

Symantec Enterprise Security Manager™ Security Update 22 Release Notes

Symantec ESM 6.0, 6.1, and 6.1.1

For Windows, UNIX, and Linux modules

Symantec ESM Security Update 22 Release Notes

The software that is described in this document is furnished under a license agreement and may be used only in accordance with the terms of the agreement.
040909

Copyright Notice

Copyright © 2005 Symantec Corporation.
All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. Symantec Enterprise Security Manager, LiveUpdate, and Symantec Security Response are trademarks of Symantec Corporation. Microsoft, MS-DOS, Windows, Windows NT, Windows XP, and Windows 2003 Server are registered trademarks of Microsoft Corporation. Other product names that are mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged. Printed in the United States of America.

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, security alerts, patch updates, and new vulnerabilities.

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 (TAM), 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 license keys, 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 also 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 resellers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Symantec Software License Agreement

Symantec Enterprise Security Manager

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

1. License:

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

You may:

- A. use that number of copies of the Software as have been licensed to You by Symantec under a License Module. Permission to use the software to assess Desktop, Server or Network machines does not constitute permission to make additional copies of the Software. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software you are authorized to use on a single machine.
- B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
- C. use the Software to assess no more than the number of Desktop machines set forth under a License Module.

“Desktop” means a desktop central processing unit for a single end user;

D. use the Software to assess no more than the number of Server machines set forth under a License Module.

“Server” means a central processing unit that acts as a server for other central processing units;

E. use the Software to assess no more than the number of Network machines set forth under a License Module.

“Network” means a system comprised of multiple machines, each of which can be assessed over the same network;

F. use the Software in accordance with any written agreement between You and Symantec; and

G. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license.

You may not:

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

2. Content Updates:

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

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

3. Limited Warranty:

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

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

4. Disclaimer of Damages:

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

LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

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

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

5. U.S. Government Restricted Rights:

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

6. Export Regulation:

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

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the

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

Contents

Symantec ESM Security Update Release Notes

Security Update 22	13
New Supported Operating Systems	14
File Attributes (Windows)	14
Network Integrity (Windows XP/2003)	14
Password Strength (UNIX)	15
Registry (Windows)	15
Resolved issues	16
System requirements	17
Security Update 21	18
Update Report Content	19
File Attributes (Linux)	20
File Attributes (Windows)	20
File Find (UNIX)	20
File Watch (All)	20
Group Policy (Windows 2000 server/ 2003 server)	21
Login Parameters (Solaris)	29
Network Integrity (Windows)	29
Network Integrity (Solaris, AIX,)	29
Password Strength (HP-UX)	30
Password Strength (Solaris)	30
Password Strength (Windows 2000/ 2003)	31
Startup Files (Windows 2000/ NT/ XP/ 2003)	31
Symantec Product Information (Windows 2000/ NT/ XP)	32
Symantec Product Information (Windows)	33
System Mail (UNIX)	33
System Mail (UNIX)	34
Known issues	34
Resolved issues	36
System requirements	38
Security Update 20	39
Active Directory Services (Windows)	39
File Attributes (SUSE ES 8)	41
File Attributes (UNIX)	41
File Attributes (Windows)	42
File Find (Windows 2000/ 2003/ XP)	43

Using regular expressions	52
File Watch (Windows)	56
File Watch (Linux)	57
Login Parameters (Windows)	57
Login Parameters (UNIX)	58
Network Integrity (Windows 2003/XP)	62
Network Integrity (UNIX)	66
OS Patches (SUSE ES 8)	70
Startup Files (UNIX)	70
Changed messages	71
Known issues	71
Resolved issues	71
System requirements	72
Security Update 19	73
Account Integrity (Windows)	73
Account Integrity (UNIX)	75
Account Integrity (Windows/UNIX)	77
Active Directory (Windows)	77
File Attributes (Windows/UNIX)	80
File Attributes (Windows)	80
File Attributes (UNIX)	81
File Find (UNIX)	82
File Watch (Windows/UNIX)	85
Login Parameters (Windows)	86
Network Integrity (Windows/UNIX)	86
Network Integrity (Windows)	87
Object Integrity (UNIX)	88
OS Patches (AIX)	88
OS Patches (Solaris/HP-UX)	89
Password Strength (Windows)	90
Registry (Windows)	92
Startup Files (Windows/UNIX)	93
Known issues	93
Resolved issues	94
System requirements	95
Security Update 18	97
SUSE LINUX	97
Account Integrity (Windows)	97
File Attributes (Windows/UNIX)	100
File Attributes (Windows)	100
File Attributes (UNIX)	103
File Find (UNIX)	107
File Watch (Windows/UNIX)	108

Login Parameters (UNIX)	109
Network Integrity (UNIX)	110
Network Integrity (Windows)	110
Password Strength (Windows)	111
Registry (Windows)	112
Startup Files (UNIX)	112
System Auditing (Windows)	113
Resolved issues	115
Documentation updates	116
System requirements	117
Frequently asked questions	119

Symantec ESM Security Update Release Notes

These Release Notes describes the security updates for Symantec Enterprise Security Manager 6.0, 6.1, and 6.1.1 that have been released since the latest Symantec Enterprise Security Manager Security Update user guides were published. Security updates will be added to the ESM Release Notes until the next version of Symantec ESM is released. At that time, this content will be integrated into new Security Update user guides.

Note: When Windows checks do not run on all Windows operating systems, the supported systems appear after the check name. For example, User Files (Windows NT) runs only on Windows NT.

Security Update 22

The following are new in SU 22:

- SUSE 9 full platform support
- Red Hat AS 3.0 Itanium, EM64T, AMD64 full platform support
- Red Hat AW 3.0 AMD64 full platform support
- AIX 5.3 support
- Three new checks
- Five modified checks
- One new message
- One new option

New Supported Operating Systems

SU 22 includes the following newly supported platforms:

- IBM AIX 5.3
- Red Hat Enterprise Linux AS 3.0 on Itanium, EM64T, and AMD64
- Red Hat Enterprise Linux WS 3.0 on AMD64
- SUSE LINUX Enterprise Server 9 for x86

File Attributes (Windows)

SU 22 includes one new check and four modified checks in the File Attributes module.

Auditing ACL (Windows)

This new check reports a problem if auditing settings (System ACLs) do not match the values in their associated template records. Auditing ACLs are checked for files and folders in enabled templates that have the Enabled ACL Checking option selected and Auditing ACLs specified in the Auditing ACL template entry sublist.

File ACL

This check is modified to report a problem only if file and folder permissions do not match the values in the enabled templates. Auditing ACLs are now checked by the new Auditing ACL check.

The following options were modified to apply to both the Auditing ACL and File ACL checks:

- Allow any privileged account
- Do not notify if file permissions are increased in security
- Do not notify if User/Group In ACL is not on system

Network Integrity (Windows XP/2003)

SU 22 includes one new check and one new message in the Network Integrity module.

ICMP messages (Windows XP/2003)

This check reports a problem if an unauthorized ICMP message is exposed to the Internet through the Internet Connection Firewall. All ICMP messages are disabled by default. If a key is disabled, ESM ignores the ICMP message setting.

When the ICMP messages check is enabled, ESM checks the ICMP settings on the system to find enabled keys. If the firewall is disabled, all ICMP checks are ignored.

[Table 1-1](#) shows the new message for this check.

Table 1-1 ICMP messages message

Message name	Title	Severity
ESM_ICMP_VIOLATION	Unauthorized exposure of an ICMP message	Yellow-3

Password Strength (UNIX)

SU 22 includes one new option in the Password Strength module.

Repeating characters (UNIX)

This option monitors user passwords to find instances of a single repeating character. Passwords that include a single repeating character may be easy to guess.

Registry (Windows)

SU 22 includes one new check and one modified check in the Registry module.

Auditing permissions (Windows)

This new check reports a problem if registry key auditing permissions or System ACLs do not match the values in their associated template records. Auditing permissions are checked for registry keys in enabled templates that have the Enable ACL Checking option enabled and Auditing ACLs specified in the Auditing template entry sublist.

Key permissions

This check is modified to report a problem only if registry key permissions do not match the permissions specified in the enabled templates. Auditing permissions are now checked by the new Auditing Permissions check.

Resolved issues

The following issues are resolved in SU 22:

Account, File Find, File Watch, User Files (UNIX)	The /proc directory has been added to the File Find module and is excluded by default.
All Modules (AIX)	AIX 5L 5.3 has been added to the drop-down lists for the templates.
File Access (UNIX)	The info field for the User file access message has changed. Previously it displayed, “user 1: read, write, execute; user 2: read, write; . . .” Now it displays, “user 1: rwx; user 2: rw-; . . .”
File Attributes (Windows)	The File Version check and the ESMT_FILE_VERSION message have been removed from the File Attributes module. The ESMT_NO_FILE_VERSION and ESMT_UNMATCH_FILE_VERSION messages are grouped with the Template File List check.
Login Parameters (Solaris)	The configuration of the Solaris 9 FTPD banner has changed. The /etc/ftpd/ftppass file has been applied.
Network Integrity (Windows)	When the Hidden Shares option is checked, it displays all hidden shares including IPC\$.
Password (All Platforms)	ASCII and UTF-8 Word files are supported by ESM and can be selected in a policy.
Startup Files (Solaris)	The File system setuid protection check reads mount points from mounted file systems rather than checking the file system tables (/etc/vfstab, /etc/fstab or /etc/filesystem).
Account Integrity Login Parameters Password Strength User Files (UNIX)	The Local Accounts Only check description has been changed to Local Accounts/Groups Only.
File Attributes (Windows)	In the File Attributes template, if Optional is in the Required column you will not receive an error message if the designated drive does not exist.
Login Parameters (Windows)	The Last user name hidden check now checks the Windows NT key as well as the Windows 2000 key.

System requirements

[Table 1-2](#) lists the supported operating systems for SU 22.

