Symantec Enterprise Security Manager™ Baseline Policy Manual for Security Essentials

Solaris 10

Symantec

Symantec ESM Baseline Policy Manual for Security Essentials for Solaris 10

Documentation version: 4.0

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, DVDs, or manuals

Support agreement resources

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

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

Symantec Enterprise Security Manager™ policy for Security Essentials for Solaris 10

This document includes the following topics:

Introducing the policy

The Symantec Enterprise Security Manager (ESM) policy for the Security Essentials for Solaris 10 assesses a host's compliance with the CIS benchmark recommendations. This release of the policy was built based on the CIS benchmark version 4.0 for Solaris 10.

This policy can be installed on Symantec ESM 6.0 and later managers running Security Update 36 or later on Sun Solaris version 10.

For information on the Center for Internet Security benchmarks, visit the following URL:

http://www.cisecurity.org

Installing the policy

Before you install, you must decide which Symantec ESM managers require the policy. Policies run on the managers. They do not need to be installed on the agents. The policy runs only on Symantec ESM 6.0 or later, with Security Update 36 or later. Update any managers that do not meet these requirements.

Obtaining and Installing the policy using LiveUpdate

The standard installation method is to use the LiveUpdate™ feature in the Symantec ESM console. Another method is to use files from a CD or the Internet to install the policy manually.

Install the policy by using the LiveUpdate feature in the Symantec ESM console.

To install the policy using LiveUpdate

1. Connect the Symantec ESM Enterprise Console to managers on which you want to install the policy.
2. Click the LiveUpdate icon to start the LiveUpdate Wizard.
3. In the wizard, ensure that Symantec LiveUpdate (Internet) is selected, and then click **Next**.
4. In the Welcome to LiveUpdate panel, click **Next**.
5. In the Available Updates panel, do one of the following:
   - To install all checked products and components, click **Next**.
   - To omit a product from the update, uncheck it, and then click **Next**.
   - To omit a product component, expand the product node, uncheck the component that you want to omit, and then click **Next**.
6. In the Thank you panel, click **Finish**.
7. In the list of managers panel, ensure that all the managers that you want to update are checked, and then click **Next**.
8. In the Updating Managers panel, click **OK**.
9. In the Update Complete panel, click **Finish**.

Installing the policy manually

If you cannot use LiveUpdate to install the policy directly from a Symantec server, you can install the policy manually.

Note: To avoid conflicts with updates that are performed by standard LiveUpdate installations, copy or extract the files into the LiveUpdate folder, which is usually Program Files/Symantec/LiveUpdate.

To install the policy manually

1. Connect the Symantec ESM Enterprise Console to the managers that you want to update.
2. From the Symantec Security Response webpage download the executable files for Solaris 10.
3. On a computer running Windows NT/2000/XP/Server 2003 that has network access to the manager, run the executable that you downloaded from the Symantec Security Response web page.
4. Click **Next** to close the Welcome panel.
5. In the License Agreement panel, if you agree to the terms of the agreement, click **Yes**.
6. In the Question panel, click Yes to continue installation of the best practice policy.
7. In the ESM Manager Information panel, type the requested manager information, and then click **Next**.

   If the manager's modules have not been upgraded to Security Update 36 or later, the installation program returns an error message and stops the installation. Upgrade the manager to Security Update 36 or later, and then rerun the installation program.
8. Click **Finish**.

Policy modules

The security essentials for Solaris policy include the modules that ensure compliance with various technical and administrative aspects. Each module lists the enabled checks with the standards that they address, the associated name lists, and the templates. As specific values are not required everywhere, default values and templates are provided. Although the policy appears as read only, you can copy or rename the policy, depending on the requirements of your corporate security policy.

Account Integrity

The Account Integrity module creates and maintains user and group snapshot files on each agent on which the module runs. The module reports new, changed, and deleted users and groups between snapshot updates, as well as account privileges and other information.

Table 1-1 Account Integrity

Check	CIS section
Home directory permissions	7.10
Reserved UID/GID	7.6
Reserved UID ranges	7.6

File Attributes

The File Attributes module reports changes to file creation and modification times, file sizes, and CRC/MD5 checksum signatures. It also reports violations of the file permissions that are specified in the template files.

