Symantec Enterprise Security Manager™ Security Update 17 User's Guide

Release for Symantec ESM 6.0 and 5.5 UNIX modules

Symantec ESM Security Update 17 for UNIX

Copyright Notice

Trademarks

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 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.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at www-secure.symantec.com/platinum/.

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

Index

Chapter 1

Introducing Security Update 17 for UNIX

Symantec ESM modules

The Account Integrity module reports new, changed, and deleted accounts, account name and rights vulnerabilities, and user rights.

For example, the Login Parameters module includes checks for excessive login failures, expired passwords, and so on. Each check examines a specific area of concern such as inactive accounts or password length.

Account Integrity

The Account Integrity module reports new, changed, and deleted accounts, user rights, and vulnerabilities of account names and rights. See "Account Integrity" on page 47.

Discovery

The Discovery module reports computers that could run Symantec ESM or Symantec Intruder Alert but are not running them. See "Discovery" on page 62.

File Access

The File Access module examines read, write, and execute permissions on specified files and access control lists (ACLs) on AIX and HP-UX operating systems. It is in the Queries policy. "File Access" on page 66.

File Attributes

The File Attributes module reports changes in system file attributes including file ownership, permissions, size, and creation and modification times. See "File Attributes" on page 67.

File Find

The File Find module examines certain file attributes and settings, uneven permissions, specified text strings, and unowned files. See "File Find" on page 75.

File Watch

The File Watch module reports changes to specified files and directories, and the presence of files with suspicious file names or signature patterns. See "File Watch" on page 95.

Integrated Command Engine (ICE)

The Integrated Command Engine (ICE) is a unique, extensible module in the Dynamic Assessment policy. It contains no security checks or templates, but gives users the ability to integrate user scripts and executables and with Symantec ESM. In effect, they become the module's security checks. Because the ICE module is so different from all other modules, it is documented in the Appendix. See "Integrated Command Engine (ICE)" on page 225.

Login Parameters

The Login Parameters module reports system login vulnerabilities such as old and unused accounts, failed logins, expired passwords, etc. See "Login Parameters" on page 112.

Network Integrity

The UNIX Network Integrity module reports vulnerabilities in NFS software and NIS or NIS+ services, and identifies user accounts that can access the host and user accounts in a UNIX domain through file transfer protocol (FTP) and trivial file transfer protocol (TFTP) utilities. See "Network Integrity" on page 122.

Object Integrity

The Object Integrity module reports changes in device ownership, permissions, and IDs. See "Object Integrity" on page 163.

OS Patches

The OS Patches module reports patches that have been released for UNIX operating systems but are not found on the agent. See "OS Patches" on page 166.

Password Strength

The Password Strength module reports passwords that do not conform to specified format, length, and expiration requirements. It also applies dictionary tests to detect passwords that are easily guessed. See "Password Strength" on page 174.

Startup Files

The Startup Files module examines rc scripts and system startup files, looking for discrepancies with system-owned services that are defined in the Services templates. It also reports new, changed, and deleted services. See "Startup Files" on page 191.

System Auditing

The System Auditing module reports 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. See "System Auditing" on page 202.

System Mail

The System Mail module reports security holes in mail configuration files, mail file attributes, and the Morris worm. See "System Mail" on page 209.

System Queues

The System Queues module reports AT and CRON subsystem access, and executables and configuration files that are in the crontab file. See "System Queues" on page 212.

User Files

The User Files module examines user file ownership and permissions, PATH and umask settings in startup files, files with the same names as system commands, hidden directories, special device files, and remote mount points. It is in the Queries module. See "User Files" on page 214.

Chapter 2

Installing Symantec ESM security modules

This chapter includes the following topics:

System requirements

SU17 installation requires the following free disk space:

Agent operating system	Disk space
Windows Server 2003	24 MB
Windows XP Professional (Intel)	24 MB
Windows 2000 Professional or Server (Intel)	26 MB
Windows NT (Intel)	23 MB
AIX	82 MB
Digital UNIX/Tru64/OSF1	66 MB
HP-UX	62 MB
IRIX	87 MB

Agent operating system	Disk space
Red Hat Linux	28 MB
Solaris	52 MB
Sequent	45 MB

The LiveUpdate installation of SU17 for all supported operating systems requires approximately 520 MB per manager.

Getting the update

Symantec ESM Security Updates are available:

- Through LiveUpdate.
  Running LiveUpdate is the standard method of installing Security Updates. Symantec ESM 6.0 or 5.5 upgraded to SU 9 or later is required.
- On the Internet at http://www.symantec.com/downloads.
- On a Security Update CD.
  Two or three times a year, Symantec publishes a set of recent updates on a CD. If you are unable to obtain Security Updates through LiveUpdate and cannot download them from the Symantec Security Response Web site, use the form at the end of this document to order the most recent CD.

Getting ready to install

Before you start installing the modules:

- Make sure that each computer where you plan to install the security modules has an installed agent.
- Prepare a list of all UNIX agents that need to be updated.
  Include the names of all manager computers where each agent is registered.
  Include the user name, password, and communication protocol that each agent uses to contact the manager.
  The user name and password must have privileges to register agents on the manager.
- Have access to an account with root privileges on the computers where you plan to install the security modules.

Installing the update

Symantec distributes the security modules in tuneup packs on a CD-ROM. They are also available on the Internet at http://www.symantec.com/techsupp.

On the CD-ROM, a tuneup pack named esm.tpk is in each subdirectory that is named for specific UNIX architectures.

To install the security modules

1. At the command line, use **su** or **login** to access an account with root privileges.
2. Open the directory that is named by the *vendor*/*operating system*/*architecture* of the computer that you are installing.
3. Type **./esm.tpk** to run the tuneup pack.
4. Type **2** to continue with installation.
5. Press **Enter**.
6. The first time you install the Security Update on an operating system, type **Y** to register the template and .m files with the manager.
   On subsequent installations, type **N** to skip the registration. The Security Update only has to be registered with each manager once for each operating system.
7. Press **Enter**.
   If this is the first time you are installing the Security Update on the operating system, and you typed **Y** in step 6, proceed to the next step.
   If this is not the first time you are installing the Security Update on the operating system, and you typed **N** in the previous step, this completes the installation.
8. Type the name of the manager that you want to register the template and .m files with.
9. Press **Enter**.
10. Press **Enter** to log on to the manager with the default user name, ESM.
    Otherwise, type the name of a user that has the advanced manager right, Register agents with manager.
11. Type the password that gives the user access to the manager.
12. Press **Enter**.
13. Press **Enter** to accept the TCP protocol.
    Otherwise, type **1** to select the IPX protocol, then press **Enter**.

14 Press **Enter** to the accept the default port, 5600.
Otherwise, type the number of the port that you use for Symantec ESM, then press **Enter**.

15 Press **Enter** to use the default name.
Otherwise, type the name of the agent as it is known to the manager, then press **Enter**.

16 Press **Enter** to approve the information that you have entered.

17 When prompted, press **Enter** to exit the installation program.

When an agent is registered to multiple managers, rerun esmtpk.exe on the agent to register the modules with each manager.

Note: Do not register different versions of Symantec ESM agents to the same manager. This can cause manager database errors.

Although agents that were registered to a manager before it was upgraded continue to function with the manager after the upgrade, you should upgrade agents to the same version as the manager.

Registering the modules

Although tuneup packs prompt for a decision to register templates and .m files each time they install security modules on an agent, you do not need to register the updated files more than one time for each manager.

Using remote tuneup options

From the Symantec ESM console you can install security modules on one UNIX agent, or on all of the UNIX agents in the same domain that are running the same UNIX operating system and version.

To use the remote tuneup option

1 Log in to the Symantec ESM console on a Windows computer where the console has been installed.

2 Click on **ESM Enterprise** > **All Managers** > [a UNIX manager] > **Domains** > **UNIX agents**.

3 Right-click **UNIX agents** or a specific UNIX agent, then click **Remote Tuneup**.

4 Click **Next** to confirm the identities of the remote agents.

5 Select the tuneup pack location:

- Select **Install from CD** to install a tuneup pack from a CD-ROM. Select a drive letter to identify the location of the CD-ROM, then select the tuneup pack for the architecture of the UNIX agents that you want to install.
- Select **Install from hard drive** to install a tuneup pack from a hard drive. Click **Directory** to open the Select Directory dialog box, select the directory path to the tuneup pack for the architecture of the UNIX agents that you want to install, then click **OK.**

6 Click **Next**.

7 Click **Finish** to start the remote installation.

Remote tuneup skips any agents in the UNIX agents branch with architectures that cannot be installed by the selected tuneup pack and installs all agents with architectures that can be installed by the selected tuneup pack.

Repeat the preceding steps 1 through 6 to rerun Remote tuneup using tuneup packs with the correct architecture for all skipped agents.

Resolving connection errors

If an agent reports connection errors while running security checks, check the /esm/config/manager.dat file on the agent.

To resolve connection errors, add the manager's fully-qualified name to the file. If the file is missing, run the esmsetup program to re-register the agent to the manager.

Chapter 3

Reviewing policies, modules, and messages

This chapter includes the following topics:

For additional information, see the chapter 3 of the *Symantec Enterprise Security Manager 6.0 User's Guide* or of the *Symantec Enterprise Security Manager 5.5 User Manual*.

Reviewing policies

A policy is a set of modules with enabled security checks that look for security vulnerabilities.

Symantec ESM is installed with seven sample policies.

Baseline policies and best practice policies can be installed through LiveUpdate or downloaded and installed from the Internet or a CD.

Policies for application products are sold separately.

Implementing best practice policies

Symantec ESM best practice policies are configured to protect specific applications and/or operating systems from security vulnerabilities.

Operating system (OS) hardening policies incorporate Symantec security research based on ISO 17799 and other industry standards and best practices. OS policies can be used in place of the default policies.

OS policies are configured by Symantec with values, name lists, templates, and word files that apply to targeted operating systems. They use Security Update modules and templates to check OS patches, password settings, and other vulnerabilities on the operating system. They may also introduce new templates and word lists to examine conditions that are required by supported standards or regulations.

Maintenance-paying Symantec ESM customers can download OS Policies without charge through LiveUpdate or at the Symantec Security Response Web site, http://securityresponse.symantec.com.

Responding to incidents

Maintenance-paying Symantec ESM customers can download Response policies for specific security incidents such as Code Red 2 and Nimda without charge at the Symantec Security Response Web site, http://securityresponse.symantec.com.

Creating and editing your own policies

Creating and editing Symantec ESM policies requires Create New Policies and Modify Policy access rights. See “Assigning access rights to manager accounts” in your Symantec ESM 6.0 *Symantec Enterprise Security Manager 6.0 User’s Guide* or *Symantec Enterprise Security Manager 5.5 User Manual*.

You can create a new policy from scratch (add) or copy (duplicate) an existing policy. After creating a policy, edit it to add or delete modules that the policy runs when it executes.

Warning: The manager does not keep multiple copies of policies with the same names. If users on different consoles add different policies with the same names, the latest version of the new policy overwrites all prior versions.

To add a new policy

1. In the enterprise tree, do one of the following:
   - Right-click a manager, then click **New** > **Policy**.
   - Right-click **Policies**, then click **New Policy**.
2. Type a new policy name of not more than 31 characters.
3. Press **Enter**.

To duplicate a policy

1 In the enterprise tree, right-click a policy, then click **Duplicate**.

2 Type a new policy name of not more than 31 characters.

3 Press **Enter**.

To edit a policy

1 In the enterprise tree, double-click the policy that you want to edit.

2 Edit the name lists:

- In the Available Modules list, click a module that you want to add to the policy, then click the left arrow.
- In the Current Modules list, click a module that you want to remove from the policy, then click the right arrow.

3 Click **OK**.

To rename a policy

1 In the enterprise tree, right-click a policy, then click **Rename**.

2 Type a new policy name of no more than 31 characters.

3 Press **Enter**.

To delete a policy

- In the enterprise tree, right-click the policy, then click **Delete**.
  The manager must have the Modify Policy access right.
  You cannot delete a policy when more than one Symantec ESM Enterprise Console is connected to the manager.
  To delete report files that are associated with the policy, delete the /reports/<policy> subdirectory in the manager's ESM folder.

Sample policies

Seven sample policies are shipped with Symantec ESM. After installing Symantec ESM, make copies of the sample policies, then rename and edit the copies to implement your company's security policy.

Phase policies

Five phase polices let you begin with the most basic security issues and resolve any weaknesses before proceeding to the next level of complexity.

The policies and their modules are:

- Phase 1 policy includes the following g modules:
  "Account Integrity" on page 47.
  "File Find" on page 75.
  "File Watch" on page 95.
  "Network Integrity" on page 122.
  "OS Patches" on page 166.
  "Password Strength" on page 174.
  "Password Strength" on page 174.
  "User Files" on page 214.
- Phase 2 includes all modules in Phase 1, with more security checks enabled, plus:
  "File Attributes" on page 67.
  "Login Parameters" on page 112.
  "Object Integrity" on page 163.
  "System Mail" on page 209.
  "System Queues" on page 212.

Phase 3 policies let you apply different standards to various networks or computers, such as Relaxed for development or testing, Cautious for production, and Strict for sensitive areas such as finance or strategic planning.

- Phase 3:a Relaxed includes all modules in Phase 2, with more security checks enabled.
- Phase 3:b Cautious includes all modules in Phase 3:a, with more security checks enabled.
- Phase 3:c Strict includes all modules in Phase 3:b, with more security checks enabled.

Queries policy

The Queries policy reports account information and file permissions. Two modules—File Watch and User Files—are used in both Phase and Queries policies. Queries policy modules are described in:

- "Discovery" on page 62.
- "File Access" on page 66.
- "File Find" on page 75
- "File Watch" on page 95
- "User Files" on page 214

Dynamic Assessment policy

The Dynamic Assessment policy integrates your customized scripts and programs with Symantec ESM. It uses the Integrated Command Engine (ICE). See "Integrated Command Engine (ICE)" on page 225.

Copying and moving policies

Copying policies ensures that policies are identical on multiple managers.

Moving policies removes a policy from one manager and adds it to another, overwriting any policy-related information on the destination manager.

Copying and moving policies requires the Create New Policies access right. See "Assigning access rights to manager accounts" in the Symantec ESM 6.0 *User's Guide* or 5.5 *User Manual*.

To copy a policy to another manager

- In the enterprise tree, drag and drop a policy on a destination manager.
  You can also right-click a policy, drag and drop it on a destination manager, then click **Copy**.

To move a policy

1. In the enterprise tree, drag the source manager policy and drop it on the destination manager.
2. Click **Move**.

Running policies

To run a policy

- In the enterprise tree, do one of the following:
  - Drag and drop your policy on the agent or domain.
  - Drag and drop your agent or domain on the policy.

Demonstrating security checks

Before you apply a new security check to your systems, create a demo policy and add the check to it. Then verify the check on a representative computer. By using a demo policy, you can obtain results without disturbing the settings of policies that are created and named by the Symantec Security Response team.

Delete the demo policy after you complete your demonstrations.

Reviewing modules

A module is a set of security checks and options that looks for security vulnerabilities and reports messages in the console grid.

Enabling and disabling security checks

Only enabled security checks provide information when you run a module.

To enable and disable checks

1. In the enterprise tree, expand the Policies branch.
2. Expand a module branch.
3. Do one of the following:
   - Double-click the UNIX icon.
   - Right-click the UNIX icon, then click **Properties**.
4. Do one of the following:
   - Check to enable.
   - Uncheck to disable.

Specifying options

You control the behavior of security checks by specifying options. For example, in the Users to check option of the Password Strength module, you specify which users and groups you want the checks to examine or skip. This option is permanently enabled, as indicated by the dot in the box.

Other options, such as Local disks only and Local accounts only can be checked or unchecked to turn them on or off.

To display option items, click Users to check on the left side of the window. In the two name list panels, specify the users and groups to include or exclude when you run the module. When applicable, check one of the boxes to define whether entries will be included or excluded.

Name lists are the most common items that are available for editing in options. Other items include check boxes to turn an option on or off, and text string values, where you can specify parameters such as the minimum number of non-alphabetic characters that are required in a password.

A description of the option is displayed in the upper right area of the module editing window.

Editing name lists

Use name lists to specify items that are included or excluded by all or some of the security checks in a module.

Type	Contents
Users	User accounts, such as user1 and user2
Groups	User account groups such as system operators and administrators
Files/Directories	Files or directories such as /etc/passwd or /var/spool/mail
Enabled/Disabled word files	Word files containing groups of words
Enabled/Disabled Template	Template files
Key (word)	Sets of keys or keywords
Generic strings	Sets of generic character strings

Some name list panes contain:

- New, Delete, Move Up, and Move Down buttons
- List area
- Include and Exclude icon buttons

To add an item to a name list

1. Click **New**.
2. Type the item name.
   You can use the asterisk (*) character as a wildcard character to represent a set of items. For example, /usr/myapp/* specifies all files in the /usr/myapp directory.
   To add another item, press **Enter**, then repeat steps 1–2.
3. Click **Include** or **Exclude** to indicate whether to examine or skip the listed items.
4. Click **OK**.

To remove an item from a name list

1. Click the item.
2. Click **Delete**.
3. Click **OK**.

To move an item up or down in a name list

1 Click the item.

2 Click **Move Up** or **Move Down**.

3 Click **OK**.

Users and Groups name list precedence

When a module or security check contains Users and Groups name lists, the names in the Groups list are processed first. Then, within each selected group, names in the Users list are processed.

The following table summarizes the results that you can expect from name lists that include or exclude Users and/or Groups entries:

If the check	And the users list	And the groups list	Then the check reports
Includes a users or groups name list	contains user entries	is blank	Data for all reported users
Includes a users or groups name list	is blank	contains group entries	Data for all reported groups and users that are in them
Excludes a users or groups name list	contains user entries	is blank	Data for all groups and users except the reported users
Excludes a users or groups name list	is blank	contains group entries	Data for all groups except the reported groups and users that are in them
Includes or excludes blank name lists	is blank	is blank	Data for all groups and users

Some modules have Users to check options with name lists that are used by more than one security check. Some of the security checks that use the Users to check name lists also have their own name lists.

When a security check uses two Users and Groups name lists, the combined contents of the name lists are processed as follows:

If the Users to check option	And the check name lists	Then the check reports
Includes user or group entries	Include user or group entries	Data about all groups and their users, and all users, in both user lists

If the Users to check option	And the check name lists	Then the check reports
Includes user or group entries	Exclude user or group entries	Nothing about groups and users in the check name lists (exclude entries override include entries)
Excludes user or group entries	Include user or group entries	Nothing about groups and users in Users to check name lists (exclude entries override include entries).
Excludes user or group entries	Exclude user or group entries	Nothing about groups and users that are in the name lists
Includes or excludes blank name lists	Include or exclude blank name lists	Data for all groups and users

Creating and editing templates

A template is a file that contains module control directives and definitions of objects with their expected states.

The Integrated Command Engine (ICE) and the following UNIX modules use templates:

- Account Integrity
  See "Editing the Shells template" on page 59.
- File Attributes
  See "Editing the New File template" on page 69.
- File Find
  See "Creating the File Content Search template" on page 85.
- File Watch
  See "Editing the File Watch template" on page 96.
  See "Using the Malicious File Watch template" on page 102.
  See "Editing the Malicious File Watch template" on page 103.
  See "Editing the File Signatures template" on page 109.
- Network Integrity
  See "Editing the Netgroup Info template" on page 150.
- OS Patches
  See "Editing the Patch template" on page 193.
- Startup Files
  See "Editing the Services template" on page 195.

- System Auditing
  See “Editing the Events template” on page 203.
- See “Editing the Event Maps template” on page 206.

Creating a template

To create a template

1. In the enterprise tree, right-click **Templates**, then click **New**.
2. Select an available template type.
3. Type a name for the template without a file extension. Symantec ESM provides the extension based on the template type that you select.
4. Click **OK**.
   Your new template will be listed in the Templates branch of the console with other template files that use the same file extension.

Editing template rows

If you edit templates that are shipped with Symantec ESM, your changes will be overwritten by the next Security Update. To avoid this problem, create and edit your own templates.

To edit a template, open it in the Template Editor, add and delete rows, and specify the contents of row fields.

To open a template in the Template Editor

1. In the enterprise tree, expand the Templates branch.
2. Double-click the template that you want to open.

The Template Editor organizes templates into rows and columns. Each row describes a single file, patch, or other item. Columns contain the information that Symantec ESM attempts to match with agent settings.

To add a template row

1. Open a template in the Template Editor, then click **Add Row**.
2. Specify row information, including any sublist information needed .
3. Click **OK** to save the row.
4. Click **Close** to exit the Template Editor.

To remove one or more rows

1 In the Template Editor or Sublist Editor, click the leftmost, numbered button of the row that you want to remove.
   - For a range of rows, hold down the Shift key while you click the first and last row numbers.
   - For multiple non-sequential rows, hold down the Ctrl key while you click the row numbers.
2 Click **Remove Rows**.
3 Click **Save**.
4 Click **Close** to exit the editor.

Editing template fields

In the Template Editor, you can:

- Change the contents of a string or numeric field.
  String fields can contain free-form text such as Directory/File Name, User, Group, and Permissions fields in the New File template.
  Numeric fields can store positive or negative integers or real (floating point) numbers. The Severity field in the Patch template is an example of a numeric field.
- Check or uncheck a check box.
  Some fields have check boxes that you can check to direct the module to examine specified items, such as the New and Removed check boxes in the File Watch template.
- Select a context menu item.
  Some fields have context menus that are displayed when you click a field, such as Signature fields in File and File Watch templates and Signature Type fields in File Signatures templates.
- Edit a sublist.
  Some fields contain sublists. Sublist fields display the number of items in the sublist (initially, 0). Examples include the OS/Rev columns in New File and ICE templates. C
  Click a numbered sublist button (not a row number) to access the Template Sublist Editor.
  Clicking a sublist button opens the Template Sublist Editor.
  Edit sublist rows in the Template Sublist Editor the same way that you edit template rows in the Template Editor.

Reviewing messages

Messages consist of:

- A message name, in all caps. Message names link Symantec ESM code to the text of the message title and must not be changed. Message names appear only in .m files.
- A message title, in upper and lower case, that is displayed in the console grid. You can edit message titles in .m files. See "Editing messages" on page 43.
- Message text, in upper and lower text, that is displayed in a separate window of the summary report when you "mouse-over" the Message field in the console grid. You can edit message text in .m files. See "Editing messages" on page 43.
- Class (0–4). Class 0 displays a green message (no action needed), classes 1–3 display yellow messages (needs attention), and class 4 displays a red message (needs immediate attention).
- Some messages display a code in the Updateable/Correctable field of the console grid that identifies the message as template-updateable (TU) or snapshot-updateable (SU). You can click the code to update the template or snapshot file to match the current agent settings. See "Updating template and snapshot files in messages" on page 42.
- Some messages also display a code in the Updateable/Correctable field that identifies the message as correctable (C). You can click the code to reverse agent settings or disable a vulnerable account. See "Correcting agents in messages" on page 42.

Most messages are reported in the console grid, though some common messages are reported in a separate window.

Reporting duplicate records

Records with identical content are reported in a single message. This eliminates repetition of identical messages.

Reviewing message types

Symantec ESM reports three types of messages:

- Common messages, available to all modules, report Symantec ESM operational information such as Correction succeeded, Disk write error, etc.
- Correctable messages can be used to reverse current agent settings.

- Updateable messages can be used to change template or snapshot settings to the current agent settings.
- Informative messages report administrative information such as lists of user accounts, or security vulnerabilities that require manual adjustments.

Reviewing common messages

Several messages that report system conditions are stored in the esm/register /<architecture>/common.m file. Some of these common messages are displayed in the console grid, others in separate windows.

The following messages can be generated by more than one module:

Message name	Title	Class
CANCELED	Module execution canceled by user	4
CHECK_NOT_ PERFORMED	Warning - check could not be performed	1
CORRECT_FAIL	Correction failed	0
CORRECT_SUCCEED	Correction succeeded	0
DISK_WRITE_FAIL	Disk write error	0
EOF	End of file	0
FEATURE_NOTSUP	Module feature not supported	0
HEADER	No problems found	0
NOMEM	Failed to allocate memory	4
NOTE	Note	0
SNAPSHOT_CREATED	Snapshot created	4
SYSERR	Unexpected system error	4
TEMPLATE_ITEM	Template item	0
TEMPLATE_SUBLIST	Template sublist item	0
TOOMANYERR	Too many report records, please correct problems and rerun	4
UPDATE_FAIL	Update failed	0
UPDATE_SUCCEED	Update succeeded	0

Correcting agents in messages

Correctable messages display a C in the Updateable/Correctable field of the console grid.

You can use the Correct feature to correct agent rights or settings. For example, in the Account Integrity module, the Generate security audits check reports accounts with rights to generate entries in the security log. If you correct a reported user account, the right is revoked. You can restore the right by repeating the same process that you used to revoke it.

You can also use the Correct feature to disable a vulnerable account. In the Password Strength module, for example, you can immediately disable a reported account that has no password.

To correct the agent reported in the console grid

1. In the console grid, right-click an item that contains C in the Updateable/Correctable field, then click **Correct**.
2. Type the name and password of a user that has the right to change the setting (usually a member of the Administrators security group).
3. Click **OK**.

To reverse a correction, use the same procedure except in step 1, right-click an item that contains Corrected in the Updateable/Correctable field, then click **Correct**.

Updating template and snapshot files in messages

Some modules use template files that specify authorized settings. When you run a module with enabled checks that examine these settings, discrepancies are reported with a TU code in the console grid.

Similarly, some modules use snapshot files that contain settings that were found the last time the module was run. (The snapshot file is created when you run the module for the first time. Changes are detected in subsequent policy or module runs.) Settings that do not match the snapshot file are reported with a SU code in the console grid.

To update a template or snapshot file in the console grid

1. Right-click **TU** (or **SU**) in the Updateable/Correctable field.
2. Click **Update Template** (or **Update Snapshot**).

Editing messages

Messages are contained in module initialization files, called .m (dot-m) files. The .m file of each module:

- Specifies security checks and options for the module.
- Associates the module with specified name lists.
- Contains a descriptive name for the module.
- Supplies default values for the module's security checks.
- Supplies message text that is reported in the console grid.

During agent registration, the current version of each .m file is stored in the manager database at esm/register/<operating system>/<module name>.m. You can specify the location of .m files on each agent.

.m files contain ASCII text. Some lines begin with directives—words that are preceded by a period (.)—that classify file information. Directives are usually followed by data and sometimes by descriptive text.

Messages begin with .begin directives, which always occurs after information about security checks, options, and templates. Do not delete or reorder any messages.

To edit messages

1. Select an agent with an operating system that reports messages that you want to edit.
2. Open the common.m file or <module>.m file in a text editor.
3. Edit the following directives as needed:

Directive	Description
.title	Brief description of a security problem, in quotation marks, not exceeding 79 characters. For example, .title “Maximum password age too high” The description is displayed in the console grid when the module is run.

Directive	Description
.class	Severity of the problem, 0–4. For example: .class 2 0 = Green message (no action required) 1 = Yellow message (deserves attention) 2 = Yellow message (deserves attention) 3 = Yellow message (deserves attention) 4 = Red message (deserves immediate attention)
.text	Explanation of the problem. Lines of text cannot exceed 128 characters, and the total explanation cannot exceed 1023 characters. Begin text on the line after the .text directive. Include: ■ Nature of the problem. ■ Why it is a security risk. ■ How to remedy the problem. The .endtext directive should occur on a line by itself after the text (required even if you omit an explanation). For example, .text The maximum password age is set too high. Infrequent password changes allow anyone with a stolen password long term access to your system. Set the maximum password age to 60 days. .endtext **Note:** Do not begin a line of text with a period. This character is used as a control delimiter and improper usage causes the module to fail.

4 Change the .customized directive value of each modified message to 1.
This prevents the edited message from being overwritten when the module is updated to a later version.

5 Increment the module version number in the .module directive by 1. In the following example, 1300 was the last version number:
.module “Account Integrity” account 1301 UNIX

6 Save the edited .m file.

7 Re-register the module with appropriate managers.

8 Verify that the modified messages appear in the message.dat file in the default location on the manager computers.

System	Directory
UNIX	Symantec ESM creates a symbolic link: /esm/system/<system name>/db/message.dat

Chapter 4

Modules

Account Integrity

The Account Integrity module reports new, changed, and deleted accounts, user rights, and vulnerabilities of account names and rights.

Updateable Account Integrity messages

The UNIX Account Integrity module has six security checks that report snapshot-updateable messages. These messages let you update records in the sifuser.dat and sifgroup.dat snapshot files to match current values on the agent.

Snapshot-updateable messages display SU in the Updateable/Correctable column of the console grid.

Note: You must run the Account Integrity module one time to create baseline user and group snapshot files on an agent before you rerun the module to detect agent account changes

---

Security check	Message name
New Accounts	NEWUSER
Deleted Accounts	DELUSER
Changed Accounts	CHGUSER
New Groups	NEWGROUP
Deleted Groups	DELGROUP
Changed Groups	CHGGROUP

Users to check

Use this option to specify users and groups that are excluded or included for all Account Integrity checks that use this option. See “Editing name lists” on page 35.

This option is not used by security checks that are listed under the header, Options always checked for all accounts and groups.

Illegal login shells

This security check reports user accounts that do not have a shell and accounts with login shells that are not listed in the /etc/shells file. On AIX computers, the check reports accounts with shells that are not listed in the /etc/security/login.cfg file.

Note: This check is not supported on NCR, Irix, or Sequent operating systems.

The check includes its own Users/Groups name list, which you can use to exclude user accounts that are not already excluded by the Users to check option.

The check returns the following messages:

Message name	Title	Class
NOETCSHELL	/etc/shells does not exist	1
NOLOGIN_CFG	/etc/security/login.cfg does not exist	1
NOSHELLS	Shells stanza missing in login.cfg	1
NOTASHELL	Shell not in /etc/shells	1
NOTASHELL_AIX	Shell not in /etc/security/login.cfg	1

Nonexistent login shells

This security check reports user accounts with login shells that do not exist on the agent.

The check includes its own Users/Groups name list, which you can use to exclude user accounts that are not already excluded by the Users to check option.

The check returns the following message:

Message name	Title	Class
NONEXISTSHELL	Non-existent shell	0

Non-executable login shells

This security check reports user accounts with login shells that are not executable.

The check includes its own Users/Groups name list, which you can use to exclude user accounts that are not already excluded by the Users to check option.

The check returns the following message:

Message name	Title	Class
NONEXECSHELL	Non-executable shell	0

Setuid login shells

This security check reports user accounts with login shells that have setuid privileges.

The check includes its own Users/Groups name list, which you can use to exclude user accounts that are not already excluded by the Users to check option.

Files that set the user ID (UID) of the user account that is executing the files to the UID of the file owner may provide unauthorized access to other files on your computers.

The check returns the following message:

Message name	Title	Class
SETUIDSHELL	Setuid shell	4

Setgid login shells

This security check reports user accounts with login shells that have setgid privileges.

The check includes its own Users/Groups name list, which you can use to exclude user accounts that are not already excluded by the Users to check option.

Files that set the group ID (GID) of the user account that is executing the files to the GID of the file owner may provide unauthorized access to other files on your computers.

The check returns the following message:

Message name	Title	Class
SETGIDSHELL	Setgid shell	4

Login shell owners

This security check reports user accounts with login shells that are not owned by root or bin.

The check includes its own Users/Groups name list, which you can use to exclude user accounts that are not already excluded by the Users to check option.

The check returns the following message:

Message name	Title	Class
SHELL_OWNER	Shell owner	0

Login shell permissions

This security check reports user accounts with login shells that have group or world write permissions.

The check includes its own Users/Groups name list, which you can use to exclude user accounts that are not already excluded by the Users to check option.

The check examines only the basic user/group/other and read/write/execute UNIX file permissions. The check does not consider any extended permissions such as access control lists (ACLs), which are available on some UNIX operating systems and through some third-party extensions.

