

# Symantec™ Enterprise Security Manager Baseline Policy Manual for CIS Benchmark

For HP-UX 11i



# Symantec™ Enterprise Security Manager Baseline Policy Manual for CIS Benchmark for HP-UX 11i

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

## Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, ActiveAdmin, BindView, bv-Control, and LiveUpdate 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.

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 Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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  
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/](http://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/](http://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/](http://www.symantec.com/business/support/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/business/support/](http://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](mailto:customercare_apac@symantec.com)

Europe, Middle-East, and Africa [semea@symantec.com](mailto:semea@symantec.com)

North America and Latin America [supportsolutions@symantec.com](mailto:supportsolutions@symantec.com)

# Contents

Technical Support .....	4	
Chapter 1	Symantec™ ESM Baseline Policy Manual for CIS	
	Benchmark for HP-UX 11i .....	9
	Introducing the policy .....	9
	Installing the policy .....	9
	Obtaining and Installing the policy using LiveUpdate .....	10
Chapter 2	Policy modules .....	13
	Policy modules .....	13
	Account Integrity .....	14
	File Attributes .....	14
	File Find .....	14
	Login Parameters .....	15
	Network Integrity .....	15
	Object Integrity .....	16
	OS Patches .....	16
	Password Strength .....	16
	Startup Files .....	17
	User Files .....	17
	System Auditing .....	17
	System Queues .....	18





# Symantec™ ESM Baseline Policy Manual for CIS Benchmark for HP-UX 11i

This chapter includes the following topics:

- [Introducing the policy](#)
- [Installing the policy](#)
- [Obtaining and Installing the policy using LiveUpdate](#)

## Introducing the policy

The Symantec Enterprise Security Manager (ESM) Baseline Policy for the Center for Internet Security (CIS) Benchmark for HP-UX 11i version 2 and 3 through update 4 assesses a host's compliance with the benchmark's recommendations.

This release of the policy was built based on the CIS benchmark version 1.5.0 for HP-UX 11i. This policy can be installed on Symantec ESM 9.0.1 and 10.0 managers running Security Update 41 or later on HP-UX 11i.

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

<http://www.cisecurity.org>

## Installing the policy

Before you install the policy, you must decide on the Symantec ESM Managers that you want to install the policy. Since policies run on Managers, you do not

require to install policies on agents. You must install the policy on Symantec ESM 9.0.1 and 10.0 managers with Security Update 41 or later.

## Obtaining and Installing the policy using LiveUpdate

You can install the LiveUpdate feature in the following ways:

- By using the LiveUpdate feature on the Symantec ESM console
- By using files from a Product disc or from the Internet

### To install the policy using LiveUpdate

- 1 Connect the Symantec ESM Enterprise Console to the 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**.

If you cannot use LiveUpdate to install the policy directly from a Symantec server, you can install the policy manually, using files from a Product disc or the Internet.

---

**Note:** To avoid conflicts with the 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 from a Product disc or from the Internet

- 1 Connect the Symantec ESM Enterprise Console to the managers that you want to update.
- 2 From the Symantec Security Response Web site, download the executable files for HP-UX 11i. You can go to the following link:  
<http://securityresponse.symantec.com>
- 3 On a computer running Windows NT/XP/Server 2003 that has network access to the manager, run the executable that you downloaded from the Symantec Security Response Web site.
- 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

This chapter includes the following topics:

- [Policy modules](#)
- [Account Integrity](#)
- [File Attributes](#)
- [File Find](#)
- [Login Parameters](#)
- [Network Integrity](#)
- [Object Integrity](#)
- [OS Patches](#)
- [Password Strength](#)
- [Startup Files](#)
- [User Files](#)
- [System Auditing](#)
- [System Queues](#)

## Policy modules

The CIS Benchmark for HP-UX 11i 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 reports new, changed, and deleted accounts, account name and rights vulnerabilities, and user rights.

[Table 2-1](#) gives a list of the checks and their CIS sections.

