their data types, and possible values.

<table>
<thead>
<tr>
<th>Registry key</th>
<th>Data type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>DefsMonitorDaysThreshold</code></td>
<td>REG_DWORD</td>
<td>Specifies the number of days after which a definition is considered as old and a notification is sent to the administrator. The default value of this registry key is 2 days. If the value of the registry key is set to zero, then administrator is not notified about the old virus definitions. The minimum value of this registry key is two.</td>
</tr>
</tbody>
</table>
Table 12-1  Registry key settings (continued)

<table>
<thead>
<tr>
<th>Registry key</th>
<th>Data type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>DefsMonitorResendIntervalInHr</td>
<td>REG_DWORD</td>
<td>Specifies the interval (in hours) at which a notification is sent to the administrator. The default value of this registry key is 6 hours. The minimum value of this registry key is one.</td>
</tr>
</tbody>
</table>

Note: With this feature, Mail Security has discontinued using the older mechanism of sending alerts on LiveUpdate failure.
Using variables to customize alerts and notifications

This appendix includes the following topics:

- Alert and notification variables

Alert and notification variables

Mail Security lets you customize notification and alert messages by using variables.

**Note:** The percent (%) sign is used to surround variables in the replacement text and email notification boxes. However, when a single percent sign (%) is placed in the text, it is filtered out and does not appear in the email notifications.

Table A-1 lists the replacement variables that you can use in any violation notification.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%n%</td>
<td>Starts a new line in the notification message</td>
</tr>
<tr>
<td>%server%</td>
<td>Autofills with the name of the server on which a violation was discovered</td>
</tr>
</tbody>
</table>

Table A-2 lists the replacement variables that you can use in rule violation notifications.
### Table A-2  Replacement variables for rule violation notifications

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%action%</td>
<td>Autofills with the action description that is taken in response to a rule violation</td>
</tr>
<tr>
<td>%attachment%</td>
<td>Autofills with the name of the attachment in which a rule violation has been found</td>
</tr>
<tr>
<td>%datetime%</td>
<td>Autofills with the date and time of a violation</td>
</tr>
<tr>
<td>%details%</td>
<td>Autofills the details of the violation. This variable is only available for the quarantine threshold notification</td>
</tr>
<tr>
<td>%information%</td>
<td>Autofills with any general information available about the violation</td>
</tr>
<tr>
<td>%location%</td>
<td>Autofills with the name of the location at which a violation was discovered. For example, inbox, outbox, public folder</td>
</tr>
<tr>
<td>%recipient%</td>
<td>Autofills with the name of the intended recipient of a message in which a violation was discovered</td>
</tr>
<tr>
<td>%scan%</td>
<td>Autofills with the scan name that discovered a violation</td>
</tr>
<tr>
<td>%sender%</td>
<td>Autofills with the name of the sender of a message in which a violation was discovered</td>
</tr>
<tr>
<td>%subject%</td>
<td>Autofills with the contents of the subject line</td>
</tr>
<tr>
<td>%violation%</td>
<td>Autofills with the name of the violation detected</td>
</tr>
<tr>
<td>%ViolatingTerm%</td>
<td>Autofills with the list of violating terms that triggered content filtering policy</td>
</tr>
</tbody>
</table>

### Table A-3  Replacement variables for outbreak notifications

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%count%</td>
<td>Autofills with the number of messages that violate the outbreak trigger</td>
</tr>
<tr>
<td>%threshold%</td>
<td>Autofills with the threshold level of an identified outbreak trigger</td>
</tr>
<tr>
<td>%trigger%</td>
<td>Autofills with the outbreak trigger name that detected an outbreak</td>
</tr>
<tr>
<td>%outbreak_rule%</td>
<td>Autofills with the outbreak rule name that triggers an outbreak</td>
</tr>
<tr>
<td>%outbreak_count%</td>
<td>Autofills with the number of times that an outbreak triggers</td>
</tr>
</tbody>
</table>

See "Configuring outbreak notifications" on page 199.
Why a file triggers the Unscannable File Rule

A file can trigger the Unscannable File Rule when Mail Security is unable to scan the file.

