Symantec™ ESM Policy for Payment Card Industry Data Security Standard (UNIX) v1.1 User’s Guide

Symantec ESM Policy for Payment Card Industry Data Security Standard (UNIX) v1.1 User's Guide

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

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

As part of Symantec Security Response, the Symantec Global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/ function, installation, and configuration, as well as to author content for our Web-accessible 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 as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that gives you the flexibility to select the right amount of service for any size organization.
- Telephone and Web support components that provide 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 from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages.
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, that offer enhanced response and proactive security support.

Please visit our Web site at http://www.symantec.com/techsupp/ for current information on Support Programs. The specific features that are available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.htm, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp.

Platinum Technical Support customers have access to the PlatinumWeb site: https://www-secure.symantec.com/platinum/login.html.

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

- 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 performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and 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 on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT
Symantec Enterprise Security Manager

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES (“SYMANTEC”) IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS “YOU” OR “YOUR”) ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE “AGREE” OR “YES” BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE “I DO NOT AGREE” OR “NO” BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License:

The software and documentation that accompanies this license (collectively the “Software”) is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a “License Module”) that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use that number of copies of the Software as have been licensed to You by Symantec under a License Module. Permission to use the software to assess Desktop, Server or Network machines does not constitute permission to make additional copies of the Software. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software you are authorized to use on a single machine.
B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
C. use the Software to assess no more than the number of Desktop machines set forth under a License Module. “Desktop” means a desktop central processing unit for a single end user;
D. use the Software to assess no more than the number of Server machines set forth under a License Module. “Server” means a central processing unit that acts as a server for other central processing units;
E. use the Software to assess no more than the number of Network machines set forth under a License Module. “Network” means a system comprised of multiple machines, each of which can be assessed over the same network;
F. use the Software in accordance with any written agreement between You and Symantec; and
G. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license.

You may not:

A. copy the printed documentation which accompanies the Software;
B. use the Software to assess a Desktop, Server or Network machine for which You have not been granted permission under a License Module;
C. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
D. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
E. continue to use a previously issued license key if You have received a new license key for such license, such as with a disk replacement set or an upgraded version of the Software, or in any other instance;
F. continue to use a previous version or copy of the Software after You have installed a disk replacement set, an upgraded version, or other authorized replacement. Upon such replacement, all copies of the prior version must be destroyed;
G. use a later version of the Software than is provided herewith unless you have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;
H. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module; nor
I. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following

Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as “Content Updates”). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are “Commercial Items,” as that term is defined in 48 C.F.R. section 2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of the Software to any entity not authorized by, or that is specified by, the United States Federal Government is strictly prohibited.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

Symantec™ ESM Policy for Payment Card Industry Data Security Standard (UNIX) v1.1 User’s Guide

Chapter 1 Introducing Symantec™ ESM Policy for Payment Card Industry Data Security Standard (UNIX) v1.1

Introducing Symantec™ ESM Policy for Payment Card Industry Data Security Standard (UNIX) v1.1

This document includes the following topics:

About the policy

The Symantec ESM policy for the Payment Card Industry Data Security Standard (PCI-DSS) v1.1 assesses compliance with the technical requirements of the standard that can be checked automatically, and also provides reports that facilitate auditing systems.

The Symantec ESM policy for PCI-DSS v1.1 assesses compliance with many of the standard's requirements.

The policy can be installed on Symantec ESM 5.5 or later. The minimum Security Update (SU) requirement to enable all the checks that are included in PCI-DSS v1.1 is SU 27. However, Symantec recommends that you install SU 33.

For information on the operating systems on which the policy is supported, refer the release notes of the latest SU at the following URL:

http://securityresponse.symantec.com/avcenter/security/Content/Product/Product_ESM_SU_Releases.html

For information on the databases on which the policy is supported, refer the User Guide of the latest Oracle application module at the following URL:

http://securityresponse.symantec.com/avcenter/security/Content/Product/Product_ESM_AM_Releases.html

About the Payment Card Industry Data Security Standard

The PCI-DSS was introduced in January 2005. The standard is drawn from the Visa Cardholder Information Security Program (CISP) and the MasterCard Site Data Protection program, and has been endorsed by Visa, MasterCard, American Express, Diner's Club, Discover and JCB. The standard is intended to allow merchants to demonstrate compliance with a common agreement for information security due care, rather than requiring them to comply with differing requirements from each payment processing company.

