System Center Monitoring Pack for Endpoint Protection for Linux

Microsoft Corporation

Published: 10/26/2015

Send feedback or suggestions about this document to mpgfeed@microsoft.com. Please include the management pack guide name with your feedback.

The Operations Manager team encourages you to provide feedback on the monitoring pack by providing a review on the management pack's page in the Management Pack Catalog (http://go.microsoft.com/fwlink/?LinkID=82105).

Contents

SCEP Management Pack Guide

This management pack allows you to manage System Center Endpoint Protection (SCEP) from System Center 2012 Operations Manager in a networked environment, including workstations and servers – from one central location. With Operations Manager task management system, you can manage SCEP on remote computers, view alerts and health states and quickly respond to new problems and threats.

System Center 2012 Operations Manager itself does not provide any other form of protection against malicious code. System Center 2012 Operations Manager depends on the presence of an SCEP solution on computers with Linux operating system installed.

This guide was written based on version 4.5.10.1 of the Management Pack for SCEP.

Guide History

Version	Release Date	Changes
4.5.9.1	05/16/2012	Original release of this guide.
4.5.10.1	11/06/2012	New Linux distributions supported. Better description for some management pack tools.
4.5.10.1	10/15/2015	Product names naming changes. Bugfixes.

Changes in Version 4.5.10.1

Version 4.5.10.1 of the management pack for System Center Endpoint Protection includes the following changes:

- New Linux distributions supported:
  - Red Hat Enterprise Linux Server 5
  - SUSE Linux Enterprise 10
  - CentOS 5, 6
  - Debian Linux 5, 6
  - Ubuntu Linux 10.04, 12.04
  - Oracle Linux 5, 6

  Note: These new distributions will only be supported using System Center 2012 Operations Manager Service Pack 1 and above.
- Added better description for:
  - Active Malware monitor
  - Active Malware (from Rule) alert

Supported Configurations

In general, the supported configurations are outlined in Operations Manager 2007 R2 Supported Configurations (http://go.microsoft.com/fwlink/?LinkId=90676).

This management pack requires System Center 2012 Operations Manager 2007 R2 or later. The following table details the supported operating systems for this management pack:

Operating System Name	x86	x64
Red Hat Enterprise Linux Server 5, 6	Yes	Yes
SUSE Linux Enterprise 10, 11	Yes	Yes
CentOS 5, 6	Yes	Yes
Debian Linux 5, 6	Yes	Yes
Ubuntu Linux 10.04, 12.04	Yes	Yes
Oracle Linux 5, 6	Yes	Yes

Prerequisites

The following requirements must be met to run this management pack:

- System Center Operations Manager 2007 R2 Cumulative Update 5 (http://support.microsoft.com/kb/2449679)

The management packs for SCEP listed below are either integrated in System Center 2012 Operations Manager 2007 R2 or available for download from the online catalog.

ID	Name	Version
Microsoft.Linux.Library	Linux Operating System Library	6.1.7000.256
Microsoft.SystemCenter.InstanceGroup.Library	Instance Group Library	6.1.7221.0
Microsoft.SystemCenter.Library	System Center Core Library	6.1.7221.0
Microsoft.SystemCenter.WSManagement.Library	WS-Management Library	6.1.7221.0
Microsoft.SystemCenter.DataWarehouse.Library	Data Warehouse Library	6.1.7221.0
Microsoft.Unix.Library	Unix Core Library	6.1.7000.256
Microsoft.Unix.Service.Library	Unix Service Template Library	6.1.7221.0
Microsoft.Windows.Library	Windows Core Library	6.1.7221.0
System.Health.Library	Health Library	6.1.7221.0
System.Library	System Library	6.1.7221.0

Important: The monitoring of the Linux SCEP product using System Center 2012 Operations Manager must first be enabled in the configuration file */etc/opt/microsoft/scep/scep.cfg* or via the SCEP Web interface to function correctly. Please make sure that the 'scom_enabled' parameter in the aforementioned configuration file is set as follows *'scom_enabled = yes'* or change the appropriate setting in the Web interface under **Configuration** > **Global** > **Daemon options** > **SCOM enabled**.

Files in this Management Pack

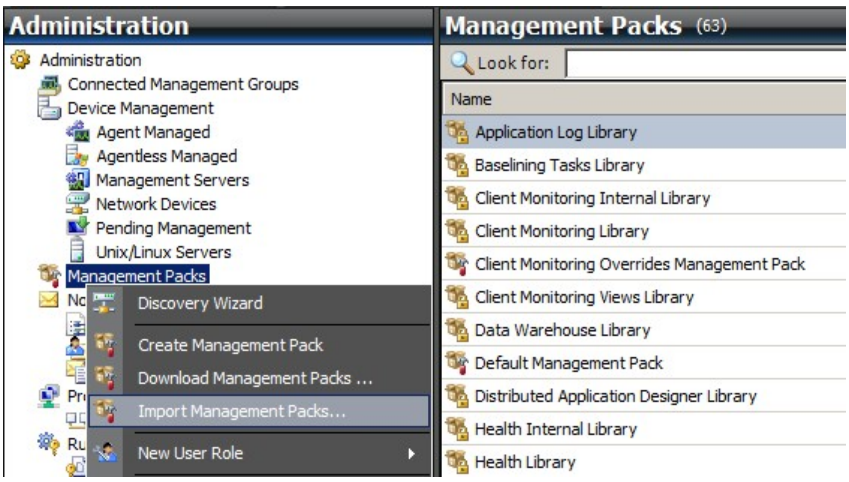
The Management Pack for SCEP includes the following files:

Filename	Description
Microsoft.SCEP.Linux.Library.mp	Contains class definitions and their mutual relationships and also monitor types and module types definitions.
Microsoft.SCEP.Linux.Application.mp	Implements monitoring and alerting, tasks and views.

Quick Start

The prerequisite to start monitoring SCEP is importing management packs into Operations Manager and identifying computers to be monitored (process referred to as "discovery").