Some examples of when a file might trigger the Unscannable File Rule are as follows:

- File extension is not supported by Mail Security.
- File is encrypted and cannot be decrypted by Mail Security.
- File is opened in a binary mode, preventing Mail Security from reading it.
- File is compressed and cannot be decompressed by Mail Security.
- File is a type of file that Mail Security does not recognize.
- File is a type of file that Mail Security cannot scan due to its nature or content.
Mail Security cannot access the file.

This scenario can occur when another thread or process accesses the file. For example, two separate antivirus software programs (a file system-based program and an email-based program) attempt to scan the same file simultaneously.

Configure your other antivirus programs to exclude certain folders from scanning. If another antivirus program scans the Exchange directory structure or the Mail Security processing folder, it can cause:

- False-positive threat detection
- Unexpected behavior on the Exchange server
- Damage to the Exchange databases

See “About using Mail Security with other antivirus products” on page 49.

For information about how to prevent Symantec AntiVirus products from scanning the Exchange directory, go to the following Symantec Knowledge Base article:


The file is corrupt.

Mail Security correctly identifies the file, but the file is corrupt.

The file is incorrectly identified.

Mail Security misidentifies the file based on the message header. The actions that the program performs on the file are incorrect and invalid for the file type.

This scenario can also occur in a file that contains invalid characters or values in the header.

The scanner or decomposer times out.

The antivirus scanner or decomposer times out when it attempts to scan the file.

This scenario can occur when a file meets or exceeds the scanning limits that you specify.

See “Configuring file scanning limits” on page 94.
The temporary working directory is missing, or the path to the directory is incorrect.

This scenario could occur if the temporary working directory is deleted or moved. Check to see if the \Temp directory exists. If it has been deleted, create it in the following location:

C:\Program Files\Symantec\SMSMSE\7.9\Server \Temp

The file contains a large compressed attachment.

A file that contains a large attachment might trigger the Unscannable File Rule. For example, a 100-MB attachment that is compressed into a 4-MB zip file.

See “Configuring file scanning limits” on page 94.

See “Configuring rules to address unscannable and encrypted files” on page 95.

A Symantec AntiVirus product attempts to scan files in Mail Security folders.

You must configure the Symantec AntiVirus product to exclude Mail Security folders from being scanned.

See “About using Mail Security with other antivirus products” on page 49.

Note: If the Encrypted File Rule is enabled, encrypted files trigger the Encrypted File Rule instead of the Unscannable File Rule.

See “Configuring rules to address unscannable and encrypted files” on page 95.

Reducing the incidence of malformed MIME false positives

A message body or attachment might trigger the Unscannable File Rule and appear in the event log as Event ID 218. However, the MIME container in the email appears to be correct.

You can either reduce the sensitivity for malformed MIME identification or disable detection of malformed MIME containers. This action reduces the incidence of malformed MIME false positives.

To reduce malformed MIME identification sensitivity

◆ Create or modify the following DWORD registry value:

HKEY_LOCAL_MACHINE\Software\Symantec\SMSMSE\7.9\Server\DecMIMEIdentificationStrength

The value can be a decimal between 1 and 5. The higher the number, the sensitivity lowers and reduces the incidence of false positives.
To disable malformed MIME container detection

♦ Create or modify the following DWORD registry value to decimal 0.

\HKEY_LOCAL_MACHINE\Software\Symantec\SMSMSE\7.9\Server\BlockMalformedContainers

Common error messages

Table B-1 lists some common error messages that might occur.