Table 1-2 SU 22 supported operating systems

Agent operating system	Versions
AIX /RS 6000	4.2.1, 4.33, 5.1
AIX-PPC	5.2, 5.3
HP-UX	10.20, 11, 11.11, 11.23
Red Hat Linux	7.x, 8, 9
Red Hat Linux Enterprise Server (ES) (x86)	2.1, 3.0
Red Hat Enterprise Linux WS and AS (AMD64)	3.0
Red Hat Enterprise Linux AS (Itanium)	3.0
Red Hat Enterprise Linux AS (EM64T)	3.0
Solaris	2.5.1, 2.6, 2.7, 2.8, 2.9
SUSE LINUX Standard Server	8
SUSE LINUX Enterprise Server	8, 9
Windows 2000 Professional and Server (Intel)	All
Windows NT Workstation and Server (Intel)	4.0 SP6a
Windows Server 2003	All
Windows Server 2003 (Itanium®)	All
Windows XP Professional (Intel)	All

Symantec reserves the right to certify the security update on the new versions of the supported operating systems before officially supporting them.

The LiveUpdate installation of SU 22 on all supported operating systems requires approximately 560 MB on each Symantec ESM manager. The amount of disk space required by each agent depends on its operating system.

[Table 1-3](#) lists the agent disk space requirements.

Table 1-3 SU 22 agent disk space requirements

Agent operating system	SU 22
AIX /RS 6000	92 MB
AIX-PPC	120 MB
HP-UX	72 MB
Red Hat Linux	36 MB
Red Hat Linux Enterprise Server (ES) (x86)	36 MB
Red Hat Enterprise Linux WS and AS (AMD64)	44 MB
Red Hat Enterprise Linux AS (Itanium)	133 MB
Red Hat Enterprise Linux AS (EM64T)	44 MB
Solaris	58 MB
SUSE LINUX Standard Server 8	36 MB
SUSE LINUX Enterprise Server 9	36 MB
Windows 2000 Professional and Server (Intel)	31 MB
Windows NT Workstation and Server (Intel)	31 MB
Windows Server 2003	31 MB
Windows Server 2003 (Itanium®)	104 MB
Windows XP Professional (Intel)	31 MB

Security Update 21

The following are new in SU 21:

- One new module
- Nineteen new checks
- Two new options
- Fourteen new messages
- Twelve new templates
- Eight new utility options in .tpk installation

Update Report Content

SU 21 includes one new utility at the end of the ESM tuneup pack (tpk) installation. The `pushfiles.exe` (Windows) or `pushfiles.` (Unix) lets you correlate check message mapping between the ESM agent and the ESM manager. The Report Content File (.rdl) is the name of the file that is sent from the agent to the manager. You can change the location of the .rdl or update the content manually from the command prompt at anytime.

At the end of the tpk installation process you now receive the following prompt:

```
Report content file: update/ble/SU_2100/en/UpdatePackage.rdl
If you have already pushed this report content for other
agents of the same type of operating system with the same manager
you can skip this step.
```

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

If you type no, the installation will end. If you type yes, you will receive the following:

```
Update ESM check message mapping file: <location of Update Package
.rdl>
... Please wait...
```

```
DoCheckMsgMapping: running <location of pushfiles.exe> <options>
End of installation.
```

[Table 1-4](#) lists the options for the pushfiles utility.

Table 1-4 pushfiles options

Options	Description
-i	Connect to the manager via IPX (Windows only)
-m	Specify the manager name
-U	The ESM access record name (default: ESM)
-P	The ESM access record password
-p	The TCP port to use (default: 5600)
-s	The source file
-d	The destination file and directory (relative to ESM_HOME on the destination system)
-t	Connect to the manager via TCP (this is the default)

File Attributes (Linux)

SU 21 includes one enhancement to one check in the File Attributes module. The File Permissions check on the Linux OS checks the immutable bit, in addition to the normal permissions, and appends an 'i' if the immutable bit is set when adding a file to a template using the Add File button in the template editor. The File Permissions check reports if there is a change to the status of the immutable bit. Corrections update the immutable bit on the filesystem to match what is in the template and template updates modify the template to match the filesystem.

File Attributes (Windows)

SU 21 includes one new check box and one new file version field in the File template of the File Attributes module. If you check the enable file version checking check box, ESM searches for the file version that you have defined in the file version field. The file version field supports operators such as =, !=, <, >, <=, and >=. The default operator is =. For example, if you want ESM to check for version 1.0.0.1, check the enable file version checking check box and type =1.0.0.1 or 1.0.0.1 in the file version field.

File Find (UNIX)

SU 21 includes one new check in the Find File module.

Unprintable characters in file names (UNIX)

This check reports a problem if files or directory names contain unprintable characters.

[Table 1-5](#) lists the Unprintable characters in filenames message.

Table 1-5 Unprintable characters in file names message

Message name	Title	Severity
STKU_UNPRINTABLE	Unprintable character(s) in file name	Yellow-3

File Watch (All)

SU 21 includes one option in the File Watch module.

Ignore Directories (All)

Enable this option to monitor the contents of a directory and subdirectory without monitoring the directories themselves. This option enables file watch security checks to ignore directories on file systems.

Group Policy (Windows 2000 server/ 2003 server)

SU 21 includes a new Group Policy (GPO) module for Windows 2000 Server and Windows 2003 Server computers. The Group Policy module reports discrepancies between the Group Policy security settings and your security policy defined in ESM. This new module contains eleven checks and eleven template files that correspond to and are enabled by each check.

The Group Policy module provides increased support for Active Directory by comparing these security settings to ESM policy settings. The ESM Group Policy templates relate directly to the Windows Group Policies. The majority of the templates are pre-populated with default values. Do not create new templates from the original, pre-populated templates. Instead, you must copy the original template and then make your modifications. You cannot add or delete rows in these pre-populated templates.

Note: This module should run only on domain controllers.

To copy templates

- 1 In the Windows Explorer, navigate to the template that you want to copy and rename.
- 2 Right-click the template.
- 3 Click **Copy**.
- 4 Navigate to the location where you want to save the copied template.
- 5 Right-click the directory and then click **Paste**.
- 6 Rename the template.

The Group Policy name in the GPO Name field of each template is a regular expression and must match the policy name. ESM searches for only the policies that are defined in the GPO Name field.

Account Policies - Password Policy (Windows 2000/ 2003)

This check reports a problem if there is a discrepancy between the Windows Group Policy settings and the settings that you defined in the ESM GPO Password Policy template.

The message severities for this check can be green, yellow, or red level severities based on how you define the severity in the corresponding template.

[Table 1-6](#) lists the Account Policies - Password Policy messages

Table 1-6 Account Policies - Password Policy messages

Message name	Title	Severity
ESM_GPO_POLICY_NOT_DEFINED_	Group Policy not defined	user-defined in template
ESM_GPO_POLICY_DEFINED	Group Policy defined	user-defined in template
ESM_GPO_INCORRECT_VALUE	Incorrect Group Policy value	user-defined in template

The template associated with this check is pre-populated and must be copied and renamed before it can be modified. You cannot add or delete rows in this template.

Account Policies - Account Lockout Policy (Windows 2000/2003)

This check reports a problem if there is a discrepancy between the Windows Group Policy settings and the settings that you defined in the ESM GPO Account Lockout Policy template.

The message severities for this check can be green, yellow, or red level severities based on how you define the severity in the corresponding template.

[Table 1-7](#) lists the Account Policies - Account Lockout Policy messages.

Table 1-7 Account Policies - Account Lockout Policy messages

Message name	Title	Severity
ESM_GPO_POLICY_NOT_DEFINED_	Group Policy not defined	user-defined in template
ESM_GPO_POLICY_DEFINED	Group Policy defined	user-defined in template
ESM_GPO_INCORRECT_VALUE	Incorrect Group Policy value	user-defined in template

The template associated with this check is pre-populated and must be copied and renamed before it can be modified. You cannot add or delete rows in this template.

Account Policies -Kerberos Policy (Windows 2000/ 2003)

This check reports a problem if there is a discrepancy between the Windows Group Policy settings and the settings that you defined in the ESM GPO Kerberos Policy template.

The message severities for this check can be green, yellow, or red level severities based on how you define the severity in the corresponding template.

[Table 1-8](#) lists the Account Policies - Kerberos Policy messages.

Table 1-8 Account Policies - Kerberos Policy messages

Message name	Title	Severity
ESM_GPO_POLICY_NOT_DEFINED_	Group Policy not defined	user-defined in template
ESM_GPO_POLICY_DEFINED	Group Policy defined	user-defined in template
ESM_GPO_INCORRECT_VALUE	Incorrect Group Policy value	user-defined in template

The template associated with this check is pre-populated and must be copied and renamed before it can be modified. You cannot add or delete rows in this template.

Local Policies - Audit Policy (Windows 2000/ 2003)

This check reports a problem if there is a discrepancy between the Windows Group Policy settings and the settings that you defined in the ESM GPO Audit Policy template.

The message severities for this check can be green, yellow, or red level severities based on how you define the severity in the corresponding template.

[Table 1-9](#) lists the Local Policies - Audit Policy messages.

Table 1-9 Local Policies - Audit Policy messages

Message name	Title	Severity
ESM_GPO_POLICY_NOT_DEFINED_	Group Policy not defined	user-defined in template
ESM_GPO_POLICY_DEFINED	Group Policy defined	user-defined in template

Table 1-9 Local Policies - Audit Policy messages

Message name	Title	Severity
ESM_GPO_INCORRECT_VALUE	Incorrect Group Policy value	user-defined in template

The template associated with this check is pre-populated and must be copied and renamed before it can be modified. You cannot add or delete rows in this template.

Local Policies - User Rights Assignment (Windows 2000/ 2003)

This check reports a problem if there is a discrepancy between the Windows Group Policy settings and the settings that you defined in the ESM GPO User Rights Assignment template.

The message severities for this check can be green, yellow, or red level severities based on how you define the severity in the corresponding template.

[Table 1-10](#) lists the Local Policies - User Rights Assignment messages.