The check returns the following message:

Message name	Title	Class
WRITABLE_SHELL	Writable shell	0

Home directories

This security check reports user accounts that do not have home directories and home directories that do not have correct user or group ownership.

The check includes its own Users/Groups name list, which can be used to exclude user accounts that are not excluded by the Users to check option.

The check returns the following messages:

Message name	Title	Class
NOHOME	Home directory does not exist	0
HOMENOTDIR	Not a directory	0
HOMEUID	UID of home directory is incorrect	1
HOMEGID	GID of home directory is incorrect	1

List of users

This security check generates a list of users that are checked by the Account Integrity module. The UID, GID, comment field, home directory, and shell are shown for each user.

The check returns the following message:

Message name	Title	Class
SHOW	Show user	0

Group IDs

This security check reports user accounts that do not have a group ID (GID) that is listed in the /etc/group file.

The check returns the following message:

Message name	Title	Class
NOGROUP	No such group	0

Local disks only

Enable this option to restrict module checks to users whose home directories reside on the agent's local disks. This ensures that even when NFS is deployed, users are examined only once.

The option does not affect security checks that are listed under the Options always checked for all accounts and groups header.

Note: On AIX operating systems, remote mount points on NFS, AFS, or DFS file systems are not examined. On Solaris and HP-UX, remote mount points on AFS and NFS are not examined.

Local accounts only

Enable this option to restrict module checks to user accounts that are defined in the agent's /etc/passwd file. This ensures that even when NIS is deployed, users are examined only once.

The option does not affect security checks that are listed under the Options always checked for all accounts and groups header.

Options always checked for all accounts and groups

The Users to check and Local disks only options do not apply to the security checks under this header. These checks include all user and group accounts in the agent's /etc/passwd and /etc/group files.

Home directory permissions

This security check reports users with home directory permissions that are less restrictive than the value that you specify in the check. Use three-digit octal numbers. The default value is 750.

Use the Users/Groups name list to specify user accounts that are to be excluded or included for the check (the Users to check option does not apply).

The check returns the following message:

Message name	Title	Class
HOMEDIRPERMISSION	Home directory permissions	0

New accounts

This security check reports accounts in the /etc/passwd file that were added after the last time the user snapshot update.

The check returns the following message:

Message name	Title	Class
NEWUSER	New user account	1

To protect your computers

- For authorized new accounts, update the snapshot.
- Delete unauthorized accounts.

Deleted accounts

This security check reports accounts in the /etc/passwd file that were deleted after the last snapshot update.

The check returns the following message:

Message name	Title	Class
DELUSER	Deleted user account	0

To protect your computers

- For authorized deletions, update the snapshot.
- Restore unauthorized deletions.

Changed accounts

This security check reports accounts in the /etc/passwd file that changed after the last snapshot update.

The check returns the following message:

Message name	Title	Class
CHGUSER	Changed user account	1

To protect your computers

- For authorized changes, update the snapshot.
- For authorized changes, restore the previous settings.

New groups

This security check reports any groups that have been added since the last time the group snapshot was updated. The security check looks at group accounts that are listed in the /etc/group file.

If these groups were not added by the system administrator, they may represent a security breach.

The check returns the following message:

Message name	Title	Class
NEWGROUP	New system group	1

To protect your computers

- Review all new group accounts to verify that they should have been added, and update the snapshot if appropriate.

Deleted groups

This security check reports any groups that have been deleted since the last time the group snapshot was updated. The security check looks at group accounts that are listed in the /etc/group file.

If the reported groups were not deleted by the system administrator, they may represent a security breach.

The check returns the following message:

Message name	Title	Class
DELGROUP	Deleted system groups	0

To protect your computers

- Review all named accounts to verify that they should have been deleted, and update the snapshot if appropriate.

Changed groups

This security check reports any groups that have been changed since the last time the group snapshot was updated. The security check looks at group accounts that are listed in the /etc/group file.

If reported group changes were not made by the system administrator, they may represent a security breach.

The check returns the following message:

Message name	Title	Class
CHGGROUP	Changed system group	1

To protect your computers

- Review all account changes to verify that they were authorized, and update the snapshot if appropriate.

Duplicate IDs

This security check reports user IDs (UIDs) that are shared by two or more accounts and group IDs (GIDs) that are shared by two or more groups. The security check looks at entries in /etc/passwd and /etc/group files.

User and group accounts that share IDs have access to each other's files. This right should be granted with care to prevent a security breach.

The check returns the following messages:

Message name	Title	Class
DUPUID	Duplicate UID	0
DUPGID	Duplicate GID	0

To protect your computers

- Change the user ID or group ID for each named account to a unique number and change file ownerships to match the new IDs.

Privileged users and groups

This security check reports users and groups with UIDs or GIDs that give them super-user privileges or privileged access to system files. The security check looks at /etc/passwd and /etc/group file entries.

Privileged users and groups that are part of the standard operating system distribution are not reported. Use the check's Users/Groups name lists to exclude or include users and groups for the security check.

The check returns the following messages:

Message name	Title	Class
GRPKERNPRIV	Group has kernel capabilities	0

Message name	Title	Class
PRIVUID	Privileged user	4
PRIVGID	Privileged group	4
SHUTDOWN_ PRIV	User has shutdown privileges	0
SHUTDOWN_ ANY_USER	Any user has shutdown privileges from these systems	1
SHUTDOWN_ ANY_SYS	User has shutdown privileges from any system	0
SHUTDOWN_ ANY_SYS_USER	Any user has shutdown privileges from any system	1

Excessive number of accounts

This security check reports a problem when the number of accounts that is listed in the /etc/passwd file is greater than the maximum number that you specify in your policy. The default policy setting for the maximum value is three accounts.

The check is intended for agents such as Web servers, where an excessive number of accounts can be a security risk.

The check returns the following message:

Message name	Title	Class
TOO_MANY_ ACCOUNTS	Too many accounts	1

To protect your computers

- Limit the number of accounts on named computers to the minimum number required for them to accomplish their purposes.

Disabled accounts

This security check examines login shells and passwords to identify user accounts that are disabled. The security check uses the following default list of disabling login shells: /bin/true, /bin/false, /dev/null, true, and false.

For this check, Red Hat Linux operating systems must be configured to use the shadow password file.

Use the check's name list to specify user accounts for the check. If you simultaneously enable the Accounts should be disabled check, the Disabled

accounts check automatically excludes the user accounts that are included in the Accounts should be disabled check.

The check returns the following message:

Message name	Title	Class
DISABLED	Account disabled	0

Accounts should be disabled

This security check examines login shells and passwords to identify and report user accounts that should be, but are not, disabled. The security check uses the following default list of disabling login shells: /bin/true, /bin/false, /dev/null, true, and false.

For this check, Red Hat Linux operating systems must be configured to use the shadow password file.

Use the check's name list to include users such as bin and adm in the check. If you simultaneously enable the Disabled accounts check, the Accounts should be disabled check automatically excludes the user accounts that are included in the disabled accounts check

The check returns the following message:

Message name	Title	Class
NOT_DISABLED	Account not disabled	1

Remote-only accounts

This security check examines login shells and passwords to identify user accounts that do have disabling passwords but do not have disabling shells and non-empty .rhosts files in their home directories.

For this check, Red Hat Linux operating systems must be configured to use the shadow password file.

The reported accounts can be accessed by remote login commands such as rsh, rlogin, rfcp, and rcp. Use the check's name list to exclude or include accounts for the check.

The default list of disabling shells includes /bin/true, /bin/false, /dev/null, true, and false.

The check returns the following message:

Message name	Title	Class
REMOTEONLY	Account is disabled but available remotely	1

Password in /etc/passwd

This security check reports user accounts that have passwords in the /etc/passwd file when the computer is using or has access to shadow files or enhanced security files.

Use the Users/Groups name lists to exclude users from the check. This check does not use the Users to check option.

The check returns the following messages:

Message name	Title	Class
PASSEXISTED	Password existed	0
CHECK_NOT_ PERFORMED	Warning: check could not be performed	1

Disallowed home directory

This security check reports user accounts that are using disallowed directories as their home directories. It examines accounts that are listed in the /etc/passwd file. Use the directory list to specify disallowed directories for the check. The default directory list excludes /, /etc, and /usr/bin.

Use the Disallowed home directory (cont'd) option to specify users that are excluded or included for this check. The check does not use the Users to check option.

The check returns the following message:

Message name	Title	Class
USINGHOMEDIR	Disallowed home directory	0

Disallowed home directory (cont'd)

Use this option to specify users that are excluded or included for the Disallowed home directory check. The default name list excludes the daemon, sys, bin, and nobody accounts.

/etc/passwd syntax

This security check looks at the /etc/passwd file and reports users with entries that include syntax errors.

Use the check's Users/Groups name lists to exclude users from the check. This check does not use the Users to check option.

The check returns the following message:

Message name	Title	Class
PASSSYNTAX	/etc/passwd syntax error	0

General information field required

When this option is enabled, the /etc/passwd syntax check reports users with incomplete or invalid entries in the GECOS field in the /etc/passwd file. Enable the /etc/passwd syntax check before selecting this option.

User shell compliance

This security check reports user accounts that are using login shells that are not defined in the Shells template.

Use the check's file list to enable or disable the Shells template files that are used by this check. This check does not use the Users to check option.

Note: Make sure you do not enable the default.shc template file before you add netgroup records to that template. If you use the blank default template, the check returns the common message, No problems found.

The check returns the following message:

Message name	Title	Class
NO_SHELLCOMPLIANCE	Shell compliance	0

Editing the Shells template

The User shell compliance security check uses the Shells template to specify authorized login shells for specified users on specified host computers.

If your system has been upgraded and includes the blank default template Shells-all (default.shc), you can open and edit it. Otherwise, create and edit a new Shells template.

To create the Shells template

1. In the enterprise tree, right-click **Templates**, then click **New**.
2. Select **Shells-all**.
3. Type a new template file name with no more than eight characters and no file extension. Symantec ESM adds a .shc file extension.
4. Click **OK** to open the new template in the Template Editor.
5. Add template records that define the authorized login shells on your computers.
6. Click **Save**.
7. Click **Close** to exit the Template Editor.

To add a record to the Shells template

1. In the Template Editor, click **Add Row**.
2. In the User Name field, replace <NEW> with the user name. To specify all users, type an asterisk (*).
3. In the Host Name field, replace <NEW> with the computer name. To specify all hosts, type an asterisk (*).
4. In the Shell field, replace <NEW> with a path name that begins with the /root directory, such as /usr/bin/sh.
5. Click the sublist button in the Additional Shells field to open the Template Sublist Editor and define additional authorized login shells for the user and host that are specified on the same template row.

To add Additional Shells sublist rows

1. In the Template Editor, click the sublist button in the Additional Shells field of the row that you are editing. The button displays the number of line rows in the sublist. Initially, the number is 0.
2. In the Template Sublist Editor, click **Add Row**.
3. In the Shell field, replace <NEW> with the path name of an additional, authorized login shell. Specify a path name that begins with the / root directory, such as /usr/bin/sh.
4. Click **Apply**, then repeat steps 2–4 to add additional sublist rows.

To remove Additional Shells sublist rows

1. In the Template Sublist Editor, click the leftmost, numbered button on the row that you want to remove.

To select a range of rows, hold down the **Shift** key while you click the numbered buttons on the first and last rows that you want to remove.

To select non-sequential rows, hold down the **Ctrl** key while you click the numbered buttons on each of the rows that you want to remove.

2 Click **Remove Row(s)**.

3 Click **Apply**.

4 Click **Close** to exit the Template Sublist Editor and return to the Template Editor.

To remove Shells template records

1 In the Template Editor, click the leftmost, numbered button on the row that you want to remove.

To select a range of rows, hold down the **Shift** key while you click the first and last row numbers.

To select non-sequential rows, hold down the **Ctrl** key while you click the row numbers.

2 In the Template Editor, click **Remove Row(s)**.

3 Click **Save**.

4 Click **Close** to exit the Template Editor.

Accounts can be locked

This security check reports user accounts that can be locked due to consecutive unsuccessful login attempts because the maximum number of retry failures is not set to 0. This check is intended only for privileged system accounts such as root.

Note: This security check is supported only on AIX, HP-UX, and Digital UNIX/ Tru64 computers.

Use check name lists to specify system accounts that are to be examined by this check. The check does not use the Users to check option.

The check returns the following message:

Message name	Title	Class
ACCOUNT_ LOCKED_OUT	Accounts can be locked out	0

Discovery

The Discovery module reports computers that could run Symantec ESM or Symantec Intruder Alert but are not running them. The Discovery module is in the Queries policy.

Using wildcard characters

Standard wildcard usage is supported in four Discovery checks.

See "Setuid files" on page 78, "Setgid files" on page 78, "Device files not in /dev" on page 82, and "Unowned directories/files" on page 84.

Use the * character to substitute for any number of ASCII characters in a string. Use the ? character to substitute for any one ASCII character in a string.

Wildcards used as partial file or directory names such as fil*.bat and *.* are accepted.

Wildcard characters are used differently to specify IP addresses.

See "Targets" on page 64.

In addition to the Discovery module, standard wildcard usage is supported in:

- Name lists throughout Symantec ESM
  See "To add an item to a name list" on page 35.
- Services template
  See "Editing the Services template" on page 195.

Symantec ESM device status

This check examines specified TCP ports on targeted devices and reports devices that are not running Symantec ESM. To report computers that could run Symantec ESM but are not, enable Profile candidate devices. To report computers that are running Symantec ESM, enable Report if found.

In check name lists, specify TCP port numbers to be examined.

- If agents run the current version of Symantec ESM but do not use the current default port number, change the port number in the name list.
- Agents running previous versions of Symantec ESM may use different port numbers. For these port numbers, see Appendix A in the *Symantec ESM 6.0 Installation Guide* or Appendix B in the *Symantec ESM 5.5 Installation and Getting Started Guide*.

The check returns the following messages, depending on which options are enabled:

Message name	Title	Class
ESM_CANDIDATE	ESM candidate	2
ESM_FOUND	ESM found	0
INV_ADDRQUAL	Invalid address qualifier	2
NOT_ESM_CANDIDATE	Non-ESM candidate	0
TIMED_OUT	Timed out while profiling	0

Note: Security measures can prevent identification of remote operating systems, which can cause Non-ESM candidate to be erroneously reported.

Symantec Intruder Alert device status

This check examines specified TCP ports on targeted devices and reports devices that are not running Symantec Intruder Alert. To report computers that could run Symantec Intruder Alert but are not, enable Profile candidate devices. To report computers that are running Symantec Intruder Alert, enable Report if found.

The check returns the following messages, depending on which options are enabled:

Message name	Title	Class
ITA_CANDIDATE	ITA candidate	2
ITA_FOUND	ITA found	0
INV_ADDRQUAL	Invalid address qualifier	2
NOT_ITA_CANDIDATE	Non-ITA candidate	0
TIMED_OUT	Timed out while profiling	0

Note: Security measures can prevent identification of remote operating systems, which can cause Non-ESM candidate to be erroneously reported.

Report if found

Enable this option to have the Symantec ESM device status and Symantec Intruder Alert device status report computers that are running the programs.

Profile candidate devices

Enable this option to identify agents that could run Symantec ESM and Symantec Intruder Alert but are not. Disable the option to report only systems currently running these products. When the option is disabled, all devices that are not running these products are reported as non-candidates.

This is a time consuming option. Though it does not tax CPU usage, profiling can take several minutes per IP address. Profiling examines the following ports to determine the type of network device: tcpmux 1, echo 7, discard 9, systat 11, daytime 13, netstat 15, quote 17, ttytst 19, ftp 21, telnet 23, smtp 25, time 37, domain 53, finger 79, http 80, pop-2 109, pop-3 110, rpcbind 111, loc-srv 135, netbios-ssn 139, exec 512, login 513, shell 514, printer 515, uucp 540, and x-server 6000.

Targets

Use this option to specify the target TCP addresses to be scanned. Each target address has four parts with periods separating the parts, and can represent one or more IP addresses. Each part consists of a number between 1 and 254, a range of numbers, or a wildcard character (* or ?). A range of numbers is specified as n-m where n is the lower limit and m is the upper limit. If the lower limit is not specified (for example, -127), 1 is used. If the upper limit is not specified (for example, 17-), 254 is used.

A * represents the range of numbers 1-254. A ? represents the matching part of the agent's IP address. These numbers, ranges of numbers, and wildcard characters can be used in combinations to specify complex sets of IP addresses. For example, if the range 172.17.10-20.* is specified, the addresses 172.17.10.1, ..., 172.17.10.254, 172.17.11.1, ..., 172.17.11.254, ..., 172.17.20.254 are scanned. The range of IP addresses an agent can scan is limited based on the Class of the agent's IP address.

Note: This option must be enabled to obtain an accurate report of Symantec ESM or Symantec Intruder Alert candidates from TCP port checks. Otherwise, all computers are reported as non-candidates.

When the option is enabled, IP addresses for the following TCP ports are examined:.

Service	Port	Service	Port	Service	Port
tcpmux	1	echo	7	discard	9
systat	11	daytime	13	netstat	15
quote	17	ttytst	19	ftp	21
telnet	23	smtp	25	time	37
domain	53	finger	79	http	80
pop-2	109	pop-3	110	rpcbind	111
loc-srv	135	netbios-ssn	139	exec	512
login	513	shell	514	printer	515
uucp	540	x-server	6000		

Profile timeout

Use this option to specify the maximum number of seconds that a module spends profiling a candidate system before aborting and going to the next address. The timeout value cannot be less than 15 seconds or greater than 900 seconds (15 minutes).

Scan non-responding addresses

Enable this option to scan all specified TCP addresses including those that do not respond to a ping. The time required to complete the scan will be greatly increased.

File Access

The File Access module examines read, write, and execute permissions on specified files and access control lists (ACLs) on AIX and HP-UX operating systems. It is in the Queries policy.

Files to check

Use this option to specify files that are to be included in File Access checks.

Users to check

Use this option to specify the users and user groups that are examined by the File Access module. See “Editing name lists” on page 35.

Read permission

This security check reports user accounts that have read access to files that are specified by the Files to check option. Use the Users to check option to specify users and user groups that are to be examined.

The security check returns the following messages:

Message name	Title	Class
FILEEXPOSE	User file access	0
NOEXPOSE	No user file access	0

Write permission

This security check reports user accounts that have write access to files that are specified by the Files to check option. Use the Users to check option to specify users and user groups that are examined.

The check returns the same messages as the Read permission check.

Execute permission

This security check reports user accounts that have execute privileges for files that are specified by the Files to check option. Use the Users to check option to specify users and user groups to examine.

The check returns the same messages as the Read permission check.

File Attributes

The File Attributes module reports changes in system file attributes including file ownership, permissions, size, and creation and modification times.

Common File Attributes messages

The File Attributes module can generate any of the following messages after it checks enabled template files and before it runs enabled security checks.

Message name	Title	Class
NOTEMPLATES	No template files specified	1
NOEXIST	Mandatory file does not exist	4
FORBID	Forbidden file exists	4
NOEXISTWC	Mandatory wild card entry	0
FORBIDWC	Forbidden wild card file exists	4
ITEMCOUNT	Number of matched templates and items	0

Updateable snapshot files and templates

Seven of the module's security checks report messages that let you update snapshots or templates to match current values for the agent.

In the Updateable/Correctable column of the console grid, snapshot-updateable messages display the letters SU. Template-updateable messages display the letters TU,

Security check	Code	Message name
Changed files (creation time)	SU	DIFFATTRIB
Changed files (modification time)	SU	DIFFATTRIB
Changed files (size)	SU	DIFFATTRIB
Changed files (signature)	SU	DIFFATTRIB
User ownership	TU	DIFFOWN
Group ownership	TU	DIFFOWN
Permissions	TU	DIFFPERM

Run the File Attributes module one time to create a baseline snapshot file on each agent before you rerun the module to detect changes.

Running CRC and MD5 signature checks on UNIX directories

Templates in the UNIX File Attributes module and the UNIX File Watch module let you select options that generate signatures on specified files and directories. This function is enabled on UNIX computers because directories are treated as files with a special format.

To generate a signature on a UNIX directory, the module opens the directory as if it were a regular file and reads the raw data it contains. There are some directories on UNIX computers, however, that cannot be read in this way. For example, directories that are mounted from a remote file system using NFS cannot be read as files. On some versions of UNIX, the /tmp directory and its subdirectories are also not readable as files.

When the module attempts to generate a file signature for a directory that cannot be read as a file, the result is the signature of an empty file (i.e., a CRC value of zero or an MD5 value of d41d8cd98f00b204e9800998ecf8427e.)

When the module generates a signature for a directory that can be read as a file, it is important to understand what the file contains. The contents are dependent on the type of file system.

The most common file systems store the names of the files contained in the directory along with the files' inode numbers, which specify their locations on the disk. Other information about the files that are contained in a directory (such as size, permissions, and modification times) are not stored in the directory file. In these file systems, the directory signature does not normally change unless a file is added, removed, or renamed in the directory.

Changing the contents of a file in a directory is usually not sufficient to change the signature of the directory.

Template files

Enable this option to enable or disable the New File template files that are to be used for File Attribute checks.

By default, all templates are enabled. Only enabled templates that apply to the operating systems of the agents that are being examined are used during a single policy run.

For messages that are generated regardless of which checks are enabled, see "Common File Attributes messages" on page 67.

Editing the New File template

The File Attributes module uses New File templates to define attributes of critical system files and directories.

Note: The New File template has replaced an earlier File template. The File template still appears in the Templates list for backwards compatibility. Do not use the File template.

Eight default templates are available for each supported operating system. The template file name extensions identify the operating system and revision. For example, template files for Solaris versions 2.6 and later are:

fileatt.sol

internet.sol

mail.sol

nfs.sol

objects.sol

queues.sol

sysstart.sol

uucp.sol

Template file name extensions for all supported operating systems are:

Operating system	Extension
AIX	..aix
HP-UX 10-11	..hpx
Irix	..sgi
OSF/1 (Digital UNIX)	..osf
Red Hat Linux	..li
Sequent	..sqt
Solaris 2.5	..so5
Solaris 2.6+	.s.ol

To add a New File template

1. In the enterprise tree, right-click **Templates**, then click **New**.
2. Select the type of template that you want to add (see the table above).
3. Type a new template name of no more than eight characters. Symantec ESM adds the file extension.
4. Press **Enter** or click **OK**.
5. Add one or more records as described below.
6. Click **Close**.

To add a record to a New File template

1. In the Template Editor, click **Add File**.
2. In the Add Items to Template dialog box, click the Agent name drop-down list and select the agent where the file is located.
3. In the Item name text box, type the path of the file on the agent.
4. Click **OK**.
5. Specify directory and file settings and, if needed for Solaris and HP-UX, OS/Rev sublist rows (see below).
6. Click **Save**.
7. Click **Close**.

To add a directory

1. In the Template Editor, click **Add Directory**.
2. In the agent name field, select an agent that has the directory.
3. In the Item to add text box, type the path of the directory on the agent.
4. Select the option that describes the level of subordinate directories and files that you want to load. Each level includes the files that are in that level.
5. Click **OK**.

To add a row to the OS/Rev sublist

1. In the Template Editor, click the OS/Rev field on the row that you are editing.
2. In the Template Sublist Editor, check the Exclude check box to exclude (or uncheck to include) the item for File Attributes checks.

3 Click the OS field, then select one of the following options:
- All (All platforms)
- UNIX (All UNIX platforms)
- NT (All WIN NT platforms)
- WIN2K (All WIN 2000 platforms)
- WINXP (All WIN XP platforms)
- WIN2K3 (All WIN 2003 platforms)
- aix-rs6k
- hpux-hppa
- irix-mips
- ncr-x86
- osf1-axp
- solaris-sparc
- sunos-sparc
- sequent-x86
- redhat-x86
- redhat-s390
- nt-ix86

4 In the Release/Revision field, replace <NEW> with a revision ID using the following conventions:

Option	Description
all	All releases and revisions of the specified operating system.
-2.5	A revision ID with a leading minus (-) sign: the specified revision and all previous revisions.
+2.6	A revision ID with a leading plus (+) sign: the specified revision and all later revisions.

5 Click **Apply**.

6 Click **Close**.

User ownership

This security check verifies proper user ownership of files, using values that are specified in templates.

To suppress reporting of ownership transfers between privileged users, enable the option, Allow any privileged user.

The security check returns the following messages:

Message name	Title	Class
DIFFOWN	Different file ownership	1
NOUSER	User in template does not exist	0

Group ownership

This security check verifies proper group ownership of files, using values specified in templates.

To suppress reporting of ownership transfers between privileged user groups, enable the option, Allow any privileged group.

The security check returns the following messages:

Message name	Title	Class
DIFFOWN	Different file ownership	1
NOGROUP	Group in template does not exist	0

Permissions

This security check verifies proper file permissions, using values that are specified in templates.

Note: The module examines only basic user/group/other and read/write/execute permissions. It does not consider extended permissions such as access control lists (ACLs).

The security check returns the following message:

Message name	Title	Class
DIFFPERM	Different file permissions	1

Changed files (creation time)

This security check verifies the creation times of files that have the Create Time option checked in their template records. File creation times are compared to values that are stored in the agent's snapshot file.

The security check returns the following message:

Message name	Title	Class
DIFFATTRIB	File attributes have changed	1

Changed files (modification time)

This security check compares modification times on files (that have the Modify Time option checked in their template records) with modification time values that are stored in the agent's snapshot file.

The security check returns the following message:

Message name	Title	Class
DIFFATTRIB	File attributes have changed	1

Changed files (size)

This security check compares file size on files (that have the File Size option checked in their template records) with file size values that are stored in the agent's snapshot file.

The security check returns the following message:

Message name	Title	Class
DIFFATTRIB	File attributes have changed	1

Changed files (signature)

This security check compares CRC, MD5, or CRC and MD5 signature checks on files (that have the CheckSum option checked in their template records) with CRC, MD5, or CRC and MD5 values stored in the agent's snapshot file.

Comparing file checksums is superior to comparing creation time, modification time, and file size because it is significantly more difficult for someone to change a checksum without detection.

See "Running CRC and MD5 signature checks on UNIX directories" on page 68.

The security check returns the following message:

Message name	Title	Class
DIFFATTRIB	File attributes have changed	1

Allow any privileged user

This option modifies the behavior of the User ownership check. When this option is enabled, the module allows any privileged user to own a file if the template specifies a privileged owner. Privileged users are users with low UID values (usually less than 20).

Usually, ownership of system files by any privileged user is acceptable. For example, if the template specifies user ownership by root and this option is enabled, the module allows ownership by any privileged user including root, bin, daemon, sys, or admin.

Use this option to accommodate variations in ownership between different versions or installations of the same operating system and still use the same templates.

Allow any privileged group

This option modifies the behavior of the Group ownership check. When this option is enabled, the module allows any privileged group to own a file if the template specifies a privileged group owner. Privileged groups are groups with low GID values.

Usually, ownership of system files by any privileged group is acceptable. For example, if the template specifies group ownership by root, then the module allows ownership by any privileged group including system, staff, bin, sys, or admin.

Use this option to accommodate variations in ownership between different versions or installations of the same operating system and still use the same templates.

Exclude decreased permissions

This option modifies the behavior of the Permissions check. When this option is enabled, only increases in file access permissions are reported. When this option is disabled, all changes to file permissions are reported.

Files not listed in template

This security check reports all files that are not found in enabled templates. This report can be very long. Use the check's name list to specify files that should not be reported by the check.

The security check returns the following message:

Message name	Title	Class
FILE_NOT_IN_ TEMPLATE	File/directory not in template	0

Local disks only

Enable this option to examine only file systems that are on local disks.

Ignore symbolic links

Enable this option to ignores symbolic links on a user directory tree (both to files and to directories). Most symbolic links point to files or directories on another file system and are often owned by a different UID or GID.

File Find

The File Find module examines certain file attributes and settings, uneven permissions, specified text strings, and unowned files.

Snapshot file

The File Find module creates and maintains the filefind.dat snapshot file to detect changes in setuid and setgid attributes.

You must run the File Find module one time to create a baseline snapshot file on an agent before you rerun the module to detect changes.

Six of this module's security checks report snapshot updateable or correctable messages.

Snapshot updateable messages let you update the snapshot file to match the agent's current values. These messages display the letters SU in the Updateable/Correctable column of the console grid.

Correctable messages let you correct file attributes on the agent. These messages display the letter C in the Updateable/Correctable column of the console grid.

Security check	Code	Message name
New setuid files	SU	SETIDNEW
New setuid files	SU	SETIDNOT
New setuid files	SU	SETIDDEL
New setgid files	SU	SETIDNEW
New setgid files	SU	SETIDNOT
New setgid files	SU	SETIDDEL
World writable directories without sticky bit	C	NOTSTICKY
World writable files	C	WWFILES
Group writable files	C	GWFILES
Uneven file permissions	C	UNEVEN

Starting directories

Use this option to specify starting directories and depth levels for File Find directory traversals.

To search a directory and all of its subdirectories

- In the file list, type the directory's full path name.

To search a directory and only some of its subdirectories

- In the file list, type the directory's full path name followed by a plus sign (+) and the number of levels that you want to search.
  For example, to search a directory and two levels of subdirectories and files under that directory, type **/usr/<directory_name>+2**

Note: The default starting directory in the file list of the Starting directories option is the / root directory. If the file list is empty, and you enable one or more File Find checks in addition to the File content search check, the module assumes that the starting point for creating a snapshot and executing the checks is the root directory.

To execute a File content search check that does not start with the root directory, delete all entries from the Starting directories file list and disable all checks except the File content search check.

Directories/files excluded

Use this option to specify files and directories that are to be excluded from all File Find checks. The file list can contain full directory and file path names or file names without directory paths (e.g., /etc/passwd or passwd).

The File Find module returns the following message when the root directory (/) is specified without a subdirectory in an Exclude list. The File Find module cannot execute when the root directory is excluded in a file list.

Message name	Title	Class
EXCLUDE_ROOT	Exclude Root	0

Owners disallowed

This security check reports files that are owned by unauthorized users. Use the name list to specify users that are authorized to own files and directories and are, therefore, excluded from the check.

The security check returns the following message:

Message name	Title	Class
DISALLOWED_ OWNER	Disallowed owner	1

Group owners disallowed

This security check reports files that are owned by unauthorized groups. Use the name list to specify groups that are authorized to own files and directories and are, therefore, excluded from the check.

The security check returns the following message:

Message name	Title	Class
DISALLOWED_GROUP_OWNER	Disallowed group owner	1

Setuid files

This security check reports files that have been assigned the setuid attribute. Type full path names in the file list to specify files that should not be reported by this check. Wildcard characters are accepted. For example, /etc/* excludes all files in the /etc directory.

A user who runs a file with the setuid attribute is temporarily assigned the user ID of the file. While many system files depend on the setuid attribute for proper operation, security problems can result if setuid is assigned to programs that allow reading and writing of files or escapes to shell.

The security check returns the following message:

Message name	Title	Class
SETUID	File is setuid	0

To protect your computers

1. Examine the named setuid files for read, write, and escape to shell privileges.
2. Use the chmod command to change the setuid property if it is not required.

Setgid files

This security check reports files that have been assigned the setgid attribute.

A user who runs a file with the setgid attribute is temporarily assigned the group ID of the file. Although some system files depend on the setgid attribute for proper operation, assignment of setgid privileges to programs that allow reading and writing of files or escapes to shell creates a security risk.

To specify files and directories to exclude from the check, type full path names. Wildcard characters are accepted. For example, /etc/* excludes all files in the /etc directory.

The security check returns the following message:

Message name	Title	Class
SETGID	File is setgid	0

To protect your computers

1. Examine the setgid files for read, write, and escape to shell privileges.
2. Use the chmod command to change the setgid property if it is not required.

