

Symantec Enterprise Security Manager™ Modules for ESX Server User's Guide

Release 1.0 for Symantec ESM 6.0, 6.1, and 6.5.x

For ESX Server 3.0.x



Symantec ESM Modules for ESX Server User's Guide

Release 1.0

Legal Notice

Copyright ©2008 Symantec Corporation.

All Rights Reserved.

Symantec, the Symantec Logo, LiveUpdate, Symantec Enterprise Security Architecture, Enterprise Security Manager, and NetRecon 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.

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, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. 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.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

<http://www.symantec.com>

Third Party Legal Notices

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 Code of Use Documentation accompanying this Symantec product for more information on the Third Party Programs.

Privacy; Data Protection:

Symantec may collect and store certain non-personally identifiable information for product administration and analysis. Symantec may disclose the collected information if asked to do so by a law enforcement official as required or permitted by law or in response to a subpoena or other legal process. In order to promote awareness, detection and prevention of Internet security risks, Symantec may share certain information with research organizations and other security software vendors. Symantec may also use statistics derived from the information to track and publish reports on security risk trends. By using the Licensed Software, You acknowledge and agree that Symantec may collect, transmit, store, disclose and analyze such information for these purposes. From time to time, the Licensed Software will collect certain information from the computer on which it is installed, which may include: (a) Information regarding installation of the WebClient Installer including username and password which should not be personally identifiable if You have chosen an alias to protect Your identity. (b) Information collected by the WebClient Profile such as mandatory user/employee information including, name, e-mail address, title, position, physical address and use ID/employee ID as well as IP address and username. (c) Other information including username, user events and IP addresses which is used for product administration and analysis. All of the above information is collected and stored on the Your side and is not transferred to Symantec. Consult Your company's privacy policy for further information.

Technical support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product feature and function, installation, and configuration. The Technical Support group also authors 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 technical 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
- A telephone and web-based support that provides rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support that is available 24 hours a day, 7 days a week worldwide. Support is provided in a variety of languages for those customers that are enrolled in the Platinum Support program
- Advanced features, including Technical Account Management

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Select your country or language under Global Support. The specific features that are available may vary based on the level of maintenance that was purchased and the specific product that you are using.

Contacting Technical Support

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

www.symantec.com/techsupp/

Select your region or language under Global 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 recreate the problem.

When contacting the Technical Support group, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
 - Error messages/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/techsupp/

Select your region or language under Global Support, and then select the Licensing and Registration page.

Customer Service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Select your country or language under Global Support.

Customer Service is available to assist with 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 insurance and maintenance contracts
- Information about Symantec Value License Program
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

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

- Asia-Pacific and Japan: contractsadmin@symantec.com
- Europe, Middle-East, and Africa: semea@symantec.com
- North America and Latin America: supportsolutions@symantec.com

Additional Enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively. Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring and management capabilities, each focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

<http://www.symantec.com>

Select your country or language from the site index.

Contents

Chapter 1	Introducing Symantec ESM Modules for ESX Server 3.0.x	
	About the Symantec ESM Modules for ESX Server 3.0.x	9
	Where you can get more information	10
	Templates	10
	Modules	10
Chapter 2	Installing Symantec ESM Modules for ESX Server 3.0.x	
	Before you install	13
	Minimum account privileges	14
	System requirements	14
	Disk space requirements	14
	Installing the ESM Modules for ESX Server 3.0.x	14
	Installation log	15
	Installing the ESM modules for ESX Server 3.0.x silently	21
Chapter 3	ESM Modules for ESX Server 3.0.x	
	ESX Configurations	23
	Guest installed	23
	Guest status	24
	Copy disabled	24
	Paste disabled	24
	Setinfo messages disabled	24
	Guest time synchronization	25
	Guest connection control	25
	Host time synchronization	25
	Guest logging	25
	VMware Tools logging	26
	Guest log rotate size	26
	Guest old log keeping	26
	Set GUI Options disabled	26
	ESX Network	27
	iSCSI enabled	27
	iSCSI CHAP authentication	27
	MAC address changes	27
	Forged transmission	28

Promiscuous mode	28
Service console firewall	28
Port groups in VLAN	28
ESX Patches	29
Patch templates	29
Superseded	30
Disable patch module	30
Patch results summary	30
Installed Patches	31
ESX System	31
Boot loader password	31
Root file system fill up	32
Shell access	32
Roles and privileges	32
SU PAM Authentication	32
ESX log auditing	33

Introducing Symantec ESM Modules for ESX Server 3.0.x

This chapter includes the following topics:

- [About the Symantec ESM Modules for ESX Server 3.0.x](#)
- [Templates](#)
- [Modules](#)

About the Symantec ESM Modules for ESX Server 3.0.x

The Symantec Enterprise Security Manager (ESM) modules for ESX Server provides protection to your ESX Servers.