Table 1-10 Local Policies - User Rights Assignment messages

Message name	Title	Severity
ESM_GPO_POLICY_NOT_DEFINED	Group Policy not defined	user-defined in template
ESM_GPO_POLICY_DEFINED	Group Policy defined	user-defined in template
ESM_GPO_INCORRECT_VALUE	Incorrect Group Policy value	user-defined in template

The template associated with this check is pre-populated and must be copied and renamed before it can be modified. You can add rows to the User /Group sublist in this template.

Local Policies - Security Options (Windows 2000/ 2003)

This check reports a problem if there is a discrepancy between the Windows Group Policy settings and the settings that you defined in the ESM GPO Security Options template.

The message severities for this check can be green, yellow, or red level severities based on how you define the severity in the corresponding template.

[Table 1-11](#) lists the Local Policies - Security Options messages.

Table 1-11 Local Policies - Security Options messages

Message name	Title	Severity
ESM_GPO_POLICY_NOT_DEFINED_	Group Policy not defined	user-defined in template
ESM_GPO_POLICY_DEFINED	Group Policy defined	user-defined in template
ESM_GPO_INCORRECT_VALUE	Incorrect Group Policy value	user-defined in template

The template associated with this check is pre-populated and must be copied and renamed before it can be modified. You cannot add or delete rows in this template but you can add rows to the sublist in this template.

Event Log (Windows 2000/ 2003)

This check reports a problem if there is a discrepancy between the Windows Group Policy settings and the settings that you defined in the ESM GPO Event Log template.

The message severities for this check can be green, yellow, or red level severities based on how you define the severity in the corresponding template.

[Table 1-12](#) lists the Event Log messages.

Table 1-12 Event Log messages

Message name	Title	Severity
ESM_GPO_POLICY_NOT_DEFINED_	Group Policy not defined	user-defined in template
ESM_GPO_POLICY_DEFINED	Group Policy defined	user-defined in template
ESM_GPO_INCORRECT_VALUE	Incorrect Group Policy value	user-defined in template

The template associated with this check is pre-populated and must be copied and renamed before it can be modified. You cannot add or delete rows in this template.

Restricted Groups (Windows 2000/ 2003)

This check reports a problem if there is a discrepancy between the Windows Group Policy settings and the settings that you defined in the ESM GPO Restricted Groups template.

The message severities for this check can be green, yellow, or red level severities based on how you define the severity in the corresponding template.

[Table 1-13](#) lists the Restricted Groups messages.

Table 1-13 Restricted Groups messages

Message name	Title	Severity
ESM_GPO_POLICY_NOT_DEFINED_	Group Policy not defined	user-defined in template
ESM_GPO_POLICY_DEFINED	Group Policy defined	user-defined in template
ESM_GPO_INCORRECT_VALUE	Incorrect Group Policy value	user-defined in template

The template associated with this check is not a pre-populated template. You can create a new template and add rows to the template and sublists.

System Services (Windows 2000/ 2003)

This check reports a problem if there is a discrepancy between the Windows Group Policy settings and the settings that you defined in the ESM GPO System Services template.

The message severities for this check can be green, yellow, or red level severities based on how you define the severity in the corresponding template.

[Table 1-14](#) lists the System Services messages.

Table 1-14 System Services messages

Message name	Title	Severity
ESM_GPO_POLICY_NOT_DEFINED_	Group Policy not defined	user-defined in template

Table 1-14 System Services messages

Message name	Title	Severity
ESM_GPO_POLICY_DEFINED	Group Policy defined	user-defined in template
ESM_GPO_INCORRECT_VALUE	Incorrect Group Policy value	user-defined in template

The template associated with this check is not a pre-populated template. You can create a new template and add rows to the template.

Note the Service Name and the Service Display Name in the System Services template. The Service Name is the actual service name or executable name in the service control panel properties. The Service Display Name is the display name in the service control panel. For example, the Display Name for the Bluetooth service is Bluetooth Service. However, the Service Name is btwdins. The Display Name is simply a description of the service, but the Service Name must match the actual service name in the control panel or the check will not work. When you create your template, you must include both the Service Name and the Service Display Name in the template or you will receive an error message.

To find the Services name

- 1 On the Windows taskbar, click **Start**.
- 2 Select **Settings**.
- 3 Click **Control Panel**.
- 4 Click **Administrative Tools**.
- 5 Click **Services**.
- 6 Right-click the service that you need in the Name column.
- 7 Click **Properties**. The correct service name is in the Service Name field of the Properties window.

Registry (Windows 2000/ 2003)

This check reports a problem if there is a discrepancy between the Windows Group Policy settings and the settings that you defined in the ESM GPO Registry template.

The message severities for this check can be green, yellow, or red level severities based on how you define the severity in the corresponding template.

[Table 1-15](#) lists the Registry messages.

Table 1-15 Registry messages

Message name	Title	Severity
ESM_GPO_POLICY_NOT_DEFINED_	Group Policy not defined	user-defined in template
ESM_GPO_POLICY_DEFINED	Group Policy defined	user-defined in template
ESM_GPO_INCORRECT_VALUE	Incorrect Group Policy value	user-defined in template

The template associated with this check is not a pre-populated template. You can create a new template and add rows to the template.

If extra settings are defined in your Windows Group Policy but are not defined in the template or if extra settings are defined in the template but are not defined in your Windows Group Policy, then the discrepancies regarding these extra defined items are reported.

File System (Windows 2000/ 2003)

This check reports a problem if there is a discrepancy between the Windows Group Policy settings and the settings that you defined in the ESM GPO File System template.

The message severities for this check can be green, yellow, or red level severities based on how you define the severity in the corresponding template.

[Table 1-16](#) lists the File System messages.

Table 1-16 File System messages

Message name	Title	Severity
ESM_GPO_POLICY_NOT_DEFINED_	Group Policy not defined	user-defined in template
ESM_GPO_POLICY_DEFINED	Group Policy defined	user-defined in template
ESM_GPO_INCORRECT_VALUE	Incorrect Group Policy value	user-defined in template

The template associated with this check is not a pre-populated template. You can create a new template and add rows to the template.

If extra settings are defined in your Windows Group Policy but are not defined in the template, or if extra settings are defined in the template but are not defined in your Windows Group Policy, then the discrepancies related to these extra defined items are reported.

Note: GPO_POLICY_NOT_DEFINED typically means that the policy information that is specified in the template is not found in the GPO INF file. However, it may also indicate inadvertent template modifications that have corrupted the template.

Login Parameters (Solaris)

SU 21 includes one enhancement to the Login Parameters module. All data that is returned from the syslog.conf file is checked for valid log files. If more than one non-existent log file is found in syslog.conf, only the last invalid file is reported.

Network Integrity (Windows)

SU 21 includes one enhancement to one check in the Network module. The Shared folders giving all users Full Control check lets you use the name list to include or exclude shared names of shared folders for this check. If a shared folder is on the include list, ESM will check it to be sure that it does not give full control to the Everyone security group.

Network Integrity (Solaris, AIX,)

SU 21 includes one new check and three new messages in the Network Integrity module.

Promiscuous mode

This check reports a problem if a network interface is in promiscuous mode. Promiscuous mode lets a sniffer run on a computer.

Table 1-17 lists the Promiscuous mode messages.

Table 1-17 Promiscuous mode messages

Message name	Title	Severity
STKU_PROMISC_OS_NOT_SUPPORTED	The OS is not supported for promiscuous mode detection	Yellow-3
STKU_PROMISC_ERROR	Promiscuous Mode Error	Red-4
STKU_PROMISC_DETECTED	Promiscuous Mode Detected	Red-4

Note: The Promiscuous mode check only works in 64-bit mode on AIX and Solaris 2.5.1 and later, with the exception of version 2.7. Therefore, you must install the tpk that supports large files and not the standard tpk.

Password Strength (HP-UX)

SU 21 includes one enhancement to one check in the Password Strength module. The Password length restrictions check for HP_UX versions 11.00 and higher lets you determine the minimum password settings in the security file. The minimum password length for new passwords is user-defined.

Password Strength (Solaris)

SU 21 includes one new message in the Password Strength module. This enhancement reports a problem if PAM is not configured to use the pam_unix_auth module. This enhancement ensures that all new Solaris 9 PAM functionality is configured so that ESM attempts to crack passwords. This enhancement enables ESM to crack Md5 and blowfish passwords in addition to traditional UNIX hashes.

Table 1-18 lists the new message for this module.

Table 1-18 Password Strength message

Message name	Severity
STKU_UNKNOWN_PAM_MODULE	Yellow-1

The following checks/options are those affected by the enhancement:

- password=username

- password=any username
- password within GECOS field
- password=wordlist word
- reverse order
- double occurrences
- plural forms
- uppercase
- lowercase
- add prefix
- add suffix

Password Strength (Windows 2000/ 2003)

SU 21 includes one new message to the Passwords stored using reversible encryption check in the Password Strength module.

Passwords stored using reversible encryption (Windows 2000/ 2003)

This check reports a problem if the domain policy on a domain controller is set to “Store passwords using reversible encryption – enabled.” Enable this check to report domain accounts that have passwords that are stored with reversible encryption.

[Table 1-19](#) lists the Passwords stored using reversible encryption message.

Table 1-19 Passwords stored using reversible encryption message

Message name	Title	Severity
ESM_REVERSIBLE_ENCRYPTION	Password stored using reversible encryption	Yellow-3

Startup Files (Windows 2000/ NT/ XP/ 2003)

SU 21 includes two new checks and one new template in the Startup module.

Disallow services cont. (Windows 2000/ NT/ XP/ 2003)

This check reports a problem if the services that you have enabled in the new template are disallowed and installed. There are two columns in the new template. The first column contains the check box that enables or disables the

service and the second column contains the service name. Only services that are enabled are checked.

Filter disallow services not running (Windows 2000/ NT/ XP/ 2003)

This check filters the disallow services. The check filters from the namelist and the new template. When the filter is enabled, it will report services that are disallowed and running. When the filter is disabled, it will report services that are disallowed and not running. This check only applies if the Disallow services checks are enabled.