Where to get more information about the standard

The full text of the standard can be downloaded from the following PCI Security Standards URL:

https://www.pcisecuritystandards.org/

Installing the policy

You must decide which Symantec ESM managers require the policy. Policies are installed on managers, not on agents. The policy can be installed on Symantec ESM 5.5 or later. The minimum SU requirement to enable all the checks that are included in PCI-DSS v1.1 is SU 27. However, Symantec recommends that you install SU 33. You should update any manager that does not meet these requirements.

You can install the policy by using one of the following methods:

- LiveUpdate installation form the Symantec ESM Console
- Manual installation from the CD or the Internet

To install the policy by 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 checked, and then click **Next**.
4. In the Welcome to LiveUpdate dialog box, click **Next**.
5. Do one of the following:
   - To install all checked products and components, click **Next**.
   - To exclude a product from the update, uncheck it, and then click **Next**.
   - To exclude a product component, expand the product node, uncheck the component that you want to exclude, and then click Next..
6. Click **Next**.
7. Click **Finish**.

To obtain policy files from the Internet

1. Connect the Symantec ESM Enterprise Console to managers that you want to update.
2. Go to the Security Response Web site at the following URL:
   http://securityresponse.symantec.com
3. Download the executable file for the supported UNIX platforms.
   To avoid conflicts with updates that are performed by standard LiveUpdate installations, copy or extract the files into the LiveUpdate folder. Save the downloaded files to the Program Files/Symantec/LiveUpdate folder, or to the alternative location of your LiveUpdate folder.

To install the policy on a Symantec ESM manager

1. On a computer running Windows 2000/XP/Server 2003 that has network access to the manager, run the executable that you downloaded from the Symantec Security Response Web site, or from the CD.
2. Click **Next** to close the Welcome panel.
3. In the License Agreement panel, if you agree to the terms of the agreement, click **Yes**.
4. Click **Yes** to continue the installation of the policy.
5. Type the manager information.
6. Click **Next**.

7 Click **Finish**.

Policy modules

The Symantec ESM policy for PCI-DSS v1.1 includes the following modules to assess compliance with the standard. The policy runs on all supported UNIX operating systems.

See the current Security Update user's guide for UNIX for check, message, and template information.

The following topics describe the modules in this policy, and list the checks that are enabled for each module:

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.

Check	PCI-DSS section	Rationale
Changed accounts	8.5.1	Select a sample of user IDs and verify that the IDs are implemented in accordance with the authorization form with specified user privileges. Review all changes that were made to the /etc/ password and /etc/ group files after the last snapshot update to ensure that unauthorized access has not been granted.
Changed groups	8.5.1	Select a sample of user IDs and verify that the IDs are implemented in accordance with the authorization form with specified user privileges. Review all changes that were made to the /etc/ password and /etc/group files after the last snapshot update to ensure that unauthorized access has not been granted.

Check	PCI-DSS section	Rationale
Illegal login shells	7.1 2.2.3	The presence of unauthorized login shells could indicate compromised access controls.
Nonexistent login shells	7.1 2.2.3	The presence of unauthorized login shells could indicate compromised access controls.
Setuid login shells	2.2.3 11.1	Setuid login shells could allow inadvertent access to unauthorized users.
Setgid login shells	2.2.3 11.1	Setgid login shells could allow inadvertent access to unauthorized users.
Login shell owners	2.2.3	Login shells that are not owned by system accounts (root or bin) can be replaced with Trojan versions that are capable of unauthorized activity.
Login shell permissions	2.2.3 11.1	Login shells that are writable by group or world can be replaced with Trojan versions that are capable of unauthorized activity.
Home directories	2.2.3	Inconsistent home directory configurations could indicate incomplete account termination and could result in unauthorized access.
Group IDs	2.2.3	Undefined groups could result in inadvertent inheritance of unauthorized access privileges.
New accounts	8.5.1	Select a sample of user IDs and verify that the IDs are implemented in accordance with the authorization form with specified user privileges. Review all changes that were made to the /etc/password and /etc/group files after the last snapshot update to ensure that unauthorized access has not been granted.