SUID/GUID shell escape files

This security check finds files with setuid or setgid attributes that allow shell escape access. This check examines files that are listed in the agent's /etc/shells file, as well as files that you specify with full path names in the file list.

A user who runs a setuid or setgid file is temporarily assigned the user ID or group ID of the file. Because the reported files allow escape to shell privileges, the setuid and setgid attributes can be security risks.

The security check returns the following messages:

Message name	Title	Class
SUID_SHELL_FILE	SUID bin/shell file	1
SGID_SHELL_FILE	SGID bin/shell file	1

To protect your computers

1. Carefully review all reported files.
2. Use the chmod command to remove setuid and setgid properties from files that do not require them.

New setuid files

This security check reports files with setuid attribute changes.

The first time that the File Find module is run, it creates a snapshot file that lists all files with setuid properties. On subsequent runs, executable files with new or deleted setuid attributes, and setuid files that cannot be found, are reported.

New setuid files and New setgid files checks return the following messages.

Message name	Title	Class
SETIDNEW	New setuid/setgid file	4
SETIDNOT	File is no longer setuid/setgid	0
SETIDDEL	Setuid/setgid file not found	0

To protect your computers

1. Examine the setuid properties changes on all files listed.
2. Use the chmod command to change setuid properties if appropriate, or update the snapshot file in the console grid to include authorized changes.

New setgid files

This security check reports files with setgid attribute changes.

The first time that the File Find module is run, it creates a snapshot file that lists all files with setgid properties. On subsequent runs, executable files with new or deleted setgid attributes, and setgid files that cannot be found, are reported.

The check returns the same messages as the messages returned by the New setuid files check (see the preceding table).

To protect your computers

1. Examine the setgid properties changes on all files listed.
2. Use the chmod command to change setgid properties if appropriate, or update the snapshot file in the console grid to include authorized changes.

Sticky files

This security check reports files that have the save text after execution (sticky) bit set.

When this bit is set on an executable file, the computer retains the program code in the file buffer cache after the program has finished. When this bit is set on a directory, only the owner of a file or the owner of the directory can delete files from the directory.

System performance can degrade if the sticky bit is set on too many programs. Some UNIX operating systems are vulnerable to security problems when the sticky bit is not set on system directories.

The security check returns the following message:

Message name	Title	Class
STICKY	Sticky bit set	0

To specify files to exclude from the check

- Type full path names in the file list.

To protect your computers

1. Examine the named files to ensure that the sticky bit settings are appropriate.
2. Use the chmod command to make necessary changes.

World writable directories without sticky bit

This security check reports world-writable directories that do not have the sticky bit set.

Any user can delete any file in these directories, including files that have been created by other users.

The security check returns the following message:

Message name	Title	Class
NOTSTICKY	World writable directory w/o sticky bit set	4

To specify files to exclude from the check

- Type full path names in the file list.

To protect your computers

1. Examine the reported files to ensure that they should be world writable.
2. After running the check, use the Correct function in the console grid to set the sticky bit for the named directory on the agent.
   You can also use the command:
   chmod o+t <filename>

Device files not in /dev

This security check reports special device files that are found in a location other than the /dev or /devices directory.

These files are normally located only in the /dev directory (or, on Solaris, the /devices directory). Special device files that are not in the /dev directory can be used to gain unauthorized access to the data on the device.

Type full path names and appropriate wildcard characters in the file list to specify files and directories that you want to exclude from the check. For example, /proc/* excludes all files in the /proc directory.

The security check returns the following message:

Message name	Title	Class
DEVICES	Device special file outside /dev	1

To protect your computers

- Move all special device files to the /dev directory (on Solaris, to /devices).

World writable files

This security check reports files that are writable by everyone. Some files, such as the directory /usr/tmp), must be world writable for correct system operation.

When checking UNIX file permissions, this module examines only the basic user/group/other and read/write/execute permissions. The module does not consider extended permissions such as access control lists (ACLs) that are available on some UNIX operating systems and through some third-party extensions.

World writable files are security risks because there are no controls over who can modify or delete these files.

Type full path names in the file list to exclude files that should be world writable from the check.

The security check returns the following message:

Message name	Title	Class
WWFILES	World writable	3

To protect your computers

1. Examine the reported files to determine whether they should be writable by everyone.
2. Use the chmod command to change the permissions on files that should not be world writable.
   After running the check, you can also use the Correct function in the console grid to change permissions for a file.

Group writable files

This security check reports files that are writable by anyone with group access. Most system files do not need to be modified or deleted during normal operation. Other files, such as /usr/tmp, must be group writable for system operation.

When checking UNIX file permissions, the module examines only the basic user/group/other and read/write/execute permissions. The module does not consider extended permissions such as access control lists (ACLs) that are available on some UNIX operating systems and through some third-party extensions.

Type full path names in the file list to exclude certain files from the check.

The check returns the following message:

Message name	Title	Class
GWFILES	Group writable	0

To protect your computers

1. Examine the reported files to determine whether they should be writable by anyone with group access to the files.
2. After running the check, use the Correct function in the console grid to change the permissions for a named file on the agent.
   You can also use the following command to change permissions:
   chmod g-w <filename>

Uneven file permissions

This security check reports files with uneven permissions. Uneven permissions mean that other access is greater than group access or user access. It can also mean that group access is greater than user access. A file with uneven permissions is inconsistent and does not make sense from a security perspective.

When checking UNIX file permissions, this module examines only the basic user/group/other and read/write/execute permissions. The module does not consider extended permissions such as access control lists (ACLs) that are available on some UNIX operating systems and through some third-party extensions.

Type full path names in the file list for files to be excluded from the check.

The security check returns the following message:

Message name	Title	Class
UNEVEN	Uneven permissions	0

To protect your computers

1. Determine the proper permissions for the named files.
2. After running the check, use the Correct function in the console grid to change the permissions for a reported file.
   You can also use the chmod command to make corrections.

Unowned directories/files

This security check reports directories or files with ownerships (UID or GID) that cannot be associated with user or group names on the computer being checked. These files are not accounted for and do not make sense from a security perspective.

Type full path names and appropriate wildcard characters in the file list to specify files and directories that you want to exclude from the check. For example, /home/* excludes all files in the /home directory.

The security check returns the following messages:

Message name	Title	Class
UNOWNED_UID	Unowned UID	1
UNOWNED_GID	Unowned GID	1

To protect your computers

1. Determine the proper owners and groups for the named files.
2. Use the chown and chgrp commands to make corrections.

File content search

This security check, not currently supported on IRIX 6.2, reports files that contain prohibited text strings and files that are missing required text strings as defined in File content search (.fcs) template files.

The security check returns the following messages:

Message name	Title	Class
FCS_GREEN	Green level content search matched	0
FCS_YELLOW	Yellow level content search matched	1
FCS_RED	Red level content search matched	4
INVALID_FCS_ENTRY	No block specified for 2nd pattern	3

Creating the File Content Search template

You must create and enable a new File Content Search template before you run the File content search check.

To create a File Content Search template

1. In the enterprise tree, right-click **Templates**, then click **New**.
2. In the Create New Template dialog box, select **File Content Search - all**.
3. Type a new template file name of no more than eight characters, without a file extension. Symantec ESM adds the .fcs extension to the file name.
4. Click **OK**.

To add a record to the File Content Search template

1. In the Template Editor, click **Add Row**.
2. Add one or more OS/Rev sublist rows. See "To add a row to the OS/Rev sublist" on page 86.
3. In the Description field, replace <NEW> with descriptive text that will display in the Information field of the console grid with the messages that report your file content search results.
4. In the new row, click the Severity field, then select **Green**, **Yellow**, or **Red**. This defines the security level that the module uses to report matches for specified text or text patterns.
5. Click the Report if field, then select **Any violate** or **All violate**. This setting defines conditions that are required to return an error message and quit the current search.

For example, if you select **Any violate** and create a set of File List sublist rows that define two Prohibited text strings, the search returns a message and stops as soon as either one of the text strings is encountered. If you select **All violate**, the search continues to the end of the specified text block and returns a message only if both Prohibited text strings are encountered.

Note: The preceding example describes how the file content search uses the Report if value to search for text patterns when both text strings are defined in the Pattern column. When a File List sublist entry includes both a Pattern and 2nd Pattern value, the Report If value applies only to the second pattern.

---

6 Add one or more File List sublist rows to define search criteria for each record that you create in the File Content Search template. See "Editing the File List sublist" on page 87.

7 Click **Save** to save changes to the File Content Search template.

8 Click **Close** to exit the Template Editor.

To add a row to the OS/Rev sublist

1 In the Template Editor, click the OS/Rev sublist field.

2 In the Template Sublist Editor, click **Add Row**.

3 In the Exclude field, select the check box to exclude the specified operating system and revision from checks in the File Watch template or uncheck it to include the operating system and revision.

4 Click the OS field, then select the value that describes the operating system or systems that you want to exclude or include for enabled checks. Select from the following options:

- All (All platforms)
- UNIX (All UNIX platforms)
- NT (All WIN NT platforms)
- WIN2K (All WIN 2000 platforms)
- WINXP (All WIN XP platforms)
- WIN2K3 (All WIN 2003 platforms)
- aix-rs6k
- hpux-hppa
- irix-mips
- ncr-x86
- osf1-axp

- solaris-sparc
- sunos-sparc
- sequent-x86
- redhat-x86
- redhat-s390
- nt-ix86

5 In the Revision field, replace <NEW> with the value of operating system revisions that you want to exclude or include for enabled checks. Use these conventions to identify multiple revisions:

Convention	Explanation
all	All releases and revisions.
-5.5	(Leading minus sign): The specified revision and all earlier revisions.
+5.6	(Leading plus sign): The specified revision and all later revisions.

6 Click **Apply**.
To add another row, repeat steps 2–6.

7 Click **Close**.

To delete rows from the File Content Search template

1 Click the leftmost, numbered button of the row you want to delete.
Use the **Shift** or **Ctrl** keys to select multiple template rows if you want to delete more than one record at a time.

2 Click **Remove Entry(s)**.

Editing the File List sublist

The File List sublist defines search criteria for text and text patterns in specified files and text blocks.

Add one or more rows to the File List sublist to define:

- The order used for multiple line searches
- The starting directory path and depth of subdirectories to be searched
- The file name that you want to search
- Whether the search will look for Required or Forbidden text patterns
- Pattern, Delimiter, and 2nd Pattern values that narrow search criteria and identify blocks for text searches.

To create or edit a File List sublist row

1. In the Template Editor, click the File List sublist button on the template row that contains the sublist.
2. In the Template Sublist Editor, click **Add Row**.
3. In the Order field, replace <NEW> with a number that specifies the sequence in which sublist rows will be considered by the File content search check.
   The search order is critical to searches that are defined by multiple sublist records, using the No Rewind or Block Delimiter values. See "Using multiple File List sublist entries" on page 91.
4. In the Path field, type the absolute path name of the directory where the File content search check will begin its search for files that match the file name or file name pattern that is specified in the File Name column of the same sublist record.
   You can also use the predefined macro %HOME_DIR% to specify the home directories for all users on the system in this field.
   Leave the Path field blank to define a sublist record that uses both the Path value and the File Name value from the preceding sublist record.
5. Click the Depth field, then select one of the following:

Depth option	Searches
All - Dir + all sub-dirs	The directory that is specified in the Path field and all of its subdirectories.
1 - Dir Only	Only the directory that is specified in the Path field and none of its subdirectories.
0 - Item Only	Only files with names that exactly match the value in the File Name field. Note: This option does not translate regular expressions to match file name patterns as the first two Depth options do.

   In sublists that include multiple records, the Depth option is ignored in second and subsequent records. See "Using multiple File List sublist entries" on page 91.
6. In the File Name field, replace <NEW> with the name of the file that you want to search for the text or text pattern that is specified in the Pattern field.
   You can use regular expressions syntax to define a file name pattern that could be matched by one or more files in the first row in a sublist. See "Using regular expressions" on page 93 for commonly-used syntax.

The file name is ignored when the path is blank. See "Using multiple File List sublist entries" on page 91.

7 In the Option field, select one of the following:

- **Required** if the specified text or text pattern must exist in the specified file or files.
- **Prohibited** if the text or text pattern must not exist in the file or files.

8 In the Pattern field, replace <NEW> with regular expressions to specify the text or text pattern that the File content search check will look for. See "Using regular expressions" on page 93 for commonly-used syntax.

Note: The check does not detect text pattern matches that span lines if they are not joined by the T (line continuation) character, which is defined in the Delimiter field of the sublist row where the text pattern is defined.

---

9 In the Delimiter field, assign values to one or more of the following options using the format:
<option_letter>=<value>

Opt	Description	Valid values
C	Comment character. Text following on the same line is not searched.	Any character
T	Line continuation character.	Any character
B	Block begin character for search defined in subsequent sublist entries or in 2nd Pattern field. Note: B=. searches to the end of the current line.	Any character
E	Block end character for search defined in subsequent sublist entries or in 2nd Pattern field.	Any character
N	No rewind. Search does not restart from beginning of file.	1 (On) | 0 (Off) Default = 0
I	Case insensitive.	1 (On) | 0 (Off) Default = 0
G	Define blocks without B or E options.	1 (On) | 0 (Off) Default = 0
R	Reuse text block from previous record for current record.	1 (On) | 0 (Off) Default = 0

Opt	Description	Valid values
D	Separator for multiple delimiter values.	Any character Default = ,

The following escape sequences are supported in all delimiter options that specify values as any character:
\n = newline
\t = tab
\ = hard space (represented by backslash-space)
\\ = literal backslash
You can combine multiple delimiter options in a single File List sublist record. For example, to ignore all comment lines that begin with the # character and find a block of text that begins and ends with the : characters, type **C=#,B=:,E=:**

10 In the 2nd Pattern field, use regular expressions to specify the text or text pattern that the File content search check will look for if the module finds a match for the text or text pattern that is specified in the Pattern field on the same sublist line.

Note: The File content search check looks for text defined in the 2nd Pattern field when it matches text that is defined in the Pattern field. If it doesn't find the first pattern, it doesn't look for the second pattern.

---

11 Click **Apply**.
To add another sublist row, repeat steps 1–11.

12 Click **Close**.

To delete a File List sublist row

1 In the Template Sublist Editor, click the leftmost, numbered button in the row that you want to delete.
You can also use the **Shift** or **Ctrl** keys to select more than one sublist row.

2 Click **Remove Rows**.

3 Click **Close** to exit the Template Sublist Editor and return to the File Content Search template.

Using multiple File List sublist entries

Multiple File List sublist entries are used to define file content searches that look for one or more text patterns in one or more blocks of text in one or more text files.

The File Find module reports error messages when it finds Prohibited text patterns and also when it fails to find Required text patterns in any block of text or text file that is defined in a set of sublist records.

Each of the following examples describes a set of sublist records that could be used to define one file content check.

- To search for more than one text pattern in one or more files in the same directory path, define values for the Path and File Name fields in the first record. Then create subsequent records without Path or File Name values. Each record in this set of records would contain a different required or prohibited text pattern in the Pattern field.
- To search for multiple text patterns that occur in a specific order in the same file, define values for the Path and File Name fields in the first record, and leave these fields blank in subsequent records. Type text patterns in the Pattern fields of both the first and subsequent records. Use the Order field to number the records to match the order that specified text patterns should occur in the file. Then specify N=1 in the Delimiter fields of the second and subsequent records to force pattern matching in sequential order.
- To search blocks of text for one or more text patterns, specify values for the B, E, or G options in the Delimiter field in the first record. Type R=1 in the Delimiter field in all subsequent records that define each required or prohibited text pattern to be searched in the defined block. Any sublist record or set of records that includes the R=1 Delimiter value must be preceded by a record that defines the B, E, or G Delimiter options.
  Specify the Path and File Name in the first record only in record sets that define blocks.
  Type the text pattern where the search for the B (beginning of block) character will start in the Pattern field in the first record. If no text pattern is entered, the block will start at the first occurrence of the B character in the file.
  If the B character is not defined, the block starts at the start of the text pattern, or at the beginning of the file if no text pattern is defined in the first sublist record. If the E (end of block) character is not defined, the block ends at the end of the file.
  Use the G=1 Delimiter value to define a block without the B and E characters and specify a text pattern in the Pattern field in the first sublist

record. The block will begin at the start of the specified text pattern and end at the end of the file.

- Define text patterns in both the Pattern and 2nd Pattern fields on the same sublist row line to require that a match exists for the first pattern before the module looks for the Required or Prohibited text that is defined as the second pattern.

Editing the Conditions sublist

The Conditions sublist in the File Content Search template defines the search criteria for running processes or configured services. The operating system must own the process, that is, have a PPID of 0 or 1 for the search to succeed on all operating systems except AIX. On AIX, system-owned processes can also have PPIDs that are equal to the process ID of the System Resource Controller.

The Conditions sublist has two columns: one lets you specify whether the sublist entry is a process, service, or file, and the other lets you specify the name of the process, service, or file.

To create or edit a Conditions sublist row

1. In the Template Editor, click the Conditions sublist button on the template row that contains the sublist.
2. In the Template Sublist Editor, click **Add Row**.
3. Click the Type field, then select one of the following:

Opt	Description	Valid types
I	Check inetd for service	Inetd
P	Check in running processes	Process
F	Check for existing file	File

4. In the Name field, type the name of the service, process, or file. The File content search check searches for running services, processes, or files that match the specified names.
5. Click **Apply**.
   To add another sublist row, repeat steps 1–4.
6. Click **Close**.

To delete a Conditions sublist row

1. In the Template Sublist Editor, click the leftmost, numbered button in the row that you want to delete.
   You can also use the **Shift** or **Ctrl** keys to select more than one sublist row.
2. Click **Remove Rows**.
3. Click **Close** to exit the Template Sublist Editor and return to the File Content Search template.

Using regular expressions

Regular expressions are used in:

- File Content Search template
  See "To create or edit a File List sublist row" on page 88.
- Login Parameters module
  See "Warning banners" on page 116

The File Content Search template applies regex C library functions, which support POSIX 1003.2 regular expressions:

Pattern	Description
. (period)	Matches any one character
\ (backslash)	Takes the next character literally. Used if the character you want to match is a special character, for example: *, +, ?
*	Matches zero or more occurrences of the previous atom, which is a regular expression in parentheses, a single character, a single character preceded by a backslash, or a range
+	One or more occurrences of the previous atom
?	Zero or one occurrences of the previous atom
(...)	Encloses a part of the regular expression to be considered as an atom when applying *, +, ?, or the | (vertical bar) operator
[<char1> <char2>...]	A range that matches any one of the characters listed in the range
[>...]	A range that matches any one character not listed in the range
[<char1>- <char2>...]	A range that matches any character in the range of ASCII characters from char1 to char2

Pattern	Description
| (vertical bar)	Or operator. The expression matches if either the atom before or the atom after this character matches
<	Matches the beginning of a word in the string. Words are separated by white space
>	Matches the end of a word in the string. Words are separated by white space
^	Matches the beginning of the string
$	Matches the end of the string

For more information, see the UNIX regex(7) man pages or search for POSIX 1003.2 regular expressions on the Internet.

Local disks only

This option restricts File Find checks to file systems that are on local disks. File systems that are on remote disks (served by NFS) are not examined.

File Watch

The File Watch module reports changes to specified files and directories, and the presence of files with suspicious file names or signature patterns.

- Creates and maintains an agent snapshot file (fwatch.dat) to detect file changes.
- Looks for files with file names or signature patterns that match specified names and patterns.
- Searches for malicious files and compares file signatures with snapshot or template files, depending on the checks enabled.

Common File Watch messages

File Watch messages that are not mapped to specific security checks are generated by:

- The function that creates the baseline snapshot file the first time the File Watch module is run on an agent.
- Checks and options that require enabled templates (specified in the Files/directories to watch option, the Malicious files check, and the Invalid signature check).
- Security checks that cannot locate, and therefore cannot check, a file or directory that is listed in a template.
- Security checks that find a template entry for a remote file or directory that cannot be checked because the Local disks only option is enabled on a UNIX agent.

Message name	Title	Class
SNAPSHOT_ TAKEN	Snapshot taken	4
NO_TEMPLATE	No template specified	4
FILE_NOT_CHECKED	File not checked	0

Updateable File Watch messages

Six File Watch checks report snapshot updateable messages. Two checks report template updateable messages. Updateable messages let you update snapshots or templates to match current agent values.

In the Updateable/Correctable column of the console grid, snapshot updateable messages display the letters SU and template updateable messages display the letters TU.

Security check	Code	Message name
Changed files (ownership)	SU	DIFF_OWN
Changed files (permissions)	SU	EXP_PERM
Changed files (permissions)	SU	DIFF_PERM
Changed files (signature)	SU	MODIFIED
New files	SU	NEW
Removed files	SU	REMOVED
Invalid signature	TU	SIG_NOTMATCH
Invalid signature	TU	SIGTYPE_ NOTMATCH

Files/directories to watch

Use this option to enable or disable template files that define files and directories to be watched. These files have .fw file extensions.

Editing the File Watch template

The File Watch template contains definitions of files and directories to bed watched, the depth of directory traversal, and the types of changes to evaluate.

To add a new File Watch template

1. In the enterprise tree, right-click the **Templates** icon, then click **New**.
2. In the Available template types list, select **File Watch - all**.
3. Type a new template name of no more than eight characters, without a file name extension. Symantec ESM adds the file watch (.fw) extension.
4. Press **Enter**.
5. Add one or more rows as described below.
6. Click **Save**.

7 Click **Close**.

To add a record to a File Watch template

1 In the Template Editor, click **Add Row**.

2 Add one or more OS/Rev sublist rows. See "To add a row to the OS/Rev sublist" on page 97.

3 In the File/Directory to watch field, replace <NEW> with the path name of a directory or file that you want to monitor.

4 Click each of the following fields, then select a value.

Field	Value that defines
Depth	How far down the directory tree to report changes.
Permissions	Type of permissions changes to report on UNIX agents only.
Signature	Type of file signature to store in agent snapshot files for the Changed files (signature) check. Note: The Invalid signature check uses the signature type in the File Signatures template. See "To add a new File Signatures template" on page 109.

5 In the following fields, check or uncheck the check box:.

Field	Option
Ownership	Report changes in file or directory ownership.
New	Report new files in specified volumes or directories.
Removed	Report files that have been removed from specified volumes.

6 Click the Excludes field, then define files or subdirectories that you want to exclude from all or some of the enabled checks. See "To add a row to the Excludes sublist" on page 99.

7 Click **Save**.

8 Click **Close**.

To add a row to the OS/Rev sublist

1 In the Template Editor, click the OS/Rev sublist field.

2 In the Template Sublist Editor, click **Add Row**.

3 In the Exclude field, check the check box to exclude the specified operating system and revision or uncheck it to include the operating system and revision for enabled checks.

4 Click the OS field, then select the value that describes the operating system or systems that you want to exclude or include for enabled checks:

- All (All platforms)
- UNIX (All UNIX platforms)
- NT (All WIN NT platforms)
- WIN2K (All WIN 2000 platforms)
- WINXP (All WIN XP platforms)
- WIN2K3 (All WIN 2003 platforms)
- aix-rs6k
- hpux-hppa
- irix-mips
- ncr-x86
- osf1-axp
- solaris-sparc
- sunos-sparc
- sequent-x86
- redhat-x86
- redhat-s390
- nt-ix86

5 In the Revision field, replace <NEW> with the value of operating system revisions that you want to exclude or include for enabled checks. Use these conventions to identify multiple revisions:

Convention	Explanation
all	All releases and revisions.
-5.5	(Leading minus sign): The specified revision and all earlier revisions.
+5.6	(Leading plus sign): The specified revision and all later revisions.

6 Click **Apply**.
To add another row, repeat steps 2–6.

7 Click **Close**.

To add a row to the Excludes sublist

1 In the Template Editor, click Excludes.

2 In the Template Sublist Editor, click **Add Row**.

3 In the File/Directory to exclude field, replace <NEW> with the name of the file or subdirectory that you want to exclude from checks on the same template row.
For example, if the template row defines File Watch checks for the /usr directory, type the name of a file or subdirectory in that directory.

4 Click each of the following fields, then select a value.

Field	Value defines
Depth	How far down the directory tree to report changes.
Permissions	Type of permissions changes to report on UNIX agents only.
Signature	Type of file signature to store in agent snapshot for the Changed files (signature) check. The Invalid signature check uses the signature type in the File Signatures template. See "To add a new File Signatures template" on page 109.

5 Click **Apply**.
To add another row, repeat steps 2–4.

6 Click **Close**.

To remove File Watch template records or sublist rows

1 In the Template Editor, click the number of the record that you want to remove, or in the Template Sublist Editor, the number of the row. This number is in the leftmost column.
To select a range of records or rows, hold down the **Shift** key while you click the first and last row numbers in the range.
To select non-sequential records or rows, hold down the **Ctrl** key while you click the row numbers.

2 In the Template Editor, click **Remove Rows** or, in the Template Sublist Editor, click **Remove Rows**.

3 Click **Apply**.

4 Click **Close**.

Changed files (ownership)

This security check reports ownership changes for files and directories for which Ownership checks are selected in the enabled File Watch template. See "Editing the File Watch template" on page 96.

The security check returns the following message:

Message name	Title	Class
DIFF_OWN	File ownership modified	1

To protect your computers

- For authorized changes, update the snapshot.
- Delete unauthorized files and directories.

Changed files (permissions)

This security check reports changes to file and directory permissions after the last snapshot update. Permissions checks must be selected in the enabled File Watch template.

The security check returns the following messages:

Message name	Title	Class
EXP_PERM	Directory or file permissions expanded	1
DIFF_PERM	Directory or file permissions changed	1

Note: When checking UNIX file permissions, this module examines only the basic user/group/other and read/write/execute permissions. The module does not consider any extended permissions such as access control lists (ACLs), which are available on some UNIX operating systems and through some third-party extensions.

To protect your computers

- For authorized changes, update the snapshot.
- Delete unauthorized files and directories.

Changed files (signature)

This security check calculates MD5 and/or CRC signatures on files and directories for which signature checks are selected in enabled File Watch templates and compares the results with the signatures that are stored in the agent's snapshot file to detect file changes. The signature type is specified in the File Watch template. See "Editing the File Watch template" on page 96.

See "Running CRC and MD5 signature checks on UNIX directories" on page 68.

The security check returns the following message:

Message name	Title	Class
MODIFIED	File modified	1

To protect your computers

1. In the console grid, update the snapshot file to include authorized changes.
2. Remove unauthorized files and directories from the volume.

New files

This security check reports new directories or files in directory trees that are specified for new checks in enabled File Watch templates. See "Editing the File Watch template" on page 96.

The security check returns the following message:

Message name	Title	Class
NEW	New file or folder	0

To protect your computers

1. In the console grid, update the snapshot file to include authorized changes.
2. Remove unauthorized files and directories from the volume.

Removed files

This security check reports directories or files that have been removed from directory trees that are specified for removed checks in enabled File Watch templates. See "Editing the File Watch template" on page 96.

The security check returns the following message:

Message name	Title	Class
REMOVED	File or folder removed	0

To protect your computers

1. In the console grid, update the snapshot file to include authorized changes.
2. Remove unauthorized files and directories from the volume.

Malicious files

This security check reports files with signatures that match file names or attack signatures that are defined in Malicious File Watch templates.

Use the check's name list to enable or disable Malicious File Watch (.mfw) templates.

The security check returns the following messages on UNIX operating systems:

Message name	Title	Class
MALICIOUS_FILE	Possible malicious file found	2
MFW_TEMPLATE_ERR	MFW template error	1

Warning: Do not attempt to demonstrate this check's messages. The messages indicate the presence of files and processes that can be used for malicious purposes on your computer.

Using the Malicious File Watch template

Default Malicious File Watch templates identify files that could be used for malicious purposes by file names and known attack signatures. These templates are identified by .mfw file extensions and are used only by the Malicious files check in the File Watch module.

Unix.mfw, nt.mfw, and 32k.mfw templates define attack signatures for files and processes that could indicate the presence of trojan horse programs. Attackers use trojan horse programs to deny service to authorized users.

Other default Malicious File Watch templates are:

File name/OS	Searches for files that may indicate
unixhide.mfw UNIX	Hide rootkit, a set of back door programs that attackers use for privileged access to a computer where they can modify system commands and install trojan horse programs.
lnxadore.mfw Red Hat Linux	Adore worm. Worms search for vulnerabilities, gather information, deny services, and/or install rootkits. The Adore worm spreads to other computers by exploiting LPRng, rpc-statd, wu-ftpd, and BIND vulnerabilities.
lnxlion.mfw Red Hat Linux	Lion worm, which installs the t0rn rootkit and spreads to other computers by exploiting a BIND TSIG vulnerability.
lnxt0rn.mfw Red Hat Linux	A t0rn rootkit. A rootkit is a set of back door programs that allows an attacker to gain privileged access to a computer, modify system commands, and install trojan horse programs. The t0rn rootkit is known to be installed by the Lion worm.
ntnipc.mfw Win2K WinNT	Attacks on e-commerce and e-finance/banking businesses. Based on NIPC advisories 00-060 and 01-003.
nthacktl.mfw Win2K WinNT	Hackers. Because these files may have legitimate uses on Windows computers, their presence does not necessarily indicate a compromised computer.

Editing the Malicious File Watch template

You can edit records of existing malicious files, add new malicious file records, and remove file records from the template.

To add a new Malicious File Watch template

1. In the enterprise tree, right-click **Templates**, then click **New**.
2. In the Available template types list, click **Malicious File Watch - all**.
3. Type a new template name of no more than eight characters. Symantec ESM adds the .mfw file name extension.
4. Press **Enter** or click **OK**.
5. Add information about other files that you want to watch for.
6. Click **Close**.

To add files that you want to watch for

1 If the Template Editor is not already open, double-click the name of the template in the enterprise tree.

2 In the Template Editor, click **Add Row**.

3 Replace <NEW> with the name and description of the malicious file.

4 In the OS/Rev field, specify the operating system revision number to watch.

5 Add one or more rows to the following sublists:

- OS/Rev (see "To add a row to the OS/Rev sublist" on page 97).
- Directories (see "To add a row to the Folders sublist" on page 104).
- File Type (see "To add a row to the File Type sublist" on page 104).
- Signature (see "To add a row to the Signature sublist" on page 105).
- Signature Patterns (see "To add a row to the Signature Patterns sublist" on page 107).
- File Extension (see "To add a row to the File Extension sublist" on page 108).

6 Click **Save**.

7 Click **Close**.

To add a row to the Folders sublist

1 In the Template Editor, click the Folders field on the row that you are editing.

2 In the Template Sublist Editor, click **Add Row**.

3 Replace <NEW> with the name of the volume or directory that you want to watch.

4 In the Depth field, select one of the following:

- **All** to watch the directory and all subdirectories.
- **0** to watch only the parent directory.

5 Click **Apply**.
To add another row, repeat steps 2–5.

6 Click **Close**.

To add a row to the File Type sublist

1 In the Template Editor, click the File Type field of the row that you are editing.

2 Click **Add Row**.

3 In the Exclude field, select the check box to exclude the specified file type from enabled checks or uncheck the check box to include the specified file type.

4 In the File Type field, select one of the following values:

File Type	Description
All	All file types
directory	Directories only
FIFO	Fifo special files (named pipes), UNIX systems only
block special	Block special files, UNIX systems only
character special	Character special files, UNIX systems only
executable	Directories or special files with executable bits set, UNIX systems only
regular file	Regular files
symbolic link	Symbolic links, UNIX systems only
socket	Sockets, UNIX systems only
executable program	Executable, regular files (not directories or special files)
file extension	File extensions that are selected in the File Extension sublist
DLL programs	Dynamic link library files, Windows systems only

5 Click **Apply**.
To add another row, repeat steps 2–5.

6 Click **Close**.

To add a row to the Signature sublist

1 In the Template Editor, click the Signature field on the row that you want to edit.

2 Click **Add Row**.

3 In the Signature ID field, replace <NEW> with an ID name or number that uniquely identifies the row that you are adding.
The IDs that you type in this column are the same as the values in the Signature IDs field of the Signature Patterns sublist to link the two rows.