Symantec Product Information (Windows 2000/ NT/ XP)

SU 21 includes one new option and four new messages in the Symantec Product Information module.

Either SAVCE or NAV (Windows 2000/ NT/ XP)

Enable this option if your security policy allows either Norton AntiVirus or Symantec AntiVirus Corporate Edition to be installed on your systems. This option is used in combination with the checks for Norton AntiVirus and Symantec AntiVirus Corporate Edition to report systems that are not in compliance with the configured check settings. If this option is enabled, checks enabled under Norton AntiVirus should also be enabled under Symantec AntiVirus Corporate Edition for proper reporting of system compliance.

[Table 1-20](#) lists the Either Symantec AntiVirus Corporate Edition or Norton AntiVirus messages.

Table 1-20 Either Symantec AntiVirus Corporate Edition or Norton AntiVirus

Message name	Title	Severity
ESM_AV_AND_AVCE_VERSION_VIOLATION	Installed SAVCE and/or NAV version outdated	Red-4
ESM_AV_NOR_AVCE_NOT_INSTALLED	Either SAVCE or NAV not installed	Red-4
ESM_AV_AND_AVCE_LU_VIOLATION	Installed SAVCE and/or NAV LiveUpdate overdue	Yellow-3
ESM_AV_AND_AVCE_LASTSCAN_VIOLATION	Installed SAVCE and/or NAV scan overdue	Yellow-3

For example, this option lets you select all checks for the module without reporting that, for example Norton AntiVirus, is not installed, as long as Symantec AntiVirus is installed and configured correctly. Enabling this option prevents the module from reporting a message for the AntiVirus version that is not installed, if a valid version is installed.

Symantec Product Information (Windows)

SU 21 includes one new check and one new message in the Symantec Product Information module.

File System Auto-Protected (Windows)

This check reports a problem if Auto-Protect for Symantec AntiVirus Corporate Edition is not enabled.

[Table 1-21](#) lists the File System Auto-Protected message.

Table 1-21 File System Auto-Protected message

Message name	Title	Severity
AVCE_AP_VIOLATION	Symantec AntiVirus Corporate Edition Auto_Protect not enabled	Red-4

[Table 1-22](#) lists the File System Auto-Protected unexpected system error messages for the SymSentry Collector.

Table 1-22 SymSentry Collector system error messages

Message name	Title	Severity
SYSERR	Unable to find SymSentry	Red-4
SYSERR	Unable to register SymSentry	Red-4

System Mail (UNIX)

SU 21 includes one new check and three new messages in the System Mail module.

Sendmail Restricted Shell

This check reports a problem if the smrsh is not configured in the sendmail.cf file or if disallowed programs are in the /usr/adm/sm.bin directory.

[Table 1-23](#) lists the Sendmail Restricted Shell messages.

Table 1-23 Sendmail Restricted Shell messages

Message name	Title	Severity
STKU_SMRSH_NOT_USED	Smrsh not used in sendmail configuration	Red-4
STKU_SMRSH_FILE_FORBIDDEN	Forbidden file insmrsh executables directory	Red-4
STKU_SMRSH_DIR_NOT_FOUND	Sendmail restricted directory was not found	Red-4

System Mail (UNIX)

SU 21 includes one new check in the System Mail module.

FX/path directives (UNIX)

This check reports a problem if there are files that are not owned by root or files that allow group or world access. This check examines the files listed for the FX/path directives in the sendmail.cf configuration file.

[Table 1-24](#) lists the FX/path directives message.

Table 1-24 FX/path directives message

Message name	Title	Severity
STKU_FXPATH	Invalid owner/permissions for FX/Path directive	Yellow-2

Known issues

The following are known issues for SU 21:

- All Modules (NetWare) Running eDir does not specify Symantec ESM 6.0, it only provides the Security Update number.
- Account Information (NetWare) You may receive an unexpected system error if you incorrectly add a volume to Directory Trustees Cont'd.
- System Audit (NetWare) The System Audit module is not supported on NetWare 6.x.
- Object Integrity (NetWare) The Stealth Objects check fails on any NetWare host running eDir 8.x. Do not run the Stealth Objects check on any NetWare host running Novell supported versions of eDir.

Object Integrity (NetWare)	The ESM object's access to agent's context check fails on any NetWare host running eDir. Do not run this check on any NetWare host running Novell supported versions of eDir.
Object Integrity (NetWare)	The Missing object property list check reports that the list is empty when it is populated.
Password Strength (NetWare)	All password cracking checks fail on any NetWare host running Novell supported versions of eDir. Do not run password cracking checks on NetWare hosts running Novell supported versions of eDir.
Password Strength (NetWare)	The word list check templates do not appear the first time the policy properties are edited. Save, close, and reopen the policy after modifying it.
OS Patches (NetWare)	The Patch templates appear only the first time that the policy is edited.
Startup Files (NetWare)	The Console Parameters templates list appears only the first time that the policy is edited.
Startup Files (NetWare)	An incomplete list of loaded modules may be reported when you run a server check.
Password Strength (NetWare)	Some checks may not report incompliant user(s) or object(s). Use a non-supported version of NetWare and/ or eDir.
Password Strength (NetWare)	In the Users can change password check, subordinate objects and containers may get excluded and therefore not checked. Suppress the parent objects instead of excluding them.
File Attributes (NetWare)	You may receive an unexpected error message when you try to add any file(s) or folder(s), that reside on the dos partition, to the template.
All Modules (NetWare)	A 6.00 agent will not register to a 6.0 or 5.5 manager. Modify the agent version file in the setup directory to version 6.0.
All Modules (NetWare)	When you run esmsetup.nlm, NetWare may load spxs and ipxs nlms on NetWare computers when ipx is disabled.
All Modules (NetWare)	The NetWare installation does not register the Security Update version information.
Account Integrity (NetWare)	No checks are enabled by default.
OS Patches (NetWare)	No template exists for the module.
Network Integrity (NetWare)	No checks are enabled by default.

Startup Files (NetWare)	You may receive an unexpected system error that incorrectly states that the HOSTMIB and NWTRAP files do not exist.
Startup Files (NetWare)	The Console Parameters template does not allow 6.x agent(s) when using the Add Parameters button. Use the Add Row button and manually enter information into each field.
File Find (Solaris)	<p>On the Solaris standard TPK, the Unprintable Characters in Filenames check finds only the unprintable ASCII characters 1-31. It does not find the ASCII characters 127-255, if the locale is set to the default C locale.</p> <p>To find the expanded unprintable characters on Solaris, you must set your locale instead of using the default C locale or use the Extended Support TPK (built on Solaris 2.7).</p>

Resolved issues

The following issues have been resolved for SU 21:

All Modules (All Operating Systems)	Regular expression pattern matching and wildcard characters are supported in the namelist.
Active Directory (Windows)	The check message description Security Group without applied GPO's has been changed to Computer without applied GPO's.
Startup File (UNIX)	There was a buffer overflow that caused a Startup killed on signal 11 message. This has been resolved.
Console error (Windows)	The Policy file names have been updated to use the new template names after LiveUpdate runs.
File Watch (Windows)	A double-byte character in a directory name was causing a Dr. Watson message. This has been resolved.
File Find (UNIX)	The world-writable check no longer checks symbolic links in the file systems as defined in the name list.
Registry (Windows)	An Optional field was added to the Windows 2003 Registry template.
Symantec Product Info (Windows)	Symantec Product Information module checks both Norton AntiVirus and Symantec AntiVirus Standard and Corporate editions. You can use the Symantec Product Information module to check version, frequency of liveupdates, and scans, instead of using the registry.

Password Strength (Windows)	Error messages regarding residual SIDs have been improved to provide more information at the point where the API problem occurs.
File Watch (Windows)	The FileWatch module no longer fails with an Unexpected system error message due to an autosnapshotupdate function.
Startup Files (Windows)	Disallowed Services correctly checks Windows 2003 agents.
File Watch (Windows)	The File Watch module consistently reports New Files for Windows 2000 agents.
File Attributes (UNIX)	The File Attributes module does not report a disabled setuid/setgid bit if the Exclude Decreased Permissions option is enabled.
File Information (Netware)	Two subdirectories have been added to the include list and the information files. When the Walk Directories check is enabled no subordinate directory or files are identified.
File Attributes (Netware)	The Owner column in the File Attributes template is populated using the typeful method so that the policy does not report a change in owner.
Network Integrity (Linux)	The Linux Network Integrity module only checks the /var/lib/nfs/etab file. It does not check the /etc/xtab, /etc/dfs/sharetab, or /etc/exports files.
All Modules All Operating Systems	The event log message IDs have been merged into the regular message IDs.

System requirements

[Table 1-25](#) lists the supported operating systems for SU 21.

Table 1-25 SU 21 supported operating systems

Agent operating system	Versions
AIX	4.2.1, 4.33, 5.1, 5.2
HP-UX	10.20, 11, 11.11, 11.23
NetWare	4.22, 5.1, 6.0, 6.5
Red Hat Linux	7.x, 8, 9
Red Hat Linux Enterprise Server (ES) (x86)	2.1, 3.0
Solaris	2.5.1, 2.6, 2.7, 2.8, 2.9
SUSE LINUX Standard Server	8
SUSE LINUX Enterprise Server	8
Windows 2000 Professional and Server (Intel)	All
Windows NT Workstation and Server (Intel)	4.0 SP6a
Windows Server 2003	All
Windows Server 2003 (Itanium®)	All
Windows XP Professional (Intel)	All

SU 21 may run on newer versions of the supported operating systems, but Symantec reserves the right to certify the security update on the new versions before officially supporting them.

The LiveUpdate installation of SU 21 on all supported operating systems requires approximately 560 MB on each Symantec ESM manager.

The amount of disk space required by each agent depends on its operating system.

[Table 1-26](#) lists the agent disk space requirements.