Table B-1 Common error messages

<table>
<thead>
<tr>
<th>Error message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Mail Security service is stuck in a starting state</td>
<td>The following are the most common reasons that the Mail Security service gets stuck in a starting state:</td>
</tr>
<tr>
<td></td>
<td>■ Timing conflicts occur with the operating system.</td>
</tr>
<tr>
<td></td>
<td>A solution is to make the Mail Security service dependent upon another service, such as the Microsoft Exchange Information Store service (MSExchangeIS).</td>
</tr>
<tr>
<td></td>
<td>For more information, see the Microsoft knowledge base. On the Internet, go to the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://support.microsoft.com/default.aspx?scid=kb;en-us;193888">http://support.microsoft.com/default.aspx?scid=kb;en-us;193888</a></td>
</tr>
<tr>
<td></td>
<td>■ The Temp and Quarantine folders are not excluded from scanning by other antivirus products.</td>
</tr>
<tr>
<td></td>
<td>The Temp and Quarantine folders are located in the following directories:</td>
</tr>
<tr>
<td></td>
<td>■ \Program Files\Symantec\SMSMSE\7.9\Server\Temp</td>
</tr>
<tr>
<td></td>
<td>The exclusion of the Temp folder is critical to the operation of the product.</td>
</tr>
<tr>
<td></td>
<td>The product uses the Temp folder as a processing folder.</td>
</tr>
<tr>
<td></td>
<td>■ \Program Files\Symantec\SMSMSE\7.9\Server\Quarantine</td>
</tr>
</tbody>
</table>
### Table B-1  Common error messages (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam data is not collected by default</td>
<td>If spam-related data does not appear in reports, ensure that the &quot;Include spam data&quot; check box is enabled on the Report Settings page. See “Specifying the duration for storing data in the Reports database” on page 206.</td>
</tr>
<tr>
<td>Cannot connect to server</td>
<td>One possible cause for this error is if the domain controller is running on the same server as Microsoft Exchange. Microsoft acknowledges this scenario as a defect and has provided a manual workaround for this issue. For more information, refer to the Microsoft knowledge base. On the Internet, go to the following URL: <a href="http://support.microsoft.com/?id=824308">http://support.microsoft.com/?id=824308</a> This article references ASP.NET 1.1, but the article also applies to ASP.NET 2.0.</td>
</tr>
<tr>
<td>Unique identifier (UID) errors might occur in Outlook or Outlook Express when you use IMAP</td>
<td>This error can occur when the mail client is open on the desktop at the same time a violation is detected on the server. These warnings can be ignored. Refresh the mailbox. Outlook, Exchange, and Mail Security continues to function normally.</td>
</tr>
<tr>
<td>OWA message: The action cannot be completed because of a conflict with the original item</td>
<td>A message sender who uses Outlook web access might get the following error message if Mail Security detects a violation: The action cannot be completed because of a conflict with the original item. The conflict may have occurred when an existing item was updated on another computer or device. Open the item again and try making your changes. If the problem continues, contact technical support for your organization. This issue is a defect in Exchange 2010. Currently, there is no workaround. For more information, see the Microsoft website. This error only occurs on Outlook web access 2010.</td>
</tr>
</tbody>
</table>
Table B-1  Common error messages (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error in assigning Application Impersonation right to user. Please check whether the SMSMSE_RBAC right is already there or change user name.</td>
<td>Please check whether the SMSMSE_RBAC right is already there or change user name.</td>
</tr>
<tr>
<td>User does not have mailbox or Error in checking mailbox.</td>
<td>Check whether user has a mailbox. If not, create a mailbox for the user, or give some other user who has mailbox.</td>
</tr>
<tr>
<td>User is not member of Administrators group. Please add user to Administrators group.</td>
<td>User must be a member of the following groups: Administrators and Exchange Organization Management</td>
</tr>
<tr>
<td>Existing RBAC user is different from the given user name.</td>
<td>Already there is a user with RBAC rights. During silent install, different user is provided.</td>
</tr>
<tr>
<td>The scan &lt;ScanName&gt; cannot be completed as Microsoft Exchange's Client Access server is not reachable.</td>
<td>This error occurs if the status of manual scan on the UI is FAILED. This error also occurs if there is an error in the event log with event ID 396. The possible cause is that Mail Security is unable to determine or connect to the Client Access server (CAS) of the mailbox databases. To resolve this issue, ensure that CAS server is up and running and can be accessed from the mailbox server.</td>
</tr>
</tbody>
</table>

Following are some error messages that might occur when a user's password expires.

**Resolving installation issues**

You may encounter installation and post-installation issues. Web links can assist you to resolve these issues. They provide information about product installation and configuration details and are available for both 32-bit and 64-bit installers.

You are recommended to access web links to resolve any issues you may encounter during installation and post-installation.

**To access web links during wizard based installation**

- During wizard based installation, you can access the web links from the wizard.
  
  From the MSI installer user interface, click the link for which you need information.