The Symantec ESM modules for ESX Server contains four modules that are specific to ESX Server 3.0.x. The ESM modules for ESX Server protect your ESX 3.0.x servers from known security vulnerabilities.

The ESM Modules for ESX Server is a host-based application. The modules have to be installed on the ESX servers.

You can use the Symantec ESM Modules for ESX Server in the same way that you use other Symantec ESM Modules.

Where you can get more information

For more information about Symantec ESM Modules and Security Updates, see the latest versions of the following documents:

- Symantec Enterprise Security Administrator's Guide
- Symantec ESM Security Update User's Guide

You can find the following information from the Symantec Security Response Web site:

- Symantec Enterprise Security Manager (ESM)
- Symantec ESM Security Updates
- Symantec ESM support for database products

The address of Symantec Security Response Web site is as follows:

<http://securityresponse.symantec.com>

Templates

Templates store the predefined object settings. Modules use templates to report vulnerabilities based to the predefined object settings. When you run the modules, the differences between current object settings of the computer and the template values are reported.

[Table 1-1](#) shows the modules and checks that use template files in Symantec ESM Modules for ESX servers.

Table 1-1 Modules and checks that use template files

Module	Check name	Template name	Predefined template
ESX Patches	Patch templates	esxpatch.elx	esxpatch.elx
ESX Network	Port groups in VLAN	ESX Port group in VLAN	none
ESX System	ESX log auditing	ESX log audit	none

Modules

The Symantec ESM Modules for ESX Server contains four modules that assess vulnerabilities in ESX 3.0.x servers. These modules are host-based and collect

data from ESX servers to report vulnerabilities. You can install the Symantec ESM modules for ESX Server on ESX 3.0.x.

The modules are as follows:

- [ESX Configurations](#)
- [ESX Network](#)
- [ESX Patches](#)
- [ESX System](#)

Installing Symantec ESM Modules for ESX Server 3.0.x

This chapter includes the following topics:

- [Before you install](#)
- [System requirements](#)
- [Installing the ESM Modules for ESX Server 3.0.x](#)
- [Installing the ESM modules for ESX Server 3.0.x silently](#)

Before you install

Before you install Symantec ESM Modules for ESX Server 3.0.x, you must make sure that you have Security Update 22 or later applied on the ESM agents.

When ESX server is installed, the firewall default setting blocks the incoming and outgoing ports. To establish communication between the ESM manager and the agent on the ESX server, you must open the ports 5600 and 5601 before you install the ESM agent.

To install the modules, you need the following:

- **CD-ROM access**
At least one computer on your network must have a CD-ROM drive.
- **Account privileges**
You must have access to an account with superuser privileges on each computer where you plan to install the modules.

- Connection to the manager
Verify that the Symantec ESM enterprise console can connect to the Symantec ESM manager.
- Agent and manager
The Symantec ESM agent must be running and registered to at least one Symantec ESM manager.

Minimum account privileges

Only root user can install the Symantec ESM Modules for ESX Server 3.0.x.

System requirements

Table 2-1 indicates the system requirements and the supported operating system on which you can install the ESM modules for ESX Server 3.0.x.

Table 2-1 System requirements for installing ESX Server 3.0.x module

Supported operating system	Architecture
ESX 3.0.x	Opteron, x86, EM64T

Disk space requirements

Table 2-2 indicates the free disk space that you require to install the ESM modules for ESX server.

Table 2-2 Disk space requirements

Supported operating system	Architecture	Disk space
ESX 3.0.x	Opteron, x86, EM64T	6.3 MB

Installing the ESM Modules for ESX Server 3.0.x

You must install the modules on a Symantec ESM agent that is installed on the ESX server.

Modules are in an installation package that is named `esmesx.tpi`.

To install the ESM modules for ESX server:

- 1 From command prompt, run `esmesx.tpi`.

