Symantec™ Enterprise Security Manager Modules for ESX and ESXi server Release Notes

Release 2.0 for Symantec ESM 9.0.x and 10.0 For ESX, ESXi, and vCenter servers

Symantec

Symantec™ Enterprise Security Manager Modules for ESX and ESXi server Release Notes

Documentation version: 2.0

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 Web site 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 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

What's new

This document includes the following topics:

What's new

This release includes the following features and enhancements:

- New esxsetup utility
- New platform support
- Two new checks in the ESX Configurations module
- One new check in the ESX Network module
- One new check in the ESX Patches module
- Six new checks in the ESX System module
- One new check in the ESX Patches module
- One new message in the ESX Patches module

- Three new messages in the ESX System module
- One new template in the ESX Configurations module
- One new template in the ESX Patches module

New esxsetup utility

You can now configure the ESX ESM modules with ESX/ ESXi 3.5 or later versions and vCenter server 4.0.x by using the esxsetup utility. The utility is present at the following location:

<install directory>/bin/lnx_x86

The configuration utility lets you create and manage the configuration records of the ESX, ESXi, and the vCenter servers in your enterprise. You can run the utility on your ESX agent computers or on the Red Hat Enterprise Linux agent computers, where the ESM modules for ESX are installed.

Note: For more information on the esxsetup utility, see the*Symantec™ Enterprise Security Manager Modules for ESX and ESXi server User Guide*.

New support

This release supports the following platforms:

- ESX 4.0 and 4.1
- ESXi 3.5, 4.0, and 4.1
- vCenter 4.0.x
- Red Hat Enterprise Linux ES (5.1, 5.2, 5.3, 5.4) (32-bit and 64-bit) x86, x64

New checks

Table 1-1 gives a list of the new checks that are added to the ESX modules.

Table 1-1 Module name, check name, and description

Module name	Check name	Check description
ESX Configurations	Host config option parameters	This check reports the unauthorized values for the configuration parameters that you specify in the enabled ESX/ESXi Host Configuration Parameters templates. See "New templates" on page 11.
	NX/XD flag exposed to guest	This check verifies if the NX flag is exposed to the guest OS.
ESX Network	SNMP traps setting	If you specify zero in the **SNMP service disabled/enabled** text box, then the check verifies whether the SNMP is disabled. If you specify a value, which is greater than zero, then the check verifies that if SNMP is in use, then either at least one trap destination must be configured or the trap destinations are acceptable, or both.
ESX Patches	ESXi updates	This check verifies if the ESXi host system is patched with the latest patch updates. See "New templates" on page 11.

Table 1-1 Module name, check name, and description *(continued)*

Module name	Check name	Check description
ESX System	Local accounts only	This check works only with the **Shell access** check. This check filters the NIS and the LDAP users that are reported by the **Shell access** check when run on the host-based mode.
	Grub OS level password	This check verifies if the **GRUB boot loader password** is enabled on the host system for the individual operating systems that are present in the **GRUB boot** menu.
	Lockdown mode	This check verifies if lockdown mode is enabled for an ESXi host system.
	Maintenance mode	This check verifies if maintenance mode is disabled.
	List users and groups	This check reports all the local users and groups that are present on the host.
	Execute on vCenter	Enable this check to execute the supported checks on the vCenter server.

Note: For more information on the checks, see the*Symantec™ Enterprise Security Manager Modules for ESX and ESXi server User Guide.*

New messages

New messages are added to the following checks:

- Roles and Privileges (ESX System module)
- Superseded (ESX Patches module)

Roles and Privileges (ESX System module)

Three new messages are added to the Roles and privileges check in the ESX System module. The check reports these messages when it finds a user or a group that has been assigned a role or when the reported role is a user-defined role.

Table 1-2 lists the new messages.

Table 1-2 New messages for the Roles and privileges check

Message ID	Message Title	Message Severity
STKU_USERWITHROLE	Role assigned to user	Green (0)
STKU_GROUPWITHROLE	Role assigned to group	Green (0)
STKU_USERDEFINEDROLE	User defined role	Green (0)

Superseded (ESX Patches module)

One new message is added to the Superseded check in the ESX Patches module. The check reports this message if a particular patch and its superseding patches are not installed on the host system.

Table 1-3 lists the new message.

Table 1-3 New message for the Superseded check

Message ID	Message Title	Message Severity
ESM_SS_PATCH_NOT_INSTALLED	Superseded patch is not installed	Yellow (2)

New templates

Following new templates are added in this release:

- ESX Configuration Parameters template in the ESX Configurations module
- ESXi Patch template in the ESX Patches module

ESX Configuration Parameters template (ESX Configurations)

In the ESX Configurations module, the **Host config option parameters** check uses the ESX Configuration Parameters template. The check reports the unauthorized configuration parameter values that you specify in the template.

Creating the ESX Configuration Parameters template

You must create and enable a new ESX Configuration Parameters template before you run the **Host config option parameters** check.