4 Click the Signature Type field, then select the type of attack signature or file name that you want to watch for:

Signature type	Description
Bytes	Byte sequence
Word	16-bit word sequence
DWord	32-bit double word sequence
File Name	Case-sensitive file name
FILE NAME	Case-insensitive file name

5 In the Signature Pattern column, replace <NEW> with the signature pattern or file name that you want to watch.
Valid entries depend on values that are specified in the Signature Type field:

Signature type	Signature pattern entries
Bytes	One ASCII character per byte. You can also use the \x escape sequence to specify any byte sequence as a hexadecimal value in the format \xn or \xnn, where x is not case sensitive and n is one of the following digits: 0123456789abcdef See supported escape sequences bellow.
Word	Each word is a hexadecimal value, including up to four hexadecimal digits per word, preceded by the \x escape sequence.
DWord	Each double word is a hexadecimal value, including up to eight hexadecimal digits per word, preceded by the \x escape sequence.
File Name	Case-sensitive file path name.
FILE NAME	Case-insensitive file path name.

The Malicious files check compares File Name and FILE NAME signature patterns with the end of each file path.
If you do not precede Windows path names with two backward slashes (\\), or UNIX path names with one forward slash (/), Symantec ESM adds the slashes.

For example, if you specify the File Name pattern lib/lib on a UNIX computer, the module reports matches for /lib/lib as well as for /usr/lib/lib, but not for /usr/mylib/lib or /lib/lib/subdir.

Symantec ESM supports the following escape sequences in byte sequence signature patterns:

Sequence	Description
\a	Bell
\b	Backspace
\f	Formfeed
\n	Newline
\r	Carriage return
\t	Horizontal tab
\v	Vertical tab
\x	Hexadecimal escape sequence followed by n or nn, where n is one of the following hexadecimal digits: 0123456789abcdef

6 Click **Apply.** To add another sublist row, repeat steps 2–6.

7 Click **Close**

To add a row to the Signature Patterns sublist

1 In the Template Editor, click the Signature Patterns field on the row that you want to edit.

2 Click **Add Row**.

3 In the Probability field, replace <NEW> with a number between 1 and 100 that defines the probability that a file containing all of the signatures in the Signature ID column indicates the presence of a malicious file on your computer.

4 In the Message field, replace <NEW> with an explanation of how attackers can use the file that is identified in the Signature IDs field.

5 In the Signature IDs field, replace <NEW> with Signature IDs from the Signature Sublist on the same template row. Use commas to separate multiple Signature ID values.

6 Click **Apply**
To add another sublist row, repeat steps 2–6.

7 Click **Close**

To add a row to the File Extension sublist

1. In the Template Editor, click the File Extension field on the row that you are editing.
2. Click **Add Row**.
3. In the Include field, select the check box to include files with the specified file extension or uncheck the check box to exclude files with the specified extension.
   This sublist is used only when File Extension is selected in a File Type sublist record on the same template row.
4. In the Extension field, replace <NEW> with the file name extension to include or exclude.
5. Click **Apply**.
   To add another row, repeat steps 2–5.
6. Click **Close**.

To protect your computers

- Obtain the latest counter-measure information from the following Internet sites:

Organization	URL
Symantec	http://securityresponse.symantec.com
CERT Coordination Center	http://www.cert.org
Coast Project	http://www.cs.purdue.edu/coast
Computer Incident Advisory (CIAC)	http://ciac.llnl.gov/ciac
First	http://www.first.org
InfoSysSec	http://www.infosyssec.com
Internet/Network Security	http://netsecurity.about.com
Microsoft Corporation	http://www.microsoft.com
NTBugtraq	http://www.ntbugtraq.com
NTSecurity Net	http://www.ntsecurity.net
Security Focus	http://www.securityfocus.com

Invalid signature

This security check reports files with CRC, MD5, or combined CRC and MD5 file signatures that do not match the signatures and signature types that are in the manager's File Signatures template. This lets you verify that all agents have identical versions of critical files and protects signature data from tampering by users who can access agents but not managers.

You must create a File Signatures template to use the check.

Use the Changed files (signature) check to compare current file signatures with snapshot records that are on the agent.

The Invalid signature check returns the following messages:

Message name	Title	Class
SIG_NOTMATCH	File signature does not match template	1
SIGTYPE_ NOTMATCH	File signature type does not match template	0
FILE_NOTEXIST	Mandatory file does not exist	3

Editing the File Signatures template

In the Files Signatures template, you specify files that you want to monitor for changes. Three methods of specifying files are available:

- Add File: Individual file on an agent.
- Add Directory: All files in a specified directory. Optionally you may include all files in all sublevel directories or all files in a specified number of sublevel directories.
- Add Entry: Individual files with specific criteria. Seldom used.

You can use one or more of these methods to specify files.

To add a new File Signatures template

1. In the enterprise tree, right-click **Templates**, then click **New**.
2. In the Create New Template dialog box, select **File Signatures - all**.
3. Type a new template name of no more than eight characters. Symantec ESM adds a .fs file name extension.
4. Press **Enter**.
5. Add one or more records.

6 Click **Save**.

7 Click **Close**.

To specify individual files that you want to monitor

1 If the Template Editor is not already open, double-click the name of the template in the enterprise tree.

2 In the Template Editor, click **Add File**.

3 In the Add Items to Template dialog box, select an agent.

4 Type the path and name of the file that you want to monitor.

5 Press **Enter** or click **OK**.
To add another file using this method, repeat steps 2–4.

6 Click **Save**.
You can now add files using the Add Directory or Add Entry methods.

7 Click **Close**.

To specify files that you want to monitor by directory structure

1 If the Template Editor is not already open, double-click the name of the template in the enterprise tree.

2 In the Template Editor, click **Add Directory**.

3 In the Add Hierarchal Items to Template dialog box, select the agent where the directories and files are located.

4 Type the path and name of the parent directory. Do not specify an empty directory.

5 Select the option that describes the level of subdirectories and files that you want to load.

- This item and all subordinates
- This item only (no subordinates)
- Include <number> subordinate levels

6 Press **Enter** or click **OK**.
To add another file using this method, repeat steps 2–6.

7 Click **Save**.
You can now add files using the Add File or Add Entry methods.

8 Click **Close**.

To specify files that you want to monitor according to certain criteria

1. If the Template Editor is not already open, double-click the name of the template in the enterprise tree.
2. In the Template Editor, click **Add Row**.
3. Replace <NEW> with the agent name, file name, and file signature.
4. In the Required field, select one of the following:
   - **Optional** – File existence is optional.
   - **Mandatory** – File must exist.
5. In the Signature Type field, select the signature type that you want to watch for changes. Symantec ESM loads new entries with MD5 signatures.
   - CRC: 16-bit signature
   - MD5: 128-bit signature
   - CRC+MD5: Combined CRC and MD5

   When you change the Signature Type value after a template record is loaded, the check reports that fact and lets you update the template signature
6. Click **Save**.
   To add another row, repeat steps 2–6.
   You can now add files using the Add File or Add Directory methods.
7. Click **Close**.

To remove File Signatures records

1. In the Template Editor, click the number of the record that you want to remove or the number of the row. This number is in the leftmost column.
   To select a range of records, hold down the **Shift** key while you click the first and last row numbers in the range.
   To select non-sequential records, hold down the **Ctrl** key while you click the row numbers.
2. Click **Remove Entry(s)**.
3. Click **Save**.
4. Click **Close**.

Local disks only

This option restricts security checks to file systems that are located on local disks. File systems that are on remote disks (served by NFS) are not checked.

Login Parameters

The Login Parameters module report system login vulnerabilities such as old and unused accounts, failed logins, expired passwords, etc.

Users to check

Enable this option to specify users and groups that are excluded or included for all Login Parameters security checks that examine user and group accounts. See "Editing name lists" on page 35.

Local disks only

Enable this option to restrict checks to users with home directories that are located on disks that are local to the computer running the check. This ensures that user files are examined only once in sites that serve user directories with NFS, even though the module can be run on more than one computer.

Note: When the Local disks only option is enabled on an AIX computer, the module does not check remote mount points on NFS, AFS, or DFS file systems. On Solaris and HP-UX, the Local disks only option excludes remote mount points on AFS and NFS.

Local accounts only

Enable this option to restrict checks to user accounts that are defined in the agent's /etc/passwd file. This ensures that users are checked only once in sites that serve user accounts with NIS.

Inactive accounts

This this security check reports accounts that have never been logged into and accounts that have not been logged into for a specified number of days before the check is run. (The default value is 30 days.)

For this check, Red Hat Linux operating systems must be configured to use the shadow password file.

You can use the check's Users/Groups name lists to exclude users that are not excluded by the Users to check option.

The check returns the following messages:

Message name	Title	Class
CANNOT_LOGIN	Cannot login	0
NO_LOGIN_ RESTRICT	No login restrictions	0
LASTLOG	Inactive account	1
LOGIN_RESTRICTIONS	Login restrictions	0

Login failures

This security check reports failed login attempts to user accounts for a specified number of days prior to the day the check is run. (The default value is 15 days.)

The check is supported on the following operating systems under the following conditions:

Operating System	Conditions
Solaris	Symantec ESM requires the existence of /var/adm/loginlog for this check to work. If /var/adm/loginlog does not exist, failed login attempts are not logged and Symantec ESM reports the NOLOGINLOG message suggesting that you create the file.
HP-UX	Symantec ESM reads /etc/btmp. Also, if the system is in trusted mode, Symantec ESM reads /tcb/files/auth/*/*.
AIX	Symantec ESM reads /etc/security/failedlogin.
Linux	Symantec ESM reads /var/log/btmp or /var/log/messages.
OSF1	Symantec ESM requires that the operating system be running in trusted mode and reads /tcb/files/auth/*/*.
IRIX	Symantec ESM requires the existence of /var/adm/loginlogfile for this check to work. If /var/adm/loginlog does not exist, failed login attempts are not logged and Symantec ESM reports the NOLOGINLOG message suggesting that you create the file.
Sequent	Symantec ESM requires the existence of the /usr/adm/loginlog for this check to work. If /usr/adm/loginlog does not exist, failed login attempts are not logged and Symantec ESM reports the NOLOGINLOG message suggesting that you create the file.

You can use the check's Users/Groups name lists to exclude users that are not excluded by the Users to check option.

The check returns the following messages:

Message name	Title	Class
LOGFAIL	Failed login attempt	1
NOLOGINLOG	Failed login attempts not logged	0

Password expired

This security check reports user accounts with expired passwords on computers that support password expiration. The security check also reports expired user accounts and other conditions that could make your computer vulnerable to potential intruders with unauthorized password knowledge.

For this check, Red Hat Linux operating systems must be configured to use the shadow password file.

You can use the check's Users/Groups name lists to exclude users that are not excluded by the Users to check option.

The check returns the following messages:

Message name	Title	Class
EXPIRED	Password expired	1
EXPIRED_AIX_ACC	Account expired	0
PASS_LSTCHG	Password last change	0
PASS_NOCHECK	Any password good	1
PASS_WARN	Password warnings	0
CAN_CHANGE	Others can change password	1

Successful login attempts not logged

This security check reports agents where successful login attempts are not being logged.

The check returns the following message:

Message name	Title	Class
SUCLOGNOLOG	Successful login attempts not logged	0

Unsuccessful login attempts not logged

This security check reports agents where unsuccessful login attempts are not being logged. The security check also reports Red Hat Linux computers that are not logging this data to a regular file.

The check returns the following messages:

Message name	Title	Class
UNSUCLOGNOLOG	Unsuccessful login attempts not logged	0
NOT_REGULAR	Unsuccessful logins not logged to regular file	0

When Unsuccessful login attempts not logged is reported

- On OSF1 or TRU64, turn on security mode, then run the check again.

Successful su attempts not logged

This security check reports agents where successful su attempts are not being logged. The su command is commonly known as the super-user or substitute user command on UNIX operating systems.

The check returns the following message:

Message name	Title	Class
SUCCESS_SU_NOT _LOG	Successful su attempts not logged	1

Unsuccessful su attempts not logged

This security check reports agents where unsuccessful su attempts are not being logged. The su command is commonly known as the super-user or substitute user command on UNIX operating systems.

The check returns the following message:

Message name	Title	Class
UNSUCCESS_SU_NOT_LOG	Unsuccessful su attempts not logged	1

Remote root logins

This security check reports a problem when the root account can be accessed remotely through rlogin or telnet. The root account should be accessed only through the system console.

The check returns the following message:

Message name	Title	Class
ROOTRLOGIN	Root can be accessed remotely	3
SECURETTY_ MISSING	No tty security file	1
DEFAULT_ LOGIN_MISSING	No default login configuration file exists	1

Warning banners

This check looks for appropriate warning banners in the /etc/motd, /etc/issue (/etc/security/login.cfg on AIX), /etc/default/telnetd, and /etc/default/ftpd files. The check reports files that are missing and banners that do not match at least one of the regular expressions that are specified in the check's name list.

On Solaris, the check also executes the eeprom command to check the banner that displays at boot time. The eeprom check does not recognize the regular expressions syntax that is used for other banner checks.

The check returns the following messages:

Message name	Title	Class
BANNER_NOT_MATCHED	File does not contain required banner phrase	3
NO_BANNER_FILE	Named banner file does not exist	3

To protect your computers

- Use warning banners to provide legal notice to users that your computers are monitored to detect unauthorized uses.

Trusted mode only

This header identifies five UNIX security checks (Locked accounts, Password changes failed, Devices with failed logins, Devices with no user restrictions, and Login retries) that have the ability to run in a trusted security mode. This is called enhanced security mode on some computers, and formally is known as the Trusted Computing Base (TCB). These five ESM security checks can run successfully only on computers that are TCB enabled.

Trusted Computing Base

Trusted Computing Base (TCB) is the whole assemblage of security critical components, both hardware and software, responsible for enforcing information security policies on UNIX operating systems. Operating systems that are TCB enabled install a group of TCB files, configuration files, and trusted commands that coordinate the enhanced security mode.

TCB is currently supported on Digital UNIX/Tru64, AIX 4.2+, and HP/UX 10.x+ operating systems.

To verify if TCB is enabled on AIX computers

- Log on to the AIX computer as root and type **/usr/bin/tcbck**
  If TCB is not enabled, the tcbck command displays the following message:

  ```
  3001-101 The Trusted Computing Base is not enabled on this
  machine.   To enable the Trusted Computing Base, you must
  reinstall and set the 'Install Trusted Computing Base' option to
  YES. No checking is being performed.
  ```

  If TCB is enabled, the tcbck command returns usage information. For example:

  ```
  Usage: tcbck -a <filename> ...
  ```

To verify if TCB is enabled on Digital/DEC computers

- Log on to the Digital/DEC computer as root and look for the protected password daemon (prpasswdd) in the /usr/bin directory.
  If the protected password daemon exists, enhanced security is enabled.

To verify if TCB is enabled on HP-UX computers

- Log on to the HP-UX computer as root and type **/usr/lbin/modprdef**
  If TCB is not enabled, the modprdef command returns the following message:

  ```
  System is not trusted
  ```

  If TCB is enabled, the modprdef command returns usage information. For example:

  ```
  Usage: modprdef -m opt=value[,opt=value]
  ```

Locked accounts

This security check reports user accounts that are locked on computers running in trusted or enhanced security modes. If possible, Symantec ESM reports the reason that the account is locked. For more information on trusted security mode, see "Trusted Computing Base" on page 117.

Use the check's Users/Groups name lists to exclude users that are not excluded by the Users to check option.

Note: This check is supported only on AIX, HP-UX, and Digital UNIX(Tru64) computers.

The check returns the following messages:

Message name	Title	Class
LOCKED	Locked accounts	1
LOCKNOTSUP	Account locking not supported in non-trusted mode	0

Password changes failed

This security check reports user accounts that have failed password changes on computers that are running in trusted or enhanced security modes. If possible, Symantec ESM reports information on the failed password change. For more information on trusted security mode, see "Trusted Computing Base" on page 117.

Use the check's Users/Groups name lists to exclude users that are not excluded by the Users to check option.

Note: This check is supported only on AIX, HP-UX, and Digital UNIX(Tru64) computers.

The check returns the following messages:

Message name	Title	Class
UNSUCCESSFUL	Unsuccessful password changes	1
AIXUNSUCCESSFUL	Unsuccessful password changes not logged	0
UNSUCNOTSUP	Failed Password Changes not supported in non-trusted mode	0

Devices with failed logins

This security check reports devices that have reported failed logins on computers that are running in trusted or enhanced security modes. If possible, Symantec ESM reports information on the failed logins. For more information on trusted security mode, see "Trusted Computing Base" on page 117.

Note: This check is supported only on AIX, HP-UX, and Digital UNIX(Tru64) computers.

The check returns the following messages:

Message name	Title	Class
FAILDEVICE	Devices with failed logins	1
AIXPORT	Devices with failed logins	0
AIXPORTERROR	AIX /etc/security/portlog	0

Devices with no user restrictions

Administrators are able to limit the users that can come in on individual or specific devices on computers that are running in trusted or enhanced security modes. This security check reports devices that do not have such user restrictions. For more information on trusted security mode, see "Trusted Computing Base" on page 117.

Note: This check is supported only on AIX, HP-UX, and Digital UNIX(Tru64) computers.

The check returns the following message:

Message name	Title	Class
NORESTRICTIONS	Devices with no restrictions	0

Login retries

This security check reports user accounts on computers running in trusted or enhanced security modes that have login retries settings that are greater than the Login retries value that is specified in your policy. For more information on trusted security mode, see "Trusted Computing Base" on page 117.

Use the check's name list to exclude accounts that should not be reported.

Note: This check is supported only on AIX, HP-UX, and Digital UNIX(Tru64) computers.

The check returns the following message:

Message name	Title	Class
LOGIN_RETRIES_EXCEED_LIMIT	Login retries setting exceeds policy value	1

To protect your computers

- Restrict the number of login retries on your computers to five or less to protect your computer from brute force password attacks.

Excessive failed logins for users

This security check reports users that have exceeded the allowed number of failed login attempts within a specified time period and incorrect parameters entered in the Failed Login/Login period text box.

The Failed logins/Login period value is the number of allowed failed login attempts within a specified number of hours. Separate the two numbers with a forward slash (/). The default value is 5/24, which means that this check reports an error if users have more than 5 failed login attempts within a 24-hour period.

Use the check's name lists to specify users and groups that are to be included or excluded for the check.

Note: This check is not supported on IRIX, OSF1/Tru64, or Sequent operating systems

---

The check returns the following messages:

Message name	Title	Class
INVALID_DATA	Invalid failed login parameters	1

Message name	Title	Class
USER_LIMIT	User failed login limit exceeded	4
CHECK_NOT_PERFORMED	Warning - check could not be performed	1

Excessive failed logins on agent

This security check reports agents whose users have exceeded the allowed number of failed login attempts within a specified time period. This check also reports incorrect parameters entered in the Failed Login/Login period text box.

The Failed logins/Login period value is the number of allowed failed login attempts within a specified number of hours. The two numbers must be separated by a forward slash (/). The default value is 20/24, which means that this check reports an error if users on the agent have more than 20 combined failed login attempts within a 24-hour period.

Note: This check is not supported on IRIX, OSF1/Tru64, or Sequent operating systems

---

The check returns the following messages:

Message name	Title	Class
INVALID_DATA	Invalid failed login parameters	1
AGENT_LIMIT	Agent failed login limit exceeded	4
CHECK_NOT_PERFORMED	Warning - check could not be performed	1

Report all inactive account instances

Enable this option to report all inactive user accounts on all agents instead of reporting each account name on only one agent per job run. If you are not using NIS and want accounts with the same names on different systems to be treated separately, enable this option.

This check returns the following message:

Message	Title	Class
INACTIVE_ACCT	Inactive account	1

Network Integrity

The UNIX Network Integrity module reports vulnerabilities in NFS software and NIS or NIS+ services, and identifies user accounts that can access the host and user accounts in a UNIX domain through file transfer protocol (FTP) and trivial file transfer protocol (TFTP) utilities.

Warning: Backup any system administration file that you intend to modify before changing it. Incorrectly modifying administration files can cause serious, system-wide problems. agent

Correctable Network Integrity messages

The UNIX Network Integrity module has two security checks that report correctable messages. These messages let you correct system file owners and permissions on the agent from the console grid.

Correctable messages display the letter C in the Updateable/Correctable column of the console grid.

Security check	Message name
Anonymous FTP owner	ROOTOWN
Anonymous FTP permissions	NOTWRITE

Trusted hosts/users

This security check examines the /etc/hosts.equiv file on the agent and reports trusted hosts and users. Trusted users can access the computer from trusted hosts without supplying passwords through remote login and remote shell commands such as rlogin, remsh, rsh, rcp, and rcmd.

See the man pages for the hosts.equiv file for more information about how the hosts.equiv and .rhosts files are used to authenticate trusted users on your operating system.

Use the name list to specify trusted hosts, trusted users, and combinations of trusted hosts and users that are excluded from the check. The syntax for a host/user entry in the name list is *host user* where a space separates the host name from the user name. You can also type netgroup names in the host field to exclude all members of a netgroup from the check.

The check returns the following messages:

Message name	Title	Class
ALLIN	All users on all hosts are trusted	4
ALLUSER	User is trusted from any host	1
CLUSTERIN	All hosts in your cluster are trusted	0
GROUPIN	Network group on host is trusted	0
GROUPOUT	Network group on host is not trusted	0
HOSTIN	All users on host are trusted	1
HOSTOUT	Host is not trusted	0
USERIN	User on host is trusted	0
USEROUT	User on host is not trusted	0

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except Trusted Hosts/Users.
2. Verify that the /etc/hosts.equiv file exists on the test agent. If a permanent file is not authorized by your security policy, you can create a temporary file to verify this check, then delete the file.
   If the hosts.equiv file does not exist, the check reports No problems found.
3. Add line entries to the hosts.equiv file to produce each of the following messages:

To produce the message	Add a line to the hosts.equiv file that
All users on all hosts are trusted	Contains only the plus sign (+) character. On Digital UNIX (Tru64), this line must not be preceded by a line that contains only the keyword NO_PLUS.
User is trusted from any host	Begins with the plus sign (+) followed by a blank space and user name, such as **+ user**
All hosts in your cluster are trusted	Begins with the percent (%) character. (Supported only on HP-UX computers.)
Network group on host is trusted	Begins with the plus sign and ampersand (+@) characters joined to a host netgroup name, such as **+@netgroup**

To produce the message	Add a line to the hosts.equiv file that
Network group on host is not trusted	Begins with the minus sign and ampersand (-@) characters joined to a host netgroup name, such as **@netgroup**
All users on host are trusted	Specifies only the host name. The host name can be, but does not have to be, joined to a preceding plus sign (+), such as **host** **+host**
Host is not trusted	Contains only a minus sign (-) joined to a host name, such as **-host**
User on host is trusted	Begins with the host name followed by a blank space and user name. The host name can be, but does not have to be, joined to a preceding plus sign (+), such as **host user** **+host user**
User on host is not trusted	Begins with a minus sign (-) character joined to a host name, followed by a blank space and user name, such as **-host user**

4 Verify that none of the host/user entries in the preceding examples are excluded by the check's name list.

5 Run the demo policy on the test agent to verify that each of the described line formats produces the expected message.

6 Reverse any editing changes that you made to the test agent's permanent hosts.equiv file if this file is authorized by your security policy.

To protect your computers

- Do not allow users to bypass standard password-based login procedures to access your computer as trusted users through remote shell and remote login commands. Remove the /etc/hosts.equiv and .rhosts files from your computers if possible.

Adding and removing export entries

To demonstrate the next ten security checks that are documented in this chapter, you must add and remove entries from export files that vary depending on the UNIX operating system that is running on the test agent.

AIX and Sequent operating systems

- Run **exportfs -i** to export a directory that is not listed in the /etc/exports file, and add it to the /etc/xtab file.
- Run **exportfs -a** to add a test export entry to the /etc/exports file.
- Run **exportfs -u** to remove a test export entry from the /etc/exports file.

Solaris and NCR operating systems

- Run **share** to add a test export entry to the /etc/dfs/sharetab file.
- Run **unshare** to remove a test export entry.

HP-UX, Linux, IRIX, and Digital UNIX (Tru64) operating systems

- Directly edit the /etc/exports file to add or remove a test entry.

NFS exported directory

This security check examines the file that stores exported or shared NFS directory listings on the agent and reports exported directories with the options that are specified for each export.

Specify full path names in the check's name list for exported directories that should not be reported by the check.

The check returns the following message:

Message name	Title	Class
FSEXPORT	File system exported	0

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except NFS Exported Directories.
2. Verify that the test agent's /etc/xtab, /etc/dfs/sharetab, or /etc/exports file contains at least one directory path name entry. You can temporarily add a test entry to the file if necessary. See "Adding and removing export entries" on page 125.

3 Verify that the check's file list does not exclude any of the exported directories that you expect the check to report.

4 Run the demo policy on the test agent and verify that the check produces the File system exported message.

5 Reverse any changes that you made to the agent's /etc/xtab, /etc/dfs/sharetab, or /etc/exports file after verification.

To protect your computers

- Export only those directories that have explicit access lists, and limit access to necessary computers.

NFS exported directory access

This security check reports the names of hosts that have remote access to exported file systems. Use the check's file list to specify full path names for exported directories that should not be reported by the check.

The check returns the following message:

Message name	Title	Class
EXPACCCHK	Access check for exported file systems	1

To demonstrate the security check

1 Disable all checks in your Network Integrity module demo policy except NFS exported directory access.

2 Verify that the /etc/xtab, /etc/dfs/sharetab, or /etc/exports file has at least one exported directory listing that contains the access, rw, or ro option with one or more computer names.
Look for directory path names that are followed by a blank space and one or more computer names without the option keywords. Some computers use this format to define access lists without option keywords.
You can temporarily add a new test entry to the file if necessary. See "Adding and removing export entries" on page 125.

3 Verify that the check's file list does not exclude any of the exported directories that you expect the check to report.

4 Run the demo policy on the test agent and verify that the check produces the message, Access check for exported file systems.

5 Reverse any changes that you made to the agent's /etc/xtab, /etc/dfs/sharetab, or /etc/exports file after verification.

To protect your computers

- Carefully review the list of remote computers with access to NFS exported directories and remove any computers that are potential security risks.

NFS exported directory no access lists

This security check examines the file that stores exported or shared NFS directory listings and reports directories that are exported without access lists.

Use the check's file list to specify full path names for exported directories that should not be reported by the check.

The security check returns the following message:

Message name	Title	Class
EXPTOANY	File system exported to any host	4

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except NFS exported directory no access lists.
2. Verify that the /etc/xtab, /etc/dfs/sharetab, or /etc/exports file has at least one exported directory listing that contains the access, rw, or ro option with one or more computer names.
   Look for directory path names that are followed by a blank space and one or more computer names without the option keywords. Some computers use this format to define access lists without option keywords.
   You can temporarily add a test entry to the file if necessary. See "Adding and removing export entries" on page 125.
3. Verify that the check's file list does not exclude any of the exported directories that you expect the check to report.
4. Run the demo policy on the test agent and verify that the check produces the message, File system exported to any host.
5. Reverse any changes that you made to the agent's /etc/xtab, /etc/dfs/sharetab, or /etc/exports file after verification.

To protect your computers

- Use access lists with all NFS exported directories to limit access to intended users. Without access lists, exported directories allow world access.

NFS exported directory write permissions

This security check reports the names of hosts that have write permissions to NFS exported directories.

Use the check's file list to specify full path names for exported directories that should not be reported by the check.

The security check returns the following message:

Message name	Title	Class
EXPWRCHK	Write check for exported file systems	1

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except NFS exported directory write permissions.
2. Verify that the /etc/xtab, /etc/dfs/sharetab, or /etc/exports file has at least one exported directory listing that does not contain the ro option, but does contain the rw option with one or more computer names.
   You can temporarily add a test entry to the file if necessary. See "Adding and removing export entries" on page 125.
3. Verify that the directory in the identified listing is not excluded by the check's file list.
4. Run the demo policy on the test agent to produce the message, Write check for exported file systems.
5. Reverse any changes that you made to the agent's /etc/xtab, /etc/dfs/sharetab, or /etc/exports file.

To protect your computers

- Block write access to all NFS exported directories unless such access is absolutely necessary.

NFS exported directory writable by any host

This security check reports NFS exported directories that are writable by any host.

Use the check's file list to specify full path names for exported directories that should not be reported by the check.

The check returns the following message:

Message name	Title	Class
EXPANYWR	Exported file system can be written by any host	1

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except NFS exported directory writable by any host.
2. Verify that /etc/xtab, /etc/dfs/sharetab, or /etc/exports has at least one exported directory listing that does not contain the ro option.
   You can temporarily add a test entry to the file if necessary. See "Adding and removing export entries" on page 125.
3. Verify that the directory in the identified listing is not excluded by the check's file list.
4. Run the demo policy on the test agent to produce the message, Exported file system can be written by any host.
5. Reverse any changes that you made to the agent's /etc/xtab, /etc/dfs/sharetab, or /etc/exports file.

To protect your computers

- Block write access to all NFS exported directories unless such access is absolutely necessary. If you must export a directory with write access, explicitly specify each host that can NFS mount the directory.

NFS exported directory root access

This security check reports the names of hosts that have root access to NFS exported directories.

Use the check's file list to specify full path names for exported directories that should not be reported by the check.

The check returns the following message:

Message name	Title	Class
EXPROOTCHK	Root access check for exported file systems	1

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except NFS exported directory root access.
2. Verify that the /etc/xtab, /etc/dfs/sharetab, or /etc/exports file has at least one exported directory listing that contains the root option with one or more computer names.
   On a Digital UNIX (Tru64) computer, verify that the /etc/exports file has a listing that contains both the root=0 option and the access= option with one or more computer names.
   You can temporarily add a test entry to the file if necessary. See "Adding and removing export entries" on page 125.
3. Verify that the directory in the identified listing is not excluded by the check's file list.
4. Run the demo policy on the test agent to produce the message, Root access check for exported file systems.
5. Reverse any changes that you made to the agent's /etc/xtab, /etc/dfs/sharetab, or /etc/exports file after verification.

To protect your computers

- Block root access to all NFS exported directories unless such access is absolutely necessary.

NFS exported directory root access by any host

This security check reports NFS exported directories that allow root access from any host.

Note: This check is supported only on Digital UNIX (Tru64) operating systems.

Use the file list to specify full path names for exported directories that should not be reported by the check.

The security check returns the following message:

Message name	Title	Class
EXPROOTANY	Root access available to any host	4

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except NFS exported directory root access by any host.
2. Verify that the /etc/exports file has at least one exported directory listing that contains the root=0 option, but does not contain the access= option with one or more computer names.
   You can temporarily add a test entry to the file if necessary. See "Adding and removing export entries" on page 125.
3. Verify that the directory in the identified listing is not excluded by the check's file list.
4. Run the demo policy on the test agent to produce the message, Root access available to any host.
5. Reverse any editing changes that you made to the agent's /etc/exports file.

To protect your computers

- Block root access to all NFS exported directories unless such access is absolutely necessary. If you must export a directory with root access, you should explicitly specify each host that can NFS mount the directory.

NFS exported directory anonymous access

This security check reports NFS exported directories that can be accessed by anonymous users.

Note: This check is not supported on Red Hat Linux computers.

Use the check's file list to specify full path names for exported directories that should not be reported by the check.

The security check returns the following message:

Message name	Title	Class
EXP_ANON_ ACCESS	Anonymous access is enabled	1

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except NFS exported directory anonymous access.
2. Verify that the /etc/xtab, /etc/dfs/sharetab, or /etc/exports file has at least one exported directory listing that contains the anon= option with one or more user IDs.
   Temporarily add a new exported directory listing if necessary.
3. Verify that the directory in the identified listing is not excluded by the security check's file list.
4. Run the demo policy on the test agent to produce the message, Anonymous access is enabled.
5. Reverse any changes that you made to the agent's /etc/xtab, /etc/dfs/sharetab, or /etc/exports file.