Check	PCI-DSS section	Rationale
Deleted accounts	8.5.4	Immediately revoke accesses of terminated users. Select a sample of user IDs and verify that the IDs are implemented in accordance with the authorization form with specified user privileges. Review all changes that were made to the /etc/ password and /etc/group files after the last snapshot update to ensure that authorized access has not been removed.
New groups	8.5.1	Select a sample of user IDs and verify that the IDs are implemented in accordance with the authorization form with specified user privileges. Review all changes that were made to the /etc/ password and /etc/ group files after the last snapshot update to ensure that unauthorized access has not been granted.
Deleted groups	8.5.1	Select a sample of user IDs and verify that the IDs are implemented in accordance with the authorization form with specified user privileges. Review all changes that were made to the /etc/ password and /etc/ group files after the last snapshot update to ensure that unauthorized access has not been granted.
Duplicate IDs	8.1 8.5.1	Each user must have a unique ID.
Reserved UID/GID	2.2.3 7.1	Privileged access to system files could lead to unauthorized access. UIDs and GIDs between 0 and 100 should be reviewed for appropriateness.
Accounts should be disabled	8.5.4	Allowing logins on these accounts could lead to unauthorized access.

Check	PCI-DSS section	Rationale
Remote-only accounts	8.5.6	These accounts could provide a channel for unauthorized network access to the host.
Accounts can be locked	8.5.13	Accounts that are locked out due to consecutive unsuccessful login attempts could indicate possible intrusion attempts.

File Access

The File Access module reports user accounts with write permission on specified files.

Check	PCI-DSS section	Rationale
Write permission	2.2.3 7.1	Granting write permissions to accounts other than relevant users for the listed files could allow unauthorized access.
Execute permission	2.2.3 7.1	Granting execute permissions to accounts other than relevant users for the listed files could allow unauthorized access.

File Attributes

The File Attributes module reports changes to file creation and modification times, file sizes, and CRC/MD5 checksum signatures. This module also reports violations of file permissions that are specified in template files. GPO settings can be applied to sites, domains, and organizational units.

Check	PCI-DSS section	Rationale
User ownership	7.1	Improper file ownership controls could result in unauthorized access.
Group ownership	7.1	Improper group ownership controls could result in unauthorized access.
Changed files (change time)	11.5	Changes to the change time of these files could indicate unauthorized access.

Check	PCI-DSS section	Rationale
Changed files (size)	11.5	Changes to the size of these files could indicate unauthorized access.
Changed files (signature)	11.5	Changes to the checksums of these files could indicate unauthorized access.

File Attributes template files

You can make changes to the template files even though the policies are read-only. However, Symantec uses LiveUpdate every two weeks to overwrite the template files loaded on your system. If you want to keep the changes you have made to template files, you should copy them into another directory and rename them.

File and directory permissions are based on the operating system in the File Attributes template.

The following table lists the extensions that the File Attributes template files contain.

OS	File name	Template name
AIX	pci_fileatt.aix, pci_internet.aix	New File - AIX
HP-UX 10 and 11	pci_fileatt.hpx, pci_internet.hpx	New File - HP-UX 10-11
HP-UX ia64	pci_fileatt.hpi, pci_internet.hpi	New File - HP-UX (IA64)
Red Hat ES	pci_fileatt.li, pci_internet.li	New File - Linux
SuSE Linux	pci_fileatt.sl, pci_internet.sl	New File - SuSE Linux
Solaris 2.6 to 10	pci_fileatt.sol, pci_internet.sol	New File - Solaris 2.6

File Find

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

Check	PCI-DSS section	Rationale
Setuid files	2.2.3	Setuid files should be carefully examined to ensure that they are not used for unauthorized access.
Setuid executable files	2.2.3	Setuid executable files should be carefully examined to ensure that they are not used for unauthorized access.
Setgid files	2.2.3	Setgid files should be carefully examined to ensure that they are not used for unauthorized access.
Setgid executable files	2.2.3	Setgid executable files should be carefully examined to ensure that they are not used for unauthorized access.
New setuid files	2.2.3	New Setuid files should be carefully examined to ensure that they are not used for unauthorized access.
New setgid files	2.2.3	New setgid files should be carefully examined to ensure that they are not used for unauthorized access.
World writable directories without sticky bit	2.2.3	World writable directories without the sticky bit allows any user to delete files in the directory.
Device files not in /dev	2.2.3	Misplaced device files could indicate system compromise and could be used to gain unauthorized access to other system resources.
World writable files	2.2.3	World writeable files can be used to gain unauthorized access.
Uneven file permissions	2.2.3	Uneven file permissions could result in unauthorized access.