- 2 Type **2** to select the option that installs the module.
- 3 Do one of the following:
 - Type **yes** to register the template or .m files.
 - Type **no** if you already registered the .m files when you installed the module on another agent. This option is selected by default.
- 4 Do the following if you typed **yes**:
 - Type the ESM manager IP to which the agent is registered.
 - Type the ESM access name to log on to the ESM manager. By default, the ESM manager name is ESM.
 - Enter the ESM password used to log on to the ESM manager.
 - Enter the port that is used to contact the ESM manager. By default, the port number is 5600.
 - Enter the name of the agent as it is registered to the ESM manager.
 - Type **yes** or **no** to the question "Is this information correct?"
 - Type **yes** or **no** to the question "Do you wish to push the report content file?"
- 5 Do the following if you typed **no**:
 - Type **yes** or **no** for "Do you wish to register the product?"If you type **no**, then the installation continues till end without further user intervention.

If you type **yes**, then do the following:

 - Enter the ESM manager name that the agent is registered to.
 - Enter the ESM access name to log on to the ESM manager.
 - Enter the ESM password that is used to log on to the ESM manager.
 - Enter the port that is used to contact the ESM manager.
 - Enter the name of the agent as it is registered to the ESM manager
 - Type **yes** or **no** to the question "Is this information correct?"If you type **no**, then the questions are repeated till confirmation. If you type **yes**, then it installation continues till the end without further user intervention.

Installation log

The following log is an example of an ESM Modules for ESX Server 3.0.x installation log. Your log may look different, depending on how your manager and agents are configured.

Symantec Corporation tune-up/installation package

Options:

- 1) Display the description and contents of the tune-up/
installation package
- 2) Install the tune-up/installation package on your system
- 3) Quit

Enter option number [1]: 2

Installing package: Symantec ESM Modules for ESX 1.0.0 (2007/12/17)

This package includes the following templates and/or ".m" files:

File: /esm/register/unix/esxpatch.m.gz

Description: ESM ESX Patch module. module definition file

File: /esm/register/unix/esxconfig.m.gz

Description: ESM ESX Configuration file. module definition
file

File: /esm/register/unix/esxnetwork.m.gz

Description: ESM ESX Network module. module definition file

File: /esm/register/unix/esxsystem.m.gz

Description: ESM ESX System module. module definition file

File: /esm/register/unix/i18n/esxpatch.m.gz

Description: ESM ESX Patch module. module definition file

File: /esm/register/unix/i18n/esxconfig.m.gz

Description: ESM ESX Configuration file. module definition
file

File: /esm/register/unix/i18n/esxnetwork.m.gz

Description: ESM ESX Network module. module definition file

File: /esm/register/unix/i18n/esxsystem.m.gz

Description: ESM ESX System module . module definition file

```
File: /esm/template/unix/esxpatch.elx.gz
Description:      ESM template file
```

Template or *.m files need to be registered only once from the same type of agent with the same manager.

If you have already registered this package for other agents of the same type of operating system with the same manager, you can skip this step.

Do you wish to register the template or .m files [no]? Yes

ESM manager that the agent is registered to:

ESM access name to log on to the ESM manager [ESM]:

Password:

Enter the port used to contact the ESM manager [5600]:

Enter the name of the agent as it is registered to the ESM manager [manager]:

```
ESM Manager      : manager
ESM user name    : USER
Protocol         : TCP
Port             : 5600
ESM agent       : agent
```

Is this information correct? [yes]

```
Extracting /esm/bin/lnx-x86/mtpkreg.gz...
Extracting /esm/bin/lnx-x86/pushfiles.gz...
Extracting /esm/bin/lnx-x86/mergemanifest.gz...
Extracting /esm/register/unix/esxpatch.m.gz...
Extracting /esm/register/unix/esxconfig.m.gz...
Extracting /esm/register/unix/esxnetwork.m.gz...
Extracting /esm/register/unix/esxsystem.m.gz...
Extracting /esm/register/unix/il8n/esxpatch.m.gz...
Extracting /esm/register/unix/il8n/esxconfig.m.gz...
Extracting /esm/register/unix/il8n/esxnetwork.m.gz...
Extracting /esm/register/unix/il8n/esxsystem.m.gz...
```

```
Extracting /esm/config/esmsu-esx.properties.gz...
Extracting /esm/bin/lnx-x86/esxpatch.gz...
Extracting /esm/bin/lnx-x86/esxconfig.gz...
Extracting /esm/bin/lnx-x86/esxnetwork.gz...
Extracting /esm/bin/lnx-x86/esxsystem.gz...
Extracting /esm/template/unix/esxpatch.elx.gz...
Extracting /esm/update/ble/SU_3300/en/UpdatePackage.rdl.gz...
Extracting /tmp/esmthird.gz...
```