Table 1-26 SU 21 agent disk space requirements

Agent operating system	SU 21
AIX	92 MB
HP-UX	72 MB

Table 1-26 SU 21 agent disk space requirements

Agent operating system	SU 21
Netware	135 MB
Red Hat Linux	36 MB
Red Hat Linux Enterprise Server (ES) (x86)	36 MB
Solaris	58 MB
SUSE LINUX Standard Server 8	36 MB
SUSE LINUX Enterprise Server 8	36 MB
Windows 2000 Professional and Server (Intel)	31 MB
Windows NT Workstation and Server (Intel)	31 MB
Windows Server 2003	31 MB
Windows Server 2003 (Itanium®)	104 MB
Windows XP Professional (Intel)	31 MB

Security Update 20

The following are new in SU 20:

- One new module
- Seventeen new checks
- Five new options
- Sixty new messages
- Sixteen new templates and 7 enhanced templates

Active Directory Services (Windows)

SU 20 includes one new check.

Security Options

This check reports a problem if a Windows security setting is not set to the value that is specified in the Security Options template. The Windows security settings that the Security Options check examines are listed in the Administrative tools>Local Security Policy>Local Policies>Security Options folder.

Security Options templates come preconfigured according to security best practice standards and do not need to be modified. However, you can determine the security option checks that Symantec ESM examines by enabling or disabling the check in the template.

SU 20 includes four Security Options templates:

- Security Options - Windows 2000 Professional (secopts.o2p)
- Security Options - Windows 2000 Server (secopts.o2s)
- Security Options - Windows 2003 (secopts.o3s)
- Security Options - Windows XP (secopts.oxp)

The template list in the ESM Console displays the appropriate template for the computer on which the module is installed. You must enable a Security Options template to use the Security Options check.

Do not edit the default Security Options templates. Any changes that you make will be overwritten by the next Security Update. To avoid this problem, you can make a copy of the appropriate template and edit the copy to your requirements. Security updates will not replace or override templates that you create.

[Table 1-27](#) lists the messages for the Security Options check.

Table 1-27 Security Options check messages

Message name	Title	Severity
ESM_SECURITY_OPTION_VIOLATION_G	Security Option setting violates policy	Green
ESM_SECURITY_OPTION_VIOLATION_Y	Security Option setting violates policy	Yellow
ESM_SECURITY_OPTION_VIOLATION_R	Security Option setting violates policy	Red
ESM_SEC_OPT_TEMPLATE_MISSING	No Security Option template files were specified	Red

Enabling a security options template

You must enable a security options template to use the security options check.

To enable the template

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the Active Directory module that you want to edit.

- 3 Double-click **Active Directory**.
- 4 Click **Security options**.
- 5 In the Security options dialog box, select the template.
- 6 Click the **Left Arrow** to move the template to the Enabled Template Files list.
- 7 Click **Ok**.

File Attributes (SUSE ES 8)

SU 20 includes new SUSE Enterprise Server 8 templates for the File Attributes module.

SUSE ES 8 Templates

The new templates for SUSE ES 8 include:

- fileatt.sl
- internet.sl
- mail.sl
- nfs.sl
- objects.sl
- queues.sl
- uucp.sl

In the Template Sublist Editor, the SUSE Enterprise Server 8 templates are listed as SuSE-x86 in the OS field. You can use ES in the Rev/OS field to indicate that it is an Enterprise Server. For example, 8ES indicates Enterprise Server, version 8.

File Attributes (UNIX)

SU 20 includes one new check.

NFS exported files

This check reports if the files that are listed in the File Attributes templates are exported over insecure versions of NFS. NFS versions 3 and under are considered insecure.

A message is reported when the files that are listed in the templates are exported.

[Table 1-28](#) lists the NFS files exported message.

Table 1-28 NFS files exported message

Message name	Title	Severity
STKU_NFS_EXPORTED	NFS Exported	Yellow-1

Specifying files to check

In the Files Attributes templates, you can indicate the files that this check examines by checking the NFS Exported check box. If a file in the template does not have NFS Exported checked, the check will not report on that file.

To specify the files that the check examines

- 1 In the enterprise tree, expand the manager that contains the template that you want to edit.
- 2 Expand **Templates**.
- 3 Double-click the File Attributes template that you want to edit.
- 4 In the file row, check **Prohibit NFS**.
- 5 Click **Ok**.

File Attributes (Windows)

SU 20 includes one new check and one new option.

File Version

This check reports the file version information of files that are listed in the File Attributes templates.

[Table 1-29](#) lists the new messages for this check.

Table 1-29 File Attributes check messages

Message name	Title	Severity
ESMT_FILE_VERSION	File version information	Green - 0
ESMT_NO_FILE_VERSION	No file version information	Green - 0

Event Log Info

You can use this option to get file access information from the Windows Event Logs when the File Attributes module finds a problem. This option works by

querying the event log for relevant events that have occurred since the last snapshot.

If a check does not use a snapshot, you can specify the number of days to search the Event log.

Table 1-4 lists the message for this option.

Table 1-30 Event Log Info option messages

Message name	Title	Severity
ESM_EVENTLOG_INFO	Event Log Information	Yellow

Enabling the Event Log Info option

You must enable the Event Log Info option to display event log information when the File Attributes module reports a problem.

To enable the Event Log Info option

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the File Attributes module that you want to edit.
- 3 Double-click **File Attributes**
- 4 Expand the **File Attributes** tree.
- 5 Expand the operating system branch.
- 6 Click **Event Log Info**.
- 7 Do one of the following:
 - If the check uses snapshots, leave this box empty.
 - If the check does not use snapshots, In the Edit box, type the number of days back to search the event log.
- 8 Click **OK**.

File Find (Windows 2000/ 2003/ XP)

SU 20 includes a new File Find module for Windows computers. The File Find module reports files for contents that contain prohibited text strings or files that are missing required test strings. This new module contains one check, one option, and two new template files.

Windows file content search

This check reports files with contents that match text or text patterns that are defined in the Windows file content search templates (.wfs).

FileFind keywords

You can use this option to enable or disable the FileFind Keywords templates that the File Find module uses to locate the file. You must enable this template to use keywords in the File Content Search templates.

[Table 1-31](#) lists the new messages for the Windows File Find module checks.

Table 1-31 Messages for Windows File Find checks

Message name	Title	Severity
FCS_GREEN	Green level content search matched	Green - 0
FCS_YELLOW	Yellow level content search matched	Yellow - 1
FCS_RED	Red level content search matched	Red - 4
INVALID_FCS_ENTRY	No block specified for 2nd pattern	Yellow - 3
INVALID_FCS_REGEX	Invalid regex syntax	Yellow - 3

Creating the Windows file content search template

You must create and enable a new Windows file content search template before you run the Windows file content search check.

To create a Windows file content search template

- 1 In the tree view, right-click **Templates**, then click **New**.
- 2 In the Create New Template dialog box, select **Windows 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 .wfc extension to the file name.
- 4 Click **OK**.
- 5 In the Template Editor, click **Add Row**.
- 6 Add one or more OS/Rev sublist rows. See [“To add a row to the OS/Rev sublist”](#) on page 45.
- 7 In the Description box, 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.

- 8 In the new row, click the Severity list, and then select **Green**, **Yellow**, or **Red**. This defines the security level that the module uses to report matches for specified text or text patterns.
- 9 Click the Report if list, 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.

- 10 Add one or more File List sublist rows to define search criteria for each record that you create in the Windows file content search template. See [“Editing the File List sublist”](#) on page 46.
- 11 Click **Save** to save changes to the Windows file content search template.
- 12 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 list.
- 2 In the Template Sublist Editor, click **Add Row**.
- 3 In the Exclude box, select the check box to exclude the specified operating system and revision from checks in the template or uncheck it to include the operating system and revision.
- 4 Click the OS list, 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 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
 - red hat-x86
 - red hat-s390
 - nt-ix86
- 5 Click **Apply**.
To add another row, repeat steps 2–6.
 - 6 Click **Close**.

Note: In the OS/Rev Sublist Editor, the Revision box does not apply to the Windows operating systems.

To delete rows from the Windows file content search template

- 1 Click on the left most, 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 in the Windows file content search template 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 that you want to search
- 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 box, replace **<NEW>** with a number that specifies the sequence in which sublist rows will be considered by the Windows 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 50.

- 4 In the Path box, type the absolute path name of the directory where the Windows 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 box.

Leave the Path box 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 list, then select one of the following:

Depth option	Searches
All - Dir + all sub-dirs	The directory that is specified in the Path box and all of its subdirectories.
1 - Dir Only	Only the directory that is specified in the Path box and none of its subdirectories.
0 - Item Only	Only files with names that exactly match the value in the File Name box. 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 50.

- 6 In the File Name box, 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 box.

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 52 for commonly-used syntax.

The file name is ignored when the path is blank. See [“Using multiple File List sublist entries”](#) on page 50.

- 7 In the Option list, 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 box, 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 52 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 list, 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 box. 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 box.	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

Opt	Description	Valid values
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
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 box, use regular expressions or numeric expressions to specify the text or text pattern that the Windows 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 box on the same sublist line.

The specified pattern is treated as a regular expression for string comparisons. If the specified pattern begins with a numeric expression, it will use the corresponding numeric comparisons (equal to, less than, greater than, not equal, less than or equal to, greater than or equal to).

Note: The Windows file content search check looks for text defined in the 2nd Pattern box only when it matches the text that is defined in the Pattern box. If it does not find the first pattern, it will not 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.