Importing management packs

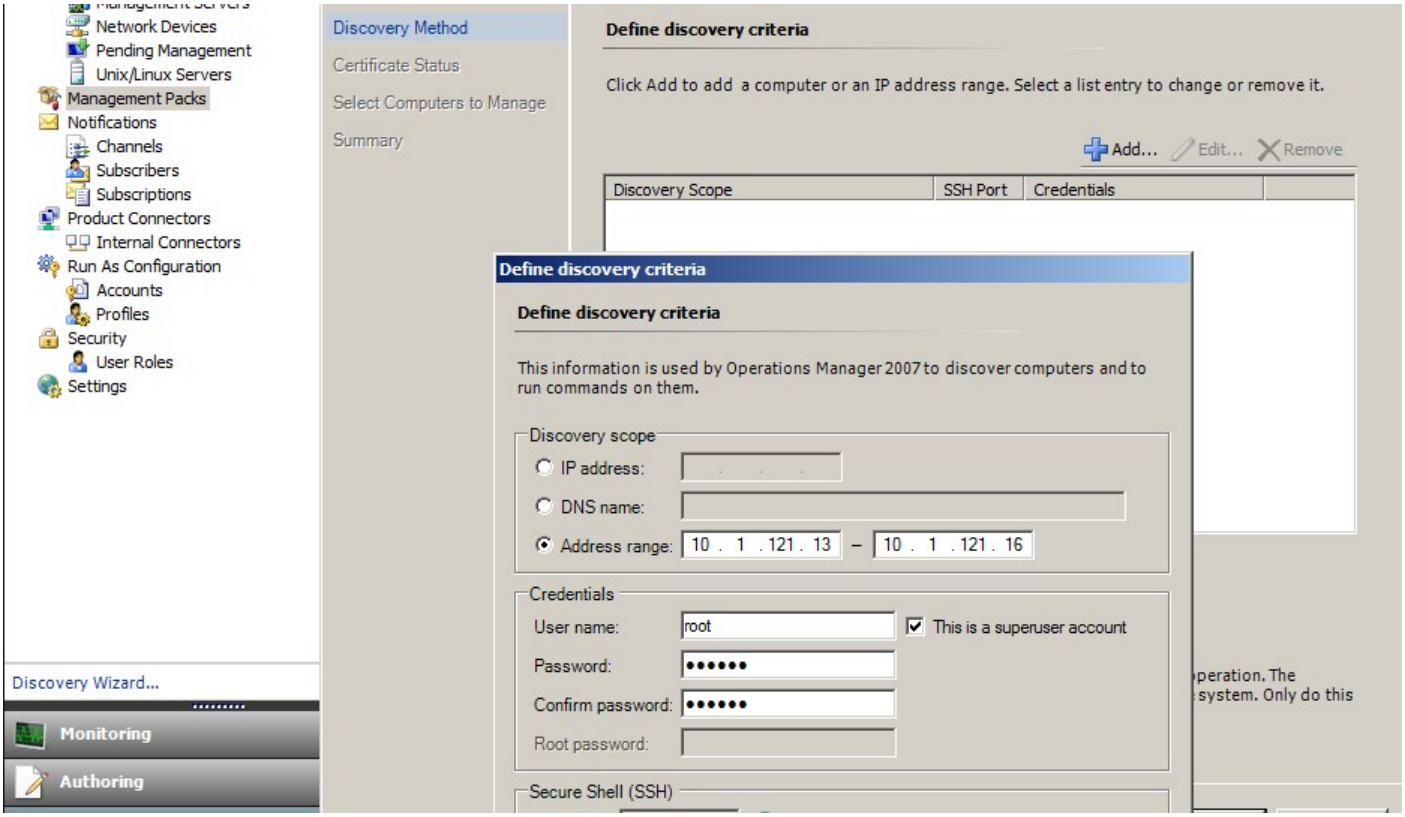


1. Click the **Administration** workspace in the left pane of the Operations Console window.
2. Right-click **Management Packs** and select **Import Management Packs...** from the context menu.
3. In the Management Packs window click the **Add** button and select **Add from disk...** from the drop-down menu.
4. Confirm, that you wish Operations Manager to search for and install also dependencies not on the local disc, by clicking **Yes** in the **Online Catalog Connection** popup window.
5. Make sure to select both listed files (Microsoft.SCEP.Linux.Application.mp, Microsoft.SCEP.Linux.Library.mp) and click **Install**.

Note: For more instructions about importing a management pack, see How to Import a Management Pack in Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkId=142351).

Discovery

After the *.mp files have been successfully imported you need to perform computer discovery.



1. In the **Administration** workspace (on the left pane of the Operations Console window) click the **Discovery wizard...** link (at the bottom of the left pane).
2. In the Computer and Device Management Wizard select the **Unix/Linux computers** option and click **Next** to continue.
3. In the Define discovery criteria section click the **Add** button.
4. Set an IP **Address range** to be scanned and SSH **Credentials** applicable to computers, to which System Center 2012 Operations Manager will install its agent.
5. Confirm your scope and credentials criteria by clicking **OK** and click the **Discover** button to start the discovery process.
6. Upon completion, a list will be displayed, allowing you to select systems for monitoring/management.

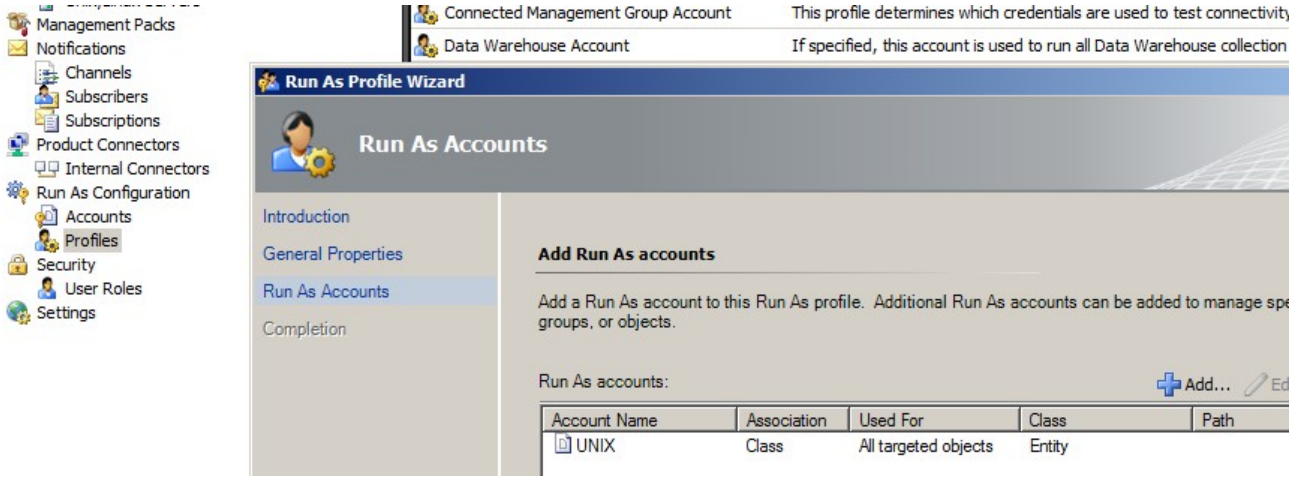
Note: Installation of a Linux Agent is supported on the following Linux Distributions. If the Linux Agent cannot be installed using Discovery, please see the manual installation instructions in the following Microsoft article Manually Installing Cross Platform Agents (http://technet.microsoft.com/en-us/library/dd789016.aspx).

