Symantec™ Mail Security for Microsoft® Exchange

Management Pack Integration Guide

v7.5.3

Symantec

Symantec™ Mail Security for Microsoft® Exchange Management Pack Integration Guide

Documentation version: 1.0

06 October, 2015.

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

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:

www.symantec.com/business/support/

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:

www.symantec.com/business/support/

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:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Management Pack Integration Guide

About the Symantec Mail Security for Microsoft Exchange Management Pack

Symantec Mail Security for Microsoft Exchange Management Pack lets you integrate Symantec Mail Security for Microsoft Exchange events with Microsoft System Center Operations Manager (SCOM) 2007 R2/2012. When you import the management pack in SCOM, it immediately begins monitoring objects based on default configurations and thresholds. These default configurations and thresholds (such as monitors, rules, and tasks) monitor specific Symantec Mail Security for Microsoft Exchange events in the Windows Event Log and the Windows Performance Monitor.

When a rule is triggered, the SCOM agent collects data about the event and forwards it to SCOM. SCOM provides you with a central repository that you can use to monitor critical events that occur on your Exchange servers.

For more information about Microsoft System Center Operations Manager 2007 R2/2012, see the Microsoft System Center Operations Manager 2007 R2/2012 documentation.

For more information about Symantec Mail Security for Microsoft Exchange, see the *Symantec Mail Security for Microsoft Exchange Implementation Guide*.

Importing the management pack

The system requirements for the computer on which you import the management pack are as follows:

- Microsoft System Center Operations Manager 2007 R2/2012

- Microsoft SQL Server 2005 Enterprise Edition with SP1 (or later) or Microsoft SQL Server 2008 Enterprise Edition with SP1 (or later)
  The Microsoft SQL Server and SQL Agent services must be running when you install the management pack.
- Microsoft Exchange Server 2007/2010/2013/2016
- Windows Server 2008

The management pack is supported for Symantec Mail Security for Microsoft Exchange 7.0.x events only. The SCOM agent must be deployed to the servers on which Symantec Mail Security for Microsoft Exchange is installed. This agent collects events and performance data and forwards the information to SCOM. For information about how to deploy the agent or remove the Symantec Mail Security for Microsoft Exchange Management Pack, see the appropriate Microsoft documentation.

To import the management pack in SCOM

1. Copy SMSMSESCOM.mp to the following folder:

   \Program Files\System Center Management Packs
2. In the SCOM 2007 R2/2012 Operator Console in the left pane, right-click **Management Packs**, and then click **Import Management Pack**.
3. Browse and locate the SMSMSESCOM.mp management pack in the \Program Files\System Center Management Packs folder.
4. In the **Import Management Packs** panel, click **Install**.
5. In the **Import Status** window, click **Close** when the program finishes importing the management pack.

About the Symantec Mail Security for Microsoft Exchange rules

When you import the management pack, a Symantec Mail Security for Microsoft Exchange directory structure is automatically created and populated with pre-configured rules. These are rules that collect data about specific critical events.

Symantec Mail Security for Microsoft Exchange event rules are as follows:

Event rules — These are rules that collect data about specific critical events.

The following event rules come under this category:

- Licensing
  See "About Licensing rules" on page 10.
- LiveUpdate
  See "About LiveUpdate rules " on page 11.
- Outbreak
  See "About Outbreak rules " on page 12.
- Rapid Release
  See "About Rapid Release rules" on page 12.
- Services
  See "About Service rules" on page 13.

Performance rules — These are rules that measure specific performance criteria. The following event rules come under this category.

See "About Performance rules " on page 12.

Note: Rules are not categorized for SCOM.

For information about how to modify rules or create new rules, see the appropriate Microsoft documentation.

About Licensing rules

Table 1 lists the default Licensing rules and the events that trigger the rules.

Table 1 Default Licensing rules

Rule	Description of event trigger
Antivirus License Error	The content license expired or is not installed, or the license file is damaged.
Invalid License - Console LiveUpdate Failed To Update	The content license expired or is not installed, or the license file is damaged.
Invalid License - LiveUpdate Failed to Update	The content license expired or is not installed, or the license file is damaged.
Invalid License - LiveUpdate Virus Definitions Not Updated	Your content license expired or is not installed, or the license file is damaged.
Invalid License - Rapid Release Failed to Update	Could not find a valid content license.

Table 1 Default Licensing rules *(continued)*

Rule	Description of event trigger
Invalid Symantec Premium AntiSpam License	The license file is expired, invalid, or damaged.
Symantec Premium AntiSpam License Error	The Symantec Premium AntiSpam license expired or is not installed, or the license file is damaged.
Unable to Install Antivirus License	The license file is expired, invalid, or damaged.
Unknown Symantec Enterprise Licensing Error	The license file is expired, or the license file is damaged.

About LiveUpdate rules

Table 2 lists the default LiveUpdate rules and the events that trigger the rules.

Table 2 Default LiveUpdate rules

Rule	Description of event trigger
Console Communication Error with LiveUpdate	An error occurred with LiveUpdate. The LiveUpdate server is temporarily unavailable, or the server has lost network connectivity. Check the Event Log for more information.
LiveUpdate Critical Error	The LiveUpdate server is temporarily unavailable, or the server has lost network connectivity.
LiveUpdate Error	The LiveUpdate server is temporarily unavailable, or the server has lost network connectivity.
LiveUpdate Host Busy	Many people are attempting to access the LiveUpdate server simultaneously.
LiveUpdate No Carrier	The LiveUpdate server is temporarily unavailable.
LiveUpdate Unknown Error	The LiveUpdate server is temporarily unavailable.
Missing Virus Definitions	Definition files are damaged or missing.