- 2 Click **Remove Rows**.
- 3 Click **Close** to exit the Template Sublist Editor and return to the Windows 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 boxes 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 box.
- To search for multiple text patterns that occur in a specific order in the same file, define values for the Path and File Name boxes in the first record, and leave these fields blank in subsequent records. Type text patterns in the Pattern boxes of both the first and subsequent records. Use the Order box to number the records to match the order that specified text patterns should occur in the file. Then specify N=1 in the Delimiter box 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 box 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 boxes 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 Windows file Content Search template defines the search criteria for services, registry keys, or files. The Conditions sublist has two columns: one lets you specify whether the sublist entry is a service, registry key, or file, and the other lets you specify the name of the service, registry key, 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 list, then select one of the following:

Key	Value	Explanation
S	service	Verify that the service is running
s	No service	Verify that the service is not running
I	Installed	Verify that the service is installed
i	Not installed	Verify that the service is not installed
R	Registry	Verify that the registry key exists
r	No registry	Verify that the registry key does not exist
V	Registry value	Verify that the registry value exists and satisfies the equation
v	No registry value	Verify that the registry value does not exist
F	File	Verify that the file exists
f	No file	Verify that the file does not exist.

- 4 In the Name box, type the name of the service, registry key, or file. The File content search check searches for running services, registry keys, 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 Windows file content search template.

Using regular expressions

The Windows file content search check applies regex C library functions, which support POSIX 1003.2 regular expressions.

[Table 1-32](#) lists the regular expressions syntax.

Table 1-32 Regular expression syntax

Pattern	Description
.	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

Table 1-32 Regular expression syntax

Pattern	Description
[<char1>-<char2>...]	A range that matches any character in the range of ASCII characters from char1 to char2
(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

Creating the FileFind keywords template

You must create and enable a new FileFind keywords template before you run the Windows file content search check.

To create a FileFind keywords template

- 1 In the tree view, right-click **Templates**, then click **New**.
- 2 In the Create New Template dialog box, select **FileFind Keywords - all**.
- 3 Type a new template file name of no more than eight characters, without a file extension. Symantec ESM adds the .ffk extension to the file name.
- 4 Click **OK**.
- 5 In the Template Editor, click **Add Row**.
- 6 In the new row, in the Keyword box, type keyword that you want to use to represent the registry key value or directory name.
Keywords begin and end with percentage characters. For example, %KeywordName%
- 7 In the Keyword value box, do one of the following:
 - If the keyword is associated with a directory, type the directory's full path.
 - If the keyword is associated with a registry key value, type the value's full path.
- 8 In the Keyword type list, select one of the following values:
 - Registry

- Directory
- 9 Click **Save**.
 - 10 Click **Close**.

File Watch (All)

SU 20 includes enhanced File Watch templates. The enhanced templates contain a new severity column that you can use to specify the severity level of File Watch messages on a file or directory basis.

Assigning a severity level

You can assign a severity level to files or directories listed in the File Watch template. If the File Watch module detects changes to the file or directory, it reports with a security message of the severity level assigned in the template.

To assign a severity level to a file or directory

- 1 In the Template Editor, click the Severity list in the template row that contains the sublist.
- 2 In the list, select the severity.
- 3 Click **Save**.
- 4 Click **Close**.

SU 20 also includes all new messages for the File Watch module.

[Table 1-33](#) lists the new messages for File Watch checks on UNIX.

Table 1-33 New messages for File Watch checks on UNIX

Message name	Title	severity
NEW_GREEN	New directory or file (Green level)	Green - 0
NEW_YELLOW	New directory or file (Yellow level)	Yellow - 2
NEW_RED	New directory or file (Red level)	Red - 4
REMOVED_GREEN	Directory or file removed (Green level)	Green - 0
REMOVED_YELLOW	Directory or file removed (Yellow level)	Yellow - 2
REMOVED_RED	Directory or file removed (Red level)	Red - 4
MODIFIED_GREEN	File modified (Green level)	Green - 0
MODIFIED_YELLOW	File modified (Yellow level)	Yellow - 2
MODIFIED_RED	File modified (Red level)	Red - 4

Table 1-33 New messages for File Watch checks on UNIX

Message name	Title	severity
DIFF_OWN_GREEN	File ownership modified (Green level)	Green - 0
DIFF_OWN_YELLOW	File ownership modified (Yellow level)	Yellow - 2
DIFF_OWN_RED	File ownership modified (Red level)	Red - 4
DIFF_PERM_GREEN	Directory or file permissions changed (Green level)	Green - 0
DIFF_PERM_YELLOW	Directory or file permissions changed (Yellow level)	Yellow - 2
DIFF_PERM_RED	Directory or file permissions changed (Red level)	Red - 4
EXP_PERM_GREEN	Directory or file permissions expanded (Green level)	Green - 0
EXP_PERM_YELLOW	Directory or file permission expanded (Yellow level)	Yellow - 2
EXP_PERM_RED	Directory or file permissions expanded (Red level)	Red - 4

[Table 1-34](#) lists the new messages for File Watch checks on Windows.

Table 1-34 New File Watch messages for Windows platforms

Message name	Title	Severity
NEW_GREEN	New file or folder (Green level)	Green - 0
NEW_YELLOW	New file or folder (Yellow level)	Yellow - 2
NEW_RED	New file or folder (Red level)	Red - 4
REMOVED_GREEN	File or folder removed (Green level)	Green - 0
REMOVED_YELLOW	File or folder removed (Yellow level)	Yellow - 2
REMOVED_RED	File or folder removed (Red level)	Red - 4
MODIFIED_GREEN	File modified (Green level)	Green - 0
MODIFIED_YELLOW	File modified (Yellow level)	Yellow - 2
MODIFIED_RED	File modified (Red level)	Red - 4
DIFF_OWN_GREEN	File ownership modified (Green level)	Green - 0
DIFF_OWN_YELLOW)	File ownership modified (Yellow level)	Yellow - 2
DIFF_OWN_RED	File ownership modified (Red level)	Red - 4

File Watch (Windows)

Event Log Info

You can use this option to get file access information from the Windows Event Logs when the File Watch module finds a problem. This option works by querying the event log for relevant events that have occurred since the last snapshot.

Table 1-4 lists the message for this option.

Table 1-35 Event Log Info option messages

Message name	Title	Severity
ESM_EVENTLOG_INFO	Event Log Information	Yellow

Enabling the Event Log Info option

You must enable the Event Log Info option to display event log information when the File Watch module reports a problem.

To enable the Event Log Info option

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the File Watch module that you want to edit.
- 3 Double-click **File Watch**
- 4 Expand the **File Watch** tree.
- 5 Expand the operating system branch that contains the File Watch module that you want to edit.
- 6 Click **Event Log Info**.
- 7 Check **Check Enabled**.
- 8 Click **OK**.

File Watch (Linux)

SU 20 includes one new check.

Filter changed device ownership/permissions

This check filters out the file-ownership changed and file-permission changed messages for device files that change when users log on through the physical console. It is disabled by default.

Adding a permissions file

The Filter changed device ownership/permissions check requires that you add the file that lists the users with permission to physically access the console to the Console.perms file box in File Watch template sublist editor.

To add a permissions file to the sublist editor

- 1 In the Template Editor, click the OS/Rev list in the template row that contains the sublist.
- 2 In the Template Sublist Editor, in the Console.perms file box, type the name of the permissions file.
- 3 Click **Apply**.
- 4 Click **Close**.
- 5 Click **Save**.
- 6 Click **Close**.

[Table 1-36](#) lists the OS default permissions files.

Table 1-36 Linux default permissions files

OS	File
Red Hat	/etc/security/console.perms
SUSE	/etc/logindevperm

Login Parameters (Windows)

SU 20 includes one new check.

Inactive accounts with unchanged passwords

This check reports inactive user accounts that have unchanged passwords. You can use the name list to exclude user accounts from the check. You can also specify the number of days that accounts are inactive before the check will occur.

Table 1-37 lists the message for this check.

Table 1-37 Inactive accounts with unchanged passwords message

Message name	Title	Severity
ESM_LASTLOG_PSWDCCHANGE	Inactive account with unchanged passwords	Yellow - 1

Excluding users or groups from the check

You can exclude users or groups from the Inactive accounts with unchanged passwords check.

To exclude users or groups from the check

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the Login Parameters module that you want to edit.
- 3 Double-click **Login Parameters**.
- 4 Expand the **Login Parameters** tree.
- 5 Expand **Windows**.
- 6 Click **Inactive accounts with unchanged passwords**.
- 7 In the Inactive days/Password age box, type the number of days and password age that must be reached before the check reports.
- 8 Do one or more of the following:
 - On the Users tool bar, click **New**, and then type the name of the user in the Users list.
 - On the Groups tool bar, click **New**, and then type the name of the group in the Groups list.
- 9 Click **OK**.

Login Parameters (UNIX)

SU 20 includes three new checks.

Inactive accounts with unchanged passwords

This check reports inactive user accounts that have expired passwords. You can use the name list to exclude user accounts from the check. You can also specify the number of days that accounts are inactive before the check reports.

[Table 1-38](#) lists the message for this check.

Table 1-38 Inactive accounts with unchanged passwords message

Message name	Title	Severity
STKU_INACTIVE_EXPIRED	Inactive account with unchanged password	Red - 4

Excluding users or groups from the check

You can exclude users or groups from the check.

Excluding users or groups

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the Login Parameters module that you want to edit.
- 3 Double-click **Login Parameters**.
- 4 Expand the **Login Parameters** tree.
- 5 Expand **UNIX**.
- 6 Click **Inactive accounts with unchanged passwords**.
- 7 In the Inactive days/Password age box, type the number of days and password age that must be reached before the check reports.
- 8 Do one or more of the following:
 - On the Users tool bar, click **New**, and then type the name of the user in the Users list.
 - On the Groups tool bar, click **New**, and then type the name of the group in the Groups list.
- 9 Click **OK**.

Excessive failed su attempts for users

This check reports user accounts that have exceeded the allowed number of failed su attempts.

[Table 1-39](#) lists the message for this check.

Table 1-39 Excessive failed su attempts for users message

Message name	Title	Severity
FAILED_SU_EXCEED_LIMITS	Failed SU attempts exceed limits	Red - 4

Including or excluding users for the Excessive failed su attempts check

The Excessive failed su attempts check provides a name list that you can use to include substitute users in the check or exclude them from the check. Substitute users are users who use the su command to login as another user. For example, user Ted uses su root to login as root. Ted is the initiated user, while root is the substitute user.