Check	PCI-DSS section	Rationale
Unowned directories/ files	2.2.3	Access to unowned directories and files could be inadvertently inherited by newly created accounts and groups.

File Watch

The File Watch module creates and maintains a snapshot file for each agent, and reports changes to files since the last snapshot.

Check	PCI-DSS section	Rationale
Changed files (ownership)	11.5	Changes to ownership of the files could indicate unauthorized access.
Changed files (permissions)	11.5	Changes to permissions of the files could indicate unauthorized access.
Changed files (signature)	11.5	Changes to signature of the files could indicate unauthorized access and possible modifications to the files.
New files	11.5	Newly added files could indicate unauthorized access or presence of trojans of malicious files.
Removed files	11.5	Removed files could indicate unauthorized access and removal of critical of important files.
Malicious files	11.5	Malicious files indicate unauthorized access and compromised system security.

File Watch template files

You can make changes to the template files even though the policies are read-only. However, Symantec uses LiveUpdate every two weeks to overwrite the template Symantec ESM policy for Payment Card Industry Data Security Standard (Unix) 23 Policy modules files loaded on your system. If you want to keep the changes you have made to template files, you should copy them into another directory and rename them.

The File Watch template specifies which files or directories to check, and the depth of directory traversal.

OS	File name	Template name
All UNIX and Linux	pci_unix.fw	File Watch - all
All UNIX and Linux	pci_unix.mfw, pci_unixhide.mfw, pci_lnxadore.mfw, pci_lnxlion.mfw, pci_lnxt0rn.mfw	Malicious File Watch -all

Login Parameters

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

Check	PCI-DSS section	Rationale
Login failures	8.5.1	Excessive login failures could indicate an attempt to gain unauthorized access. This policy ships with a default setting of 30 days, but should be changed to reflect your corporate policy.
Password expired	8.5.1	Expired passwords could indicate an unused account that has not been terminated. Unused accounts could allow unauthorized access.
Unsuccessful su attempts not logged	8.5.13	Unsuccessful privilege escalation could indicate an attempt to gain unauthorized access. This activity must be logged and audited.
Unsuccessful login attempts not logged	8.5.13	Unsuccessful logins could indicate an attempt to gain unauthorized access. This activity must be logged and audited.

Check	PCI-DSS section	Rationale
Locked accounts	8.5.14	Accounts are usually locked due to excessive login failures. This could be a result of brute forcing tools. Locked accounts could indicate attempt to gain unauthorized access.
Password changes failed	8.5.12	Excessive password change failures could indicate an attempt to guess a password.
Login retries	8.5.13	Excessive attempts to login to the sytem could indicate an attempt to gain unauthorized access by using brute forcing or password guessing tools.
Inactive accounts	8.5.5	Unused accounts must be deleted. Unused accounts could allow unauthorized access.

Network Integrity

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

Check	PCI-DSS section	Rationale
Trusted hosts/users	8.1 7.2 11.1	The Berkeley trust mechanism is one of the most common vulnerabilities that is exploited by attackers. The mechanism does not properly authenticate users. Any other means, such as SSH, should be used instead.
FTP enabled	2.2.2 2.2.1	FTP is another frequently exploited vulnerability. Other means, such as SFTP should be used instead.
FTP allowed system accounts	2.2.3	System accounts should not be granted ftp access as attackers can obtain account passwords by using network sniffers.

Check	PCI-DSS section	Rationale
Anonymous FTP enabled	2.2.3	Anonymous FTP provides any user with access to the system. This could aid attackers to launch other attacks against the OS.
Anonymous FTP permissions	2.2.3	Anonymous FTP provides any user with access to the system. This could aid attackers to launch other attacks against the OS.
TFTP	2.2.2	TFTP is one of the most common vulnerabilities that is exploited by attackers. The mechanism does not properly authenticate users.
NIS/NIS+ enabled	2.2.2 2.2.1	NIS/NIS+ should be disabled in case it is not being used as NIS has a known history of vulnerabilities that attackers can exploit to gain privileged access to the system.
Print servers	2.2.2 2.2.1	Print services have a history of remote code execution vulnerabilities .The print service should be disabled in case it is not being used.
Listening TCP ports	1.1.5 2.2.2	Unauthorized listening ports could suggest existence of trojans, backdoors or services that can be used by attackers to log in to the system.
New listening TCP ports	1.1.5 11.1	New listening ports could suggest existance of trojans, backdoors or services that can be used by attackers to log in to the system.
Modified listening TCP ports	11.1	Modified listening ports suggest existence of trojans, backdoors or services that can be used by attackers to log in to the system.
Listening UDP ports	1.1.5 11.1	Unauthorized listening ports could suggest existence of trojans, backdoors or services that can be used by attackers to log in to the system.