Note: Discovery of Linux servers with an SCEP installation runs automatically in 8 hour intervals on all Linux Computers managed through Operations Manager (i.e. they have the appropriate Linux management pack installed for their system distribution). The discovery creates all service module entities: Protected Linux Server and nested entities or Unprotected Linux server (can be found in the appropriate sections). SCEP can be regarded as fully installed when the "scep_daemon" service is present (stopped or running). Thus the first discovery occurs when installing a management pack while the next will be realized in 8 hours, with respect to the discovery cycle. If a SCEP product is uninstalled, the respective server will be automatically moved to Unprotected (Servers without SCEP) and vice versa.

Run As Accounts configuration

To create a Unix account, please use the following instructions:

1. In the **Administration** workspace (left pane) navigate to **Run As Configuration** > **Accounts**.
2. To create a new account open the **Actions** section on the **Actions** pane (right pane) and click **Create Run As Account…**
3. In the General Properties window select **Basic Authentication** from the **Run As Account type** drop-down menu.
4. After creating an account you need to add the new account to a profile for distribution to occur. To do so, right-click the **Unix Privileged Account** profile under **Run As Configuration** > **Profiles**, select **Properties** and complete the wizard to assign the newly created account.



Note: For more information about creating a Run As Account, see the Configuring a Cross Platform Run As Account (http://go.microsoft.com/fwlink/?LinkId=160348) topic in System Center 2012 Operations Manager 2007 R2 online library.

After all the aforementioned steps are completed, the newly discovered Linux servers will shortly (in a matter of minutes) be available under **Monitoring** > **System Center Endpoint Protection Linux** > **Servers with SCEP**.

Installing a Language pack for SCEP

The format of a Language pack is as follows:
Microsoft.SCEP.Linux.Application.LNG.mp and Microsoft.SCEP.Linux.Library.LNG.mp

Use the same steps for installing the Language pack as the steps described in the **Importing Management Packs** section above. To display the installed language in System Center 2012 Operations Manager, please use the following instructions:

1. Click the Windows **Start** icon and navigate to the **Control Panel**.
2. In the Control Panel click the **Regional and Language Options**.
3. Change the system locale for non-Unicode programs in the **Administrative** tab. In the **Location** tab, change the Current location according to the installed Language pack.

Management Pack Purpose

The Management Pack for SCEP has the following functionalies:

- Real-time monitoring and alerting for security incidents and security health state.
- Enable the server administrators to perform security-related tasks remotely on their servers. These tasks' main goal is to remediate availability problems related to security.

Views

The server administrator is able to monitor, using Operations Manager console, all computers with installed SCEP. The following Views are available for "System Center Endpoint Protection Linux":

- **Active Alerts** – All SCEP Active Alerts of all severity levels. Does not include closed alerts.
- **Dashboard** – Displays both Servers with SCEP and Active Alerts workspaces.
- **Servers with SCEP** – Displays all Protected Linux Servers.
- **Servers without SCEP** – Displays all Unprotected Linux Servers.
- **Task Status** – Lists all executed Tasks.

When you monitor the state of SCEP with System Center 2012 Operations Manager management pack, you can get an instant view of SCEP health.

Rather than waiting for an alert to be raised, you can view the summary state for SCEP components at any time by clicking the

Monitoring > **System Center Endpoint Protection Linux** > **Servers with SCEP** pane of the Operations Manager Monitoring console. The state of a component is indicated in the State field with colored icons:

Icon	State	Description
	Healthy	A green icon indicates success, or it indicates that there is information available that does not require action.
	Warning	A yellow icon indicates an error or a warning.
	Critical	A red icon can indicate either a critical error or a security issue or that a service is unavailable.
	Not monitored	No icon indicates that no data affecting state has been collected.

A view can contain a lengthy list of objects. To find a specific object or group of objects, you can use the Scope, Search, and Find buttons on the Operations Manager toolbar. For more information, see the [How to Manage Monitoring Data Using Scope, Search, and Find](http://go.microsoft.com/fwlink/?LinkId=91983) (http://go.microsoft.com/fwlink/?LinkId=91983) topic.