Initiated users must be included or excluded from checks in the Global name list, which is associated with the Users to check option. However, substituted users can be included or excluded from only the Excessive failed su attempts check by using the specific name list for that check.

To exclude users from the check

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the Login Parameters module that you want to edit.
- 3 Double-click **Login Parameters**.
- 4 Expand the **Login Parameters** tree.
- 5 Expand **UNIX**.
- 6 Click **Excessive failed su attempts for users**.
- 7 In the Failed su attempts/period box, type the number of attempts per time period that must occur before the check reports.
- 8 On the Users to check toolbar, click **New**.
- 9 In the Users to check list, type the name of the user.
- 10 Do one of the following:
 - Click **Exclude** to exclude the listed substitute users from the check.
 - Click **Include** to include listed substitute users in the check.
- 11 Click **OK**.

Excessive successful su attempts for users

This check reports users that have exceeded the allowed number of successful su attempts.

Table 1-40 lists the message for this check.

Table 1-40 Excessive successful su attempts for user message

Message name	Title	Severity
SUCCESS_SU_EXCEED_LIMITS	Successful SU attempts exceed limits	Red - 4

Including or excluding users for the Excessive successful su attempts check

The Excessive successful su attempts check provides a name list that you can use to include substitute users in the check or exclude them from the check. Substitute users are users who use the su command to login as another user. For example, user Ted uses su root to login as root. Ted is the initiated user, while root is the substitute user.

Initiated users must be included or excluded from checks in the Global name list, which is associated with the Users to check option. However, substituted users can be included or excluded from only the Excessive successful su attempts check by using the specific name list for that check.

To exclude users from the check

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the Login Parameters module that you want to edit.
- 3 Double-click **Login Parameters**.
- 4 Expand the **Login Parameters** tree.
- 5 Expand **UNIX**.
- 6 Click **Excessive successful su attempts for users**.
- 7 In the Successful su attempts/period box, type the number of attempts per time period that must occur before the check reports.
- 8 On the Users to check toolbar, click **New**.
- 9 In the Users to check list, type the name of the user.
- 10 Do one of the following:
 - Click **Exclude** to exclude the listed substitute users from the check.
 - Click **Include** to include listed substitute users in the check.
- 11 Click **OK**.

Network Integrity (Windows 2003/XP)

SU 20 includes four new checks and one new template.

IPv6 Protocol

You can use this check to specify whether IPv6 protocol is required or forbidden on the computer. If the IPv6 protocol is required but is not present on the computer, the check generates an error message. Likewise, if the protocol is forbidden, but present on the computer, the check generates an error message.

Enabling IPv6 protocol on a computer can introduce the following security risks:

- Some firewalls are ineffective for IPv6 traffic. You must install a firewall that is IPv6 enabled.
- Attackers can use the autoconfiguration feature to announce rogue routers.
- Standardizing transition methods, such as 6to4, Simple Internet Transition (SIT), or IPv6 over UDP can let IPv6 traffic into the network undetected.
- IPv6 uses static keying and does not update keys when sequence numbers are reused.
- The Internet Key Exchange (IKE) in the IPv6 version of IPSec is not supported for negotiating security associations.
- The IPSec implementation that comes with the IPv6 included in Windows 2003 and Windows XP does not provide data confidentiality because it does not support ESP data encryption.

Table 1-41 lists the message for the IPv6 Protocol check.

Table 1-41 IPv6 Protocol check message

Message name	Title	Severity
ESM_IPV6_VIOLATION	IPv6 Protocol	Yellow

Specifying the IPv6 protocol requirement

You can specify whether IPv6 protocol is required or forbidden on the computers that are examined by the Network Integrity check.

To specify the IPv6 Protocol requirement

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the Network Integrity module that you want to edit.
- 3 Double-click **Network Integrity**.

- 4 Click **IPv6**.
- 5 In the Network Integrity dialog box, do one of the following:
 - To specify that IPv6 protocol is required to be enabled on the computer, select **IPv6**, and then click the **Left Arrow** to move it to the Enabled list.
 - To specify that IPv6 protocol must not be enabled on the computer, leave IPv6 protocol in the Disabled list.
- 6 Click **Ok**.

Internet Connection Firewall

You can use this check to specify whether the Internet Connection Firewall is required or forbidden on the computer. If the Basic Firewall key is enabled, the firewall is required. If the Basic Firewall key is disabled, the firewall is forbidden. The check reports if the policy is violated.

[Table 1-42](#) lists the message for this check.

Table 1-42 Internet Connection Firewall check message

Message name	Title	Severity
ESM_ICF_VIOLATION	Internet Connection Firewall policy violation	Yellow

Specifying the Internet Connection Firewall requirement

You can specify whether the Internet Connection Firewall is required or forbidden on the computers that are examined by the Network Integrity check.

To specify the Internet Connection Firewall requirement

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the Network Integrity module that you want to edit.
- 3 Double-click **Network Integrity**.
- 4 Click **Internet Connections Firewall**.
- 5 In the Network Integrity dialog box, do one of the following:
 - To specify that the Internet Connection Firewall is required to be enabled on the computer, select **Basic Firewall**, and then click the **Left Arrow** to move it to the Enabled list.
 - To specify that Internet Connection Firewall must not be enabled on the computer, leave **Basic Firewall** in the Disabled list.
- 6 Click **Ok**.

Internet Connection Sharing

You can use this check to specify whether the Internet Connection Sharing service is required or forbidden on the computer. If the Sharing key is enabled, the Internet Connection Sharing service is required. If the Sharing key is disabled, the service is forbidden. The check reports if the policy is violated.

[Table 1-43](#) lists the message for this check.

Table 1-43 Internet Connection Sharing check message

Message name	Title	Severity
ESM_ICS_VIOLATION	Internet Connection Sharing policy violation	Yellow

Specifying the Internet Connection Sharing requirement

You can specify whether the Internet Connection Sharing service is required or forbidden on the computers that are examined by the Network Integrity check. The default is forbidden.

To specify the Internet Connection Sharing requirement

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the Network Integrity module that you want to edit.
- 3 Double-click **Network Integrity**.
- 4 Click **Internet Connections Sharing**.
- 5 In the Network Integrity dialog box, do one of the following:
 - To specify that the Internet Connection Sharing service is required to be enabled on the computer, select **Sharing**, and then click the **Left Arrow** to move it to the Enabled list.
 - To specify that Internet Connection Sharing service must not be enabled on the computer, leave **Sharing** in the Disabled list.
- 6 Click **Ok**.

Authorized ICF/ICS exposed network services

You can use this check to specify the local network services that are authorized to be exposed to the internet. It generates a message if an unauthorized network service is exposed to the network.

The Authorized ICF/ICS exposed network services check uses a template that lists the services that the check examines and specifies if the listed service is authorized to be exposed to the network. By default, the template extensions are

.spx for Windows XP or .s3s for Windows 2003. You must enable a services template to use this check.

The default template, `services.spx`, lists the following services:

- ESM Agent
- ESM Manager
- FTP Server
- Internet Mail Access Protocol Version 4 (IMAP 3)
- Internet Mail Access Protocol Version 4 (IMAP 4)
- Internet Mail Server (SMTP)
- Post-Office Protocol Version 3 (POP3)
- Remote Desktop
- Secure Web Server (HTTPS)
- Telnet Server
- Web Server (HTTP)

Do not edit the default `services.spx` template. Any changes that you make can be overwritten by the next Security Update. However, you can make a copy of the template and then edit it to your requirements. For example, you can add services to the template so that the check examines and reports on the service. Security updates will not replace or override templates that you create. You can add services to the template or delete services from the template.

[Table 1-44](#) lists the message for this check.

Table 1-44 Authorized ICF/ICS exposed network service check message

Message name	Title	Severity
ESM_ICS_EXPOSURE_VIOLATION	Unauthorized exposure of a network or host service.	Yellow

Enabling a services template

You must enable an .spx or .s3s template to use the Authorized ICF/ICS exposed network services check.

To enable the template

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the Network Integrity module that you want to edit.

- 3 Double-click **Network Integrity**.
- 4 Click **Authorized ICF/ICS exposed network services**.
- 5 In the Network Integrity dialog box, select the template
- 6 Click the **Left Arrow** to move the template to the Enabled list.
- 7 Click **Ok**.

Authorizing an exposed network service

There may be network services listed in the template that you have authorized to be exposed to the internet. You can configure the Authorized ICF/ICS exposed network services check not to report these services by clicking the Authorized check box in the services template.

Authorizing an exposed network service

- 1 In the enterprise tree, expand the Templates tree.
- 2 Double-click the services template that you want to edit.
- 3 In the Template Editor, in the Authorize column, click the check box in the row of each service that you want to authorize.
- 4 In the Name or address of hosting computer box, type the name or address of the computer
- 5 In the External Port box, type the number of the external port of the service.
- 6 In the Internal Port box, type the number of the internal port of the service.
- 7 In the Protocol list, select the protocol type.
- 8 Click **Save**.

Network Integrity (UNIX)

SU 20 includes five new checks and two new options.

SNMP config file path

You can use this option to specify the path to the SNMP agent configuration file.

[Table 1-45](#) lists the messages for this check.

Table 1-45 SNMP config file path check message

Message name	Title	Severity
STKU_NO_SNMPD_CONF	No configuration file found for SNMP	Yellow - 3

Table 1-45 SNMP config file path check message

Message name	Title	Severity
STKU_SNMPD_NOT_RUNNING	SNMP is not running	Yellow - 3

Specifying the SNMP configuration file path

You can specify the path to the SNMP configuration file in the Include Directories list.

To specify the SNMP configuration file path

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the Network Integrity module that you want to edit.
- 3 Double-click **Network Integrity**.
- 4 Expand the **Network Integrity** tree.
- 5 Double-click **UNIX**.
- 6 Click **SNMP config file path**.
- 7 On the Include Directories tool bar, click **New**.
- 8 In the Include Directories list, type the path to the SNMP configuration file.
- 9 Click **OK**.