Check	PCI-DSS section	Rationale
New listening UDP ports	1.1.5 11.1	New listening ports could suggest existence of trojans, backdoors or services that can be used by attackers to log in to the system.
SNMP default community strings	2.2.3	Default community strings "public &private" should be changed as they can aid attackers in reading and changing system configuration.
SNMP v3 encryption	4.1	SNMP V3 encryption should be enabled in order to enable authentication and privacy, that are required to fully secure SNMP.
Promiscuous mode	11.1	A network interface in the promiscuous mode could be used to sniff all network traffic.

Object Integrity

The Object Integrity module reports volumes that do not have Access Control Lists (ACLs).

Check	PCI-DSS section	Rationale
Disk and memory access	7.1	Disk and memory devices should be secured so that only root users have access to them.

Oracle Accounts

Note: Symantec ships the Oracle modules in separate policy files. On computers that are running one or more Oracle servers, you must install the Oracle policies separately.

The Oracle Accounts module reports on a variety of privileges that should be monitored to ensure that proper authorizations are granted, revoked, and maintained over time.

Check	PCI-DSS section	Rationale
OS authenticated users	7.1 8.2	Access to databases should be controlled by the DBMS, not just the operating system.
Inactive database accounts	8.5.4	Periodically review user accounts to verify that they are all current and authorized.
Active database accounts	8.5.1 8.5.16	Periodically review user accounts to verify that they are all current and authorized.
Database accounts	8.5.1 8.5.16	Periodically review user accounts to verify that they are all current and authorized.
New database accounts	8.5.1	Addition, deletion, and modification of new database user accounts should be controlled.
Deleted database accounts	8.5.1	Addition, deletion, and modification of new database user accounts should be controlled.
Password protected default role	8.2 7.1	Periodically review user accounts who are granted password protected default role, to verify that they are all current and authorized.

Oracle Auditing

The Oracle Auditing module reports on audit system settings that should be periodically reviewed for policy compliance.

Check	PCI-DSS section	Rationale
Audit trail enabled	10.2	Audit trails must be enabled to establish accountability.
Audit trail protection	10.5	Audit trails should be secured so that they cannot be altered.

Check	PCI-DSS section	Rationale
Auditing options	10.2	Audit trails must be enabled to establish accountability.

Oracle Configuration

The Oracle Configuration module reports on wrongly configured global settings for the Oracle server.

Check	PCI-DSS section	Rationale
DB link encrypted password	8.4	Passwords should not be transmitted in clear text.
Remote login password file	2.2.3	System security parameters should be configured properly to prevent misuse.

Oracle Objects

The Oracle Objects module reports on object privileges that should be periodically reviewed for appropriateness and authorization.

Check	PCI-DSS section	Rationale
Access to SYS.ALL_SOURCE	7.1	Ensure proper user authentication and password management for non-consumer users and administrators on all system components.

Oracle Passwords

The Oracle Passwords module reports on accounts with obviously weak passwords.

Check	PCI-DSS section	Rationale
Password = username	8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components.

Check	PCI-DSS section	Rationale
Password = any username	8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components.
Password = wordlist word	8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components.
Reverse order	8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components.
Double occurrences	8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components.
Plural	8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components.
Prefix	8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components.
Suffix	8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components.
Well known passwords	8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components.

Oracle Patches

The Oracle Patches module lists patches available from Oracle Corporation within a specified time frame.

OS	File name	Template name
Patch information	6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.
Installed patches	6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.

Oracle Patches templates files

OS	File name	Template name
All UNIX, Linux	orapatch_policy.orp	Oracle Patch - all

Oracle Profiles

The Oracle Profiles module reports on new profiles that were created since the last snapshot.