**To access web links during silent installation**

- During silent installation, you can access the web links from the installer log file.
The log file locations are:

- **For 32-bit installer**, `C:\Documents and Settings\Administrator\Local Settings\Temp\ SMSMSE70_setup.log`
- **For 64-bit installer**, `C:\Users\Administrator\AppData\Local\Temp\ SMSMSE70_setup.log`

To access web links during remote installation

- During remote installation, you can access the web links from the installer log file on the remote machine.

The log file locations are:

- **For 32-bit installer**, `C:\Documents and Settings\Administrator\Local Settings\Temp\ SMSMSE70_setup.log`
- **For 64-bit installer**, `C:\Users\Administrator\AppData\Local\Temp\ SMSMSE70_setup.log`

---

Note: Each installation error and warning in the log file has a URL. You can copy and paste the URL from the log file on to the browser to view the instructions.

---

**Table B-2** lists the errors you might encounter during remote installation and how to resolve them.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the user name that you provide while logging on to Windows is not a member of the Local Administrators group on the remote server, then the following message appears: &quot;Access to the network resource was denied.&quot;</td>
<td>Ensure that the user is a member of the Local Administrators group and retry the remote installation process.</td>
</tr>
</tbody>
</table>
### Remote installation issues (continued)

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following error occurs due to any of the following causes:</td>
<td>Ensure that the user is a member of <strong>Organization Management</strong> and that the Active Directory objects are replicated correctly. Start the remote installation process again.</td>
</tr>
<tr>
<td>■ The user name that you provide while logging on to Windows is not a member of <strong>Organization Management</strong>, one of the Exchange security groups.</td>
<td></td>
</tr>
<tr>
<td>■ The Active Directory is not in sync maybe because of the Active Directory replication latency.</td>
<td></td>
</tr>
<tr>
<td>&quot;Error in assigning Application Impersonation right to user. Please check whether SMSMSE_RBAC right is already there or change user name.&quot;</td>
<td></td>
</tr>
<tr>
<td>During the installation of Mail Security on remote mailbox role, if you provide logon credentials of a user who is not a member of the <strong>Organization Management</strong> group, then the Mail Security service does not start.</td>
<td>Ensure that you provide the user name and password of a user who is a member of the <strong>Organization Management</strong> group.</td>
</tr>
</tbody>
</table>

Sometimes it takes a long time during the launch of Mail Security console when .NET Framework 2.0 is installed on your system. If you are running .NET Framework 2.0, then it is recommended that you install SP1 of .NET Framework 2.0. However, you do not experience delay in launching Mail Security console on systems with higher versions of .NET Framework installed.

**To reduce time during the launch of Mail Security console**

1. Start Internet Explorer.
2. On the **Tools** menu, click **Internet Options**.
3. Click the Advanced tab, and then locate the Security section.
4. Uncheck **Check for publisher’s certificate revocation** and then click **OK**.
5. After the installation is complete, check **Check for publisher’s certificate revocation**.

---

**Note:** The **Check for publisher’s certificate revocation** option is set on a per-account basis.

---

## Resolving consolidated report issues

**Table B-3** lists the issues that you might encounter when working with consolidated reports.
### Table B-3  Consolidated report related issues

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export/import of scheduled consolidated reports is not supported.</td>
<td>Recreate the scheduled consolidated reports after you import settings.</td>
</tr>
<tr>
<td>Multiple users performing a <strong>Reset to factory defaults</strong> task</td>
<td>If user A has created some consolidated report schedules and user B tries to perform the <strong>Reset to factory defaults</strong> task, then only the schedules that user B creates get deleted. Schedules that user A creates are retained. SMSMSE ensures that, the schedules that remain in the Task Scheduler after you perform the <strong>Reset to factory defaults</strong> task are not triggered.</td>
</tr>
</tbody>
</table>

### About the Symantec Help utility

The Symantec Help (SymHelp) utility is a cross-product diagnostic utility that identifies the common issues that you may encounter when you use Mail Security. This utility helps you to diagnose and resolve these issues.

The SymHelp utility is a collection of script files. These script files are copied to a temporary directory on your local computer and are deleted when you exit the utility. The utility gathers information about the problem on your computer and helps you to diagnose it. You can also use the utility to ensure that your computer meets the minimum requirements to install any supported Symantec products.