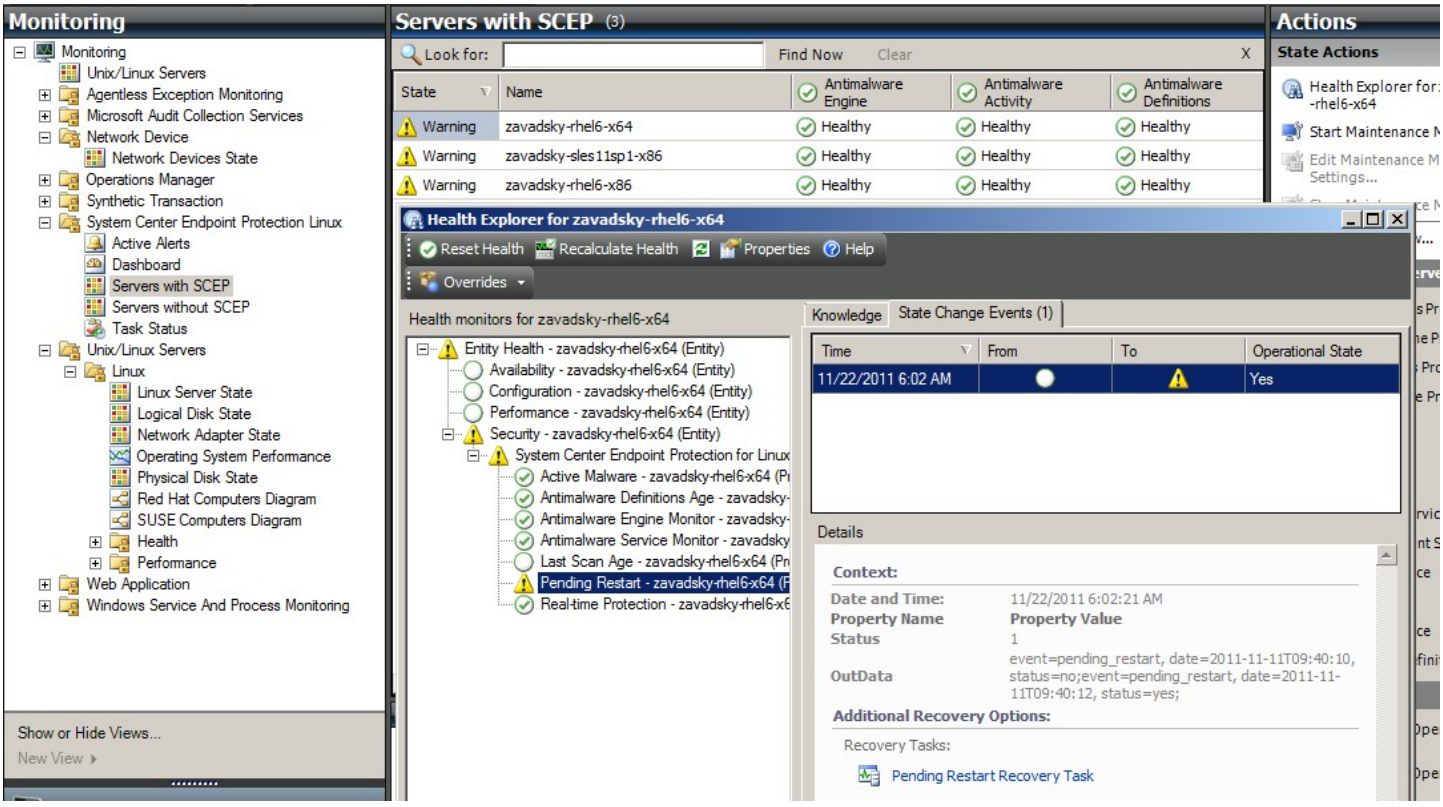
Monitors

In Operations Manager 2007, monitors can be used to assess various conditions that can occur in monitored objects.

There is a total of 17 monitors available for SCEP:

- 9 Unit monitors – The fundamental monitoring components, are used to monitor specific counters, events, scripts, and services.
- 2 Aggregate monitors – Used for an aggregate rollup to group multiple monitors into one monitor and then use that monitor to set the health state and generate an alert.
- 6 Dependency monitors – References containing status data of existing monitors.

Note: For more information about Monitors please refer to the Operations Manager 2007 R2 Help (press F1 key in System Center 2012 Operations Manager).



The SCEP Health monitors has the structure and propertiers described below.

Active Malware

Monitor type	Unit monitor
Target	Protected Linux Server
Data Source	Monitors the text log file: /var/log/scep/eventlog_scom.dat
Interval	Event driven
Alert	Yes. No auto resolve
Reset behavior	Return to the Healthy status is automatic after an 8 hour period. The alert stays active in order to retain the information about the untreated malware.

Monitor type	Unit monitor
Notes	This monitor will change state to Critical when malware was found and has not been cleaned. The state will automatically return to Healthy after 8 hours (this is because it's not possible to accurately determine whether the malware was cleaned/deleted or not). Administrator's intervention is required in order to consider the circumstances and close the ticket manually.
State	Healthy – No Malware Critical – Active Malware
Enabled	True
Recovery task	No

This monitor tracks failed malware cleanup operations. This monitor will report a Critical state if the client reports that it failed to clean the malware.

Antimalware Definitions Age

Monitor type	Unit monitor
Target	Protected Linux Server
Data Source	Command used to obtain monitoring data: /opt/microsoft/scep/sbin/scep_daemon --status
Interval	Every 8 hours
Alert	Yes. Auto resolve
State	Healthy – age <= 3 days Warning – age > 3 AND age <= 5 days Critical – age > 5 days
Enabled	True
Recovery task	Yes, manually (No auto recovery)

Up-to-date definitions help to ensure that the computer is protected against the most recent malware threats.

Antimalware Engine

Monitor type	Unit monitor
Target	Protected Linux Server
Data Source	Monitors the text log file: /var/log/scep/eventlog_scom.dat
Interval	Event driven
Alert	Yes. Auto resolve
State	Healthy – Enabled Disabled – Warning
Enabled	True
Recovery task	Yes, manually (No auto recovery)

It is recommended that the antimalware protection is enabled at all times.
Note: This monitor tracks the status of Antivirus protection which is not the same as Real-time protection. With the Antimalware engine disabled, an On-demand scan cannot be started.

Antimalware Service

Monitor type	Unit monitor
Target	Protected Linux Server
Data Source	Monitors status of the process: scep_daemon
Interval	Every 10 minutes
Alert	Yes. Auto resolve
State	Healthy – Running Critical – Not running
Enabled	True
Recovery task	Yes, manually (No auto recovery)

The monitor reports a Critical state when the antimalware service (scep_daemon) in the client machine is not running or not responsive, or when the antimalware engine is not working properly.

Last Scan Age

Monitor type	Unit monitor
Target	Protected Linux Server
Data Source	Command used to obtain monitoring data: /opt/microsoft/scep/sbin/scep_daemon --status
Interval	Every 8 hours

Alert	No
State	Healthy – age <= 7 Warning – age > 7
Enabled	True
Recovery task	Yes, manually (No auto recovery)

This monitor tracks the time since the last computer scan (regardless of the scan type). We recommend to schedule a scan to run every week.

Pending Restart

Monitor type	Unit monitor
Target	Protected Linux Server
Data Source	Monitors the text log file: /var/log/scep/eventlog_scom.dat
Interval	Event driven
Alert	Yes. Auto resolve
State	No – Healthy Yes – Warning
Enabled	True
Recovery task	Yes, manually (No auto recovery)

This monitor tracks the need to restart the system for configuration changes to take effect (typically when enabling / disabling Real-time protection). The monitor applies the following call for an on-demand update of this status: /opt/microsoft/scep/sbin/scep_daemon --status.

Real-time Protection

Monitor type	Unit monitor
Target	Protected Linux Server
Data Source	Monitors the text log file: /var/log/scep/eventlog_scom.dat The monitor can also use the following call for an on-demand status update: /opt/microsoft/scep/sbin/scep_daemon --status.
Interval	event driven
Alert	Yes. Auto resolve
State	Enabled – Healthy Disabled – Warning
Enabled	True
Recovery task	Yes, manually (no auto recovery)

Monitors the status of Real-time protection. Real-time protection alerts you when viruses, spyware, or other potentially unwanted software attempts to install itself on your computer.

System Center Endpoint Protection for Linux

Monitor type	Aggregate monitor
Target	Protected Linux Server
Condition	Worst of
Alert	No
Enabled	True
Recovery task	No

This monitor is the Health rollup (worst state) for all SCEP 7 Protected Linux Server security unit monitors. If the state is uninitialized, either monitoring has not begun for this object, or there are no security monitors defined for this object.