To protect your computers

- Disable anonymous access to NFS exported directories by setting the anon= option value to -1.

NFS exported directory anonymous UIDs

This security check reports the user IDs of anonymous users that are granted access to named NFS exported directories. A security risk exists when anonymous users are mapped to privileged user IDs.

Use the file list to specify full path names for exported directories that should not be reported by the check.

The security check returns the following message:

Message name	Title	Class
EXPANON	Anonymous mapping check for exported file systems	1

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except NFS exported directory anonymous UIDs.
2. Verify that the /etc/xtab, /etc/dfs/sharetab, or /etc/exports file has at least one exported directory listing that contains the anon option with one or more user IDs.
   You can temporarily add a test entry to the file if necessary. See "Adding and removing export entries" on page 125.
3. Verify that the directory in the identified listing is not excluded by the check's file list.
4. Run the demo policy on the test agent to produce the message, Anonymous mapping check for exported file systems.
5. Reverse any changes that you made to the agent's /etc/xtab, /etc/dfs/sharetab, or /etc/exports file.

To protect your computers

- Disable anonymous access to an NFS exported directory by setting the anon option value to -1.

NFS exported directory non-secure

This security check examines the file that stores exported or shared NFS directory listings and reports directories that are exported in non-secure mode.

Use the check's name list to specify the secure options that are checked. The following options are checked by default: secure, kerberos, sec=dh, and sec=krb4.

Note: This check is currently supported only on Solaris, AIX, and NCR operating systems.

The check returns the following message:

Message name	Title	Class
NFS_EXPORT_NON_SECURE	NFS exported directory not secure	1

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except NFS exported directory non-secure.
2. Verify that the following options are listed in the check's name list: secure, kerberos, sec=dh, and sec=krb4.
3. Verify that at least one directory listing in the /etc/xtab, /etc/dfs/sharetab, or
   /etc/exports file does not contain any of the options that are listed in the check's name list (i.e., secure, kerberos, sec=dh, or sec=krb4).
   You can temporarily add a test entry to the file if necessary. See "Adding and removing export entries" on page 125.
4. Run the demo policy on the test agent to produce the message, NFS exported directory not secure.
5. Reverse any changes that you made to the agent's /etc/xtab, /etc/dfs/sharetab, or /etc/exports file.

To protect your computers

- NFS directories should be exported in secure mode on computers that support secure mode. In secure mode, NFS uses a stronger authentication procedure to ensure that only authorized users can access the directory.

NFS mounted directory

This security check examines the file system table and reports NFS directories that are mounted on the agent. The security check also identifies NFS mount points that allow setuid operations, as well as soft-mounted directories that are writable.

Use the check's file list to specify directories that should be excluded from the check.

The check returns the following messages:

Message name	Title	Class
NFSMOUNTED	NFS mount point	1
NFSSUID	NFS set uid mount	1
NFSRWSOFT	NFS writable soft mount	1

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except NFS mounted directory.
2. Add line entries to the /etc/vfstab, /etc/fstab, or /etc/filesystems file on the agent to produce each of the following messages:

To produce the message	Add these entries to the file system table
NFS mount point	At least one directory with an nfs file system type
NFS setuid mount	A directory with an nfs file system type that does not specify the nosuid option
NFS writable soft mount	A directory with an nfs file system type that specifies the soft option but does not specify the ro option

3. Run the demo policy on the test agent to verify that each of the described formats produces the expected message.
4. Reverse any editing changes that you made to the test agent's permanent /etc/vfstab, /etc/fstab, or /etc/filesystems file.

To protect your computers

- Unmount the NFS directories that are identified as security risks and verify that listings for the unmounted directories are removed from the file system table.

- Add nosuid options to file listings for directories that you choose not to unmount.
- Change soft mounts to hard mounts by removing the soft option or change the rw option to ro to eliminate soft, writable mount points.
- Eliminate all writable mount points if possible.

FTP disabled

This security check reports agents where the file transfer protocol (FTP) utility is disabled.

The security check returns the following message:

Message name	Title	Class
NOFTP	FTP is not configured on your system	0

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except FTP disabled.
2. Verify that the inetd.conf or xinetd.conf configuration file on the test agent does not include a line entry that begins with the FTP server name. You can temporarily comment the line out if it does exist.
3. Run the demo policy on the test agent to produce the message, FTP is not configured on your computer.
4. Reverse any changes that you made to the agent's inetd.conf or xinetd.conf file.

To protect your computers

- This security check provides information and does not require any security action on your part. FTP should be disabled on all computers where it is not absolutely required.

FTP enabled

This security check reports agents where the file transfer protocol (FTP) utility is enabled.

The security check returns the following message:

Message name	Title	Class
FTP_ENABLED	FTP is configured on your system	1

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except FTP enabled.
2. Verify that the inetd.conf or xinetd.conf configuration file on the test agent includes a line entry that begins with the FTP server name. You can temporarily add this entry if it does not exist.
3. Run the demo policy on the test agent to produce the message, FTP is configured on your computer.
4. Reverse any changes that you made to the agent's inetd.conf or xinetd.conf file.

To protect your computers

- Disable FTP on all computers where it is not absolutely required. If it is required, configure it carefully to minimize security risks.

FTP denied users

This security check reports users that are denied access to an agent through the file transfer protocol (FTP) utility.

Use the name list to exclude or include specified user accounts in the check.

The security check returns the following messages:

Message name	Title	Class
NOFTPUSERS	No ftpusers file on your system	1
FTPDENIED	User denied access to FTP	0

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except FTP denied users.

2 Temporarily rename the /etc/ftpusers file if that file exists on the test agent. (On an HP-UX 11+ agent, this file is named /etc/ftpd/ftpusers.)

3 Run the demo policy on the test agent to produce the message, No ftpusers file on your computer.

4 Restore the /etc/ftpusers file (or the /etc/ftpd/ftpusers file on HP-UX 11+) on the test agent before continuing. If the ftpusers file does not exist, you can create it.

5 Verify that the test agent's ftpusers file includes at least one user account name that is not excluded by the check's name list.

6 Run the demo policy on the test agent to produce the message, User denied access to FTP.

7 Reverse any changes that you made to the agent's permanent ftpusers file.

To protect your computers

- Set up an ftpusers file to deny FTP access to the root account, guest accounts, uucp accounts, accounts with restricted shells, and any other accounts that should not copy files across the network.

FTP allowed users

This security check reports users that are allowed access to an agent through the file transfer protocol (FTP) utility.

Use the name list to exclude or include specified user accounts for the check.

The security check returns the following messages:

Message name	Title	Class
NOFTPUSERS	No ftpusers file on your system	1
USERCANFTP	User permitted to use FTP	0

To demonstrate the security check

1 Disable all checks in your Network Integrity module demo policy except FTP allowed users.

2 Temporarily rename the /etc/ftpusers file if that file exists on the test agent. (On an HP-UX 11+ agent, this file is named /etc/ftpd/ftpusers.)

3 Run the demo policy on the test agent to produce the message, No ftpusers file on your computer. Restore the agent's permanent ftpusers file before continuing.

4 Verify that at least one user account on the test agent is neither listed in the ftpusers file nor excluded by the check's name list.

5 Run the demo policy on the test agent to produce the message, User permitted to use FTP.

6 Reverse any changes that you made to the agent's permanent /etc/passwd or ftpusers files.

To protect your computers

- Periodically review the user accounts that are allowed FTP access and update the ftpusers file with account names that should be denied FTP access.

FTP allowed system accounts

This security check reports system accounts such as root and bin that are not denied access to the file transfer protocol (FTP) utility through the ftpusers file.

FTP passwords are transmitted in clear text and could be intercepted. When system accounts are allowed FTP access, attackers can gain privileged access to your computer.

The check returns the following messages:

Message name	Title	Class
NOFTPUSERS	No ftpusers file on your system	1
SYSACCMISS	System account can ftp	1

To demonstrate the security check

1 Disable all checks in your Network Integrity module demo policy except FTP allowed system accounts.

2 Temporarily rename the /etc/ftpusers file if that file exists on the test agent. (On an HP-UX 11+ agent, this file is named /etc/ftpd/ftpusers.)

3 Run the demo policy on the test agent to produce the message, No ftpusers file on your computer. Restore the agent's permanent ftpusers file before continuing.

4 Verify that the test agent's ftpusers file is missing at least one system account name such as root, daemon, or bin. Temporarily remove one of these names if necessary.

5 Run the demo policy on the test agent to produce the message, System account can ftp.

6 Reverse any changes that you made to the agent's permanent ftpuser files.

To protect your computers

- Deny FTP access to system accounts such as root, daemon, and bin by listing those accounts in the agent's ftpusers file.

FTP session logging disabled

This security check reports computers where FTP session logging is not enabled. The check examines the FTP command line parameters in the inetd.conf or xinetd.conf configuration file and configuration entries in the syslog.conf file.

Depending on the operating system, session logging may record session times, user account names, transferred file names, and session login failures.

The security check returns the following message:

Message name	Title	Class
FTP_NOLOG_ SESSION	FTP session logging not configured	1

To demonstrate the security check

1 Disable all checks in your Network Integrity module demo policy except FTP session logging disabled.

2 Edit the agent's inetd, xinetd, or syslog files to ensure that the FTP daemon is not started with the -l parameter or that facilities or priorities are incorrectly identified in the syslog configuration file.

3 Run the demo policy on the test agent to produce the message, FTP session logging not configured.

4 Reverse any changes that you made to the agent's permanent configuration files.

To protect your computers

- Start the FTP daemon with the -l parameter in the inetd.conf or xinetd.conf file to enable session logging. Make sure that facilities and priorities are accurately identified in the syslog.conf file.

FTP debug logging disabled

This security check reports computers where FTP debug logging is not enabled. The check examines the FTP command line parameters in the inetd.conf or xinetd.conf file and configuration entries in the syslog.conf file.

The security check returns the following message:

Message name	Title	Class
FTP_NOLOG_ DEBUG	FTP not configured to log debug messages	1

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except FTP debug logging disabled.
2. Verify that the FTP daemon is not configured to log debug messages in the agent's inetd, xinetd, tlid, or syslog configuration files.
3. Run the demo policy on the test agent to produce the message, FTP not configured to log debug messages.
4. Reverse any changes that you made to the agent's permanent configuration files.

To protect your computers

- See instructions from your FTP service provider to configure the FTP daemon to log debug messages.

Anonymous FTP enabled

This security check reports computers where anonymous FTP access is permitted. The check verifies that the FTP daemon is running and looks for an FTP account in the agent's /etc/passwd file.

If the check does not find the FTP account in the /etc/passwd file, it examines user information in any NIS or NIS+ services that are used by the computer.

The security check returns the following message:

Message name	Title	Class
ANONFTP	Anonymous FTP permitted	0

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except Anonymous FTP enabled.

2 Verify that the inetd.conf or xinetd.conf file includes a line entry that starts with FTP and that an account with the FTP user name exists in the /etc/passwd file.

3 Run the demo policy on the test agent to produce the message, Anonymous FTP permitted.

4 Reverse any changes that you made to the agent's permanent inetd.conf, xinetd.conf, or /etc/passwd files.

To protect your computers

- This security check provides information and does not require any security action on your part. Anonymous FTP access is not generally considered a security risk because access is limited to files that are located in the FTP home directory.

Anonymous FTP owner

This security check reports computers with anonymous FTP directories that are not owned by root.

The FTP directory should be owned by root to prevent unauthorized users from accessing or modifying the files that are transferred to and from that directory.

If the check does not find the FTP account in the /etc/passwd file, it examines user information in any NIS or NIS+ services that are used by the computer.

The security check returns the following message:

Message name	Title	Class
ROOTOWN	Root should own FTP directory	4

To demonstrate the security check

1 Disable all checks in your Network Integrity module demo policy except Anonymous FTP owner.

2 Verify that FTP is started in the agent's inetd.conf or xinetd.conf file.

3 Verify that the user ID for the owner of the FTP home directory (~ftp) does not equal 0 in the /etc/passwd file.

4 Run the demo policy on the test agent to produce the message, Root should own FTP directory.

5 Reverse any changes that you made to the agent's permanent inetd.conf, xinetd.conf, or /etc/passwd files.

To protect your computers

- Use the chown command or the Correct function in the console grid to change user ownership of the anonymous FTP account to root.

Anonymous FTP permissions

This security check reports computers with anonymous FTP directories that are writable by users other than the account owner, which should be root.

If the check does not find the FTP account in the /etc/passwd file, it examines user information in any NIS or NIS+ services that are used by the computer.

The security check returns the following message:

Message name	Title	Class
NOTWRITE	Should not have write permissions	4

. To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except Anonymous FTP permissions.
2. Verify that FTP is started in the agent's inetd.conf or xinetd.conf file.
3. Verify that at least one user account is granted write permissions to the FTP home directory (~ftp) or to the bin, etc, or pub subdirectories within that directory.
4. Run the demo policy on the test agent to produce the message, Should not have write permissions.
5. Reverse any changes that you made to the agent's permanent inetd.conf, xinetd.conf, or /etc/passwd files.

To protect your computers

- Use the chmod command or the Correct function in the console grid to remove write permissions from the FTP home directory.

TFTP

This security check examines the security of the trivial file transfer protocol (TFTP) service and reports TFTP daemons that are running as privileged users and daemons that are not running in secure mode.

The security check also examines TFTP access control on AIX computers and the security of the TFTP user account on HP-UX computers.

Note: When checking UNIX file permissions, this check does not consider extended permissions such as access control lists (ACLs), which are available on some UNIX operating systems and through some third-party extensions.

The check returns the following messages:

Message name	Title	Class
NOTFTP	TFTP is not configured on your system	0
HASTFTP	TFTP is configured on your system	1
SGID_TFTPD	TFTP daemon running as SGID	1
SUID_TFTPD	TFTP daemon running as SUID	1
TFTPD_WRAPPERS	TFTP daemon running with tcp wrappers	1
ULTRIX_UNSECURE _TFTP	TFTP daemon is not running in secure mode	4
SUNOS_UNSECURE_ TFTP	TFTP daemon is not running in secure mode	4
SVR32_UNSECURE_ TFTP	TFTP daemon is not running in secure mode	4
AIX_UNSECURE_ TFTP	TFTP daemon is not configured securely	4
AIX_NO_ TFTPACCESS	TFTP is not secure; tftpaccess.ctl is missing	4
AIX_BAD_ TFTPACCESS	TFTP is not secure; tftpaccess.ctl is ineffective	4
AIX_TFTPACCESS	TFTP daemon allows /denies access on directory	0
AIX_TFTPDENY	TFTP daemon does not allow access on any directories	0
AIX_WRONG_USER	The TFTPd server does not have the nobody user ID	1
AIX_REMOTE_ CREATE	The TFTPd server allows remote users to create files	1
AIX_DEFAULT_DIR	A default TFTP destination directory has been specified	0
AIX_TX_LOGGING	TFTP transfer logging is not enabled	1
AIX_ADDR_ LOGGING	The TFTPd server is logging IP addresses with errors	0
AIX_ADDR2HOST	The TFTPd server is converting IP addresses to host names	0
AIX_SOCKLVL_ DEBUG	Tftpd socket-level debugging is enabled	0

Message name	Title	Class
TFTP_ACC_MISS	No TFTP user account	1
TFTP_BAD_SHELL	Shell used by TFTP user account is bad	1
TFTP_BAD_DIR	Home directory for TFTP account not set	0
TFTP_NOHOME	TFTP account does not have a home directory	0
TFTP_BAD_UID	TFTP account does not own its home directory	0

To demonstrate the security check

1 Disable all checks in your Network Integrity module demo policy except the TFTP check.

2 Add entries to the test agent's inetd.conf or xinetd.conf file and to the tftpaccess.ctl and /etc/passwd files to produce the following messages:

To produce the message	Edit the named files on the test agent
TFTP is not configured on your system	Verify that inetd.conf or xinetd.conf does not include a line entry that begins with the TFTP server name. If the line exists, temporarily comment it out.
TFTP is configured on your system	Restore or create the line entry in the inetd.conf or xinetd.conf file that enables the TFTP server. The line entry begins with the TFTP server name.
TFTP daemon running as SGID	Verify that the TFTP command line in the inetd.conf or xinetd.conf file names a file that runs with SGID privileges in the Server Program field.
TFTP daemon running as SUID	Verify that the TFTP command line in inetd.conf or xinetd.conf names a file that runs with SUID privileges in the Server Program field.
TFTP daemon running with tcp wrappers	Verify that the TFTP command line in inetd.conf or xinetd.conf specifies a tcpd file in the Server Program field and does not provide a program file path name in the Server Program Arguments field.

To produce the message	Edit the named files on the test agent
TFTP daemon is not running in secure mode	On Solaris agents, verify that the TFTP command line in the inetd.conf file does not include the -s option in the Server Program Arguments field. Note: The SUNOS_UNSECURE_TFTP message returns on HP-UX, NCR, and Sequent agents even when the TFTP command is run with the -s option. On Digital UNIX (Tru64) agents, verify that the TFTP command line in the inetd.conf file does not include the -r option in the Server Program Arguments field.
TFTP daemon is not configured securely	On AIX agents, verify that the /etc/tftpaccess.ctl file does not exist or that it does not include any line entries that begin with the keywords allow: or deny: .
TFTP is not secure; tftpaccess.ctl is missing	On AIX agents, temporarily rename the /etc/tftpaccess.ctl file if it exists.
TFTP is not secure, tftpaccess.ctl is ineffective	On AIX agents, restore or create the /etc/tftpaccess.ctl on the test agent, then do one or all of the following: ■ Change the file so it is not owned by root. ■ Change the file type to a directory or device file (not a regular file). ■ Make sure that file permissions do not equal 644.
TFTP daemon allows/denies access on directory	On AIX agents, verify that the /etc/tftpaccess.ctl file includes one or more line entries that begin with the keywords, allow: or deny: .
TFTP daemon does not allow access on any directories	On AIX agents, verify that the /etc/tftpaccess.ctl file does not include any line entries that begin with the keyword, allow: .
The TFTPd server does not have the nobody user ID	On AIX agents, verify that the tftp command line in the inetd.conf file does not specify nobody in the User field.
The TFTPd server allows remote users to create files	On AIX agents, verify that the tftp command line in the inetd.conf file contains the -n option in the Server Program Arguments field.
A default TFTP destination directory has been specified	On AIX agents, verify that the tftp command line in the inetd.conf file contains the -d option in the Server Program Arguments field.
TFTP transfer logging is not enabled	On AIX agents, verify that the tftp command line in the inetd.conf file does not contain the -v option in the Server Program Arguments field.

To produce the message	Edit the named files on the test agent
The TFTPd server is logging IP addresses with errors	On AIX agents, verify that the tftp command line in the inetd.conf file contains the -i option in the Server Program Arguments field.
The TFTPd server is converting IP addresses to host names	On AIX agents, verify that the tftp command line in the inetd.conf file contains the -r option in the Server Program Arguments field.
Tftpd socket-level debugging is enabled	On AIX agents, verify that the tftp command line in the inetd.conf file contains the -s option in the Server Program Arguments field.
No TFTP user account	On HP-UX agents, verify that the TFTP user is not listed in the test agent's /etc/passwd file. You can temporarily rename the TFTP user if one exists. If this check does not find the TFTP user name in the /etc/passwd file, it checks user information in any NIS or NIS+ services that are used by the system.
Shell used by TFTP user account is bad	On HP-UX agents, verify that no shell is specified for the TFTP user in the test agent's /etc/passwd file. This message is also returned if the shell specified is not a disabling shell such as /bin/true, /bin/false, /dev/null, true, or false.
Home directory for the TFTP account not set	On HP-UX agents, verify that no home directory is specified for the TFTP user in the test agent's /etc/passwd file.
TFTP account does not have a home directory	On HP-UX agents, verify that the /etc/passwd file specifies a home directory for the TFTP user that does not exist. You can temporarily rename the directory if necessary.
TFTP account does not own its home directory	On HP-UX agents, verify that the /etc/passwd file specifies a home directory for the TFTP user that is not owned by the TFTP user.

3 Run the demo policy on the test agent to verify the preceding messages.

4 Reverse any editing changes that you made to the test agent's permanent inetd.conf, xinetd.conf, /etc/tftpaccess.ctl, or /etc/passwd files.

To protect your computers

- If the agent does not need to transfer files to and from other computers, remove the TFTP listing from the inetd.conf or xinetd.conf file to disable the TFTP daemon.
- If the TFTP daemon cannot be disabled, remove any SUID or SGID privileges and run the TFTP daemon in secure mode on all computers that support secure mode.
- On AIX computers, create and maintain the /etc/tftpaccess.ctl file to specify directories that are allowed and denied access by TFTP. Verify that this file is owned by root and that its permission bits are set to 644.
- Routinely check the directories and subdirectories that are allowed TFTP access by listings in the tftpaccess.ctl file on AIX computers to ensure that they contain only files that you wish to make available to anyone on your network.
- Edit the TFTP line in the inetd.conf file on AIX computers to make sure that the TFTP server:
  - Runs with the nobody user ID.
  - Does not run with the -n option, which allows remote users to create files on the system.
  - Runs with the -v option, which produces log entries that can be used to track suspected security breaches.
- Ensure that the TFTP account is listed in the /etc/passwd file.
- Set the TFTP user account shell to a disabling shell such as /bin/false, and specify a home directory that is owned by the TFTP user.

NIS/NIS+ enabled

This security check examines the network information name service that is used by the agent. The check reports:

- Whether NIS or NIS+ is enabled and, if enabled, which version is being used.
- The agent's default domain name and the domain name server.

The check returns the following messages:

Message name	Title	Class
NIS_ENABLED	NIS enabled	0
NIS_PLUS_ ENABLED	NIS+ enabled	0
NIS_DISABLED	NIS not enabled	0

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except the NIS/NIS+ enabled check.
2. Run **ps** with the appropriate options to generate a list of all processes that are currently running on the test agent. For example, on Solaris, run **ps -e**
3. Verify that the NIS and/or NIS+ daemons are set to produce the following messages in the test agent's active process list:

To produce the message	Verify that
NIS enabled	The NIS daemon, ypbind, is included in the list of active processes.
NIS+ enabled	The NIS+ daemon, rpc.nisd, is included in the list of active processes.
NIS not enabled	Neither ypbind nor rpc.nisd are running as active processes. You can temporarily stop these processes, if you want to, then restart them after verification.

4. Run the demo policy on the test agent to verify that each of the preceding formats produces the expected message.

To protect your computers

- Check your agent configuration to determine whether NIS or NIS+ should be enabled.
- If NIS is enabled, verify that the domain name and domain server are set correctly. If NIS+ is enabled, verify that the domain name and master server are set correctly.

Netgroup information

This security check compares netgroup listings that are stored in the NIS network information name service with Netgroup Info template records that define the netgroups on your computers. Netgroup listings identify which hosts and users have remote access.

Note: This security check is not currently supported on agents that are using the NIS+ network information name service.

Use the check's template file lists to enable a Netgroup Info template for the check. Do not enable the default netgroup.ngr template file before you edit the template to include authorized netgroups on your UNIX computers.

The security check returns the following messages:

Message name	Title	Class
NO_MATCHED_NETGROUP	Netgroup not matched	1
NO_MATCHED_ TRIPLE	Triple not matched	1
WILDCARD_FIELD	Wildcard field found	1
UNUSED_NETGROUP	Netgroup not used	0
UNUSED_TRIPLE	Triple not used	0

Editing the Netgroup Info template

The Netgroup information check uses the Netgroup Info template to define the netgroups that are authorized by your security policy.

To create the Netgroup Info template

1. In the tree view, right-click **Templates**, then click **New**.
2. Select the **Netgroup Info-all** template type.
3. Type a new template file name of no more than eight characters without an extension. Symantec ESM adds .ngr to the file name.
4. Click **OK**.
5. In the Template Editor, add records and sublist entries.
6. Click **Save**.
7. Click **Close**.

To add a record to the Netgroup Info template

1. If the template is not already open in the Template Editor, double-click the template file in the tree view.
2. In the Template Editor, click **Add Row**.
3. In the Netgroup Name field of the new row, replace <NEW> with the name of a netgroup on your computers.
4. Add one or more Members sublist rows.

5 Click **Save**. To add another record, repeat steps 2–5.

6 Click **Close**.

To add a row to the Members sublist

1 In the Template Editor, click the Members field of the row that you are editing.

2 In the Templates Sublist Editor, click **Add Row**.

3 Do one of the following:

- If the member is identified by the computer name, user name, domain name format, check the Triple Netgroup check box.
- If the member is identified by another netgroup name, uncheck the Triple Netgroup check box.

4 Do one of the following:

- If the member uses the triple name format, replace <NEW> with the appropriate name in the Host/Netgroup Name, User Name, and Domain Name fields.
- If the member does not use the triple name format, replace <NEW> with the netgroup name in the Host/Netgroup Name field.

5 Click **Apply**, then repeat steps 2 through 7 to add additional rows to the Members sublist.

6 Click **Close**.

To remove Members sublist rows

1 In the Template Sublist Editor, click the numbered button in the leftmost column of the row that you want to remove.

To select a range of rows, hold down the **Shift** key while you click the leftmost, numbered buttons in the first and last rows that you want to move.

To select non-sequential rows, hold down the **Ctrl** key while you click the leftmost, numbered buttons in the rows you want to remove.

2 Click **Remove Rows**.

3 Click **Apply**.

4 Click **Close** to exit the Template Sublist Editor.

To remove Netgroup Info template records

1 In the Template Editor, click the numbered button in the leftmost column of the record that you want to remove.

To select a range of rows, hold down the **Shift** key while you click the first and last numbered buttons in the range of rows that you want to remove.

To select non-sequential rows, hold down the **Ctrl** key while you click the leftmost, numbered buttons on the rows that you want to remove.

2 Click **Remove Entry(s)**.

3 Click **Apply**.

4 Click **Close** to exit the Template Editor.

To demonstrate the security check

1 Disable all checks in your Network Integrity module demo policy except the Netgroup information check.

2 Run **ps** with appropriate options to generate a list of all active processes and verify that the NIS daemon ypbind is running on the test agent.

3 Run **ypcat -k netgroup** to generate a list of netgroups that are defined on the NIS domain server that the test agent is using.
Each netgroup listing consists of a netgroup name, a blank space, and a triple. The triple, which is enclosed in parentheses, defines the netgroup member by computer name, user name, and domain name, using commas as field separators.
For example, the following netgroup listing identifies a specific host and user in a specific domain as a member of netgroup1:
netgroup1 (host1,user1,domain1)
Blank fields in a triple are read as any or all hosts, or any or all users. For example, **netgroup2 (,,domain2)** identifies all hosts and all users in a specific domain as members of netgroup2.

4 Use the Template Editor to create and/or edit the Netgroup Info template that defines authorized netgroups in the test agent's NIS domain. See "Editing the Netgroup Info template" on page 150 for editing instructions.

5 Compare the netgroup listings that are generated by the ypcat -k netgroup command with records in the Netgroup Info template to verify that the following discrepancies exist between system listings and template listings:

To produce the message	Verify that
Netgroup not matched	At least one of the netgroup names on the system is not named in the template.
Triple not matched	At least one of the triples on the system is not matched by a Members sublist record in the template.
Wildcard field found	At least one unmatched triple on the system contains a wildcard field (i.e., a field that is empty).

To produce the message	Verify that
Netgroup not used	At least one netgroup in the template is not matched by a netgroup name on the system.
Triple not used	At least one triple defined in a Members sublist record in the template is not matched by a triple on the system.

6 Enable the *.ngr template file that defines your authorized netgroups in the Netgroup information check editor.

7 Run the demo policy on the test agent to verify each of the preceding messages.

8 Reverse any template editing changes or changes to netgroup listings in NIS that you made only for test purposes.

To protect your computers

- Update the Netgroup Info template to include all authorized netgroups and netgroup members that are allowed remote access to your computers.
- Carefully review the netgroup listings in NIS to ensure that any changes to netgroups or netgroup members are authorized.

NIS netgroups

This security check lists the netgroups that are stored in the NIS network information name service that is used by the agent. Netgroup listings identify hosts and users that have remote access to computers in listed domains.

Note: This security check is not currently supported on agents that use the NIS+ network information name service.

The security check returns the following message:

Message name	Title	Class
NIS_NISPLUS_NETGROUP	NIS netgroup	0

To demonstrate the security check

1 Disable all checks in your Network Integrity module demo policy except the NIS netgroups check.

2 Run **ps** with appropriate options to generate a list of all active processes and verify that the NIS daemon ypbind is running on the test agent.

3 Run **ypcat -k netgroup** to generate a list of the netgroups that are defined on the NIS domain server that the test agent is using.

4 Run the demo policy on the test agent and verify that all netgroups that are listed by the ypcat command are reported by the NIS netgroup message.

To protect your computers

- Periodically review the netgroups and netgroup members that are allowed remote access to your computers through NIS.

Hosts.lpd allows all hosts and users

This security check reports agents with a hosts.lpd file that contains a line with only the plus sign (+) character. This entry allows all users on all hosts to use the system printers.

The security check returns the following message:

Message name	Title	Class
LPD_ALLIN	All users on all hosts trusted for printing	1

To demonstrate the security check

1 Disable all checks in your Network Integrity module demo policy except Hosts.lpd allows all hosts and users.

2 Verify that the agent's hosts.lpd file includes a line entry that contains only the plus sign (+) character. Temporarily add this entry if necessary.

3 Run the demo policy on the test agent to produce the message, All users on all hosts trusted for printing.

4 Reverse any changes that you made to the agent's hosts.lpd file.

To protect your computers

- Each line that begins with the plus sign (+) character in the agent's hosts.lpd file should specifically name the hosts and users that are authorized to use your system printers. Granting printer access to all remote users on all remote hosts makes your computer vulnerable to attackers.

Hosts.lpd invalid comment characters

This security check reports agents with a hosts.lpd file that contains lines with exclamation point (!) or pound sign (#) characters.

These characters are valid comment identifiers in other UNIX text files, but they are not valid in the hosts.lpd file.

The security check returns the following message:

Message name	Title	Class
LPD_COMMENT	Invalid comment character in hosts.lpd	1

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except Hosts.lpd invalid comment characters.
2. Verify that the agent's hosts.lpd file includes at least one line entry that begins with the exclamation point (!) or pound sign (#) character to identify the line as a comment line. Temporarily add comments using each of these characters if necessary.
3. Run the demo policy on the test agent to produce the message, Invalid comment character in hosts.lpd.
4. Reverse any changes that you made to the agent's hosts.lpd file.

To protect your computers

- Remove all lines that are identified by exclamation point (!) and pound sign (#) characters from the hosts.lpd file to avoid unexpected results with some versions of lpd.

Hosts.lpd invalid dash character

This security check reports agents where the first character in the hosts.lpd file is a dash (-) character. The location of this line at the beginning of the hosts.lpd file could give attackers unauthorized access to your computer. See CERT CA-91:12.

The security check returns the following message:

Message name	Title	Class
LPD_DASH	Invalid dash character in hosts.lpd	1

To demonstrate the security check

1. Disable all checks in your Network Integrity module demo policy except Hosts.lpd invalid dash characters.
2. Verify that the first line in the agent's hosts.lpd file includes only a dash (-) character. Temporarily add this line if necessary.
3. Run the demo policy on the test agent to produce the message, Invalid dash character in hosts.lpd.
4. Reverse any changes that you made to the agent's hosts.lpd file.

To protect your computers

- If your permanent hosts.lpd file includes a line with only a dash (-) to indicate that all remote users on all remote hosts are denied access to your system printers, it should not be at the beginning of the hosts.lpd file.