**Table 2-1** Checks and CIS sections

Check	CIS section
Accounts should be disabled	1.8.1
Home directory permissions	1.8.7

## 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 2-2](#) gives a list of the checks and their CIS sections.

**Table 2-2** Checks and CIS sections

Check	CIS section
Group ownership	1.1.2, 1.6.8, 1.7.1, 1.6.10
Permissions	1.1.2, 1.3.1, 1.3.4, 1.3.7, 1.3.8, 1.3.13, 1.4.2, 1.5.6, 1.5.8, 1.6.1, 1.6.2, 1.6.6, 1.6.7, 1.6.8, 1.6.10, 1.7.1, 1.7.5, 1.9.1, 1.9.2, 1.9.3
User ownership	1.4.2, 1.7.1, 1.9.1, 1.9.2, 1.9.3

## File Find

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

[Table 2-3](#) gives a list of the checks and their CIS sections.

**Table 2-3** Checks and CIS sections

Check	CIS section
File Content Search	1.1.2, 1.3.2, 1.3.4, 1.3.5, 1.3.7, 1.3.8, 1.3.11, 1.3.12, 1.3.14, 1.3.15, 1.6.11, 1.6.3, 1.6.5, 1.7.1, 1.7.3, 1.7.4, 1.8.11, 1.8.12, 1.8.5, 1.9.2
Setgid executable files	1.5.5
World writable directories with sticky bit	1.5.2, 1.8.6
World writable files	1.5.3, 1.5.5

## Login Parameters

The Login Parameters module reports the accounts, resources, and settings that are not complaint with the policies.

[Table 2-4](#) gives a list of the checks and their CIS sections.

**Table 2-4** Checks and CIS sections

Check	CIS section
Remote root logins	1.1.2, 1.3.1, 1.6.10
Maximum logins allowed	1.6.9
Login retries	1.6.9
Warning Banners	1.9.1, 1.9.3

## Network Integrity

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

[Table 2-5](#) gives a list of the checks and their CIS sections.

**Table 2-5** Checks and CIS sections

Check	CIS section
FTP Enabled	1.2.3
Network parameters	1.4.2, 1.4.4, 1.6.2, 1.7.4

## Object Integrity

The Object Integrity module reports changes in ownership, permissions, and device IDs.

[Table 2-6](#) gives a list of the check and its CIS section.

**Table 2-6** Check and CIS section

Check	CIS section
Stack protection enabled	1.4.1

## OS Patches

The OS Patches module reports patches that have been released for UNIX operating systems but are not found on the agent. The released patches are defined in template files. New patch templates are available bi-monthly through LiveUpdate.

[Table 2-7](#) gives a list of the checks and their CIS sections.

**Table 2-7** Checks and CIS sections

Check	CIS section
Installed patches	1.1.2
Patch results summary	1.1.2

## Password Strength

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

[Table 2-8](#) gives a list of the checks and their CIS sections.

**Table 2-8** Checks and CIS sections

Check	CIS section
Accounts without password	1.8.2
Maximum password age	1.8.3
Minimum password age	1.8.3
Minimum password history	1.8.4



## Startup Files

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

[Table 2-9](#) gives a list of the check and its CIS sections.

**Table 2-9** Check and CIS sections

Check	CIS section
Services	1.2.1, 1.2.2, 1.2.10, 1.2.4, 1.2.5, 1.2.6, 1.2.8, 1.2.9

## User Files

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

[Table 2-10](#) gives a list of the checks and their CIS sections.

**Table 2-10** Checks and CIS sections

Check	CIS section
World writable directories in PATH	1.8.6
Current directory not allowed in PATH	1.8.6
Startup File protection	1.8.8
Startup file contents	1.8.9
Umask	1.8.10

## System Auditing

The System Auditing module reports the unaudited agents, non-compliant events auditing and system call mappings, and AIX files that are not audited for read and write actions and inconsistencies with authentication databases on trusted computers.

[Table 2-10](#) gives a list of the checks and their CIS sections.

**Table 2-11** Checks and CIS sections

Check	CIS section
Auditing enabled	1.7.2

## System Queues

The System Queues module reports AT and CRON subsystem access, and the executables and configuration files that are present in the crontab file.

[Table 2-10](#) gives a list of the checks and their CIS sections.

**Table 2-12** Checks and CIS sections

Check	CIS section
Only Root access to AT subsystem	1.6.6
Only Root access to CRON subsystem	1.6.6