Antimalware Engine

Monitor type	Dependency monitor
Target	Antimalware Engine
Alert	No
Enabled	True
Recovery task	No

Displays the status of the Protected Linux Server/Antimalware Engine unit monitor in the list of monitored computers.

Antimalware Service

Monitor type	Dependency monitor
Target	Antimalware Engine
Alert	No
Enabled	True
Recovery task	No

Displays the status of the Protected Linux Server/Antimalware Service Unit monitor in the list of monitored computers.

Antimalware Definitions

Monitor type	Dependency monitor
Target	Antimalware Definitions
Alert	No
Enabled	True
Recovery task	No

Displays the status of the Protected Linux Server/Antimalware Definitions Age monitor in the list of monitored computers.

Active Malware

Monitor type	Dependency monitor
Target	Antimalware Activity
Alert	No
Enabled	True
Recovery task	No

Displays the status of the Protected Linux Server/Active Malware monitor in the Health Explorer for Antimalware Activity.

Machine Ping

Monitor type	Unit monitor
Target	Antimalware Activity
Interval	Every 60 minutes
Alert	No
State	Reachable – Healthy Unreachable – Critical
Enabled	False
Recovery task	No

Changes its status to Critical on no response from the server.

Malware Activity

Monitor type	Unit monitor
Target	Antimalware Activity
Data Source	Monitors the text log file: /var/log/scep/eventlog_scom.dat
Interval	Event driven
Alert	No
State	No Malware – Healthy Malware Activity Detected – Critical
Enabled	True
Recovery task	No

This monitor switches to Critical status within 5 minutes from malware detection (cleaned or untreated) and remains Critical for the next 60 minutes. The status Critical renews on every new positive detection and with it the length of the alert period. In other words, if no malware is detected on the system during a 60 minutes long period, the monitor returns to the Healthy status.

Server Malware Outbreak

Monitor type	Aggregate monitor
Target	Antimalware Activity
Condition	Best of
Alert	No

Enabled	True
Recovery task	No

Aggregated monitors: Malware Activity, Machine Ping.
Changes its status to Critical if there is no response from the server within 60 minutes from a positive malware detection (cleaned or untreated). The change of status to Critical can be also triggered, if, after a period of receiving no response from the server, malware is detected shortly after connection renewal.

Malware Outbreak

Monitor type	Dependency monitor
Target	Protected Servers Watcher
Condition	Worst of 95%
Alert	No
Enabled	True
Recovery task	No

Displays the status of the Antimalware Activity/Server Malware Outbreak monitor.
If more than 5% of all Linux Computers (Protected and Unprotected) register a malware detection in the past 60 minutes, this monitor changes to the Critical status.

SCEP Linux Computer Role Health Rollup

Monitor type	Dependency monitor
Target	Linux Computer
Alert	No
Enabled	True
Recovery task	No

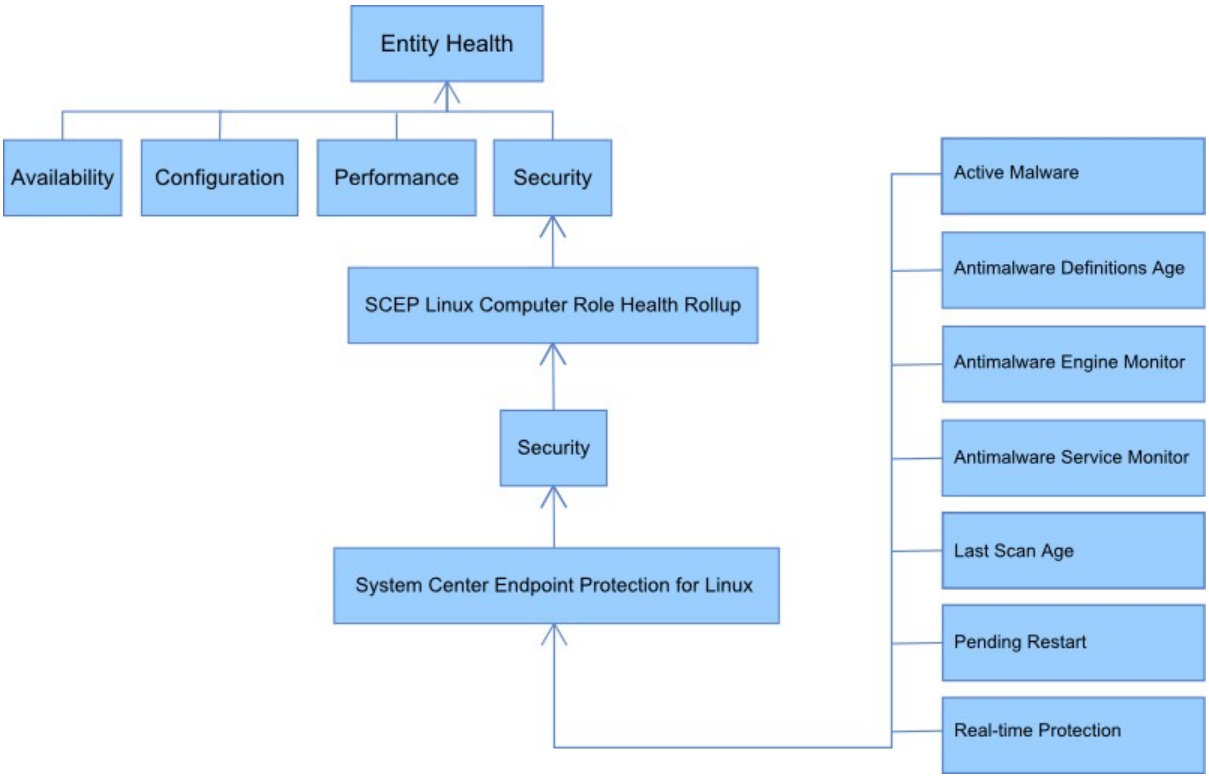
Propagates the Protected Linux Computer entity status to the Linux Computer/Security parent monitor.

How Health Rolls Up

This management pack expands the Linux operating system monitoring as a layered structure, where each layer depends on the lower layer to be healthy. The top of this structure is the entire Entity Health environment, and the lowest level of Security environments is all of the monitors. When one of layer changes state, the layer above it changes state to match. This action is called rolling up health.

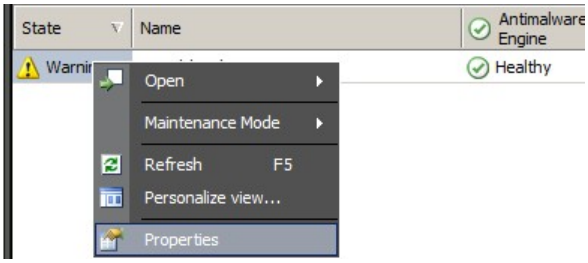
For example if the Real-time protection returns the Warning status and all of the other components are Healthy, the Warning status will be transferred via the tree structure to the root (Entity Health), which will too acquire the Warning status.