Print servers

This security check reports computers that are running as print servers. It verifies that a print spooler daemon is running, that it has at least one printer defined, and that at least one remote host can send jobs to its queues.

The security check returns the following messages:

Message name	Title	Class
LPD_SERVER	System acting as an lpd print server	1
LPSCHED_ SERVER	System acting as an lpsched print server	1

Print service without printers

This security check reports computers that are running a print spooler daemon but have not defined any printers. There is no reason to run this daemon if it isn't needed.

The check returns the following messages:

Message name	Title	Class
LPD_NO_ PRINTER	Daemon lpd is running without any defined printers	1
LPDSCHED_NO_PRINTER	Daemon lpsched is running without any defined printers	1

Listening TCP ports

This check reports listening TCP ports. The check also reports the process that opened the port if the /usr/sbin/lsof program exists on the agent. Use the check's name list to specify port numbers that should not be reported.

The check returns the following message:

Message name	Title	Class
OPEN_PORT	The named port is listening	4

To protect your computers

- If the named port should be open, add the port number to the name list of excluded ports for the Listening TCP ports check.
- If the named port should not be open, stop the process that is using the port to protect your computers from unauthorized access.

New listening TCP ports

This check reports TCP ports that have been opened for listening since the last snapshot update. The check also reports the process that opened the port if the /usr/sbin/lsof program exists on the agent. Use the check's name list to specify port numbers that should not be reported.

Note: On agents that use Security Update 12 or lower, use this check to report both TCP and UDP ports.

The check returns the following updateable message:

Message	Title	Class
NEW_LISTENING_TCP_PORT	New listening TCP port	4

To demonstrate the check

1. Run a policy with this check enabled to create the snapshot.
2. Open a new TCP port.
3. In a demo policy, disable all checks in the Network Integrity module except New listening TCP ports.
4. Run the demo policy on the agent.
5. Verify that New listening TCP port is reported.

Deleted listening TCP ports

This check reports TCP ports that have been closed for listening since the last snapshot update. The check also reports the process that opened the port if the /usr/sbin/lsof program exists on the agent. Use the check's name list to specify TCP port numbers that should not be reported.

Note: On agents that use Security Update 12 or lower, use this check to report both TCP and UDP ports.

The check returns the following updateable message:

Message	Title	Class
DELETED_LISTENING_TCP_PORT	Deleted listening TCP port	3

To demonstrate the check

1. Run a policy with this check enabled to create the snapshot.
2. Close an open TCP port.
3. In a demo policy, disable all checks in the Network Integrity module except Deleted listening TCP ports.
4. Run the demo policy on the agent.
5. Verify that Deleted listening TCP port is reported.

Modified listening TCP ports

This check reports processes that have changed TCP owners since the last snapshot update. The check also reports the process that opened the port if the /usr/sbin/lsof program exists on the agent. Use the check's name list to specify port numbers that should not be reported.

Note: On agents that use Security Update 12 or lower, use this check to report both TCP and UDP ports. Modified listening UDP ports reports no messages.

The check returns the following updateable message:

Message	Title	Class
MODIFIED_LISTENING_TCP_PORT	Modified listening TCP port	3

To demonstrate the check

1. Run a policy with this check enabled to create the snapshot.
2. Change the owner of an existing process.
3. In a demo policy, disable all checks in the Network Integrity module except Modified listening TCP ports.
4. Run the demo policy on the agent.
5. Verify that Modified listening TCP port is reported for both processes.

To protect your computers

- In the console grid, update the snapshot file for authorized changes.
- Restore the correct process owner or port for unauthorized changes

Listening UDP Ports

This check reports listening UDP ports. The check also reports the process that opened the port if the /usr/sbin/lsof program exists on the agent. Use the check's name list to specify port numbers that should not be reported.

This check returns the same message as the preceding Listening TCP ports check.

To protect your computers

- If the named port should be open, add the port number to the name list of excluded ports for the Listening UDP Ports check.
- If the named port should not be open, stop the process that is using the port to protect your computers from unauthorized access.

New listening UDP ports

This check reports UDP ports that have been opened for listening since the last snapshot update. The check also reports the process that opened the port if the /usr/sbin/lsof program exists on the agent. Use the check's name list to specify port numbers that should not be reported.

Note: On agents that use Security Update 12 or lower, this check reports no messages. Use New listening TCP ports, which reports both TCP and UDP ports.

On agents that use Security Update 13 or higher, this check returns the following updateable message:

Message	Title	Class
NEW_LISTENING_UDP_PORT	New listening UDP port	4

To demonstrate the check

1. Run a policy with this check enabled to create the snapshot.
2. Open a new UDP port.
3. In a demo policy, disable all checks in the Network Integrity module except New listening UDP ports.
4. Run the demo policy on the agent.
5. Verify that New listening UDP port is reported.

Deleted listening UDP ports

This check reports UDP ports that have been closed for listening since the last snapshot update. The check also reports the process that opened the port if the /usr/sbin/lsof program exists on the agent. Use the check's name list to specify port numbers that should not be reported.

Note: On agents that use Security Update 12 or lower, this check reports no messages. Use Deleted listening TCP ports, which reports both TCP and UDP ports.

On agents that use Security Update 13 or higher, this check returns the following updateable message:

Message	Title	Class
DELETED_LISTENING_UDP_PORT	Deleted listening UDP port	3

To demonstrate the check

1. Run a policy with this check enabled to create the snapshot.
2. Close an open UDP port.
3. In a demo policy, disable all checks in the Network Integrity module except Deleted listening UDP ports.

4 Run the demo policy on the agent.

5 Verify that Deleted listening UDP port is reported.

Modified listening UDP ports

This check reports processes that have changed UDP owners since the last snapshot update. The check also reports the process that opened the port if the /usr/sbin/lsof program exists on the agent. Use the check's name list to specify port numbers that should not be reported.

Note: On agents that use Security Update 12 or lower, this check reports no messages.

Use Modified listening TCP ports to report both TCP and UDP ports on agents that use Security Update 12 or lower.

On agents that use Security Update 13 or higher, this check returns the following updateable message:

Message	Title	Class
MODIFIED_LISTENING_UDP_PORT	Modified listening UDP port	3

To demonstrate the check

1 Run a policy with this check enabled to create the snapshot.

2 Change the owner of an existing process.

3 In a demo policy, disable all checks in the Network Integrity module except Modified Listening UDP Ports.

4 Run the demo policy on the agent.

5 Verify that Modified listening UDP port is reported for both processes.

To protect your computers

- In the console grid, update the snapshot file for authorized changes.
- Restore the correct process owner or port for unauthorized changes.

Access control (xhost)

This check reports computers that have xhost + in X Windows invoked.

If the xhost+ command is issued on an X11 server, any external X11 client could connect to the server. Using xhost + also lets remote users watch keystrokes, capture windows, or insert command strings into your windows. Computer networks are particularly vulnerable when users with root access to a computer use xhost +.

There are safer alternatives to running xhost +. You can use SSH (Secure Shell) to connect to remote computers. SSH allows the tunneling of X11 traffic, eliminating any need for xhost +. You could also use TCP wrappers to secure your xhost communications.

Note: This check reports only computers that have access control disabled at the time of the policy run. This check cannot identify computers where X Windows access control was disabled and then reenabled.

This check returns the following messages:

Message	Title	Class
NOXHOSTCHK	Error with xhost command	3
ACCESS_DISABLED	Access control disabled	3
ACCESS_UNKNOWN	Access control unknown	0

To protect you computers

- Tunnel all X11 traffic through SSH, use TCP wrappers, or use another similar method to secure your xhost communications.
- If you must use xhost, specify the computers that will be given access by name. For example, use xhost + <computer_name>.

Object Integrity

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

When checking UNIX file permissions, this module examines only basic user/group/other and read/write/execute permissions. It does not consider extended permissions such as access control lists (ACLs), which are available on some UNIX operating systems and some third-party extensions.

The module also creates and maintains the sifdev.dat device snapshot files. Run the module one time to create the baseline snapshot file on each agent, then periodically rerun the module to detect changes.

Updateable Object Integrity messages

The UNIX Object Integrity module has three security checks that let you update records in the sifdev.dat snapshot file to match current values on the agent. Snapshot-updateable messages display the letters SU in the Updateable/Correctable column of the console grid.

Security check	Message name
New devices	NEWDEVICE
Deleted devices	DELDEVICE
Changed devices	CHGDEVICE

Device directories

Use this option to specify directories that contain special device files on your computers. Missing directories are ignored. The directory list defaults to /devices on Solaris computers and to /dev on all other supported UNIX operating systems.

New devices

This security check reports any devices that have been added since the last time the agent's device snapshot file was updated.

The check returns the following message:

Message name	Title	Class
NEWDEVICE	New system device	1

To protect your computers

- Check all new devices to make sure they were authorized by a system administrator. Remove any unauthorized devices and update the agent's device snapshot file to include all authorized devices.

Deleted devices

This security check reports any devices that have been deleted since the last time the agent's device snapshot file was updated.

The check returns the following message:

Message name	Title	Class
DELDEVICE	Deleted system device	1

To protect your computers

- Check all deleted devices to make sure the deletions were authorized by a system administrator. Restore any devices that should not have been deleted and update the agent's device snapshot file to reflect all authorized deletions.

Changed devices

This security check reports any devices that have been changed since the last time the agent's device snapshot file was updated.

The check returns the following message:

Message name	Title	Class
CHGDEVICE	Changed system device	1

To protect your computers

- Check all changed devices to make sure the changes were authorized by a system administrator. Reverse any unauthorized changes and update the agent's device snapshot file to include all authorized changes.

Disk and memory access

This security check looks at disk and memory special device files to make sure that they are owned by a privileged UID or a privileged GID and do not provide any other access.

The check returns the following messages:

Message name	Title	Class
ACCUSR	Improperly owned special device file	4
ACCGRP	Special device file with non-privileged group access	4
ACCOTH	Special device file with other access	4

To protect your computers

- Make sure all named special device files are owned by privileged users and user groups and that they cannot be accessed by other users on your computers.

Exclude devices

Use this option to exclude specified, special device files from all module security checks. Exclude a file only if you are certain that the file is protected and does not pose a security risk.

OS Patches

The OS Patches module reports patches that have been released for UNIX operating systems but are not found on the agent. Released patches are defined in template files. New patch templates are avilable every two weeks through LiveUpdate.

Note: If you modify the Patch templates that are provided in Security Update releases, the security checks that are run by best practice policies will not be predictable.

Editing the Patch template

The Patch template defines the operating system patches that are checked by the OS Patches module.

You can add or delete Patch templates. You can also copy Patch template files in the /esm/template directory on a UNIX manager computer, then open the renamed template files in the Template Editor to add checks for new operating system patches and hot fixes.

Note: Do not edit the Patch templates provided in Security Updates. Instead copy them and edit the copy. If you modify Patch templates that are provided by Security Update releases, the behavior of best practice policies will not be predictable.

To add a new Patch template

1. Right-click the Templates icon in the tree view, then click **New**.
2. In the Available template types list, select the type of template that you want to add.
3. In the Template file name text box, type a new template name of no more than eight characters. Symantec ESM adds the file extension that is consistent with the template type that you selected.
4. Press **Enter**.

To copy a Patch template

1 Open the /esm/template directory on the manager that contains the template file you want to edit.

2 Copy the template file that you want to edit to a different file in the /esm/template directory.

To add a record to a Patch template

1 If the Template Editor is not already open, double-click the name of the template in the tree view.

2 In the Template Editor, click **Add Row**.

3 In the new row (record), type the following information:

Field	Description
CERT ID	ID number assigned to a CERT advisory or vendor bulletin associated with this patch.
Date	Date that an advisory or bulletin was published or last updated in the yyyy/mm/dd format.
OS	One of the following operating systems: **redhat-x86** **aix-rs6k** **osf1-axp** **hpux-hppa** **solaris-sparc**
Revision	The version of the operating system to which the patch applies. Specify the revision as it is displayed by the **uname -r** command, with the following exceptions: Redhat Linux. The **uname** command displays the version of the kernel, not the RedHat Linux version. The RedHat Linux version can be determined by executing **/bin/rpm -q redhat-release -i** and looking in the Version field. AIX. The version specified should be a combination of the version reported by **uname -v** and the revision reported by **uname -r** separated by a period (e.g. 4.2). Specifying a version more specific than the release (e.g. 4.2.1) is not supported. HP-UX. Do not include the "B" in the revision name (i.e. 11.00 not B.11.00). OSF-1. Do not include the "V" in the revision name (i.e. 4.0 not V4.0). You can also specify a letter following the version (e.g. 4.0D).

Field	Description
Patch ID	Vendor patch ID: Solaris. The patch ID (e.g. 104443-02). AIX. You can specify a fileset name and version separated by a bar (|). For example: bos.rte.printers|4.2.1.0 Or you can specify an APAR number (e.g. IX67177). Using fileset names and versions is more accurate because the APAR may not be reported as installed if it is included in the base operating system operating system or as part of a maintenance release installation. HP-UX. The patch name (e.g. PHCO_25890). Linux. An RPM name and version separated by a vertical bar (|). For example: wu-ftpd|2.6.1-0.6x.21 OSF1. The patch or software subset name (e.g.. OSFPAT00005200).
Architecture	This field is only used for HP-UX patches. Set it to S700 if the patch applies to 700 version hardware, S800 if it applies to 800 version hardware, or leave it blank if it applies to any version of hardware.
Description	Patch description (usually matches advisory or bulletin title).

4 In the Severity field, assign a severity code to the patch.
The Patch template severity code determines which of the following messages the Patch module reports if a specified patch is not installed or a forbidden patch is installed:

Severity code	Security message	Security level
0	PATCHNOTINS0	Green
1	PATCHNOTINS1	Yellow
2	PATCHNOTINS2	Yellow
3	PATCHNOTINS3	Red
0	FORBIDDEN_PATCH_0	Green
1	FORBIDDEN_PATCH_1	Yellow
2	FORBIDDEN_PATCH_2	Yellow
3	FORBIDDEN_PATCH_3	Red

If the value in the Patch ID field is PENDING, a severity code of 2 or 3 is required. In this case, the severity code determines which message to report for a patch that should be installed when it is available:

Severity code	Security message	Security level
2	PATCHNOTAVAIL2	Yellow
3	PATCHNOTAVAIL3	Red

5 Select a patch type:

- **Mandatory**. This patch must be installed.
- **Forbidden**. This patch must not be installed.
- **Optional**. This is a "rollup" patch that is not required, but supersedes other patches listed in the template. If this patch is not installed, no message is reported.
  If a patch is marked Optional but does not supersede any patches in the template, Symantec ESM reports the following message:

Message name	Title	Class
OPTIONAL_PATCH_NO_SUPERSEDE	Optional patch supersedes nothing	2

- **Feature-specific (Linux and AIX only)**. When using Feature-specific, if the RPM name and version for Linux or the fileset and version for AIX is entered in the Patch ID field, Symantec ESM reports an error message when the installed RPM or fileset is older than the specified RPM or fileset. If no version of the RPM or fileset is installed, no message is reported.
  If you select Feature-specific but do not enter the Patch ID information, the patch is treated as Mandatory.

6 Add rows to the following sublists:

- Superseded (see "To add a row to the Superseded sublist" on page 170.)
- Conditions (see "To add a row to the Conditions sublist" on page 170.)

Note: The Files sublist is currently not used in UNIX modules. Leave the Files sublist empty.

7 Click **Save**.

8 Click **OK**.

To add a row to the Superseded sublist

1. In the Template Editor, click the Superseded field of the row that you are editing.
2. In the Template Sublist Editor, click **Add Row**.
3. In the Description field, select one of the following:
   - **Replaced by**. The patch specified in the Template Editor row will be replaced by the patch specified in the newly created Superseded sublist row.
   - **Replaces**. The patch specified in the Template Editor row replaces the patch specified in the newly created Superseded sublist row
4. In the Patch ID field, type the ID number of the superseding or superseded patch.
5. Click **Apply**.
   To add another row, repeat steps 2–5
6. Click **Close**.

To add a row to the Conditions sublist

1. In the Template Editor, click the Conditions field of the row that you are editing.
2. In the Template Sublist Editor, click **Add Row**.
3. Click the Type field, then select one the following conditions:
   - **Inetd - Check inetd for service**
     When checking inetd for services, Symantec ESM looks in the inetd.conf or xinetd.conf configuration file, depending on the UNIX version.
   - **Process - Check running processes**
     Only system-owned processes, and parameters that are running on system-owned processes, are reported.
   - **File - Check for existing file**
     Symantec ESM only checks the patch if the named file exists
4. Click the Name field, then replace <NEW> with the name of a service that must be enabled, or a process that must be running, or a file that must exist before the patch that is defined on the same template row is examined.
5. Click **Apply**.
   To add another record, repeat steps 2–5.
6. Click **Close**.

To remove Patch template records or sublist rows

1. In the Template Editor, click the number of the record that you want to remove or, in the Template Sublist Editor, the number of the row. This number is in the leftmost column.
   To select a range of rows, hold down the **Shift** key while you click the first and last row numbers.
   To select non-sequential rows, hold down the **Ctrl** key while you click the row numbers.
2. In the Template Editor, click **Remove Rows** or, in the Template Sublist Editor, click **Remove Rows**.

Common OS Patches module messages

The OS Patches (Patch) module reports agents that are not running the operating system patches that are defined in Patch templates. The Template files option in the Patch module lets you enable or disable the Patch template files that are used to check your computers.

The module returns the following messages to report problems with template data and to identify operating system patches that are not installed, as well as agents where forbidden patches are installed.

Message name	Title	Class
NO_TEMPLATE_ SPECIFIED	No applicable template files specified	4
PATCHNOTINS3	Patch not installed	4
PATCHNOTINS2	Patch not installed	2
PATCHNOTINS1	Patch not installed	2
PATCHNOTINS0	Patch not installed	0
PATCHNOTAVAIL3	Patch not available	4
PATCHNOTAVAIL2	Patch not available	2
FORBIDDEN_PATCH_0	Forbidden patch found	0
FORBIDDEN_PATCH_1	Forbidden patch found	2
FORBIDDEN_PATCH_2	Forbidden patch found	2
FORBIDDEN_PATCH_3	Forbidden patch found	4
OPTIONAL_PATCH_NO_SUPERSEDE	Optional patch supersedes nothing	2

Patch templates

Use this option to enable or disable the Patch template files. The module uses only enabled template files that apply to the host. For example, .pai template files are used only on agents running AIX operating systems:

UNIX operating system	File extension
AIX	.pai
HP-UX 10+	.ph1
Solaris 2.5 -	.pso
Solaris 2.6 +	.ps6
Digital UNIX/Tru64 (OSF/1)	.pos
Linux	.plx

Superseded

Enable this option to report a patch and its superseding patches if the patch and all of its superseding patches are missing.

The following message is reported:

Message name	Title	Class
SUPERSEDED_PATCH_NOT_INSTALLED	Superseded patch not installed	0

Disable module

Policy runs that include the OS Patches module can take a significant amount of time to finish. Enable this option to eliminate unnecessary verification and speed up policy runs on computers that have already been examined for the latest patches.

Internet advisory sources

You can obtain current counter-measure information for known security vulnerabilities from Symantec Corporation and other security information clearing houses on the Internet:

Organization	URL
Symantec Corporation	http://securityresponse.symantec.com
CERT Coordination Center	http://www.cert.org
Coast Project	http://www.cs.purdue.edu/coast
Computer Incident Advisory (CIAC)	http://ciac.llnl.gov/ciac
Forum of Incident Response and Security Teams	http://www.first.org
InfoSysSec	http://www.infosyssec.com
Internet/Network Security	http://netsecurity.about.com
Microsoft Corporation	http://www.microsoft.com
NTBugtraq	http://www.ntbugtraq.com
NTSecurity Net	http://www.ntsecurity.net
Rootshell	http://www.rootshell.com
Security Focus	http://www.securityfocus.com

Password Strength

The Password Strength module reports users that can log in without a password, and passwords that do not conform to specified format, length, expiration, and history requirements. It also applies dictionary tests to detect passwords that are easily guessed. The Password Strength module:

The module checks local NIS and/or /etc/passwd files on standard UNIX computers and /tcb files and shadow password files on enhanced or trusted UNIX computers.

Red Hat Linux operating systems must be configured for both of the following:

- The pam_cracklib.so module and standard UNIX password encryption.
- The pam_pwdb.so module and the shadow password file.

Using and editing word files

Checks in the Password Strength module compare passwords to words in word files (.wrd files). The Password = wordlist word check, for example, compares passwords to dictionary word files. Passwords that match word file words (and variations of those words) can be easily guessed by intruders and are a security threat.

In the following word files, capital letters following underscores in file names indicate the languages. For example, D = German, FR= French, I = Italian, NL = Dutch, P = Portuguese, SP= Spanish.

Category	File	# of words
First name	firstnam.wrd	651
	Fname_D.wrd	1602
	Fname_FR.wrd	784
	Fname_I.wrd	952
	Fname_NL.wrd	724
	Fname_P.wrd	449
	Fname_SP.wrd	349
Last name	lastnam.wrd	2958
	Fname_D.wrd	3101
	Fname_FR.wrd	3196
	Fname_I.wrd	2848
	Fname_NL.wrd	3005
	Fname_P.wrd	723
	Fname_SP.wrd	3027

Category	File	# of words
Dictionaries	synopsis.wrd	253
	english.wrd	3489
	lenglish.wrd	34886
	Slist_D.wrd	169
	List_D.wrd	2597
	Llist_D.wrd	19319
	Slist_FR.wrd	166
	List_FR.wrd	2517
	Llist_FR.wrd	17893
	Slist_I.wrd	227
	List_I.wrd	2490
	Llist_I.wrd	14814
	Slist_NL.wrd	399
	List_NL.wrd	3038
	Llist_NL.wrd	14232
	Slist_P.wrd	217
	List_P.wrd	2169
	Llist_P.wrd	16950
	Slist_SP.wrd	162
	List_SP.wrd	2424
	Llist_SP.wrd	19580
	yiddish.wrd	639
Computers	computer.wrd	143
	Compu_D.wrd	545
	Compu_FR.wrd	346
	Compu_I.wrd	255
	Compu_NL.wrd	184
	Compu_P.wrd	226
	Compu_SP.wrd	216
	defaults.wrd	465
	nerdnet-defaults.wrd	142
	ntccrack.wrd	16870
	Oracle.wrd	37
	wormlist.wrd	432
Specialty	cartoon.wrd	133
	college.wrd	819
	disney.wrd	433
	hpotter.wrd	715
	python.wrd	3443
	sports.wrd	247
	tolkien.wrd	471
	trek.wrd	876

To enable a word file

1 In the Disabled Word Files list, select a word file.

2 Click the left arrow.

To disable a word file

1 In the Enabled Word files list, select a word file.

2 Click the right arrow.

To edit a word file

1 Do one of the following:

- Open an existing word file in a text editor. (UNIX word files are located in esm/words.)
- Create a new ASCII plain-text word file in a text editor. Name the new file with a .wrd extension (for example, medical.wrd).

2 Type only one word per line.

3 Save the file in the words directory.

Users to check

Use this option to specify users and groups that are excluded or included for all security checks in the Password Strength module. See "Editing name lists" on page 35.

Local disks only

This option restricts module checks to users with home directories that are located on disks that are local to the computer running the check. Selecting this option ensures that user files are checked only once in sites that serve user directories with NFS, even though the module can run on more than one computer.

Note: When the Local disks only option is enabled on an AIX computer, the module does not check remote mount points on NFS, AFS, or DFS file systems. On Solaris and HP-UX, the Local disks only option excludes remote mount points on AFS and NFS.

Local accounts only

Enable this option to restrict checks to user accounts that are defined in the agent's /etc/passwd file. This ensures that users are checked only once in sites that serve user accounts with NIS.

Password = username

This security check reports user accounts with passwords that match their related user names.

The check is provided for systems with a large number of user accounts. The security check is not as thorough as Password = any username. However, if the Password = any username check takes too much time or consumes too much CPU, you can use the Password = username check on a daily basis and the Password = any username check on the weekends.

Passwords that are guessed by this security check represent a serious security concern because a potential intruder can also guess these passwords.

The check returns the following message:

Message name	Title	Class
GUESSPASS	Guessed user password	4

To protect your computers

- Immediately assign new passwords to all listed accounts and instruct their owners to set more secure passwords.
  A secure password should be six to eight characters in length, should not be found in any dictionary, should include at least one non-alphabetic character, and should not match an account or computer name on your system.

Password = any username

This security check reports user accounts with passwords that match any user name in your system password files.

If this check takes too much time or consumes too much CPU to run on a normal workday, you can run the Password = username check on a daily basis and run this check on the weekends.

Passwords that are guessed by this security check represent a serious security concern because a potential intruder can also guess these passwords.

The check returns the following messages:

Message name	Title	Class
GUESSPASS	Guessed user password	4

To protect your computers

- Immediately assign new passwords to all listed accounts and instruct account owners to set more secure passwords.
  A secure password should be six to eight characters in length, should not be found in any dictionary, should include at least one non-alphabetic character, and should not match an account or computer name on your system.

Password within GECOS field

This security check reports user accounts with passwords that match words in the GECOS field in the /etc/passwd file.

The check returns the following messages:

Message name	Title	Class
GUESSPASS	Guessed user password	4
NO_PASSGECOS	No data in GECOS field	0

To protect your computers

- Immediately assign new passwords to all named accounts and instruct account owners to set more secure passwords.
  A secure password should be six to eight characters in length, should not be found in any dictionary, should include at least one non-alphabetic character, and should not match an account or computer name on your system.

Password = wordlist word

This security check compares passwords with words in enabled word files and reports user accounts with matches. Use the word files lists to enable or disable the word files for this check.

Checking passwords against enabled word lists significantly increases the time that is required to complete a policy run. You can shorten the run time by specifying the percentage of words that is included in each policy run. The default value is 100 percent. If you specify a lesser value, the check starts at the point in the word lists where the previous policy run stopped.

Passwords that are guessed by this security check represent a serious security concern because a potential intruder can also guess these passwords.

The check returns the following messages:

Message name	Title	Class
GUESSPASS	Guessed user password	4
NOWORDS	No word files specified	4

To protect your computers

- Immediately assign new passwords to all named accounts and instruct account owners to set more secure passwords.
  A secure password should be six to eight characters in length, should not be found in any dictionary, should include at least one non-alphabetic character, and should not match an account or computer name on your system.

Reverse order

This option tries to match passwords by spelling words backward from word lists that are used by enabled Password Strength checks, including Password = username, Password = any username, Password = wordlist word, and Password within GECOS field.

For example, when the Password = wordlist word check is enabled, this check tries to match passwords by spelling words backward (e.g., golf -> flog).

Double occurrences

This option tries to match passwords by doubling the words from word lists that are used by enabled Password Strength checks, including Password = username, Password = any username, Password = wordlist word, and Password within GECOS field.

For example, when the Password = wordlist word check is enabled, this check tries to match passwords by doubling words (e.g., golf -> golfgolf).

Plural forms

This option tries to match passwords by changing words to their plural forms from word lists that are used by enabled Password Strength checks, including Password = username, Password = any username, Password = wordlist word, and Password within GECOS field.

For example, when the Password = wordlist word check is enabled, this check tries to match passwords by changing words to their plural form (e.g., golf -> golfs).

Uppercase

This option tries to match passwords by converting words to all uppercase characters from word lists that are used by enabled Password Strength checks, including Password = username, Password = any username, Password = wordlist word, and Password within GECOS field.

For example, when the Password = wordlist word check is enabled, this check tries to match passwords by changing words to all uppercase characters (e.g., golf1 -> GOLF1). Note that the check changes only alphabetical characters to uppercase.

Lowercase

This option tries to match passwords by converting words to all lowercase characters from word lists that are used by enabled Password Strength checks, including Password = username, Password = any username, Password = wordlist word, and Password within GECOS field.

For example, when the Password = wordlist word check is enabled, this check tries to match passwords by changing words to all lowercase characters (e.g., GOLF1 -> golf1). Note that the check changes only alphabetical characters to lowercase.

Add prefix

This option tries to match passwords by adding prefixes to words from word lists that are used by enabled Password Strength checks, including Password = username, Password = any username, Password = wordlist word, and Password within GECOS field.

The prefixes that are used by the check are defined in the check's name list. (The default name list includes only the prefix, 1.)

For example, when the Password = wordlist word check is enabled, this check tries to match passwords by adding each prefix in the name list to each word in the word lists (e.g., golf -> progolf).

Add suffix

This option tries to match passwords by adding suffixes to words from word lists that are used by enabled Password Strength checks, including Password = username, Password = any username, Password = wordlist word, and Password within GECOS field.

Suffixes that are used by the check are defined in the check's name list. (The default name list includes only the suffix, 1.)

For example, when the Password = wordlist word check is enabled, this check tries to match passwords by adding each suffix in the name list to each word in the word lists (e.g., golf -> golfball).

Guessed password

This option controls the format of the Guessed user password message that is returned by other security checks in the module.

When the option is enabled, Password Strength security checks that attempt to match and guess passwords report passwords that are guessed using the format: <the first character>*<the last character>.

When the option is disabled, the same security checks report only accounts that had matched (guessed) passwords.

Login requires password

This security check for AIX and Solaris operating systems reports agents that allow users to log in without entering a password. This is a serious breach of security.

The check returns the following messages:

Message name	Title	Class
NO_PASSREQ	Login does not require password	4
NOTSUPPORT_PASSREQ	Login Requires Password not supported	0

To protect your computers

- Require all user logins to require passwords.

Accounts without passwords

This security check reports user accounts that can be accessed without entering a password.

Use the check's name list to exclude users and user groups that are not already excluded by the Users to check option.

Accounts without passwords represent a serious security concern because anyone who knows the user names can access these accounts.

Note: The check is not supported on Red Hat Linux computers.

The check returns the following message:

Message name	Title	Class
PASSNOPASS	No password	4

To protect your computers

- Immediately assign passwords to all unprotected user accounts. Instruct the account owner to log in with the assigned password and change the password the next time the owner connects to the system.

Password length restrictions

This security check examines the minimum password length setting on the agent. The security check reports a problem if the setting is less than the minimum length that you specify.

Short passwords are easy to guess and can expose your system to intruders.

Note: The check runs only on UNIX operating systems that support minimum password length restrictions. This includes AIX, Solaris, Digital UNIX/Tru64, and Red Hat Linux computers.

The check returns the following message:

Message name	Title	Class
MINPASSLEN	Minimum password length too short	1

To protect your computers

- Set the minimum password length to at least six characters.

Minimum password history

This security check reports:

- Agents and users that have set the number of passwords that are retained as password history to less than the minimum number that you specify.
- Agents that do not have a minimum password history setting.

The check is not supported on HP-UX 9.x, HP-UX 10.x, AIX 3.X, Solaris, or Red Hat Linux operating systems.

The check returns the following messages:

Message name	Title	Class
NO_HISTSIZE	Invalid minimum password history	1
NOTSUPPORT_ HISTSIZE	Minimum password history not supported	0
CHECK_NOT_ PERFORMED	Warning – check could not be performed	1

When the policy setting for Number of Passwords is zero (0), the check returns the common message, Warning – check could not be performed.

To protect your computers

- Require that at least five previous passwords be retained as password history.

Password age

This security check reports:

- User accounts with passwords that have not been changed within the number of days that you specify (the default is 60 days).
- Ages of invalid passwords on all computers that support password age checking.

Accounts that are disabled or locked are ignored.

The check ignores NIS accounts, because NIS does not store password ages.

The check returns the following messages:

Message name	Title	Class
NO_MINCHANGE	Invalid password age	3
NOTSUPPORT_MINCHANGE	Password age checking not supported	0

To protect your computers

- Require users to change their passwords periodically (at least one time each 60 days).

Maximum password age

This security check reports:

- Agents that have a system default maximum password age that is greater than the value that you specify.
- Agents that have not set a system default maximum password age.
- User accounts with a maximum password age greater than the value that you specify.