About Outbreak rules

Table 3 lists the default Outbreak rules and the events that trigger the rules.

Table 3 Default Outbreak rules

Rule	Description of event trigger
Outbreak Occurrence	An outbreak threshold was reached.
Outbreak Reoccurrence	An outbreak is still occurring.

About Performance rules

Table 4 lists the default Performance rules and the events that trigger the rules.

Table 4 Performance counters

Performance counter	Description
Bytes Scanned	Number of bytes scanned.
Bytes Scanned/Sec	Number of bytes scanned per second.
Total Scans	Number of scans performed on messages and attachments.
Total Scans/Sec	Number of scans performed on messages and attachments per second.
Threats and Risks Found	Number of software threats detected.
Threats and Risks Found/Sec	Number of software threats detected per second.
Content Filtering Found	Number of content violations detected.
Content Filtering Found /Sec	Number of content violations detected per second.
Spam Violations Found	Number of spam violations detected.
Spam Violations Found/Sec	Number of spam violations detected per second.

About Rapid Release rules

Table 5 lists the default Rapid Release rules and the events that trigger the rules.

Table 5 Default Rapid Release Rules

Rule	Description of event trigger
FTP Failure	An FTP failure occurred.
General Error During Rapid Release	Unknown. Check the Event Log for more information.

About Service rules

Table 6 lists the default Services rules and the events that trigger the rules.

Table 6 Default Services rules

Rule	Description of event trigger
Auto-Protect Process Failed to Start	Check the Event Log for more information.
Out of Memory	Computer resources are low.
Quarantine is Full	The Quarantine Server contains too many quarantined files.
Service Could Not Start	Check the Event Log for more information.
Service Could Not Start - Already Started	An attempt was made to start the service, but the service is already running.
Service Could Not Start – Auto-Protect Process Not Started	The Symantec Mail Security for Microsoft Exchange service cannot start.
Service Could Not Start - Configuration Invalid	The program settings could not be obtained or are invalid.
Service Could Not Start - Cannot Logon to the Exchange Server	Unable to logon to the Exchange server.
Service Could Not Start - Low Memory Conditions	There is not enough memory to start the service.
Service Could Not Start - Not Admin Account	The NT account specified does not have administrator privileges.
Service Stopped	The computer was restarted or shut down.
Unable to Record Events	The Event Log is full.

Viewing the Symantec Mail Security for Microsoft Exchange rule group

You can view the default Symantec Mail Security for Microsoft Exchange group in the SCOM console.

Each rule contains a knowledge base that provides the following information:

Summary	A brief description of the rule
Cause	What event triggered the rule
Resolution	Proposed resolutions for resolving the event issue

To view the Symantec Mail Security for Microsoft Exchange rule group

1. In the SCOM 2007 R2/2012 Operator Console in the left pane, expand **Management Packs Objects**.
2. Under **Management Pack Objects**, select **Rules**.
3. In the right pane under **Rules**, look for **SMSMSE** to view the rules that are available for Symantec Mail Security for Microsoft Exchange.
4. Double-click the rule for which you want to view the knowledge base.
5. In the **Rule Properties** dialog box, click the **Product Knowledge** tab to view the details about the rule.

Disabling default rules

All of the Symantec Mail Security for Microsoft Exchange rules are enabled by default. You can disable the rules that you do not want to apply.

To disable default rules in SCOM

1. In the SCOM 2007 R2/2012 Operator Console in the left pane, expand **Management Packs Objects**.
2. Under **Management Packs Objects**, select **Rules**.
3. In the right pane under **Rules**, look for **SMSMSE** to view the rules that are available for Symantec Mail Security for Microsoft Exchange.
4. Double-click the rule that you want to disable.
5. In the **Event Rule Properties** dialog box, uncheck **Rule is enabled**.
6. Click **Apply**, and then click **OK**.

Viewing Symantec Mail Security for Microsoft Exchange events and performance data

You can view Symantec Mail Security for Microsoft Exchange events and performance data in the SCOM console. The Events view contains the following rule violations: Licensing, LiveUpdate, Outbreak, Rapid Release, and Services. The Performance view contains Performance rule data.

To view Symantec Mail Security for Microsoft Exchange events in SCOM

1. In the SCOM 2007/2012 R2 Operator Console in the left pane, click **Monitoring**.
2. In the **Monitoring Views** pane, click **Monitoring > Symantec > SMSMSE**.
3. Click **SMSMSE Events**.

   The events appear in the SMSMSE Events in the right pane.
4. Select an event to view detailed information.

   The details appear in the **Event Details** pane.

To view Symantec Mail Security for Microsoft Exchange performance data in SCOM

1. In the SCOM 2007/2012 R2 Operator Console in the left pane, click **Monitoring**.
2. In the **Monitoring Views** pane, click **Monitoring > Symantec > SMSMSE**.
3. Select the performance rule that contains the specific criteria that you want to review.

   The performance data appears in the **SMSMSE Performance Data** pane.