Check	PCI-DSS section	Rationale
New profiles	8.5.1	Addition, deletion, and modification of user IDs, credentials, and other identifier objects should be controlled.
Deleted profiles	8.5.4	Addition, deletion, and modification of user IDs, credentials, and other identifier objects should be controlled.

Check	PCI-DSS section	Rationale
Profile resources	8.5.1	Addition, deletion, and modification of user IDs, credentials, and other identifier objects should be controlled.
Connection time	8.5.15	Idle sessions should be disconnected if idle for more than 15 mins.The user should be required to re-enter the password to re-activate the terminal.
Idle time	8.5.15	Idle sessions should be disconnected if idle for more than 15 mins. The user should be required to re-enter the password to re-activate the terminal.
Failed logins	8.5.13	Limit repeated access attempts by locking out the user ID after not more than six attempts.
Password grace time	8.5.9	A user is required to change passwords every 90 days.
Password duration	8.5.9	A user is required to change passwords every 90 days.
Password lock time	8.5.14	User accounts should be locked out for 30 mins or until the administrator reactivates the account.
Password reuse max	8.5.12	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
Password reuse time	8.5.12	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
Password verify function	8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components.

Oracle Roles

The Oracle Roles module reports on new roles, nested roles, and privileges that you have created since the last snapshot.

Check	PCI-DSS section	Rationale
Deleted roles	8.5.1	The roles reported by this check need to be reviewed in order to check if they are valid and authorized.
Privileges	7.1	The privileges granted to roles reported by this check need to be reviewed in order to check if they are valid and authorized.
New privileges	7.1 8.5.1	New privileges granted to roles reported by this check need to be reviewed in order to check if they are valid and authorized.
Grantable privileges	7.1	Grantable privileges granted to roles reported by this check need to be reviewed in order to check if they are valid and authorized.
DBA equivalent roles	7.1	The roles reported by this check need to be reviewed in order to check if they are valid and authorized.
Granted Oracle DBA role	8.5.16	The roles reported by this check need to be reviewed in order to check if they are valid and authorized.
Roles without passwords	8.2	Roles require authentication before being provided with access.
PUBLIC role access	7.1 8.5.16	Accounts reported by this check need to be reviewed to check for their need for access.

Oracle Tablespace

The Oracle Tablespace module reports on new and deleted tablespaces.

Check	PCI-DSS section	Rationale
SYSTEM tablespace assigned to user	7.1	The list produced by this check should be examined to ensure that the accounts have been configured correctly. Assigning the SYSTEM tablespace to a user is usually an error, but may be an indication of compromise.

OS Patches

The OS Patches module reports patches that are defined in the corresponding patch template files for the operating system version but are not installed on the agent.

Check	PCI-DSS section	Rationale
Superseded	6.1	Make sure all systems and software have the latest vendor-supplied security patches. Keep up with vendor changes and enhancements to security patches. Install new/ modified security patches within one month of release. To protect the security or integrity of cardholder data against anticipated threats, all information technology resources must be regularly checked to ensure that known vulnerabilities have been patched.

Check	PCI-DSS section	Rationale
Patch results summary	6.1	Make sure all systems and software have the latest vendor-supplied security patches. Keep up with vendor changes and enhancements to security patches. Install new/ modified security patches within one month of release. To protect the security or integrity of cardholder data against anticipated threats, all information technology resources must be regularly checked to ensure that known vulnerabilities have been patched.
Patch not installed and process not running	6.1	Make sure all systems and software have the latest vendor-supplied security patches. Keep up with vendor changes and enhancements to security patches. Install new/ modified security patches within one month of release. To protect the security or integrity of cardholder data against anticipated threats, all information technology resources must be regularly checked to ensure that known vulnerabilities have been patched.
Installed patches	6.1	Make sure all systems and software have the latest vendor-supplied security patches. Keep up with vendor changes and enhancements to security patches. Install new/ modified security patches within one month of release. To protect the security or integrity of cardholder data against anticipated threats, all information technology resources must be regularly checked to ensure that known vulnerabilities have been patched.

OS Patches (Patch) template files

Symantec uses LiveUpdate every two weeks to overwrite the template files loaded on your system.