To download the SymHelp utility from the Mail Security console, click **Help > Download Support Tool**.

Alternatively, you can go to the following Symantec Knowledge Base article to access information about how to download the SymHelp utility:

http://www.symantec.com/business/support/index?page=content&id=TECH170752

For information about how to use the utility, go to the following Symantec Knowledge Base article:

http://www.symantec.com/business/support/index?page=content&id=TECH170735

When you run the utility, a series of diagnostic reports are generated. For information about the Mail Security diagnostic reports, go to the following Symantec Knowledge Base article:

http://www.symantec.com/business/support/index?page=content&id=TECH171013

See “Common error messages” on page 243.
LiveUpdate fails to update the definitions

In a rare case, LiveUpdate fails to update the definitions. When you run the LiveUpdate, it reports that definitions are up-to-date; which is not the case. You may get one of the following messages:

- Unable to run LiveUpdate.
- LiveUpdate has determined that no update is necessary. You already have the most recent virus definitions.

To resolve this issue

1. Ensure that Symantec Update Manager service is running.
2. Delete csapi_defs and rep_revoc folders from the following path:
   
   C:\ProgramData\Symantec\Definitions\SymcData

3. Run LiveUpdate again.
A
Active Directory 128, 150
Active Summary 228
adware. See security risks
alert notifications 16, 236, 238
Allowed Senders list 105
antispam filtering
about 104
configuring Symantec Premium AntiSpam 107
configuring whitelists 105
licensing requirements 53
processing spam 115
processing suspect spam that exceeds a SCL threshold 113
processing suspected spam 110
antivirus
Basic Virus Rule 88
detecting mass-mailer viruses 88
enabling detection 88
how Mail Security detects viruses 87
logging detections 203
modifying virus policies 88
quarantining viruses 75
setting Bloodhound detection level 88
Unrepairable Virus Rule 88
updating protection against 230
antivirus definitions. See definitions
antivirus products, other 22, 49
attachments
Allow-Only Attachment Rule 125
blocking by attachment name 150
enforcing email attachment policies 150
filtering 120
Outbreak Triggered Attachment Names match list 154
Quarantined Triggered Attachment Names Rule 125
Sample Attachment Name match list 154
Sample Executable File Names match list 154
Sample Multimedia File Names match list 154
auto-protect scans 147, 175, 179
automated installation 39
B
background scanning 169
configure 176
stop 176
background scans 179
logging 178
stopping 178
Basic Virus Rule 88
Bloodhound heuristics technology 87
C
certificate revocation list 28
configure
content filtering 126
file type filtering 126
c console
about 46
accessing 46
Home page 48
installing 37
primary navigation bar 48
system requirements 30
consolidated report 219–220
container files
configuring limits 94
decomposing 87
denial-of-service attacks 94
encrypted 86, 95
unscannable 86, 95
content area 46
content filtering policy templates 14
about 163
editing 167
preconfigured 163
content filtering rules
about 120
configuring conditions 127
configuring violation notification 130
creating match lists 158
Index | 251

content filtering rules (continued)
deleting 148
ing editing match lists 158
elements of 141
enabling for auto-protect scanning 147
enforcing attachment policies 150
literal string 141
managing 146
managing match lists 158–159
metacharacters 161
multiple violations 120
pre-configured rules 125
prioritizing 147
refreshing Active Directory groups 150
regular expressions 160
specifying local domains 149
specifying users to whom rules apply 128
specifying violation actions 132
supported SMTP address formats 128
wildcards 141
content license 53
continuous protection scheduled scan 14
.csv (comma-separated value) report format 210

D
definitions
about 87
licensing requirements 53, 230
LiveUpdate Administration Utility, about 231
out-of-date 236
updating 230, 234
denial-of-service attacks 86, 94
deploy all settings 60
deploy changes 60
detailed report. See templates
dialers. See security risks
DirectX 29
discard changes 60
domains, specifying local 149
DOS wildcard expressions 159