ESM ESX tpi installation completed.

```
Extracting /esm/config/su/65/manifest.xml.gz...
```

Re-registering modules/template files... Please wait...

```
Running "/esm/bin/lnx-x86/mtpkreg" -v -m "manager" -N
"agent" -p 5600 -t -U "ESM" -P "*****" -L "ESM_ESX" -T
esxpatch.m,esxconfig.m,esxnetwork.m,esxsystem.m... Please wait...
```

```
Registering /esm/register/unix/i18n/esxpatch.m ...
```

```
Registering /esm/register/unix/i18n/esxconfig.m ...
```

```
Registering /esm/register/unix/i18n/esxnetwork.m ...
```

```
Registering /esm/register/unix/i18n/esxsystem.m ...
```

```
checking: ESX Patches
```

```
checking: ESX Configurations
```

```
checking: ESX Network
```

```
checking: ESX System
```

```
uploading property file: esm-unix.properties
```

```
skipping: file already uploaded ....
```

```
uploading property file: esmsu-unix.properties
```

```
skipping: file already uploaded ....
```

```
uploading property file: esmsu-esx.properties
```

```
skipping: file already uploaded ....
```

```
loading template information
```

```
updating template basic.slx (Services - Linux)
```

no update required

```
updating template fileatt.li (New File - Linux)
```

no update required

updating template internet.li (New File - Linux)

no update required

updating template lnxadore.mfw (Malicious File Watch - all)

no update required

updating template lnxlion.mfw (Malicious File Watch - all)

no update required

updating template lnx0rn.mfw (Malicious File Watch - all)

no update required

updating template mail.li (New File - Linux)

no update required

updating template nfs.li (New File - Linux)

no update required

updating template objects.li (New File - Linux)

no update required

updating template patch.plx (Patch - Linux)

no update required

updating template queues.li (New File - Linux)

no update required

updating template remote.slx (Services - Linux)

no update required

updating template sysstart.li (New File - Linux)

no update required

updating template unix.fw (File Watch - all)

no update required

updating template unixhide.mfw (Malicious File Watch - all)

```
no update required
    updating template unix.mfw (Malicious File Watch - all)
```

```
no update required
    updating template uucp.li (New File - Linux)
```

```
no update required
    updating template esxpatch.elx (ESX Patch - all)
```

```
no update required
    sync'ing policy: Dynamic Assessment
    sync'ing policy: ESXNetwork
    sync'ing policy: Phase 1
    sync'ing policy: Phase 2
    sync'ing policy: Phase 3:a Relaxed
    sync'ing policy: Phase 3:b Cautious
    sync'ing policy: Phase 3:c Strict
    sync'ing policy: Queries
```

```
Report content file: update/ble/SU_3300/en/UpdatePackage.rdl
```

If you have already pushed this report content for other agents of the same type of operating system with the same manager you can skip this step.

```
Do you wish to push the report content file [no]?
```

```
Running "/esm/bin/lnx-x86/mergemanifest"... Please wait...
```

```
Merging src file: /esm/config/manifest.xml
Merging dst file: /esm/config/su/65/manifest.xml
Adding bin/lnx-x86/esxpatch entry
Adding bin/lnx-x86/esxconfig entry
Adding bin/lnx-x86/esxnetwork entry
Adding bin/lnx-x86/esxsystem entry
Adding config/esmsu-esx.properties entry
Adding register/unix/esxpatch.m entry
```

```
Adding register/unix/esxconfig.m entry
Adding register/unix/esxnetwork.m entry
Adding register/unix/esxsystem.m entry
Adding register/unix/i18n/esxpatch.m entry
Adding register/unix/i18n/esxconfig.m entry
Adding register/unix/i18n/esxnetwork.m entry
Adding register/unix/i18n/esxsystem.m entry

Merging /esm/config/su/65/manifest.xml to /esm/config/manifest.xml
End of installation
```

Installing the ESM modules for ESX Server 3.0.x silently

You can install the ESM modules for ESX Server silently by using the `esmesx.tpi`.