The check returns the following messages:

Message name	Title	Class
NO_MAXAGE	Invalid maximum password age	1
NOTSUPPORT_ MAXAGE	Maximum password age not supported	0

To protect your computers

- Frequent password changes increase the overall security of the system. You should require users to change their passwords periodically (at least one time each 60 days).

Minimum password age

This security check reports:

- Agents that have a system default minimum password age that is less than the value that you specify.
- Agents that have not set a system default minimum password age.
- User accounts with a minimum password age that is less than the value that you specify.

The check returns the following messages:

Message name	Title	Class
NO_MINAGE	Invalid minimum password age	1
NOTSUPPORT_ MINAGE	Minimum password age not supported	0
CHECK_NOT_ PERFORMED	Warning – check could not be performed	1

When the policy setting for Minimum Age is zero (0), the check returns the common message, Warning – check could not be performed.

To protect your computers

- Require a minimum password age of at least five days. This means a password cannot be changed until it is at least five days old.

Minimum alphabetic characters

This security check reports:

- Agents and users that have set the minimum number of alphabetic characters required in passwords to less than the minimum number that you specify.
- Agents that have not set a default minimum number of alphabetic characters.

Note: This check is not supported on HP-UX, Solaris, or Red Hat Linux operating systems.

The check returns the following messages:

Message name	Title	Class
NO_MINALPHA	Invalid minimum number of alphabetic characters	1
NOTSUPPORT_ MINALPHA	Minimum number of alphabetic characters not supported	0
CHECK_NOT_PERFORMED	Warning – check could not be performed	1

When the policy setting for Minimum Number is zero (0), the check returns the common message, Warning – check could not be performed.

To protect your computers

- Require passwords to include at least four alphabetic characters.

Minimum non-alphabetic characters

This security check reports:

- Agents and users that have set the minimum number of non-alphabetic characters that is required in passwords to less than the number that you specify.
- Agents that have not set a default minimum number of non-alphabetic characters.

Note: This check is not supported on HP-UX, Solaris, or Red Hat Linux operating systems.

The check returns the following messages:

Message name	Title	Class
NO_MINOTHER	Invalid minimum number of non-alphabetic characters	1
NOTSUPPORT_ MINOTHER	Minimum number of non-alphabetic characters not supported	0
CHECK_NOT_ PERFORMED	Warning – check could not be performed	1

When the policy setting for Minimum Number is zero (0), the check returns the common message, Warning – check could not be performed.

To protect your computers

- Require passwords to include at least one non-alphabetic character.

Minimum different characters

This security check reports:

- Agents and users that have set the minimum number of different characters that is required in new passwords to be less than the number that you specify.
- Agents that have not set a default minimum number of different characters for new passwords.

Note: This check is not supported on HP-UX or Solaris operating systems.

The check returns the following messages:

Message name	Title	Class
NO_MINDIFF	Invalid minimum number of different characters	1
NOTSUPPORT_ MINDIFF	Minimum number of different characters not supported	0
CHECK_NOT_PERFORMED	Warning – check could not be performed	1

When the policy setting for Minimum Number is zero (0), the check returns the common message, Warning – check could not be performed.

To protect your computers

- Require passwords to include at least two characters that differ from the characters used in previous passwords for the same account.

Maximum repeated characters

This security check reports:

- Agents and users that have set the maximum number of times that a character can be repeated in a password to be greater than the number that you specify.
- Agents that have not set a default maximum number of repeated characters.

The check returns the following messages:

Message name	Title	Class
NO_MAXREPEATS	Invalid maximum number of repeated characters	1
NOTSUPPORT_MAXREPEATS	Maximum number of repeated characters not supported	0

To protect your computers

- Limit the number of repeated characters within a password to no more than two characters.

Trusted mode only

This header identifies the following five security checks for UNIX computers (Users without system password strength, Users can choose their passwords, Accounts can be used without a password, and System generated passwords) that have the ability to run in a trusted security mode. This is called enhanced security mode on some computers, and formally is known as the Trusted Computing Base (TCB). These four ESM security checks can run successfully only on computers that are TCB enabled.

For more information on trusted security mode, see "Trusted Computing Base" on page 117.

Users without system password strength

This security check reports user accounts that are not checked by the operating system's password strength check on UNIX computers that are running in trusted or enhanced security modes. For more information on trusted security mode, see "Trusted Computing Base" on page 117.

Note: This check is supported only on HP-UX, AIX, and Digital UNIX/Tru 64.

The check returns the following message:

Message name	Title	Class
NOSTRENGTH	User without system password strength	1

To protect your computers

- Make sure that all user passwords are checked both by the Password Strength module and by the computer's password strength program.

Users can choose their passwords

This security check for HP-UX and Digital UNIX/Tru 64 operating systems reports user accounts that are able to choose their own passwords on computers that are running in trusted or enhanced security modes. For more information on trusted security mode, see "Trusted Computing Base" on page 117.

The check returns the following message:

Message name	Title	Class
PICKOWN	User can pick password	1

To protect your computers

- Make sure that all user-picked passwords are checked both by the Password Strength module and by the computer's password strength program.

Accounts can be used without a password

This security check for HP-UX and Digital UNIX/Tru 64 operating systems reports user accounts that can be set to have NULL passwords on computers that are running in trusted or enhanced security modes. For more information on trusted security mode, see "Trusted Computing Base" on page 117.

To avoid security problems, your operating system should be allowed to enforce non-NULL passwords on all accounts when doing password maintenance.

The check returns the following message:

Message name	Title	Class
ALLOWNULL	Account can be used without password	1

To protect your computers

- Change the settings for all listed accounts so that NULL passwords are not permitted when the user changes passwords.

System generated passwords

This security check for HP-UX and Digital UNIX/Tru 64 operating systems reports user accounts that have system-generated passwords (or accounts that have to use the system-generated password option on the next password change) on computers that are running in trusted or enhanced security modes. For more information on trusted security mode, see "Trusted Computing Base" on page 117.

Although this is a valid option for generating safe passwords, system-generated passwords are sometimes written down because they are difficult to remember.

The check returns the following messages:

Message name	Title	Class
SYSTEMGENERATED	Account with system-generated password	0
AIXSYSTEMGENERATED	System-generated passwords not supported	0

Password age warning

This security check for HP-UX operating systems in secure mode reports agents that have a system password warning age greater than:

- The specified warning age
- Systems that do not have a password warning age setting

This check also reports users that have a password warning age greater than the specified value. The default password warning age is 50 days.

The check returns the following messages:

Message name	Title	Class
STKU_NOTSUPPORT_AGE_WARNING	Does not support password age warning	1
STKU_AGE_WARNING	Password age warning	1

Password age lockout

This check HP-UX operating systems in secure mode reports agents that have a system password lockout age greater than the specified value and systems that do not have a password lockout age setting. The check also reports users that have a password lockout age greater than the specified value. The default password lockout age is 70 days.

The check returns the following messages:

Message name	Title	Class
STKU_NOTSUPPORT_AGE_LOCKOUT	Does not support password age lockout	1
STKU_AGE_LOCKOUT	Password age lockout	1

Startup Files

The Startup Files module examines rc scripts and system startup files, looking for discrepancies with system-owned services that are defined in the Services templates. It also reports new, changed, and deleted services.

Common Startup Files messages

The following messages are generated by functions that check templates and maintain snapshot files for multiple security checks in the Startup Files module.

Message name	Title	Class
DUPLICATE_TEMPLATE_ENTRY	Duplicate template entry	0
FORBIDDEN_PARAMETER_FOUND	Forbidden parameter	4
FORBIDDEN_PROCESS_ FOUND	Forbidden process found	4
INFO_TEXT_MESSAGE	Changed process information	1
MANDATORY_PARAMETER_NOT_ FOUND	Mandatory parameter not found	4
MANDATORY_PROCESS_NOT_FOUND	Mandatory process not found	4
NOTEMPLATES	No template files specified	0
LARGE_FILES_NOT_ SUPPORTED	Large file not checked	1

Mandatory and Forbidden processes that are reported by the Startup Files module are defined in the Services template.

Only system-owned processes, and parameters that are running on system-owned processes, are reported by the module. System-owned processes are identified in the process table by PPIDs of 0 or 1 on all operating systems except AIX. On AIX, system-owned processes are identified by PPIDs that are equal to the process ID of the System Resource Controller.

Updateable and correctable Startup Files messages

The UNIX Startup Files module has five security checks that report snapshot-updateable or correctable messages.

Snapshot-updateable messages let you update snapshots to match current values for the agent. These messages display the letters SU in the Updateable/Correctable column of the console grid.

Run the module once to create the agent snapshot file before you run the module to look for security weaknesses.

Correctable messages let you correct file attributes on the agent. These messages display the letter C in the Updateable/Correctable column of the console.

Security check	Code	Message name
Template and snapshot comparison functions	SU	INFO_TEXT_ MESSAGE
System startup file contents	C	SYSSWW
System startup file contents	C	SYSSGW
Changed services	SU	CHANGED_ PROCESS_PARAMS
Changed services	SU	CHANGED_PROCESS_ FULLPATH
Changed services	SU	CHANGED_PROCESS_OWNER
New services	SU	NEW_PROCESS
Deleted services	SU	DELETED_PROCESS

System startup file contents

This security check examines the contents of rc scripts and verifies that files that are referenced in the scripts exist on your computer.

The module evaluates /tmp files and world-writable directories that do not have the sticky bit set. It does not evaluate world-writable directories that have the sticky bit set.

The sticky bit maintains file ownership within a world-writable directory. Although anyone can create new files in a world-writable directory, the ability to modify or delete existing files depends on individual file permissions.

Use the file list to exclude system startup files from the check. Specify full path names in the file list.

The security check returns the following messages:

Message name	Title	Class
SYSSWW	World writable file referenced in startup file	4
SYSSGW	File writable by non-privileged group referenced in startup file	1

Current directory in startup PATH

This security check examines the contents of rc scripts and warns of any that set the PATH variable to include the current directory (with . or :: commands).

This security check examines the same scripts as the System startup file contents check does. Use that check's file list to include additional system startup files for this check. Specify full path names in the file list.

The security check returns the following message:

Message name	Title	Class
CUR_DIR_IN_ PATH	Current directory command in PATH variable	1

Login/tty file contents

This security check examines the contents of the securetty and /etc/default/login files and reports pseudo-terminals that allow root logins, unrestricted root logins, and computers that allow root logins from other than the system console.

Use the file list to exclude pseudo-terminals or devices that allow root logins from the check. Specify full path names for device files.

The security check returns the following messages:

Message name	Title	Class
LOGINDEV	Root login restricted to the following devices	0
NODEFAULT LOGIN	No default login configuration file exists	1
NOLOGIN CONSOLE	Root login not restricted	1
NOSECURETTY	No tty security file	1
PTYSECURE	Pseudo-terminal listed as secure	1

Enhanced security enabled

This security check examines any enhanced security extensions that are enabled on the agent's operating system.

The security check returns the following messages:

Message name	Title	Class
NO_ENHANCED	No enhanced security features	0
SEC_DISABLE_OSF1	Enhanced OSF1 security features are disabled	4
SEC_DISABLE_HP	Enhanced HPUX security features are disabled	4
SEC_DISABLE_AIX	Enhanced AIX security features are disabled	4
SEC_DISABLE_SGI	Enhanced IRIX security features are disabled	4
SEC_UNKNOWN_ OSF1	Cannot determine state of OSF1 security enhancements	1
SEC_UNKNOWN_HP	Cannot determine state of HPUX security enhancements	1
SEC_UNKNOWN_AIX	Cannot determine state of AIX security enhancements	1

Installed services

This security check looks for installed services on your computer by parsing the /etc/inetd.conf or the xinetd.conf file for all services that are found in that file.

The security check looks at records in enabled Services templates to determine which processes are reported as forbidden. Services that are defined as Ignored in the Services template are not reported when found. Services that are defined as Optional are reported when found. See "Services" below.

The security check returns the following messages:

Message name	Title	Class
INSTALLED_SERVICES	Installed services	1
FORBIDDEN_PROCESS_ENABLED	Forbidden process enabled in inetd.conf or xinetd.conf	4
SERVICE_WRAPPER	Service wrapper	0

Service wrappers

This option specifies any service wrappers that are to be reported by the Installed services check. Service wrappers are services that are prepended to other services on the system (such as itawrap, which preprocesses a service for security reasons).

See the preceding Installed Services messages table.

Services

Use this option to enable and disable Services template files that are to be used. In the Services templates, mark services as Ignored, Optional, Mandatory, and Forbidden to run on agents.

The Startup Files module includes three default Services templates:

- Templates with basic file names (enabled by default), list commonly-used services that the Startup Files module monitors as Optional or Ignored services until you disable the template or edit the template's default settings.
- Templates with sans20 file names (disabled by default), list 25 services that the module monitors as Forbidden services when this template is enabled with its default settings.
  The sans20 template protects your UNIX computers from many security threats that are included in the SANS/FBI Twenty Most Critical Internet Security Vulnerabilities list (http://www.sans.org/top20).
- Templates with remote file names (disabled by default), forbid services that run rlogind, rexec, rwho, rsh, remsh, admind, and telnetd daemons when this template is enabled with its default settings.

Editing the Services template

The Startup Files module uses a Services template to define services and parameters that are to be run or not run in system startup files.

Entries are case sensitive and wildcard characters (* or ?) are accepted.

Services template files have the following file extensions:

UNIX operating system	File extension
AIX	.sai
Digital UNIX/Tru64 (OSF/1)	.sos
HP-UX	.shp

UNIX operating system	File extension
HP-UX 10-11	.sh1
IRIX	.ssg
Linux	.slx
NCR SVR4	.snc
Sequent	.sse
Solaris	.sso
Solaris 2.6	.ss6
SunOS	.ssu

To add a new Services template

1. Right-click the Templates icon in the enterprise tree, then click **New**.
2. In the Available template types list, select the type of template that you want to add.
3. In the Template file name text box, type a new template name of no more than eight characters. Symantec ESM adds the file extension.
4. Press **Enter**.

To copy and rename a Services template

1. Open the /esm/template directory on the manager that contains the template file you want to edit.
2. Copy the template file you want to edit to a renamed file in the /esm/template directory.
3. Exit the /esm/template directory on the UNIX manager.

To add a record to a Services template

1. In the tree view, double-click the template file name (basic.*, sans10.*, or remote.*).
2. In the Template Editor, click **Add Row**.
3. In the Services field, replace <NEW> with the name of the process or service.
4. Click the Monitoring field and select one of the following:
   - **Optional**. If you select Optional, the Services not in template check will not report the specified service. All other checks that rely on Services templates continue to report the specified service. Additionally, Symantec ESM checks for any specified Forbidden Parameters or Mandatory Parameters even though the service itself has not been designated as Forbidden or Mandatory.
   - **Forbidden**. If you select Forbidden, Symantec ESM reports any instance of the specified service.
   - **Mandatory**. If you select Mandatory, Symantec ESM reports if the specified service is not found.
   - **Ignored**. If you select Ignored, all checks that rely on Services templates will not report this service. Additionally, Symantec ESM will not check any specified Forbidden Parameters or Mandatory Parameters.
5. In the Forbidden Parameters field, replace <NEW> with prohibited parameters. For example,
6. In the Mandatory Parameters field, replace <NEW> with required parameters. For example,

   Note: Parameters that occur in both Forbidden and Mandatory fields are reported. For example, if the /etc/init process is marked with a forbidden parameter of -q and a mandatory parameter of -q, the -q option is reported as forbidden when it is encountered.

7. In the Comments field, replace <NEW> with any explanatory or descriptive comments.
8. Click **Save**.
   To add another record, repeat steps 2–6.
9. Click **Close**.

To remove Services template records

1. In the Template Editor, click the leftmost, numbered button on the row that you want to remove.
   To select a range of rows, hold down the **Shift** key while you click the first and last row numbers.
   To select non-sequential rows, hold down the **Ctrl** key while you click the row numbers.
2. In the Template Editor, click **Remove Row(s)**.
3. Click **Save**.
4. Click **Close** to exit the Template Editor.

For messages that are generated by template checking, see "Common Startup Files messages" on page 191.

Duplicate services

This security check reports all system-owned services, processes, or commands that are duplicated on the system (i.e., found in the process table more than once). This includes system-owned commands that are running multiple times in the process table.

System ownership is identified in the process table by parent process ID numbers (PPIDs) of 0 or 1 on all operating systems except AIX. On AIX, system-owned processes are identified by PPIDs that are0, 1, or equal to the process ID of the System Resource Controller.

Services that are defined as Ignored in enabled Services templates are not reported by this check.

The security check returns the following messages:

Message name	Title	Class
DUPLICATE_PROCESSES	Duplicate process	1
NO_DUPLICATE_PROCESSES	No duplicate processes found	0

Changed services

This security check reports any services with configuration changes since the last services snapshot update.

Services that are defined as Ignored in enabled Services templates are not included in the services snapshot files. Therefore, changes to these services are not reported.

The security check returns the following messages:

Message name	Title	Class
CHANGED_PROCESS_PARAMS	Changed process parameters	1
CHANGED_PROCESS_FULLPATH	Changed process full path	1
CHANGED_PROCESS_OWNER	Changed process owner	1

New services

This security check reports any services that have been added since the last time the services snapshot was updated.

The security check returns the following message:

Message name	Title	Class
NEW_PROCESS	New process	1

Deleted services

This security check reports any services that have been deleted since the last time the services snapshot was updated. This check does not report services that are identified as Ignored services in enabled template files.

The security check returns the following message:

Message name	Title	Class
DELETED_PROCESS	Deleted process	1

Services not in template

This security check reports enabled services and running system-owned processes not in the Services template.

System-owned processes are identified in the process table by PPIDs of 0 or 1 on all operating systems except AIX. On AIX, system-owned processes are identified by PPIDs that are 0, 1, or equal to the process ID of the System Resource Controller.

The security check returns the following message:

Message name	Title	Class
PROCESS_NOT_IN_TEMPLATE	Processes not listed in template	0

Non-wrapped services

This security check reports services that are not wrapped with an approved wrapper. Service wrappers provide access control and logging of inetd services. Use the check's name list to specify approved wrappers that will not be reported by the check.

The check is ignored on any computer that is not running inetd, including computers running xinetd, because xinetd provides access control and logging without the need for additional wrappers.

The security check returns the following message:

Message name	Title	Class
NON_WRAPPED_SERVICE	Non-wrapped service	1

To protect your computers

- Use wrappers to control who has access to network services and to log the use of services.

File system setuid protection

This security check reports a problem if setuid files on Solaris operating systems are allowed on a writable UFS file system.

Only UFS file systems are examined. Because the root partition cannot be mounted with the nosuid option, it is not reported by this check.

The check returns the following message:

Message name	Title	Class
MOUNT_ALLOWS_RW_OR_SUID	Mount point allows write access to setuid files	1

To protect your computers

- Do the following:
  - Locate setuid and setgid files on the /usr partition.
  - Mount the /usr partition with the read-only (ro) option.
  - Mount all other partitions with the nosuid option if possible.

Solaris EEPROM security-mode

This security check reports a problem if a Solaris computer does not prompt for a programmable read-only memory (PROM) security password.

The check returns the following message:

Message name	Title	Class
EEPROM_SECURITY_MODE_NONE	EEPROM security-mode parameter is none	1

EEPROM is erasable electronic programmable read-only memory.

To protect your computers

- Set the value of the EEPROM parameter to command or full.

Solaris EEPROM auto-boot?

This security check reports a problem if the auto-boot? parameter value of a Solaris computer is false.

The check returns the following message:

Message name	Title	Class
EEPROM_AUTO_BOOT	EEPROM auto-boot? parameter is false	1

EEPROM is erasable electronic programmable read-only memory.

To protect your computers

- Set this parameter value to true so that the computer automatically boots after power-on or reset.

System Auditing

The System Auditing module reports 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.

Accounting enabled

This security check reports agents that are not running system accounting.

The security check returns the following message:

Message name	Title	Class
NOACCT	Auditing is not enabled	4

Auditing enabled

This security check reports computers where auditing of events and system calls is not enabled. This security check is currently supported on AIX, HP-UX, and Solaris operating systems.

The security check returns the following message:

Message name	Title	Class
AUDIT_OFF	Auditing not enabled	4

Event auditing

This security check examines events that are specified in the Events template and reports events that are not being audited by the agent's operating system. This check is currently supported only on AIX, HP-UX, and Solaris operating systems.

Note: Symantec ESM provides one default Events template that includes event records for HP-UX computers only.

Because Solaris and AIX operating systems support dynamic mappings of events and system calls, you must create template records that define your configurations of events and system calls on those operating systems.

You can add records to the default template for Solaris and AIX events, or you can create new templates to define these events. See "Editing the Events template" on page 203.

The security check returns the following messages:

Message name	Title	Class
AUDIT_OFF	Auditing not enabled	4
TRUSTEDEVENT	Events not audited	3
HP_TRUSTEDEVENTMAP	HP event map error	3

Editing the Events template

Events templates let you define users, events, and system calls to be audited on selected operating systems in a UNIX domain.

To create an Events template

1. Right-click the Templates node of the tree view, then click **New.**
2. Select the **Events-all** template type.
3. Type a new template file name of no more than eight characters without a file name extension. Symantec ESM adds the .aud extension.
4. Click **OK**.
5. Add one or more records and sublist rows.
6. Click **Save.**
7. Click **Close**.

To add an Events template record

1. If the template is not already open in the Template Editor, double-click the name of the template in the tree view.
2. Click **Add Row.**
3. In the new row (record), click the field in the OS column, then select the appropriate operating system.
4. Add an row to the Users sublist. See "To add a row to the Users sublist" on page 204.
5. Add an row to the Events sublist. See "To add a row to the Events sublist" on page 204.
6. Add an row to the System Calls sublist. See "To add a row to the System Calls sublist" on page 204.
7. Click **Save**.
8. Click **Close**.

Auditing checks are performed for all users and user groups on supported computers when no User sublist entries are defined.

To add a row to the Users sublist

1. In the Template Editor, click the field in the Users column of the row that you are editing.
2. In the Template Sublist Editor, click **Add Row**.
3. In the User field, replace <NEW> with the name of a user or user group. On Solaris computers only, you can type **non-attributable** for events that cannot be attributed to specific user accounts.
4. Click **Apply**.
   To add another row, repeat steps 2–4.
5. Click **Close**.

To add a row to the Events sublist

1. In the Template Editor, click the Events field of the row that you are editing.
2. In the Template Sublist Editor, click **Add Row**.
3. Replace <NEW> with the name of the event that you want to add.
4. Select or uncheck the Success and Failure check boxes to specify the results that you want to audit.
5. Click **Apply**. To add another row, repeat steps 2–5.
6. Click **Close**.

To add a row to the System Calls sublist

Note: System calls are not audited on Solaris or AIX operating systems, where only events (not individual system calls) can be configured for auditing.

---

1. In the Template Editor, click the System Calls field of the row that you are editing.
2. In the Template Sublist Editor, click **Add Row**.
3. Replace <NEW> with the system call that you want to add.
4. Select or uncheck the Success and Failure check boxes to specify user operation results that you want to audit. AIX computers audit event usage only, not successes and failures.

5 Click **Apply**.
To add another row, repeat steps 2–5.

6 Click **Close**.

To remove Events template records or sublist rows

1 In the Template Editor or Template Sublist Editor, click the number of the row that you want to remove.
To select a range of rows, hold down the **Shift** key while you click the first and last row numbers.
To select non-sequential rows, hold down the **Ctrl** key while you click the row numbers.

2 In the Template Editor, click **Remove Row**, or in the Template Sublist Editor, click **Remove Entry**.

3 Click **Apply**.

System call mapping

This security check verifies that system calls are mapped to events that are specified in the Event Maps template. It is currently supported on AIX, HP-UX, and Solaris operating systems.

On AIX and Solaris computers, where users can modify mappings of system calls to events but only events can be audited, you can verify system calls that are mapped to a specified event so that you can determine which system calls are being audited when an event is audited. See "Editing the Event Maps template" on page 206 for instructions.

On HP-UX computers, where users cannot modify mappings of system calls to events but auditing can be turned on and off for system calls as well as events, this check reports system calls that are mapped to an event but not turned on for auditing.

The security check returns the following message:

Message name	Title	Class
EVENTMAP	Event map error	3

Editing the Event Maps template

Event Maps templates define system calls that should be mapped to specified events on Solaris, AIX, and HP-UX operating systems.

To create an Event Maps template

1. In the tree view, right-click **Templates**, then click **New**.
2. Select the **Event Maps-all** template type.
3. Type a new template file name of no more eight characters, without a file extension. Symantec ESM adds the .map extension to the file name.
4. Click **OK**.
5. Add one or more OS and Event records and System Calls Sublist rows (see below).
6. Click **Save**.
7. Click **Close**.

To add a record to the Event Maps template

1. If the template is not already open in the Template Editor, double-click the name of the template in the tree view.
2. In the Template Editor, click **Add Row.**
3. In the new row (record), click the OS field, then select the appropriate operating system.
4. In the Event field, replace <NEW> with the name of the event that you want to map to the system call.
5. Add one or more System Calls sublist rows. (See below.)
6. Click **Save**.
   To add another record, repeat steps 2–6.
7. Click **Close**.

To add a row to the System Calls sublist

Note: System calls are not audited on Solaris or AIX operating systems, where only events (not individual system calls) can be configured for auditing.

---

1. In the Template Editor, click the System Calls field of the row that you are editing.
2. In the Template Sublist Editor, click **Add Row**.

3 Replace <NEW> with the system call that you want to add.

4 Click **Apply**.
To add another row, repeat steps 2–4.

5 Click **Close**.

To remove Events Map template records

1 In the Template Editor, click the number of the record that you want to remove.
The number is in the leftmost column.
To select a range of rows, hold down the **Shift** key while you click the first and last row numbers.
To select non-sequential rows, hold down the **Ctrl** key while you click the row numbers.

2 In the Template Editor, click **Remove Row**.

3 Click **Save**.

To remove System Calls sublist rows

1 In the Template Sublist Editor, click the number of the row that you want to remove.
The number is in the leftmost column.
To select a range of rows, hold down the **Shift** key while you click the first and last row numbers.
To select non-sequential rows, hold down the **Ctrl** key while you click the row numbers.

2 Click **Remove Entry**.

3 Click **Apply**.

Authentication database internal consistency

This security check looks for inconsistencies within the authentication database on OSF1, AIX, and HP-UX computers running in trusted or enhanced security modes. (For more information on trusted security mode, see "Trusted Computing Base" on page 117.)

The security check returns the following messages:

Message name	Title	Class
INCONSISTENT	Inconsistent	1
RETRIEVE	Cannot retrieve	1

Message name	Title	Class
MULTIPLY	Multiple listings	1
NOTIN	Not in /etc/passwd	1
NOTLISTED	Not listed	1
UID	UID inconsistency	1
AIXFILE	AIX file warning	0
AIXUSER	AIX user warning	1
UNKNOWN	Warning	0
HPCONSISTENT	HP warning	0

To protect your computers

- Research each reported inconsistency and take appropriate measures.

File read auditing

This security check verifies that specified files are audited for read actions. It is currently supported only on AIX operating systems.

Specify full path names in the file list for files that should be audited.

The security check returns the following messages:

Message name	Title	Class
FILE_READ	Read actions not audited	3

File write auditing

This security check verifies that specified files are audited for Write actions. It is currently supported only on AIX operating systems.

Specify full path names in the file list for files that should be audited.

The security check returns the following messages:

Message name	Title	Class
FILE_WRITE	Write actions not audited	3

System Mail

The System Mail module reports security holes in mail configuration files, mail file attributes, and the Morris worm.

Wizard passwords

This security check reports wizard passwords in your mail configuration file. These passwords can provide unauthorized access to your computer.

The security check returns the following message:

Message name	Title	Class
POSWIZ	Wizard password in sendmail.cf	1

Decode aliases

This security check reports decode entries in your mail configuration file, which allow unencoded files to be sent to your computer.

The security check returns the following message:

Message name	Title	Class
POSDECODE	Decode entry in sendmail.cf	4

Command aliases

This security check reports mail aliases that are piped to a command. The security check parses the /etc/aliases file, flags every entry that includes a pipe, and compares the flagged entries to the list of bad aliases. Executables and scripts are not parsed.

A command alias allows outside access to the command, possibly providing unauthorized access to your computer.

Use the file list to exclude aliases from this check. Specify the full executable path name without quotes or flags.

The security check returns the following messages:

Message name	Title	Class
ALIASCMD	Alias piped to command	1
BADALIASCMD	Alias piped to shell program	4

Mail boxes

This security check examines mail boxes in the system mail directory to ensure that a user account exists for each mail box in the system and that each mail box is owned by the appropriate user.

When checking UNIX file permissions, this check examines only the basic user/group/other and read/write/execute permissions. It does not consider any extended permissions such as access control lists (ACLs), which are available on some UNIX operating systems and through some third-party extensions.

Use the Users and Groups name lists to exclude or include users for this check.

The security check returns the following messages:

Message name	Title	Class
MAILBOXMODE	Mail box grants read/write permissions	1
MAILNOTMATCHED	Mail box is not matched by a user account	0
MAILOWNERDIFF	Mail box is owned by another user	1

Sendmail log

This security check reports a problem when critical sendmail messages are not being logged. The security check verifies that sendmail logging is correctly configured on the agent, that the log file is owned by root, and that file permissions are valid.

When checking UNIX file permissions, this check examines only the basic user/group/other and read/write/execute permissions. The check does not consider any extended permissions such as access control lists (ACLs), which are available on some UNIX operating systems and through some third-party extensions.

The security check returns the following messages:

Message name	Title	Class
LOGNOTROOT	Sendmail log file not owned by root	1
LOG_NOT_CONFIG	Sendmail logging not configured	1
LOGPERMISSION	Invalid sendmail log file permissions	0
LOGNOTREGFILE	Sendmail log file not regular file	0

Log level setting

This security check reports a problem when the log level setting in the sendmail.cf file is less than the value set in your security policy. The default policy setting is 9, which logs messages caused by undeliverable mail.

The security check returns the following message:

Message name	Title	Class
LOGLEVEL	Log level less than policy setting	2

Postmaster

This security check examines the mail aliases file to verify that the postmaster alias is set to a valid user to send critical sendmail messages. The UNIX default alias is root.

The check returns the following messages:

Message name	Title	Class
CFNOEXIST	Sendmail configuration file missing	0
ALIASNOEXIST	Mail alias file missing or not a regular file	2
POSTMASTERNOTFOUND	Postmaster does not resolve to a valid user account	1

Sendmail configuration file

This security check examines the sendmail.cf configuration file for the noexpn, novrfy, and goaway settings. These settings are required to disable the expn and vrfy commands.

The security check returns the following messages:

Message name	Title	Class
NOEXPNNOEXIST	expn command is enabled	2
NOVRFYNOEXIST	vrfy command is enabled	2

System Queues

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

Correctable System Queues messages

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

Correctable messages display the letter C in the Updateable/Correctable column of the console grid.

Security check	Message name
CRONTAB file contents	CRONGW
CRONTAB file contents	CRONWW
CRONTAB file contents	CRONMODE
CRONTAB file contents	CRONOWNERDIFF
CRONTAB file contents	CRONOWNERNOTROOT

Users to check

Use this option to create name lists of users and groups to exclude or include in all System Queues checks.

AT subsystem access

This security check reports users that are allowed to use the at and batch utilities. Use the Users/Groups name lists to include or exclude users that are not included or excluded by the Users to check option.

The security check returns the following message:

Message name	Title	Class
ATALLOW	Allowed to use at and batch	0
ATDENY	Denied use of at and batch	0
ATGLOBAL	Global at and batch usage allowed	0
ATSUONLY	Only root can use at and batch	0

CRON subsystem access

This security check lists the users that are allowed to use the cron program. Use the Users/Groups name lists to include or exclude users that are not included or excluded by the Users to check option.