E
encrypted files 95
Enterprise Vault 118
error messages 243
Event Log
about 203
contents 204
Event Log (continued)
filtering contents 204
viewing 204
executable files, detecting 154
Executive Summary report. See templates
expressions
regular 160
wildcard 159

F
features
new and enhanced 14
protecting and managing your server 16
file filtering 120
file filtering rules
about 150
blocking attachments by name 150
file true type filtering 128
file type categories
supported file types 122
file type filtering 126
about 122
file true type 122
file type filtering rule
create 128
file type filtering rules
configuring violation notification 130
deleting 148
enabling for auto-protect scanning 147
managing 146
pre-configured rules 126
prioritizing 147
refreshing Active Directory groups 150
specifying local domains 149
specifying users to whom rules apply 128
specifying violation actions 132
supported SMTP address formats 128
file types 122, 128
filtering. See content filtering rules
formats, report output 210
FTP proxy server, LiveUpdate connection 232

G
Global Group 59

H
hack tools. See security risks
help 20
### Heuristics
87

### HTML
- Encoding 120
- Report output format 210

### HTTP proxy server, LiveUpdate connection
232

### Hyper-threaded processor
51

### I
- IIS (Internet Information Services) 29–30
- Impersonation 29
- Inbound/outbound settings 149

### Installation
- Before you install 22
- Customizing remote server installation 39
- Installing on a local server 33
- Installing on a remote server 39, 42
- Installing the console only 37
- Post-installation tasks 43
- Security and access permissions 27
- System requirements 29

### Intel Xeon processors
51

### ISA server, registering
106

### ISP proxy server, LiveUpdate connection
232

### J
- Joke programs. See security risks

### License
- Activating 54
- Content license 53
- Expiration 53
- Installing 56
- Locating the serial number 55
- Obtaining a license file 55
- Obtaining a serial number 55
- Renewing 57

### Literal string
141

### LiveUpdate
- About 230
- Enhancing performance 235
- Licensing requirements 53
- Updating definitions
  - On demand 234
  - Scheduled 234
- Using proxy servers 234

### Logs
209
- See also reports

### Event Log
- About 203
- Contents 204
- Filtering contents 204

### Logging destinations
203

### MMC Performance console
203, 207

### Reports database
- About 203
- Purging 207
- Storing data 206

### Windows Application Event Log
203

### M
- Mail Security for Microsoft Exchange
  - About 13
  - Accessing the console 46
  - Features 14, 16
  - Getting more information 20
- Mail Security for Microsoft Exchange Management Pack 14, 207
- Mail Security Reports folder 224
- Manual scans
  - About 169, 180
  - Configuring 181
  - Running 185
manual scans  (continued)
  stopping while in progress 185
  viewing results 185
mass-mailer worms 86
match lists
  about 154
  creating 158
  deleting 159
  editing 158
  preconfigured 154
MCC (Microsoft Management Console) 203
MDAC 29
menu bar 46
message archiving 118
messages, common errors 243
metacharacters 161
Microsoft Certificate Services 2.0 44
Microsoft Excel 210
MIME, malformed 242
MMC (Microsoft Management Console) 207
MSXML 33

N
  .NET Framework 29–30
  notification settings 192
  notification, variables 238
  notifications 16, 236

O
  Open Proxy list 107
  Operation Status 60
  outbreak. See outbreak management
  Outbreak management
    best practices 196
  outbreak management 16
    about 193
    clearing notifications 202
    configuring notifications 199
    configuring triggers 197
    defining an outbreak 194
    enabling 197
    triggers, about 196