To install the ESX modules silently:

- ◆ At the command prompt, type the following:

```
./esmesx.tpi
```

If the installation succeeds, the return value is 0. If the installation fails, the return value is 1.

[Table 2-3](#) lists the command line options for installing the ESM modules for ESX Server 3.0.x silently.

Table 2-3 Command line options to install the ESM modules for ESX Server 3.0.x silently

Option	Description
-h	Display usage help
-d	Display the description and contents of this tune-up/third-party package.
-i	Install this tune-up/third-party package.
-f	Force an installation of the package
-U	Specify the ESM user name
-P	Specify the ESM user's password.
-p	Specify the TCP port to use.

Table 2-3 Command line options to install the ESM modules for ESX Server 3.0.x silently

Option	Description
-m	Specify the ESM manager name.
-t	Connect to the ESM manager by using TCP.
-g	Specify the ESM agent name to use for re-registration.
-K	Do not prompt for nor do the re-registration of the agents.
-L	Specify the application name.
-N	Do not update the report content file on the manager.
-Y	Update the report content file on the manager.

ESM Modules for ESX Server 3.0.x

This chapter includes the following topics:

- [ESX Configurations](#)
- [ESX Network](#)
- [ESX Patches](#)
- [ESX System](#)

ESX Configurations

The ESX Configurations module reports information about the configuration of ESX server and the guest operating systems. You must verify that the configurations of the server and guests are as per your security policies.

Guest installed

The Guest installed check reports list of installed Guest and its configuration path if name list is blank. If the disallowed directory name is specified in name list, then it reports if any Guest is installed under the specified path.

[Table 3-1](#) shows the message for the Guest installed check.

Table 3-1 Guest installed check messages

Message name	Title	Severity
STKU_INSTLGUEST	Guest installed	Green (0)
STKU_DISALLOWDIR	Disallowed directory	Yellow (2)

Guest status

The Guest status check reports the status, such as power on or power off of all the Guests.

Table 3-2 Guest status check message

Message name	Title	Severity
STKU_GUESTSTATUS	Guest status	Green (0)

Copy disabled

The Copy disabled check reports vulnerability if copying is enabled for Guest.

Table 3-3 Copy disabled check message

Message name	Title	Severity
STKU_COPY	Copy enabled	Yellow (2)

Paste disabled

The Paste disabled check reports vulnerability if pasting is enabled for Guest.

Table 3-4 Paste disabled check message

Message name	Title	Severity
STKU_PASTE	Paste enabled	Yellow (2)

Setinfo messages disabled

The Setinfo messages disabled check reports vulnerability if Setinfo-messages is enabled for Guest.

Table 3-5 Setinfo messages disabled check message

Message name	Title	Severity
STKU_SETINFO	Setinfo enabled	Yellow (2)

Guest time synchronization

The Guest time synchronization check verifies whether time synchronization is enabled between Guest and ESX host.

Table 3-6 Guest time synchronization check message

Message name	Title	Severity
STKU_TIMESYNC	Guest time not synchronized	Yellow (2)

Guest connection control

The Guest connection control check reports the name of the devices that the Guest can connect or disconnect.

Table 3-7 Guest connection control check message

Message name	Title	Severity
STKU_GUESTCONNCTRL	Guest connection control	Yellow (2)

Host time synchronization

The Host time synchronization check reports if the time difference between host and time server exceeds the specified limit. Specify time server IP address and time offset in the form, IP:offset. For example, 127.0.0.1:0.000005,

Table 3-8 Host time synchronization check message

Message name	Title	Severity
STKU_NTPDSTOPPED	ntpd not running	Yellow (2)
STKU_OFFSETEXCEEDED	Offset exceeded	Yellow (2)

Guest logging

The Guest logging check verifies whether Guest logging is disabled.

Table 3-9 Guest logging check message

Message name	Title	Severity
STKU_GUESTLOGGING	Guest logging	Yellow (2)

VMware Tools logging

The VMware Tools logging check verifies whether VMware Tools logging is disabled.