OS	File name	Template name
AIX	patch.pai	Patch - AIX
HP-UX 10 and 11	patch.ph1	Patch - HP-UX 10-11
HP-UX ia64	patch.ph2	Patch - HP-UX (IA64)
RedHat ES	patch.plx	Patch - Linux
SUSE Linux	patch.psl	Patch - SuSE Linux
Solaris 2.6 to 10	patch.ps6	Patch - Solaris 2.6

Password Strength

The Password Strength module examines system parameters that control the construction, change, aging, expiration, and storage of passwords.

Check	PCI-DSS section	Rationale
Password = username	8.5.1	The user name and password should not be the same for any user account on the system as it makes it easy for anyone to gain access to a user account.
Password = any username	8.5.1	The password should not be the same as any users login name for any user account on the system as it makes it easy for anyone to gain access to a user account.
Password within GECOS field	8.5.1	The password should not be the same as any word in the GECOS field as it makes it easy for anyone to gain access to a user account.
Password = wordlist word	8.5.1	User account passwords should be complex in nature and should contain a combination of numbers and characters. Passwords should not be predictable or easily guessed or cracked by dictionary or brute force attacks.

Check	PCI-DSS section	Rationale
Reverse order	8.5.1	User account passwords should be complex in nature and should contain a combination of numbers and characters. Passwords should not be predictable or easily guessed or cracked by dictionary or brute force attacks.
Double occurrences	8.5.1	User account passwords should be complex in nature and should contain a combination of numbers and characters. Passwords should not be predictable or easily guessed or cracked by dictionary or brute force attacks.
Plural forms	8.5.1	User account passwords should be complex in nature and should contain a combination of numbers and characters. Passwords should not be predictable or easily guessed or cracked by dictionary or brute force attacks.
Uppercase	8.5.1	User account passwords should be complex in nature and should contain a combination of numbers and characters. Passwords should not be predictable or easily guessed or cracked by dictionary or brute force attacks.
Lowercase	8.5.1	User account passwords should be complex in nature and should contain a combination of numbers and characters. Passwords should not be predictable or easily guessed or cracked by dictionary or brute force attacks.

Check	PCI-DSS section	Rationale
Guessed password	8.5.1	User account passwords should be complex in nature and should contain a combination of numbers and characters. Passwords should not be predictable or easily guessed or cracked by dictionary or brute force attacks.
Login requires password	8.2	All users need to enter a password in order to login to the sytem. Accounts without passwords could allow unauthorized access.
Accounts without passwords	8.2	All users need to enter a password in order to login to the system. Accounts without passwords could allow unauthorized access.
Password length restrictions	8.5.10	The PCI-DSS standard states that the minimum length of a password should be seven characters at least.
Minimum password history	8.5.12	The PCI DSS standard states that a user should not be allowed a new password that is the same as any of the last four passwords that have been used.
Password age	8.5.9	The PCI DSS standard states that user passwords should be changed at least every 90 days.
Maximum password age	8.5.9	The PCI DSS standard states that user passwords should be changed at least every 90 days.
Minimum password age	8.5.9	The PCI DSS standard states that user passwords should be changed at least every 90 days.
Minimum alphabetic characters	8.5.11	User account passwords should be complex in nature and should contain a combination of numbers and characters. Passwords should not be predictable or easily guessed or cracked by dictionary or brute force attacks.

Check	PCI-DSS section	Rationale
Minimum non-alphabetic characters	8.5.11	User account passwords should be complex in nature and should contain a combination of numbers and characters. Passwords should not be predictable or easily guessed or cracked by dictionary or brute force attacks.
Minimum different characters	8.5.11	User account passwords should be complex in nature and should contain a number of different characters. Passwords should not be predictable or easily guessed or cracked by dictionary or brute force attacks.
Accounts can be used without a password	8.2	All users need to enter a password in order to login to the sytem. Accounts without passwords could allow unauthorized access.

Startup Files

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

Check	PCI-DSS section	Rationale
Current directory in startup PATH	2.2.3	Files writable by users other than root could allow unauthorized access or privilege escalation.
Login/tty file contents	2.2.3 2.2.4	Remote root login on an untrusted channel could allow unauthorized access.
Installed services	2.2.2	Disable all unnecessary services. Services are a common source of malicious exploitation and must be recorded and periodically examined to protect cardholder data from threats or hazards.
Changed services	11.1	Changes to an authorized service could indicate a system compromise.