The following diagram shows how the health states of objects roll up in this management pack.



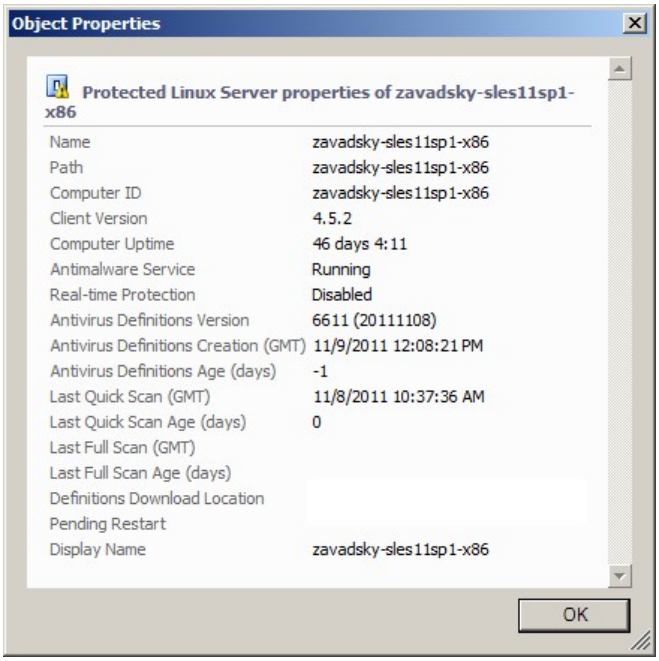
Object Properties

To view the properties of an object, right-click the object and select **Properties**.



Protected Linux Server object has the following propertiers:

- **Computer ID** – Server identifier, domain name.
- **Display Name** – Server name, domain name.
- **Client Version** – Version of the installed SCEP product.
- **Computer Uptime** – Server uptime (measure of the time a machine has been up without any downtime) is not data vital for proper operation of a management pack, its absence may therefore indicate an error in the management pack.
- **Antimalware Service** – Antimalware protection status (Running/Not running).
- **Real-time Protection** – Real-time protection status, its absence signals SCEP issues.
- **Antivirus Definitions...** – Virus database status data (version, date of creation, age), data absence signals SCEP issues.
- **Last Quick/Full Scan...** – Data about last computer scan. If the scan (Quick Scan/Full Scan) has not been performed yet, no data will appear.
- **Definitions Download Location** – Update server address/name. The information displays after the first successful update.
- **Pending Restart** – Information about the need to restart to apply changes, due to a new installation or changes in SCEP configuration.



Alerts

An alert is an item that indicates that a predefined situation with a specific severity (seriousness) has occurred on a monitored object. Alerts are defined by rules. A view in the Operations Manager console is available in **Monitoring** > **System Center Endpoint Protection Linux** > **Active Alerts** that displays the alerts that the console user has the rights to see for a specific object.

Note: If more alerts of the same type are generated repeatedly (e.g. Active Malware) from the same server, only the first one is displayed (redundant alerts are ignored).

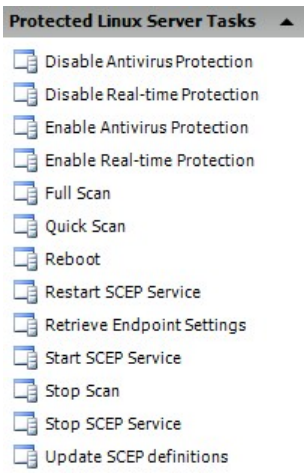
Alert	Interval	Priority	Severity	Description
Repeated Malware Infection	Event driven	High	Critical	Alert is generated in case of repeated malware detections (3 occurrences) in a given time interval (30 minutes). The alert contains data about the server and basic information about the malware.
Malware Cleaned	Event driven	Low Medium	Information – Malware cleaned successfully Warning – User interaction required, e.g. server restart	Alerts about a malware successfully cleaned. Contains all available data about the specific malware. Each malware detected generates an individual event. SCEP Linux assigns priority and severity based on the efficiency of the cleaning process where: Cleaned = Low + Information Cleaned but action (e.g. restart) required = Medium + Warning.
Active Malware (from Monitor)	Event driven	High	Critical	Alerts about malware that has not been cleaned. Contains all available data about the specific malware.
Active Malware (from Rule)	Event driven	High/Medium/ Low	Critical/Medium/Low – based on a type of Malware	The same as above. Used for connectors to other monitoring/ ticketing systems. **Note:** This rule (alert) is disabled by default.
System Center Endpoint Protection anti-malware service is down	300 seconds	Medium	Critical	Alerts about unavailability of the Antimalware service SCEP (scep_daemon). Includes the respective server name and the SCEP version.
Antimalware Protection Disabled	Event driven	Medium	Warning	Alerts about the Antimalware protection being disabled. Includes the respective server name.

Real-time Protection Disabled	Event driven	Medium	Warning	Alerts about the Real-time protection being disabled. Includes the respective server name.
Definitions Out of Date	Each 8 hours	Medium	Warning (age <= 5 days AND age > 3 days) Critical (age > 5 days)	Alerts about the virus signature database not being updated for more than 3 days. Includes the respective server name and the age of the virus signature database.
Malware Outbreak	Event driven	High	Critical	Forefront Endpoint Protection detected more than 5% active malware on your computers. It is possible that there is malware propagating on your computers. It is suggested that you will ensure that all servers use the most up-to-date definitions. If you need to change the number of active threats that cause this alert, override the parameter of the Malware Outbreak monitor (see Overrides chapter).

Tasks

Management Pack for SCEP implements 13 taks. The execution of these tasks is immediate. Outputs display immediately after task execution, or they can be viewed later from the Tasks Status window. Maximum time required for task execution is 180 seconds. Override is not available. All tasks are BASH commands executed via SSH.

Tasks can be invoked under **Monitoring** > **System Center Endpoint Protection Linux** > **Servers with SCEP** in the right pane of the Operations Console window.