Table 1-2 File Attributes

Check	CIS section
Detect Extended attributes	5.8
Group ownership	3.1, 4.3, 4.5, 4.7, 4.8, 4.9, 6.7, 6.9, 8.1, 8.2, 8.4
Permissions	3.1, 4.3, 4.5, 4.7, 4.8, 4.9, 6.7, 6.9, 6.13, 7.8, 8.1, 8.2, 8.4
Exclude decreased permissions	3.1
User ownership	2.5, 3.1, 4.3, 4.5, 4.7, 4.8, 4.9, 6.7, 6.9, 8.1, 8.2, 8.4
Local disk only	5.8

File Attributes template files

Symantec uses LiveUpdate every two weeks to overwrite the default template files that are loaded on your computer. You can edit the template files by copying them into another directory and by renaming them.

File and directory permissions are compared with New File template settings. The module uses the following File Attributes template files:

Table 1-3 File Attributes template files

OS	File name	Template name
Solaris 10	attrcis4sol10.sol	New File - Solaris 2.6

File Find

The File Find module reports weaknesses in the file permissions and the configuration files.

Table 1-4 File Find

Check	CIS section
File content search	2.5, 3.1, 3.2, 3.3, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 6.1, 6.2, 6.3, 6.4, 6.6, 6.7, 6.8, 6.10, 6.11, 7.1, 7.5, 7.7, 7.8, 7.14, 7.15, 7.16, 8.2, 8.3, 8.7
Setgid executable files	5.6
Setuid executable files	5.6
World writable directories without sticky bit	5.4
World writable files	5.5
Unowned directories/files	5.7

Login Parameters

The Login Parameters module reports accounts, resources, and settings that are inconsistent with proper authorized usage.

Table 1-5 Login Parameters

Check	CIS section
Warning banners	8.1, 8.4

Network Integrity

The Network Integrity module reports the system configuration settings that pertain to authentication and remote access.

Table 1-6 Network Integrity

Check	CIS section
FTP debug logging disabled	4.2
FTP session logging disabled	4.2
FTP allowed users	6.5

OS Patches

The OS Patches module reports the patches that are defined in the UNIX patch template files for Solaris but are not installed on the agent.

Table 1-7 OS Patches

Check	CIS section
Superseded	1.1
Patch results summary	1.1

Password Strength

The Password Strength module examines the system parameters that control a password's construction, change, age, expiration, and storage.

Table 1-8 Password Strength

Check	CIS section
Accounts without passwords	7.2
Maximum repeated characters	7.4
Maximum password age	7.3
Minimum alphabetic characters	7.4
Minimum different character	7.4
Minimum lowercase characters	7.4
Minimum non-alphabetic characters	7.4
Minimum password history	7.4
Minimum uppercase characters	7.4

Table 1-8 Password Strength *(continued)*

Check	CIS section
Minimum password age	7.3
NAMECHECK allows username=password	7.4
Password age warning	7.3
Password length restrictions	7.4
Verify DICTIONDBDIR entry	7.4
Whitespace characters	7.4

Startup Files

The Startup Files module examines the system parameters that control processes and the services that are executed at system startup time.

Table 1-9 Startup Files

Check	CIS section
Syslog	4.4
Verify Network parameter Values	3.4, 3.5
Connection logging is not enabled	4.1
Grub password	6.13
Non-wrapped services	2.5
Services which are enabled	2.2.1, 2.2.2, 2.2.3., 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.3.1, 2.3.2, 2.3.3, 2.3.4, 2.3.5, 2.3.6, 2.3.7, 2.3.8, 2.3.9, 2.3.10, 2.3.11, 2.3.12, 2.3.13, 2.3.14

System Queues

The System Queues module reports messages that let you correct crontab file owners and permissions on the agent.

This module lets you create the following:

- Name lists of users and groups to exclude or include in all System Queues checks

- Users that are allowed to use the AT and CRON batch utilities

Table 1-10 System Queues

Check	CIS section
Only Root access to AT subsystem	6.9
Only Root access to CRON subsystem	6.9

User Files

The User Files module reports issues with ownership and permissions on the files that are contained in the user home directories.

Table 1-11 User Files

Check	CIS section
Current directory not allowed in PATH	7.9
Forbidden files	7.13
World writable directories in PATH	7.9
World writable files	7.11
Group writable directories in PATH	7.9
Group writable files	7.11
Startup file protection	7.12