Check	PCI-DSS section	Rationale
New services	11.1	Unauthorized services could be used to gain unauthorized access.
Deleted services	11.1	Necessary services that are disabled deny needed services to users.
Non-wrapped services	2.2.3 8,1	TCP Wrappers should be used as they provide access control and logging to services.

Startup Files template files

Symantec uses LiveUpdate every two weeks to overwrite the template files loaded on your system.

OS	File name	Template name
AIX	pci_basic.sai, pci_remote.sai	Services - AIX
HP-UX 10 and 11	pci_basic.sh1, pci_remote.sh1	Services - HP-UX 10-11
HP-UX ia64	pci_basic.sh2, pci_remote.sh2	Services - HP-UX (IA64)
Red Hat ES	pci_basic.slx, pci_remote.slx	Services - Linux
SuSE Linux	pci_basic.ssl, pci_remote.ssl	Services - SuSE Linux
Solaris 2.6 to 10	pci_basic.ss6, pci_remote.ss6	Services - Solaris 2.6

System Auditing

The System Auditing module examines the auditing system to ensure that it is enabled and configured properly.

Check	PCI-DSS section	Rationale
Auditing enabled	10	Auditing should be enabled as per section 10 of the PCI-DSS standard.

Check	PCI-DSS section	Rationale
Event auditing	10.2 10.3	Define the specific events and system calls to be audited to review system activity.
File read auditing	10.2.1 10.3	Auditing should be enabled as per section 10 of the PCI-DSS standard.
File write auditing	10.3	Auditing should be enabled as per section 10 of the PCI-DSS standard.

System Auditing template files

Symantec uses LiveUpdate every two weeks to overwrite the template files loaded on your system.

OS	File name	Template name
AIX	pci_aix.aud	Events - all
HP-UX	pci_hpevents.aud	Events - all
Solaris	pci_solaris.aud	Events - all

System Mail

ESM provides checks for the Sendmail program. However, systems that store and process information that is used for financial reporting should not use Sendmail because of Sendmail's history of security vulnerabilities.

Note: If SMTP is required, use a more secure and reliable substitute such as qmail or Postfix.

The System Mail module reports the following:

- Wizard passwords and decode aliases in mail configuration files
- Mail aliases that are piped to a command or shell program
- Agents that are not logging Sendmail messages

- Agents that do not have properly configured logs

Check	PCI-DSS section	Rationale
Wizard passwords	2.2.3	Wizard passwords are frequently exploited and could result in unauthorized access.
Decode aliases	2.2.3	Decode aliases are a frequent vector for malicious code.
Command aliases	2.2.3	Command aliases could be used to gain unauthorized access and could indicate system compromise.
Sendmail log	10.2	Logging should be enabled as per section 10 of PCI-DSS. The log file should be owned by root and secured to prevent unauthorized access and modifications to the log files.

System Queues

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

The System Queues 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 batch utilities.

Check	PCI-DSS section	Rationale
AT subsystem access	7.1 2.2.3	The AT and CRON systems are frequent targets of attackers, as they could allow the installation of persistent unauthorized codes.
CRON subsystem access	7.1 2.2.3	The AT and CRON systems are frequent targets of attackers, as they could allow the installation of persistent unauthorized codes.

User Files

The User Files module reports on a variety of questionable ownership and permission settings in user home directories.

Check	PCI-DSS section	Rationale
World writable files	2.2.3	World writable files could be used to gain unauthorized access.
SETUID or SETGID	2.2.3	Setuid and setgid files should be examined to ensure that they do not allow unauthorized access.
Current directory only at end of PATH	2.2.3	Files that are writable by users other than root could result in unauthorized access or privilege escalation.
World writable directories in PATH	2.2.3	Files that are writable by users other than root could result in unauthorized access or privilege escalation.
Group writable directories in PATH	2.2.3	Files that are writable by group other than root group could result in unauthorized access or privilege escalation.
Umask	2.2.3	Umask values set too low could result in unauthorized access or privilege escalation. This policy ships with a default setting of 027, but should be changed to reflect your corporate policy.
Startup file contents	2.2.3	World-writable files executed by system startup scripts could result in unauthorized access or privilege escalation.
Startup file protection	2.2.3	If startup files are not properly protected, an attacker could change them and hijack the user's account.
Suspicious file names	2.2.3	Executable files with suspicious names could carry out activities which are characteristic of, but not exclusive to, samples of malware.