- **Disable Antivirus Protection** – Disables all components of antivirus protection, disables On-demand scan.
- **Enable Antivirus Protection** – Enables all components of antivirus protection.
- **Disable Real-time Protection** – Disables Real-time protection.
- **Enable Real-time Protection** – Enables Real-time protection.
- **Full Scan** – Updates virus signature database and runs a full computer scan.
- **Quick Scan** – Updates virus signature database and runs a quick computer scan.
- **Stop Scan** – Stops all running computer scans.
- **Retrieve Server Settings** – Displays current SCEP product status, the list of displayed parameters is identical with the properties of the Protected Linux Server entity. Displayed data is not transferred to Protected Linux Server.
- **Restart Antimalware Service** – Restarts the SCEP Antimalware service (scep_daemon).
- **Stop Antimalware Service** – Stops the SCEP Antimalware service (scep_daemon).
- **Start Antimalware Service** – Starts the SCEP Antimalware service (scep_daemon).
- **Update Antimalware Definitions** – Starts the virus signatures database update.
- **Reboot** – Restarts the Linux computer.

Configuring the Management Pack for SCEP

Best Practice: Create a Management Pack for Customizations

By default, Operations Manager saves all customizations such as overrides to the Default Management Pack. As a best practice, you should instead create a separate management pack for each sealed management pack you want to customize.

When you create a management pack for the purpose of storing customized settings for a sealed management pack, it is helpful to base the name of the new management pack on the name of the management pack that it is customizing, such as "SCEP 2012 Customizations".

Creating a new management pack for storing customizations of each sealed management pack makes it easier to export the customizations from a test environment to a production environment. It also makes it easier to delete a management pack, because you must delete any dependencies before you can delete a management pack. If customizations for all management packs are saved in the Default Management Pack and you need to delete a single management pack, you must first delete the Default Management Pack, which also deletes customizations to other management packs.

Security Configuration

The computer must run the SSHD service and the SSH port (default value 22) must be open. System Center 2012 Operations Manager connects via the port to remote Linux computers using the appropriate Run As Account (located in **Administration** > **Run As Configuration** pane of the Operations Manager Monitoring console) with **Basic Authentication** type.

Run As Profile Name	Notes
Unix Privileged Account	Used to remotely monitor the Unix server, as well as to restart processes where privileged rights are required.

This management pack doesn't use the Unix Action Account.

Warning: Monitoring of computers using the root account presents a potential security risk, e.g. if the password has been broken.

If you don't wish to use the root account for monitoring and managing, you can use a standard user account, but this account needs to have rights to execute *sudo* commands. Therefore, the following configuration must be present in the /etc/sudoers file on each Linux SCEP monitored workstation in order to authorize sudo elevation for selected user account. This is an example configuration for the username user1:

```
#--------------------------------------------------------------------------------
# User configuration for SCEP monitoring - for a user with the name: user1

user1  ALL=(root)    NOPASSWD:     /opt/microsoft/scx/bin/scxlogfilereader -p
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /sbin/reboot
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep restart
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep start
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep stop
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C;if \[ -e /opt/microsoft/scep/sbin/
scep_daemon \] ; then echo scep_daemon installed; else echo scep_daemon unprotected; fi; kill -0
`cat /var/run/scep_daemon.pid 2>/dev/null` 2>/dev/null; if \[ $\? -eq 0 \] ; then echo scep_daemon
running; else echo scep_daemon stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/sbin/scep_daemon *
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/lib/scep_sci --scom *
user1  ALL=(root)    NOPASSWD:     /bin/sh -c pkill scep_sci
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C; kill -0 `cat /var/run/scep_daemon.pid 2>/
dev/null` 2>/dev/null; if \[ $? -eq 0 \] ; then echo scep_daemon running; else echo scep_daemon
stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime

# End user configuration for SCEP monitoring
#--------------------------------------------------------------------------------
```

Tuning Performance Threshold Rules

The following table lists performance threshold rules that have default thresholds that might require additional tuning to suit your environment. Evaluate these rules to determine whether the default thresholds are appropriate for your environment. If a default threshold is not appropriate for your environment, you might adjust the thresholds by applying an override to them.

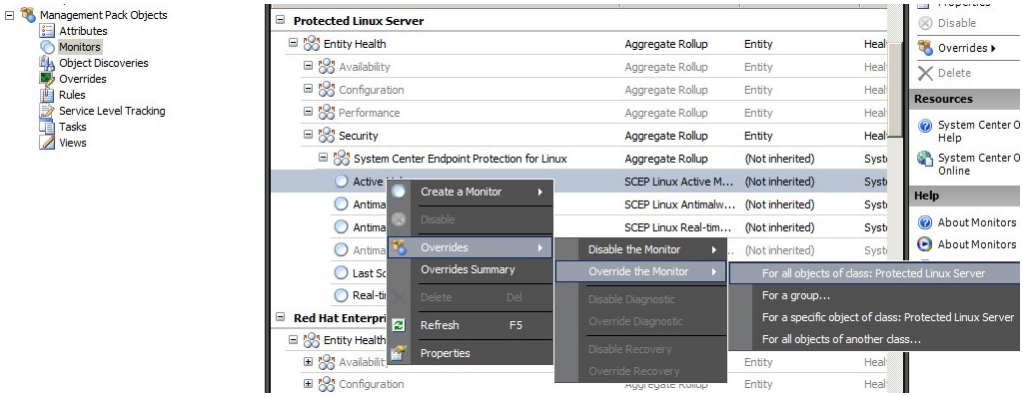
Rule Name	Override Parameter	Default Threshold	Tuning Limitations
Repeated Malware Infection Rule	Repeated Infection Count Threshold	3 occurrences	Setting a value less than 2 makes the rule obsolete.

Repeated Malware Infection Rule	Repeated Infection Time Window	30 minutes	We do not recommend setting the value to less than is the duration of an On-demand scan, since an overlap may prevent generating an alert.
Active Malware Alert Rule	Enabled	False	If you use connectors to other monitoring/ticketing systems, you can enable this alert.

Overrides

Overrides can be used to refine the settings of a monitoring object in System Center 2012 Operations Manager. This includes monitors, rules, object discoveries, and attributes that are from imported management packs.

To override a monitor, in the Operations Console click the **Authoring** button and expand **Management Pack Objects** > **Monitors**. In the Monitors pane, find and expand an object type completely and then click a monitor and then click **Overrides**.