The security check returns the following messages:

Message name	Title	Class
CRONALLOW	Allowed to use crontab	0
CRONDENY	Denied use of crontab	0
CRONGLOBAL	Global cron usage allowed	0
CRONSUONLY	Only root can use crontab	0

CRONTAB file contents

This security check looks at the contents of the crontab files on the computer. Each command in the crontab is examined for configuration files and executable programs. The module then checks the executables and configuration files for group and world write permissions.

The module evaluates /tmp directories and world-writable directories that do not have the sticky bit set, but the module does not evaluate world-writable directories that do have the sticky bit set.

The sticky bit maintains file ownership within a world-writable directory. Although anyone can create new files in a world-writable directory, the ability to modify or delete existing files depends on individual file permissions.

Use the file list to exclude executables and configuration files from this check. Specify full path names in the file list.

When checking UNIX file permissions, this check examines only the basic user/group/other and read/write/execute permissions. The check does not consider any extended permissions such as access control lists (ACLs), which are available on some UNIX operating systems and through some third-party extensions.

The security check returns the following messages:

Message name	Title	Class
CRONGW	Group writable file reference in crontab file	1
CRONWW	World writable file referenced in crontab file	4

Message name	Title	Class
CRONMODE	crontab grants read/write permissions	4
CRONNOTMATCHED	crontab not matched by a user account	0
CRONOWNERDIFF	crontab is owned by another user	1
CRONOWNERNOTROOT	crontab not owned by root	4
CRONNSUSER	Nonexistent user configured for cron or at	0

User Files

The User Files module examines user file ownership and permissions, PATH and umask settings in startup files, files with the same names as system commands, hidden directories, special device files, and remote mount points. It is in the Queries module.

Correctable User Files messages

The User Files module has six security checks that report correctable messages. These messages let you correct user file settings on the agent from the console grid.

Correctable messages display the letter C in the Updateable/Correctable column of the console grid.

Security check	Message name
File ownership	USRONOTOWNER
World writable files	USRWORLDWRITE
Group writable files	USRGROUPWRITE
Set UID or GID	SUIDOWNER
Set UID or GID	SGIDOWNER
Set UID or GID	SUIDOTHER
Set UID or GID	SGIDOTHER
Check Startup File Contents	NETRC_PASS_READ
Startup file protection	BADPERM
Startup file protection	USRSNOTOWNER

Users to check

Use this option to specify users and groups that are excluded or included for all User Files security checks. See "Editing name lists" on page 35.

File ownership

This security check identifies files in the user's directory tree that are not owned by the user. Either the user ID (UID) or group ID (GID) of the file does not match the UID or GID of the user that is defined in the /etc/passwd file. To exclude files from this check, specify their full path names in the file list.

Incorrect file ownership can allow unauthorized access to files or prevent authorized users from accessing the files.

The check returns the following message:

Message name	Title	Class
USRONOTOWNER	User does not own file	1

To protect your computers

- Change the user or group ownership of the named files. If a file is correctly owned but located in the wrong directory, move the file out of the user's directory tree.

World writable files

This security check identifies user files and directories that are world writable (i.e., writable by everyone). To exclude files that should be world writable from this check, specify their full path names in the file list.

Files that are writable by everyone represent a security risk because there are no controls to restrict who can modify or delete these files.

The check examines only the basic user/group/other and read/write/execute UNIX file permissions. It does not consider any extended permissions such as access control lists (ACLs), which are available on some UNIX operating systems and through some third-party extensions.

The check returns the following message:

Message name	Title	Class
USRWORLDWRITE	World writable	0

To protect your computers

- Use the **chmod o-w <file name>** command to remove world write permissions from the listed files.

Group writable files

This security check identifies user files and directories that are group writable (i.e., writable by anyone with group access to the files). To exclude files from this check, specify their full path names in the file list.

Group write permissions can cause security problems if all members of a group are not authorized to access the files.

The check returns the following message:

Message name	Title	Class
USRGROUPWRITE	Group writable	0

To protect your computers

- Use the **chmod g-w <filename>** command to remove group write permissions from the listed files.

SETUID or SETGID

This security check identifies all user files that have set user ID (setuid) or the set group ID (setgid) bits. To exclude files from this check, specify their full path names in the file list.

Files that set the UID or GID of users executing the files to the UID or GID of the file owner or to other users may allow unauthorized access to other files.

The check returns the following messages:

Message name	Title	Class
SUIDOWNER	Setuid to owner	4
SGIDOWNER	Setgid to owner	4
SUIDOTHER	Other setuid file	4
SGIDOTHER	Other setgid file	4

To protect your computers

- Use the **chmod ug-s <file name>** command to remove setuid and setgid properties from the listed files.

PATH (using su)

This option determines how PATH checks are performed. When this option is enabled, the check uses the su command to access each user account and run startup scripts to check PATH settings.

Do not select both this option and the PATH (modifying startup script) option. The two options are mutually exclusive.

PATH (modifying startup script)

This option determines how PATH checks are performed. When this option is enabled, the check adds a command to the end of each user's .profile or .login script to check PATH settings. The option is effective only after the user logs in subsequent to the change.

Do not select both this option and the PATH (using su) option. The two options are mutually exclusive.

Successful execution of PATH checks on a Red Hat Linux agent requires that the Linux computer be configured to use the shadow password file.

Current directory only at end of PATH

This security check reports users with current directory (. or ::) entries that are located anywhere except at the end of their PATH variables.

Use the check's name list to exclude or include users and user groups that are not already included or excluded by the Users to check option.

Before executing this check, enable one, but not both, of the PATH (using su) or PATH (modifying startup script) options.

When both this check and the check titled Current directory not allowed in PATH are run on the same user account, the check reports any current directory entry in the user's PATH variable as an error.

The check returns the following messages:

Message name	Title	Class
CURDIR	Current directory not last in path	1
NOENVCHK	Did not check user’s environment	0

Current directory not allowed in PATH

This security check reports users with current directory entries (. or ::) that are located anywhere in their PATH variables. Use the check's name list to exclude or include users and user groups that are not already included or excluded by the Users to check option.

Before executing this check, enable one, but not both, of the PATH (using su) or PATH (modifying startup script) options.

When both this check and the check titled Current directory only at end of PATH are run on the same user account, the check reports any current directory entry in the user's PATH variable as an error.

The check returns the following messages:

Message name	Title	Class
CURDIR2	Current directory found in path	1
BOTH_CURDIR	User included for both current directory PATH checks	0
NOENVCHK	Did not check user’s environment	0

User directories follow system directories in PATH

This security check reports users with user directory entries that are located before the system directory entries in their PATH variables.

Use the check's name list to exclude or include users and user groups that are not already included or excluded by the Users to check option.

Before executing this check, enable one, but not both, of the PATH (using su) or PATH (modifying startup script) options.

The check returns the following messages:

Message name	Title	Class
USERDIR	User directory too early in path	1
NOENVCHK	Did not check user’s environment	0

World writable directories in PATH

This security check reports world-writable directories that are listed in user PATH statements. This is a security risk because anyone with remote access to the directory could spoof the user by placing a new file in the directory with a commonly-used system name such as ls. The user could then unknowingly execute the new file when attempting only to execute the system command.

Use the check's name list to exclude or include users and user groups that are not already included or excluded by the Users to check option.

Before executing this check, enable one, but not both, of the PATH (using su) or PATH (modifying startup script) options.

The check returns the following messages:

Message name	Title	Class
PATHWORLDWRITE	World writable directory in user path	1
NOENVCHK	Did not check user’s environment	0

Group writable directories in PATH

This security check reports group-writable directories that are listed in user PATH statements. This is a security risk because a member of the user group could spoof the user by placing a new file in the directory with a commonly-used system name such as ls. The user could then unknowingly execute the new file when attempting only to execute the system command.

Use the check's name list to exclude or include users and user groups that are not already included or excluded by the Users to check option.

Before executing this check, enable one, but not both, of the PATH (using su) or PATH (modifying startup script) options.

The check returns the following messages:

Message name	Title	Class
PATHGROUPWRITE	Group writable directory in user path	0
NOENVCHK	Did not check user’s environment	0

Umask (using su)

Enable this option to have the Umask check use the su command to access each user account and run startup script. (Red Hat Linux operating systems must be configured to use the shadow password file.)

Do not enable this option and the Umask (modifying startup script) option. The two are mutually exclusive.

The following conditions must be met or the user will be ignored:

- User must have a home directory in /etc/passwd and the home directory must exist.
- User must have a valid password.
- User must not be using /bin/sync, /usr/bin/sync, or /usr/lib/uucp/uucico as shells.

The shell executable that is specified for the user must exist, i.e., /bin/sh.

Use the default minimum umask value of 027 for normal security. This value creates executable files with permissions of 750 and other files with permissions of 640.

Umask (modifying startup script)

Enable this option to have the Umask check add a command to the end of each user's .profile or .login script to check umask settings. The next time that the user logs in, the Umask check will be able to report the user's umask value.

Do not enable this option and the Umask (using su) option. The two are mutually exclusive.

Umask

This check reports users whose umask value is less than the minimum value that you specify in the check—an octal number between 000 and 777 that is subtracted from permissions when a new file is created. Lower values grant greater access.

Enable Umask (using su) or Umask (modifying startup script) before running this check. In the name list, specify users and user groups that are to be excluded from the check.

The check returns the following messages:

Message name	Title	Class
UMASK	Unsafe mask	1
NOENVCHK	Did not check user's environment	0

Startup file contents

This security check reports accounts that have a .rhosts file or .netrc file. For .rhosts files, the check produces a list of users and computers that are not required to type a password. For .netrc files, the check produces a list of entries containing passwords.

Use the Users/Groups name lists to exclude users that are not excluded by the Users to check option.

The check returns the following messages:

Message name	Title	Class
NETRC	Account has a .netrc file	1
NETRC_PASS	.netrc file contains password	1
NETRC_PASS_ READ	Passwords in readable .netrc file	4
RHOSTS	Account has a .rhost file	1
RLOGIN	Remote user may rlogin/rsh without password	1
RLOGIN_ANY_ HOST	Account allows rlogins from any host	4
RLOGIN_ANY_ USER	Account allows rlogins by any user	4

Startup file protection

This security check looks at the permissions of user startup files to ensure that they have the proper ownerships and permissions. Use the File Permissions list to specify the names and proper permissions of the startup files for each user. The default values are listed below:

.nodes	rw-------
.netrc	rw-------
.rhosts	rw-------
.Xdefaults	rw-r-----
.cshrc	rw-r-----
.exrc	rw-r-----
.login	rw-r-----
.profile	rw-r-----
.newsrc	rw-r--r--
.mailrc	rw-r-----
.forward	rw-r-----

The check returns the following messages:

Message name	Title	Class
BADPERM	Inadequate file permissions	1
USRSNOTOWNER	User does not own user startup file	1

Users to skip for startup file protection

Use this option to specify users and user groups that are to be excluded from the Startup file protection check.

Required files

This security check reports required files that are not found in a user's home directory. Use the name list to specify the relative path names for the files that must appear in each user's home directory.

System accounts and accounts that are not listed with home directories in the /etc/passwd file are not checked.

The check returns the following messages:

Message name	Title	Class
REQUIRED_FILE_NOT_FOUND	Required file not found	1
NO_ACCESS_TO_HOME_DIRECTORY	Cannot access user home dir	1

Users to check for required files

Use this option to specify users or user groups that are to be included or excluded in the Required files check.

Forbidden files

This security check reports forbidden files that are found in a user's home directory. Use the name list to specify the relative path names for the files that must not appear in any user's home directory.

System accounts and accounts that are not listed with home directories in the /etc/passwd file are not checked.

The check returns the following messages:

Message name	Title	Class
FORBIDDEN_FILE_FOUND	Forbidden file found	1
NO_ACCESS_TO_HOME_DIRECTORY	Cannot access user home dir	1

Users to check for forbidden files

Use this option to specify users or user groups that are included or excluded in the Forbidden files check.

Suspicious file names

This security check looks for executable files with suspicious file names in each user's home directory tree. A suspicious name is one that is the same as either a user name or the name of a system command that is listed in the man pages.

Specify full path names in the file list to exclude files from this check.

An executable file with a suspicious name can be executed by another user unknowingly when the user enters the matching user name or command name in a path that is not set up properly.

The check returns the following message:

Message name	Title	Class
SUSPFILE	Suspicious file name found	1

Device files

This security check looks for block-special and character special (device) files in the user's home directory tree.

To exclude files from this check, specify their full path names in the file list.

The check returns the following message:

Message name	Title	Class
USRDEVICE	Device special file in user area	4

Hidden directories

This security check looks for hidden directories in a user's home directory tree. A hidden directory is one that begins with a dot (.) character and does not appear in a normal directory listing. Although it is not very effective, users can try to hide information, which they are not authorized to have, in hidden directories.

Specify the names of hidden directories that are typically located in user accounts in the name list to exclude those directories from the check.

The check returns the following message:

Message name	Title	Class
HIDEDIR	Hidden directory	4

Mount points

This security check looks for mount points within a user's home directory tree. It is not standard practice to mount devices in user areas. This can represent unauthorized access to data on the device in question.

Use the file list to exclude mount points from this check. The list can consist of directory names or special device file names.

Appendix

Integrated Command Engine (ICE)

This chapter includes the following topics:

Introducing ICE

The Integrated Command Engine (ICE) in the Dynamic Assessment policy adds client/server-based functions. The executable programs and scripts that you integrate through ICE template directives function as security checks.

Use ICE options to:

- Enable and disable ICE templates.
- Enable and disable the messages that identify missing scripts and unmapped messages for debugging purposes.
- Enable and disable messages that are mapped to the output of integrated executables and scripts in ICE templates.

ICE templates integrate user provided programs or scripts into Symantec ESM and map their output to security messages. The templates apply cross-platform using the platform designations specified in ICE template OS/Rev sublists.

Symantec ESM does not provide ICE templates. You must create your own. See "Creating an ICE template" on page 228.

Applying ICE message options

Any check in ICE can return the messages listed in the table below.

ICE returns the No problems found message when the module cannot execute because required Base Path or Script Entry records are missing from your ICE templates.

To identify any missing scripts, select ICE Script Missing messages option the first time you run a new executable or script through ICE.

Other common ICE messages indicate problems with ICE templates or problems with the executables or scripts that are defined in ICE templates.

Message name	Title	Class
HEADER	No problems found	0
ILLEGALPATHINSCRIPT	Illegal path in script	0
ILLEGALBASEPATH	Illegal base path	0
SCRIPTERROR	Script error	1

Message Maps sublist

Message Maps sublist entries specify how to report the output of executables and scripts that are defined in the ICE template.

Entries in Message Maps sublists contain information needed to map the output of integrated executables or scripts to ICE messages. After you run the module, these messages are displayed in the console grid with distinctive titles and green, yellow, or red security levels.

Record	Entry maps	Notes
Script Entry	Only the executable or script that is specified on the same row as the sublist.	Takes over entries in Message Maps records. Entries are only processed with entries of a Message Maps record.
Message Maps	All executables and scripts that are specified in the template that contains the Message Maps record.	Maps different lines of output with specified character strings to a different ICE message. Entries are processed as a single list.

When you enable the Unmapped messages option, output that is not mapped in Message Maps or Script Entry records is reported as a yellow-level Unmapped Message.

Integrating a new function

The *Symantec ESM Integrated Command Engine (ICE) Module Training Guide* provides exercises that demonstrate how to:

- Integrate the Netstat command on UNIX and Windows computers
- Integrate the NTODrv utility on Windows computers
- Integrate the PSLogList utility on Windows computers

You can download the Training Guide with the current Security Update release from the Symantec Web site at http://securityresponse.symantec.com/.

To integrate a new function using ICE

1. Create or obtain a script or executable program that runs a query, executes a program, or performs another security assessment function that you want to integrate.
2. Verify the operation of the executable or script before you add it to ICE.
3. Copy the executable or script into a subdirectory on the test agent for ICE executables and scripts.
4. Create an ICE template. See "To create an ICE template" on page 228.
   The ICE template tells where to find the script or executable and how to map its output to ICE messages.
5. Add ICE to a demo policy in the console. See "To add a new policy" on page 30.
6. Enable the template in the Command Engine Templates option.
7. Select applicable ICE options in your demo policy, including options that report missing scripts and unmapped messages for debugging purposes.
8. Enable messages that are mapped in the ICE template to the integrated executables or scripts, and disable all ICE messages that are not appropriate to the integrated executables or scripts.
9. Run the demo policy on a test agent and verify that expected output from the integrated executables or scripts is reported as ICE messages. See "To run a policy" on page 33.
10. Disable ICE options that report debugging messages after testing verifies a successful integration, and deploy the module to other agents.

Creating an ICE template

Create an ICE template for each set of related functions.

To create an ICE template

1. In the Symantec ESM console tree, right-click **Templates**, then click **New**.
2. Select **Integrated Command Engine -all**.
3. Type a name for the template. Symantec ESM will add the .ice extension.
4. Click **OK**.
5. In the Template Editor, add one or more of the following records:
   - OS/Release (see "To add an OS/Release record" on page 228).
   - Base Path (see "To add a Base Path record" on page 228).
   - Script Entry (see "To add a Script Entry record" on page 229).
   - Message Maps (see "To add an entry to a OS/Rev sublist" on page 231).
6. Click **Save** and then **Close**.

To add an OS/Release record

1. In the Template Editor, click **Add Row**.
2. In the new template record, click the Name field, then select **OS/Release**.
3. In the Script ID -or- Base Path, Script Name, and Script Parameters fields, delete <NEW>.
4. Add one or more OS/Rev sublist entries (see "To add an entry to a OS/Rev sublist" on page 231).
5. Click **Save**.

To add a Base Path record

1. In the Template Editor, click **Add Row**.
2. Click the Name field of the new template record, then select **Base Path**.
3. In the Script ID -or- Base Path field, replace <NEW> with the path to the directory that contains the executables or scripts that you want to run. The path must be in the ESM directory on an agent.
   For example, to specify the path to a subdirectory named scripts in the ESM directory on a UNIX agent, type **scripts** in the Script ID -or- Base Path field. The module will look for the subdirectory at /esm/scripts.
   On a UNIX agent the scripts Base Path entry points to /esm/. On a Windows agent, the entry points to \Program Files\Symantec\ESM\.

4 Delete <NEW> from the Script Name and Script Parameters fields.

5 Click **Save**.
To add another entry, repeat steps 1-5.

6 Click **Close**.

To add a Script Entry record

1 In the Template Editor, click **Add Row**.

2 Click the Name field of the new template record, then select **Script Entry**.

3 In the Script ID -or- Base Path field, replace <NEW> with a script ID for the function of the executable or script.
This ID appears in the Name field of the console grid when the module reports the output of integrated executables or scripts.

4 In the Script Name field, replace <NEW> with the name of the executable or script.
ICE looks for the executable or script name in the ESM directory that is identified in the template's Base Path record. See "To add a Base Path record" on page 228.

5 In the Script Parameters field, replace <NEW> with the parameters of the executable or script. If there are no parameters, delete <NEW>.

6 Add one or more entries to the following sublists:
- OS/Rev (see "To add an entry to a OS/Rev sublist" on page 231).
- Message Maps (see "To add an entry to a Message Maps sublist" on page 230).

7 Click **Save**.
To add another entry, repeat steps 1-7.

8 Click **Close**.

Note: Do not put internationalized characters or semi-colons (;) in template fields Script Name For Script Entry or Script Parameters For Script Entry.

To add a Message Maps record

1 In the Template Editor, click **Add Row**.

2 Click the Name field of the new template record, then select **Message Maps**.

3 Delete <NEW> from the Script ID -or- Base Path, Script Name, and Script Parameters fields. The fields must be blank.

4 Add one or more Message Maps sublist entries. See "To add an entry to a Message Maps sublist" on page 230.

5 Click **Save**.
To add another record, repeat steps 1-5.

6 Click **Close**.

To add an entry to a Message Maps sublist

1 In the Template Editor click the Message Maps field. The Message Maps field displays the number of entries in the Message Maps sublist. Initially, the number is 0.

2 In the Message Maps Sublist Editor, click **Add Row.**

3 In the new sublist record, click the Message field, then select the message that you want to map:

Value	Security level
Passed	Green
Failed	Yellow
Informational	Green
Not Applicable	Green
Not Available	Green
User #1/0	Green
User #2/0	
User #3/0	
User #1/1	Yellow
User #2/1	
User #3/1	
User #1/2	Yellow
User #2/2	
User #3/2	
User #1/3	Yellow
User #2/3	
User #3/3	

Value	Security level
User #1/4	Red
User #2/4	
User #3/4	

4 In the Map String field, replace <NEW> with the character string for the output line that you are mapping. Type the string exactly as it appears in the output line. Message Maps sublist entries are case sensitive.

5 Click the Location field, then select one of the following values:

- **Starts with**
- **Contains**
- **Ends with**

This value tells ICE where the Map String is located in the output lines you are mapping to the selected message value.

6 Click **Apply**.
To add another entry, repeat steps 1-6.

7 Click **Close**.

To add an entry to a OS/Rev sublist

1 In the Template Editor, click the OS/Rev field on the template record that you are editing. The field displays the number of entries in the OS/Rev sublist. Initially the number is 0.

2 In the OS/Rev Sublist Editor, click **Add Row**.

3 In the Exclude field, do one of the following:

- Select the check box to exclude the specified OS and Revision from the executable or script.
- Clear the check box to include the specified OS and Revision.

The following table shows where the executable or script runs when the Exclude check box is cleared.

OS setting	Executable or script runs
ALL (or blank)	On all agents.
<Operating system>	Only on agents that have the specified operating system.
<Operating system> + one or more settings in the Release/Revision field	Only on agents that have the specified operating system, releases, and revisions.

The following table shows where the executable or script does not run when the Exclude check box is checked.

OS setting	Executable or script does not run on
ALL (or blank)	Any agent
<Operating system>	Any agent that has the specified operating system.
<Operating system> + one or more settings in the Release/Revision field	Any agent that has the specified operating system, releases, and revisions.

4 Click the OS field, then select an option.

5 In the Release/Revision field, replace <NEW> with a revision ID using the following conventions:

Option	Description
2.5	Only the specified revision.
-2.5	A revision ID with a leading minus (-) sign: the specified revision and all previous revisions.
+2.5	A revision ID with a leading plus (+) sign: the specified revision and all later revisions.

6 Click **Apply**
To add another entry, repeat steps 2-6.

7 Click **Close**.

To remove a record or sublist entry

1 In the Template Editor, click the number of the record that you want to remove, or in a Sublist Editor, the number of the entry. This number is in the leftmost column.
To select a range of records or entries, hold down the Shift key while you click the first and last row numbers in the range.
To select non-sequential records or entries, hold down the Ctrl key while you click the row numbers.

2 In the Template Editor, click **Remove Entry(s)**, or in the Template Sublist Editor, click **Remove list entry** or **Remove list entry(s)**.

3 Click **Apply**.

Applying ICE message options

The Integrated Command Engine (ICE) includes the following options:

The descriptions below include steps to demonstrate how each option works. These procedures use a demo policy that you need to create.

Script Missing messages

Enable this option to debug a newly-created ICE template before you rely on the messages generated by the template when you run ICE. When a script or executable that is defined in a Script Entry record cannot be located in the Base Path record, the green level Script Missing message is displayed. See "To add a Script Entry record" on page 229 and "To add a Base Path record" on page 228.

This option returns the following message:

Message name	Title	Class
SCRIPTMISSING	Script Missing	0

When this option is disabled, and specified executables or scripts cannot be located, the green level message, No problems found, is displayed.

To demonstrate the option

1 Create an ICE template with Base Path and Script Entry records that point to a directory and executable file in the ESM directory structure. See "To create an ICE template" on page 228, "To add a Base Path record" on page 228, and "To add a Script Entry record" on page 229.
Make sure that no OS/Rev sublist entry excludes the test agent.

2 Remove the test executable from its directory.

3 In ICE, enable the Command Engine Templates option.

4 Enable the ICE template.

5 Enable the Script Missing messages option.

6 Run the demo policy on the agent.

7 In the console grid, verify that the policy run reports the Script Missing message.

If the correct message is not reported, make sure that

- Directories and executable files or scripts that are named in ICE template Base Path and Script Entry records exist in the Symantec ESM directory structure on supported agents.
- Directory and file names are spelled correctly in template records.
- The Script Missing messages option is enabled.

Unmapped messages

Enable this option, then run ICE to debug a newly-created template before you rely on the template message mappings. It reports a yellow level Unmapped message for each line of output that is not mapped to an ICE message by a Message Map sublist entry.

The option returns the following message:

Message name	Title	Class
UNMAPPED	Unmapped Message	1

To demonstrate the option

1 Create an ICE template that includes a Message Maps sublist that omits at least one mapping to at least one output line from the executable or script. (Message Maps sublists are used in Base Path and Script Entry records.) See "To create an ICE template" on page 228.
Make sure that no OS/Rev sublist entry excludes the test agent.

2 In ICE, select the Command Engine Templates option.

3 Enable the ICE template.

4 Enable the Unmapped messages option.

5 Run the demo policy.

6 In the console grid, verify that the policy run reports each unmapped output line with the Unmapped message title.

If the correct message is not reported, make sure that

- Message Map sublist entries map all useful and informative output by executables or scripts.
- In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.
- The Unmapped messages option is enabled.

Report all stderr messages

This option enables reporting of all standard error (stderr) messages. Standard error messages are reported from the script.

This option returns the following message:

Message name	Title	Class
STDERRMSG	Stderr message	0

Redirect stderr to stdout

This option enables mapping standard errors (stderr) to defined Message Maps. This option overrides Report all stderr messages and reports all messages that are defined in the Message Maps.

Return code

This option enables checking the return code generated from defined scripts.

This option returns the following message:

Message name	Title	Class
RETCODE	Return code does not match	0

This message is displayed when the return code from the script does not match the given return code.

Passed messages

This option reports output from defined executables or scripts that is mapped to green-level Passed messages in Message Maps sublist entries.

The option returns the following message:

Message name	Title	Class
PASSED	User test passed	0

If you disable this option, the Passed message is not reported.

To demonstrate the option

1. Create an ICE template with at least one Message Maps sublist entry that maps an output line from an executable to the Passed message value. See "To create an ICE template" on page 228, "To add an entry to a Message Maps sublist" on page 230, and "To remove a record or sublist entry" on page 232. Make sure that no OS/Rev sublist entry excludes the test agent.
2. In ICE, select the Command Engine Templates option.
3. Enable the ICE template.
4. Make sure that the Passed messages option is enabled.
5. Run the demo policy on an agent.
6. In the console grid, verify that the policy run reports all output lines that are mapped to Passed messages.

If the correct message is not reported, make sure that

- In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.

Failed messages

This option reports output from defined executables or scripts that is mapped to yellow-level Failed messages in Message Maps sublist entries.

The option returns the following message:

Message name	Title	Class
FAILED	Test failed	1

If you disable this option, the Failed message is not reported.

To demonstrate the option

1. Create an ICE template that includes at least one Message Maps sublist entry that maps an output line from an executable program to the Failed message value. See "To create an ICE template" on page 228 and "To add an entry to a Message Maps sublist" on page 230. Make sure that no OS/Rev sublist entry excludes the test agent.
2. In ICE, select the Command Engine Templates option.
3. Enable the ICE template.
4. Make sure that the Failed messages option is enabled.
5. Run the demo policy.
6. In the console grid, verify that the policy run reports all output lines that are mapped to Failed messages.

If the correct message is not reported, make sure that

- In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.Information messages

This option reports output from specified executables or scripts that is mapped to green-level Information messages in the Message Maps sublist.

The option returns the following message:

Message name	Title	Class
INFORMATIONAL	User test information	0

If you disable this option, User test information is not reported.

To demonstrate the option

1. Create an ICE template that includes at least one Message Maps sublist entry that maps an output line from an executable program to the Informational message value. See "To create an ICE template" on page 228 and "To add an entry to a Message Maps sublist" on page 230.
   Make sure that no OS/Rev sublist entry excludes the test agent.
2. In ICE, select the Command Engine Templates option.
3. Enable the ICE template.
4. Make sure that the Information messages option is enabled.
5. Run the demo policy.
6. In the console grid, verify that the policy run reports all output lines that are mapped to Information messages.

If the correct message is not reported, make sure that

- In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.

Not Applicable messages

This option reports output from defined executables or scripts that is mapped to green-level Not Applicable messages in Message Maps sublist entries.

The option returns the following message:

Message name	Title	Class
NOT APPLICABLE	User test not applicable	0

If you disable this option, User test not applicable is not reported.

To demonstrate the option

1. Create an ICE template that includes at least one Message Maps sublist entry that maps an executable's or script's output to the Not Applicable message value. See "To create an ICE template" on page 228 and "To add an entry to a Message Maps sublist" on page 230.
   Make sure that no OS/Rev sublist entry excludes the test agent.
2. In ICE, select the Command Engine Templates option.
3. Enable the ICE template.
4. Make sure that the Not Applicable messages option is enabled.
5. Run the demo policy.
6. In the console grid, verify that all output lines that are mapped to Not Applicable messages are reported.

If the correct message is not reported, make sure that

- In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.

Not Available messages

This option reports output from specified executables or scripts that is mapped to green-level Not Available messages in the Message Maps sublist.

The option returns the following message:

Message name	Title	Class
NOT AVAILABLE	User test not available	0

If you disable this option, User test not available is not reported.

To demonstrate the option

1. Create an ICE template that includes at least one Message Maps sublist entry that maps an output line from an executable program to the Not Available message value. See "To create an ICE template" on page 228 and "To add an entry to a Message Maps sublist" on page 230.
   Make sure that no OS/Rev sublist entry excludes the test agent.
2. In ICE, select the Command Engine Templates option.
3. Enable the ICE template.
4. Make sure that the Not Available messages option is enabled.
5. Run the demo policy.
6. In the console grid, verify that the policy run reports all output lines that are mapped to Not Available messages.

If the correct message is not reported, make sure that

- In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.

User messages

Enable these options to report output lines from executables or scripts that are mapped to User messages in Message Maps sublist entries.

The options return the following messages:

ICE option	Message name	Title	Class
User #1/0 messages	USER_1_0	User defined #1 w/value of 0	0
User #2/0 messages	USER_2_0	User defined #2 w/value of 0	0

ICE option	Message name	Title	Class
User #3/0 messages	USER_3_0	User defined #3 w/value of 0	0
User #1/1 messages	USER_1_1	User defined #1 w/value of 1	1
User #2/1 messages	USER_2_1	User defined #2 w/value of 1	1
User #3/1 messages	USER_3_1	User defined #3 w/value of 1	1
User #1/2 messages	USER_1_2	User defined #1 w/value of 2	2
User #2/2 messages	USER_2_2	User defined #2 w/value of 2	2
User #3/2 messages	USER_3_2	User defined #3 w/value of 2	2
User #1/3 messages	USER_1_3	User defined #1 w/value of 3	3
User #2/3 messages	USER_2_3	User defined #2 w/value of 3	3
User #3/3 messages	USER_3_3	User defined #3 w/value of 3	3
User #1/4 messages	USER_1_4	User defined #1 w/value of 4	4
User #2/4 messages	USER_2_4	User defined #2 w/value of 4	4
User #3/4 messages	USER_3_4	User defined #3 w/value of 4	4

If you disable an option, its message is not reported.

To demonstrate the options that enable User messages

1. Create an ICE template with Message Maps sublist entries that map output lines from specified scripts or executables to User message values. See "To create an ICE template" on page 228 and "To add an entry to a Message Maps sublist" on page 230.
   Make sure that no OS/Rev sublists entry excludes the test agent.
2. In ICE, select the Command Engine Templates option.
3. Enable the ICE template.
4. Make sure that all User message options are enabled.
5. Run the demonstration policy.
6. In the console grid, verify that the policy run reports all output lines are mapped to User messages

If the correct message is not reported, make sure that

- In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.

Index

Symbols

A

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

W