Table 3-10 VMware Tools logging check message

Message name	Title	Severity
STKU_VMTOOLSLOGGING	VMware Tools logging	Yellow (2)

Guest log rotate size

The Guest log rotate size check reports vulnerability if log rotate size exceeds the limit as specified in the value field, Maximum size in KB. The default value of the value field is 500

Table 3-11 Guestlog rotate size check message

Message name	Title	Severity
STKU_LOGROTATESIZE	Guest log rotate size	Yellow (2)

Guest old log keeping

The Guest old log keeping check reports vulnerability if number of old log files exceeds the limit as specified in the value field, number of log files to keep. The default value of the value field is 10.

Table 3-12 Guest old log keeping check message

Message name	Title	Severity
STKU_OLDLOGKEEPING	Guest old log keeping	Yellow (2)

Set GUI Options disabled

The Set GUI Options disabled check reports vulnerability if 'Set GUI Options' is enabled for Guest.

Table 3-13 Set GUI Options disabled check message

Message name	Title	Severity
STKU_SETGUI	Set GUI Options enabled	Yellow (2)

ESX Network

The ESX Network module reports information about ESX server's network configuration. It lets you verify if the server is compliant with your security standards.

iSCSI enabled

The iSCSI enabled check verifies whether iSCSI is enabled on the system.

Table 3-14 iSCSI enabled check message

Message name	Title	Severity
STKU_ISCSIDISABLED	iSCSI disabled	Yellow (2)

iSCSI CHAP authentication

The iSCSI CHAP authentication check verifies the presence of iSCSI initiator password in accordance with the CHAP authentication support.

Table 3-15 iSCSI CHAP authentication check message

Message name	Title	Severity
STKU_ISCSICHAPDISABLED	iSCSI CHAP disabled	Yellow (2)
STKU_ISCSIDISABLED	iSCSI disabled	Yellow (2)

MAC address changes

The MAC address changes check reports if MAC address changes is set to Accept.

Table 3-16 MAC address changes check message

Message name	Title	Severity
STKU_MACADDRCHANGS	MAC address changes accepted	Yellow (2)

Forged transmission

The Forged transmission check reports if Forged transmission is set to Accept.

Table 3-17 Forged transmission check message

Message name	Title	Severity
STKU_FORGEDTRANS	Forged transmission accepted	Yellow (2)

Promiscuous mode

The Promiscuous mode check reports if Promiscuous mode is set to Accept.

Table 3-18 Promiscuous mode check message

Message name	Title	Severity
STKU_PROMISCUOUS	Promiscuous mode accepted	Yellow (2)

Service console firewall

The Service console firewall determines the service console firewall security level.

The security levels are as follows:

- HIGH - Incoming and Outgoing ports are blocked by default.
- MEDIUM - Incoming ports are blocked but Outgoing ports are not blocked by default.
- LOW - Incoming and Outgoing ports are not blocked by default.

Table 3-19 Service console firewall check messages

Message name	Title	Severity
STKU_SVCCONSFIREWALL_G	Service console firewall	Green (0)
STKU_SVCCONSFIREWALL_Y	Service console firewall	Yellow (2)
STKU_SVCCONSFIREWALL_R	Service console firewall	Red (4)

Port groups in VLAN

The Port groups in VLAN check detects whether the port groups are in the same VLAN ID as specified in template.

See “[Templates](#)” on page 10.

Table 3-20 Port groups in VLAN check messages

Message name	Title	Severity
STKU_PORTGROUPSINVLAN	Port groups in VLAN	Yellow (2)
STKU_NOTEMPLATEFILE	No template specified	Red (4)

ESX Patches

The ESX Patches module reports information about the patches that have been released. The information includes patch ID, patch release date, revision, and description. You can use the name list to specify the template files that are to be included for the check.

You must verify that all current patches are installed on your ESX servers.

Note: The ESX Patches template (esxpatch.elx) includes ESX Patches that have been released on or before 21 Dec 2007.

Patch templates

The Patch templates check lets you enable or disable the template files that the ESX Patches module use to check agent systems. The module uses only the enabled template files that match the agent's operating system. For example, on an agent running Red Hat Linux, only enabled Red Hat Linux templates are used.