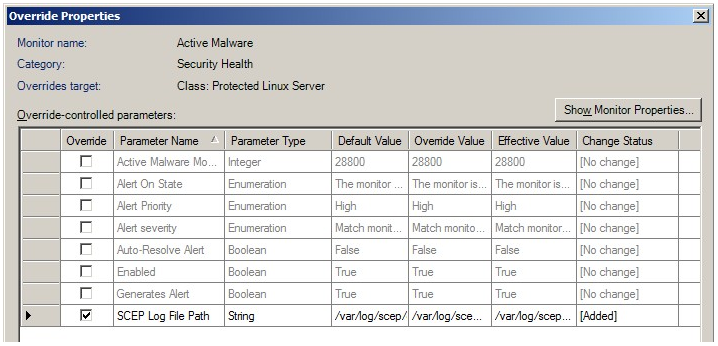
Use the Overrides window to create or modify an override for an occurrence of any of the following parameters:

- **Active Malware Monitor Fallback Time** (related only to Active Malware monitor)
- **Antimalware Definitions Age** (related only to Antimalware Definitions Age monitor)
- **Detection Interval** (related only to Last Scan Age monitor)
- **Alert On State**
- **Alert Priority**
- **Alert Severity**
- **Auto-Resolve Alert**
- **Enabled** – Determine whether the selected monitor is enabled or disabled.
- **Generates Alert**
- **SCEP Log File Path**

If a default override is not appropriate for your environment, you might adjust the thresholds by applying an override to them:

Override Parameter	Monitor Name	Default Value	Tuning Notes
Ping Interval	Machine Ping	3600 seconds	An interval to check the availability of the Protected Linux Server. Shorter duration triggers an Error status on the Server Malware Outbreak monitor faster, in case the machine stops responding due to an attack. Consequently the load on the network, monitored computer and System Center 2012 Operations Manager server increases.
Malware Outbreak Time Window	Malware Activity	3600 seconds	An interval required for the monitor to return back to the Healthy status after a malware activity. The Time Window monitor value should be higher than the Machine Ping/Ping Interval for the combination to work properly. If during the Malware Outbreak Time Window interval an amount of computers in excess of the set Malware Outbreak percentage value (see Malware Outbreak) registers malware activity, a Malware Outbreak alert is generated. Note: This is different from Server Malware Outbreak, which does not generate an alert.
Active Malware Monitor Fallback Time	Active Malware	28800 seconds	Time interval since malware detection, after which the malware is considered cleaned.

SCEP Log File Path	Active Malware	/var/log/scep/ eventlog_scom.log	Path to the file where System Center 2012 Operations Manager events are recorded. Do not change this parameter unless issues arise.
Antimalware Definitions Critical Age	Antimalware Definitions Age	5 days	After this interval an Error alert notifying about an out-of-date SCEP product is generated.
Antimalware Definitions Healty Age	Antimalware Definitions Age	3 days	Maximal allowed age of antimalware definitions, during which they can be considered up-to-date. This value should always be lower than the Antimalware Definitions Critical Age value.
Interval	Antimalware Definitions Age	28800 seconds	Interval for checking the age of antimalware definitions.
Interval	Antimalware Service	300 seconds	Interval for checking the availability of the Antimalware service.
Process Name	Antimalware Service	scep_daemon	The name of the antimalware service. Do not change this value if the monitor is operational.
Detection interval	Last Scan Age	28800 seconds	Interval for checking the last scan execution.
Maximum scan age	Last Scan Age	7 days	To be setup in accordance with the SCEP product settings. If a scan is scheduled every 7 days, set this value to 7 days.
Log File Path	Pending Restart	/var/log/scep/ eventlog_scom.log	Path to the file where System Center 2012 Operations Manager events are recorded. Do not change this parameter unless issues arise.
SCEP Log File Path	Real-time protection	/var/log/scep/ eventlog_scom.log	Path to the file where System Center 2012 Operations Manager events are recorded. Do not change this parameter unless issues arise.
Percentage	Malware Outbreak	95%	Percentage of servers from Linux Servers (Protected + Unprotected) required to return the status Healthy, for the whole monitored group to be considered Healthy. If malware is detected on 5% or more of the total, a Malware Outbreak will be generated.



Note: For more information about Overrides, see [How to Monitor Using Overrides](http://go.microsoft.com/fwlink/?LinkID=117777) (http://go.microsoft.com/fwlink/?LinkID=117777).

Links

The following links connect you to information about common tasks that are associated with this management pack:

- Administering the Management Pack Life Cycle
  (http://go.microsoft.com/fwlink/?LinkId=211463)
- How to Import a Management Pack in Operations Manager 2007
  (http://go.microsoft.com/fwlink/?LinkID=142351)
- How to Monitor Using Overrides
  (http://go.microsoft.com/fwlink/?LinkID=117777)
- How to Create a Run As Account in Operations Manager 2007
  (http://go.microsoft.com/fwlink/?LinkID=165410)
- Configuring a Cross Platform Run As Account
  (http://go.microsoft.com/fwlink/?LinkId=160348)
- How to Modify an Existing Run As Profile
  (http://go.microsoft.com/fwlink/?LinkID=165412)
- How to Export Management Pack Customizations
  (http://go.microsoft.com/fwlink/?LinkId=209940)
- How to Remove a Management Pack
  (http://go.microsoft.com/fwlink/?LinkId=209941)
- How to Manage Monitoring Data Using Scope, Search, and Find
  (http://go.microsoft.com/fwlink/?LinkId=91983)
- Monitoring Linux Using SCOM 2007 R2
  (http://blogs.technet.com/b/birojitn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx)
- Manually Installing Cross Platform Agents
  (http://technet.microsoft.com/en-us/library/dd789016.aspx)
- Configuring sudo Elevation for UNIX and Linux Monitoring with System Center 2012 – Operations Manager
  (http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx)

For questions about Operations Manager and monitoring packs, see the System Center Operations Manager community forum (http://go.microsoft.com/fwlink/?LinkID=179635).
A useful resource is the System Center Operations Manager Unleashed blog (http://opsmgrunleashed.wordpress.com/), which contains "By Example" posts for specific monitoring packs.

For additional information about Operations Manager, see the following blogs:

- Operations Manager Team Blog
  (http://blogs.technet.com/momteam/default.aspx)
- Kevin Holman's OpsMgr Blog
  (http://blogs.technet.com/kevinholman/default.aspx)
- Thoughts on OpsMgr
  (http://thoughtsonopsmgr.blogspot.com/)
- Raphael Burri’s blog
  (http://rburri.wordpress.com/)
- BWren's Management Space
  (http://blogs.technet.com/brianwren/default.aspx)
- The System Center Operations Manager Support Team Blog
  (http://blogs.technet.com/operationsmgr/)
- Ops Mgr ++
  (http://blogs.msdn.com/boris_yanushpolsky/default.aspx)
- Notes on System Center Operations Manager
  (http://blogs.msdn.com/mariussutara/default.aspx)

For troubleshooting visit the following Forum threads:

- Microsoft.Unix.Library is missing
  (http://social.technet.microsoft.com/Forums/en-US/operationsmanagermgmtpacks/thread/8469d0ff-54d6-4cb4-9909-49ab62126b74/)