To create an ESX Configuration Parameters template

1. In the tree view, right-click **Templates**, and then click **New**.
2. In the **Create New Template** dialog box, select **ESX Configuration Parameters-all**.
3. In the **Template file name (no extension)** text box, type new template file name.
4. After Symantec ESM adds the .cox extension to the template file name, click **OK**.

About using the ESX Configuration Parameters template

The ESX Configuration Parameters template contains the following fields:

Parameter Name	Specify the name of the host configuration parameter. You can refer to the default template that is provided with the check to see the default list of parameters and their default values.
Comment	Specify an additional comment.
Severity Level	Specify the severity for the messages that ESM reports when the parameter value is violated. ■ Green (Information message) ■ Yellow (Warning message) ■ Red (Error message)
Required	Specify whether you want ESM to report the unauthorized configuration parameters that are **Mandatory** or **Optional** in the sublist. The default value is Optional. When you specify the parameter as **Mandatory**, then ESM reports a message if the parameter is not found on the host. When you specify the parameter as **Optional**, then ESM do not report any message if the parameter is not found on the host. Irrespective of the type you chose, ESM reports if the parameter is found on the host, but if the values do not match with the values that you specify in the template.

ESX/ESXi Rev

ESM displays the **Template Sublist Editor** window when you click the **ESX/ESXi Rev** field. The window lists the following fields:

- Exclude
  Check the **Exclude** check box to exclude the specified operating system and revision for the security checks that use the ESX Configuration Parameters template.
- OS
  Specify the operating system that you want to include.
- Release/Revision
  Specify a revision ID for the operating system that you have selected.

If you leave this sublist empty, then the check reports on all the versions of ESX and ESXi.

In case of multiple entries, if an entry is marked as Exclude, the check does not report on the versions that are represented by the entry. This is true even if other entries representing the same version are not marked as Exclude. In short, the entry that is marked as **Exclude** takes precedence over the other entries.

For example,

- If you enter 3 as an allowed entry and 3.5 as an excluded entry, then the check reports all the ESX 3.x.x versions as a match except for 3.5.x entries, which is excluded.
- If you enter a value that starts with a plus sign (+) like +3, then the check reports on all the versions equal and later to 3. For example, 3.0.2, 3.5, or 4.0, and so on.

Parameter Values

ESM displays the **Template Sublist Editor** window when you click the **Parameter Values** field. The window lists the following fields:

- Prohibited
  Select the check box if the parameter value that you have entered is prohibited.
- Value
  Specify the value for the parameter that is expressed as a regular expression or numeric comparison. The value of a regular expression must precede by a ^ and must end with a $. For example, if the value is 32, you must enter ^32$.
  You can use the following numeric comparisons:
  - = (equal to)
  - < (less than)
  - > (greater than)
  - != (not equal to)
  - <= (less than or equal to)
  - >= (greater than or equal to)

See "New checks" on page 8.

ESXi Patch template (ESX Patches)

In the ESX Patch module, the **ESXi updates** check uses the ESXi Patch template. The check helps you verify if the ESXi host system has the latest patch updates.

Creating the ESXi Patch template

You must create and enable a new ESXi Patch template before you run the **ESXi updates** check.

1. In the tree view, right-click **Templates**, and then click **New**.
2. In the **Create New Template** dialog box, select **ESX Patch- all**.
3. In the **Template file name (no extension)** text box, type new template file name.
4. After Symantec ESM adds the .ilx extension to the template file name, click **OK**.

About using the ESXi Patch template

The ESXi Patch template contains the following fields:

Revision

Specify the ESXi version number.

Component	Specify the component of the ESXi server that has the latest patch updates. Tools, firmware, and viclient are the default components.
Build	Specify the build number.
Description	Specify a description. For example, ESX-CLIENT-119801
Date	Specify the build date.
Type	Specify whether you want ESM to report the patches that are **Mandatory** or **Optional** in the sublist. The default value is Mandatory. When you specify the parameter as **Mandatory**, then ESM reports a message if the parameter is not found on the host. When you specify the parameter as **Optional**, then ESM do not report any message if the parameter is not found on the host. Irrespective of the type you chose, ESM reports if the parameter is found on the host, but if the values do not match with the values that you specify in the template.

See "New checks" on page 8.

Known issue

The following issue is known in this release:

ESX Patches module	If run against an ESXi 4.0.0 server, the check **ESXi updates** might report an error message, **Failed to retrieve ESXi patches from the server**. **Note:** This is an ESXi server error.

Enhancement

The following module has been enhanced in this release:

ESX Configurations	Five checks are modified to report a different message if they do not find any of their respective properties configured. Earlier, if you have applied any suppressions in the Information field, then the suppressed messages will reappear with the changed information. The five checks are as follows: ■ Copy disabled ■ Paste disabled ■ Setinfo messages disabled ■ VMware Tools logging ■ Set GUI Options disabled For more information on their respective properties, see *Symantec™ Enterprise Security Manager Modules for ESX and ESXi server User Guide*.