Table 3-21 Patch templates check message

Message name	Title	Severity
ESM_NO_TEMPLATE_SPECIFIED	No applicable template files specified	Red (4)
STKU_PATCHNOTINS0	Patch not installed	Green (0)
STKU_PATCHNOTINS1	Patch not installed	Yellow (2)
STKU_PATCHNOTINS2	Patch not installed	Yellow (2)
STKU_PATCHNOTINS3	Patch not installed	Red (4)
STKU_PATCHNOTINS4	Patch, Superseded patch not installed	Red (4)
ESM_FORBIDDEN_PATCH_0	Forbidden patch found	Green (0)

Table 3-21 Patch templates check message

Message name	Title	Severity
ESM_FORBIDDEN_PATCH_1	Forbidden patch found	Yellow (2)
ESM_FORBIDDEN_PATCH_2	Forbidden patch found	Yellow (2)
ESM_FORBIDDEN_PATCH_3	Forbidden patch found	Red (4)
STKU_PATCHNOTAVAIL2	Patch not available	Yellow (2)
STKU_PATCHNOTAVAIL3	Patch not available	Red (4)

Superseded

The Superseded check reports a patch and its superseding patches if a particular patch and its superseding patches are missing.

Table 3-22 Superseded check message

Message name	Title	Severity
ESM_SUPERSEDED_PATCH_NOT_INSTALLED	Superseded patch not installed	Yellow (2)
ESM_OPTIONAL_PATCH_NO_SUPERSEDES	Optional patch supersedes nothing	Yellow (2)

Disable patch module

No patches are checked when you enable the Disable patch module check. The module can take a long time to run. To save time, enable this option if you recently ran the module.

Table 3-23 Disable patch module check message

Message name	Title	Severity
X	Disable patch module	Green (0)

Patch results summary

The Patch results summary check, when enabled, lists the following:

Total number of available patches	Includes the patches that apply to this operating system, architecture, and ESX Server version.
-----------------------------------	---

Checked patches	Includes the patches that apply and have not been skipped. Patches can be skipped due to an unsatisfied sublist condition or when they apply to an application that is not installed.
Missing patches	Includes the patches that were supposed to be installed on the system, but are not present.
Forbidden patches	Includes the patches that are present, but are not allowed.

[Table 3-24](#) lists the message that the Patch results summary check displays.

Table 3-24 Patch results summary check message

Message name	Title	Severity
ESM_PATCH_SUMMARY	Patch results summary	Green (0)

Installed Patches

The Installed Patches check lets you view all the installed patches that ESM checks.

Table 3-25 Installed Patches check message

Message name	Title	Severity
ESM_INSTALLED_PATCH	Installed patches	Green (0)

ESX System

The ESX System module reports information about ESX server's access configuration, server logs, and available storage space.

Boot loader password

The Boot loader password check verifies whether Boot loader password is enabled on the system.

Table 3-26 Boot loader password check message

Message name	Title	Severity
STKU_BOOTPASSWORD	Boot loader password	Yellow (2)

Root file system fill up

The Root file system fill up check, by default, reports the use percent of disk space in each disk partition. When you specify a value (greater than zero) in the value field of the check, the check reports the disk partitions that have used disk space more than the specified value.

Table 3-27 Root file system fill up check messages

Message name	Title	Severity
STKU_DISKFREE	Disk free	Green (0)
STKU_DISKSPACELOW	Low disk space	Red (4)

Shell access

The Shell access check reports if "grant shell access to this user" is set for a user. Users can be included or excluded using the name list.

Table 3-28 Shell access check message

Message name	Title	Severity
STKU_SHELLACCESS	Shell access	Yellow (2)

Roles and privileges

The Roles and privileges check reports the granted roles and privileges of a user/group. Users can be included or excluded using the name list.

Table 3-29 Roles and privileges check message

Message name	Title	Severity
STKU_ROLESANDPRIV	Roles and privileges	Green (0)

SU PAM Authentication

The SU PAM Authentication check reports whether non wheel group members have 'su' access. It also checks whether wheel group members are trusted implicitly without password.

Table 3-30 SU PAM Authentication check message

Message name	Title	Severity
STKU_PAMAUTH	SU PAM Authentication	Yellow (2)

ESX log auditing

The ESX log auditing check audits the ESX log files and reports if a match is found as specified in template.

Table 3-31 ESX log auditing check message

Message name	Title	Severity
STKU_LOGAUDIT_Y	ESX log auditing	Yellow (2)
STKU_LOGAUDIT_G	ESX log auditing	Green (0)
STKU_LOGAUDIT_R	ESX log auditing	Red (4)
STKU_NOTEMPLATE	No template specified	Red (4)

See [“Templates”](#) on page 10.