P
  Performance counters 207
  performance improvement
    content filtering 14
    manual scan 14
  performance improvement  (continued)
    scheduled scan 14
  performance, enhancing 235
  permissions 27
  policies 86
  port requirements 31
  post-installation tasks 43
  pre-installation requirements 22
  premium antispam service. See Symantec Premium AntiSpam
  preview pane 46
  primary navigation bar 46, 48
  processing limits 94
  protection, server 230
  proxy server
    configuring for Symantec Premium AntiSpam 107
    LiveUpdate 234
  quarantine entire message 14
  Quarantine Server 75
    See also local quarantine
    about 75
    forwarding items to 76
    location on product installation package 14
  quarantine thresholds
    specifying actions 80
  Rapid Release
    about 230
    enhancing performance 235
    licensing requirements 53
    updating definitions
      on demand 234
      scheduled 234
  regular expressions 160
  remote access programs. See security risks
  replacement variables 238
  reports 209
    See also templates
    accessing 224
    consolidated 219–220
    creating or modifying 210, 215
    deleting 227
    email notification limitations 210, 215
    generating on demand 224
    managing 219
reports  (continued)
  printing 226
  Reports page display information 224
  resetting statistics 228
  saving data 227
  scheduling 221
  viewing with third-party tools 210
Reports database
  about 203
  purging 207
  storing data 206
reputation service 107
risks 86
  See also security risks
  See also threats
Bloodhound heuristics technology 87
categories of 86
configuring security risk detection 91
configuring threat detection 88
decomposing container files 87
how risks are detected 87
setting container file limits 94
RTF encoding 120

S
Safe list 107
scan processes 51
scanning limits 94
scanning threads 51
scans
  advanced scanning options 179
  auto-protect 175
  background 176
  How messages are scanned 171
  manual 180
  notifying of violations 192
  offloading mailbox server scanning 174
  optimizing scanning performance 175
  scheduling 186
  types of scans 169
scheduled scans
  about 169, 186
  configuring 187
  creating 186
  deleting 191
  editing 186
  enabling 191
  stopping 190
  scheduling consolidated report 221
screen resolution, recommended 22
security and access permissions 27
security risks
  about 86
  categories of 91
  configuring detection 91
serial numbers, licensing 55
server groups 59
  See also servers
  adding servers 68
  creating 67
  deleting 71
  deploying all settings 60
  deploying changes 60
  Global Group 59
  managing, about 62
  moving servers from/to 69
  pushing out settings to servers 70
  restoring default settings 70
  server settings file location 59
  user-defined 59
  viewing settings 66
server protection 230
servers 59
  See also server groups
  adding to groups 68
  deploying changes 60
  importing and exporting settings 72
  managing, about 62
  modifying communication properties 73
  moving to another group 69
  removing from group management 71
  restoring default settings 70
  synchronizing settings 70
  viewing settings 66
  viewing status 67
settings, importing and exporting 72
sidebar 46
SMSMSE Admins 27
SMSMSE Viewers 27
software components 24
SPA. See Symantec Premium AntiSpam
spam. See antispam filtering
spyware. See security risks
SSL (Secure Socket Layer) communications 44, 73
statistics, resetting 228
string, literal 141
Suspect list 107
Symantec AntiVirus Corporate Edition 22, 49, 230
Symantec Brightmail AntiSpam 22
Symantec Central Quarantine 14
Symantec Endpoint Protection 22, 49
Symantec Enterprise Vault 118
Symantec Help 248
Symantec Mail Security for Microsoft Exchange. See Mail Security for Microsoft Exchange
Symantec Premium AntiSpam 104
SymHelp utility 248
system requirements 29

T
TCP (Transmission Control Protocol) port,
changing 73
templates
about 209
creating or modifying 210, 215
deleting 218
Detailed 209
output formats 210
Summary 209
threats 86
See also risks
Bloodhound technology 88
configuring detection 88
detecting mass-mailer infected messages 88
types detected 86
throttling policy
assigning 73
creating 73
toolbar 46
trackware. See security risks
transport agents
configuring 49
priorities 49
Trojan horses 86

U
UNC (Universal Naming Convention) path 56
Unfiltered Recipients list 105
uninstallation 33
Unrepairable Virus Rule 88
unscannable files 95, 240
updates. See definitions
upgrade voucher 54–55
user credentials 33

V
variables, replacement 238
version support 229
virus 86
See also risks
Basic Virus Rule 88
configuring detection 88
detecting mass-mailer viruses 88
enabling detection 88
how Mail Security detects 87
logging detections 203
modifying virus policies 88
quarantining 75
setting Bloodhound detection level 88
Unrepairable Virus Rule 88
updating protection against 230
virus definitions. See definitions
outdated 236

W
whitelists 105
wildcard expressions, DOS 159
Windows Application Event Log
about 203
viewing contents of in Mail Security 204
worms 86

X
x-headers 118

Z
.zip files. See container files