SNMP default community strings

This check reports if SNMP uses default community strings.

[Table 1-46](#) lists the message for this check.

Table 1-46 SNMP default community string check message

Message name	Title	Severity
STKU_DEFAULT_COMMUNITY	Default community string found	Yellow - 3

Specifying default community strings

You can specify the default community strings that the Network Integrity module examines.

Specifying default community strings

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the Network Integrity module that you want to edit.
- 3 Double-click **Network Integrity**.
- 4 Expand the **Network Integrity** tree.
- 5 Double-click **UNIX**.
- 6 Click **SNMP default community strings**.
- 7 On the Community strings tool bar, click **New**.
- 8 Type the name of the string.
- 9 Click **OK**.

SNMP write access

This check reports if write access is enabled

[Table 1-47](#) lists the message for this check.

Table 1-47 SNMP write access message

Message name	Title	Severity
STKU_WRITE_ACCESS	Write access is enabled	Yellow - 3

SNMP v3 encryption

This check reports if a user is not using encryption with SNMP version 3 network traffic.

[Table 1-48](#) lists the message for this check.

Table 1-48 SNMP v3 encryption message

Message name	Title	Severity
STKU_V3_ENCRYPTION	Encryption is not being used	Yellow - 3

SNMP version

This check reports if the SNMP agent is not using SNMP, version 3. SNMP, version 3 adds administration and security to SNMP.

[Table 1-49](#) lists the message for this check.

Table 1-49 SNMP version message

Message name	Title	Severity
STKU_AGENT_NOT_V3	Agent version is lower than V3	Yellow - 3

Exported non-secure exclude list

This option acts as an exclusion list for the NFS exported directory non-secure check. The NFS exported directory non-secure check will not report any directories that are listed in the NFS exported dirs to skip list.

Excluding directories from the NFS exported directory non-secure check

You can list the directories that you do not want the NFS exported directory non-secure check to report.

To create an excluded list

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the Network Integrity module that you want to edit.
- 3 Double-click **Network Integrity**.
- 4 Click **Exported non-secure exclude list**.
- 5 On the NFS exported dirs to skip list tool bar, click **New**.

- 6 Type the name of the directories that you want the check to exclude.
- 7 Click **OK**.

OS Patches (SUSE ES 8)

SU 20 includes a new SUSE Enterprise Server 8 template for the OS Patches module.

Patch.psl template

You can use the Patch.psl template to specify the operating system patches that are required on the SUSE Enterprise Server, version 8.

Startup Files (UNIX)

SU 20 includes a new option for the Installed Services check.

Approved Wrappers

You can use this option to specify approved wrappers for services. The Installed Services check will not report a process that is listed as forbidden if that process is wrapped with an approved wrapper.

Adding a wrapper to the approved wrappers list

You can add a wrapper to the approved wrapper list. If a forbidden process is wrapped in an approved wrapper, the Installed Services check does not report the process as forbidden.

To add a wrapper to the approved wrapper list

- 1 In the enterprise tree, expand the Policies branch.
- 2 Expand the policy which contains the Startup Files module that you want to edit.
- 3 Double-click **Startup Files**.
- 4 Expand the **Startup Files** tree.
- 5 Double-click **UNIX**.
- 6 Click **Approved wrappers**.
- 7 On the Approved wrapper list tool bar, click **New**.
- 8 Type the name of the wrapper.
- 9 Click **OK**.

Changed messages

The following modules contain messages that were changed in SU 20:

- UNIX File Watch (For message details, See [“File Watch \(All\)”](#) on page 54.)

Known issues

The following are known issues for SU 20:

Network Integrity (UNIX)	The Listening TCP Ports and Listening UDF Ports checks do not display process names. You can enable the checks to display process names by installing Isof in the /usr/bin or /usr/sbin directories.
SU Installation on MSSQL Server 2000	You must stop the MSSQL Services before installing SU 20 on computers that have MSSQL Server 2000 installed and running.
Password Strength (Windows 2000, XP)	Do not use DBCS characters in the word list file of the Password Strength module because the operating system does not support DBCS characters.

Resolved issues

The following issues have been resolved in SU 20:

Login Parameters (Windows)	The message returned from the Last User Name Hidden check has been changed to Last user name is not hidden.
Object Integrity	The group list in the Local Accounts check now recognizes the HelpServicesGroup group by the name %HelpServicesGroup%.
Startup Files (Windows 2003)	The Disallowed Services check now only reports services that are manually installed after installation. Services that are unavoidably installed with the operating system are not reported as violations.
File Watch (All)	You can now use either UNIX or Windows paths in the File Watch template. The UNIX or Windows regular expressions for the path in the File Watch template no longer overwrite each other.
Startup Files (UNIX)	The parsing of parameters in the Mandatory/Forbidden Parameters check now allows the user to group parameters together.

System requirements

[Table 1-50](#) lists the supported operating systems for SU 20.

Table 1-50 SU 20 supported operating systems

Agent operating system	Versions
AIX	4.2.1, 4.33, 5.1, 5.2
HP-UX	10.20, 11, 11.11
Red Hat Linux	7.x, 8, 9
Red Hat Linux Enterprise Server (ES) (x86)	2.1, 3.0
Solaris	2.5.1, 2.6, 2.7, 2.8, 2.9
SUSE LINUX Standard Server	8
SUSE LINUX Enterprise Server	8
Windows 2000 Professional and Server (Intel)	All
Windows NT Workstation and Server (Intel)	4.0 SP6a
Windows Server 2003	All
Windows Server 2003 (Itanium®)	All
Windows XP Professional (Intel)	All

SU 20 may run on newer versions of the supported operating systems, but Symantec reserves the right to certify the security update on the new versions before officially supporting them.

The LiveUpdate installation of SU 20 on all supported operating systems requires approximately 560 MB on each Symantec ESM manager.

The amount of disk space required by each agent depends on its operating system.

[Table 1-51](#) lists the agent disk space requirements.

Table 1-51 SU 20 agent disk space requirements

Agent operating system	SU 20
AIX	92 MB
HP-UX	72 MB
Red Hat Linux	36 MB

Table 1-51 SU 20 agent disk space requirements

Agent operating system	SU 20
Red Hat Linux Enterprise Server (ES) (x86)	36 MB
Solaris	58 MB
SUSE LINUX Standard Server 8	36 MB
SUSE LINUX Enterprise Server 8	36 MB
Windows 2000 Professional and Server (Intel)	31 MB
Windows NT Workstation and Server (Intel)	31 MB
Windows Server 2003	31 MB
Windows Server 2003 (Itanium®)	104 MB
Windows XP Professional (Intel)	31 MB

Security Update 19

The following are new in SU 19:

- Six new checks and ten enhanced checks
- Eleven new options
- Fifteen new messages
- Eight enhanced templates
- One known issue
- Eight resolved issues

Account Integrity (Windows)

SU 19 includes a new name list on one check.

Disabled/expired/locked accounts (Windows)

This check reports accounts that have been disabled, expired, or locked out for longer than a specified period.

Use this check's new name list to include or exclude users and groups that are not already included or excluded by the Users to check option.

Windows does not keep track of the date when it disables, expires, or locks out an account. The Account Integrity module stores the date when it first detects

the disabled, expired, or locked out account in the snapshot file. It uses this value to calculate the elapsed time for the account.

Note: This check must be enabled for other checks in the module to report information about disabled, expired, or locked out accounts.

Type the maximum number of days in the Max disabled time (days) text box. The default value is 90.

[Table 1-52](#) lists the messages for this check.

Table 1-52 Disabled/expired/locked accounts message

Message name	Title	Severity
DISABLED	Disabled, expired, or locked account	Yellow

Account Integrity (UNIX)

SU19 includes two new options, two new messages, and renames one check.

Duplicate IDs (UNIX)

This check reports two new messages: Duplicate root GID and Duplicate root UID.

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 existence of duplicate root UIDs or GIDs is a serious security risk and could allow unauthorized use of your computers.

[Table 1-53](#) lists the messages for this check.

Table 1-53 Duplicate IDs messages

Message name	Title	Severity
DUPUID	Duplicate UID	Green
DUPGID	Duplicate GID	Green
DUPROOTGID	Duplicate root GID	Red
DUPROOTUID	Duplicate root UID	Red

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.

Reserved UID/GID (UNIX)

The Privileged users and groups check is now called Reserved UID/GID.

Reserved UID ranges (UNIX)

Use this option to specify reserved user ID ranges for different operating systems to be used with the Reserved UID/GID check. If no range is specified for a particular operating system, or if the range is not properly formatted, the system default ranges are used.

Entries in this option's name list should be in the format <OS>:<RANGE>, where <OS> is the name of the operating system and <RANGE> is one or more user-defined UID ranges. A colon is used to separate these two values.

Acceptable, case-sensitive values for <OS> are AIX, HP-UX, Linux, and Solaris. Acceptable values for <RANGE> include a single numeric value (e.g., AIX:5), a hyphen-separated range of numeric values (e.g., HP-UX:0-10), or a list of ranges delimited by semicolons (e.g., Solaris:0-5;10;15-20).

Reserved GID ranges (UNIX)

This option lets you specify reserved group ID ranges for different operating systems to be used with the Reserved UID/GID check. If no range is specified for a particular operating system, or if the range is not properly formatted, the system default ranges are used.

Entries in this option's name list should be in the format <OS>:<RANGE>, where <OS> is the name of the operating system and <RANGE> is one or more user-defined GID ranges. A colon is used to separate these two values.

Acceptable, case-sensitive values for <OS> are AIX, HP-UX, Linux, and Solaris. Acceptable values for <RANGE> include a single numeric value (e.g., AIX:5), a hyphen-separated range of numeric values (e.g., HP-UX:0-10), or a list of ranges delimited by semicolons (e.g., Solaris:0-5;10;15-20).

Account Integrity (Windows/UNIX)

SU 19 includes one new option and message.

Automatically update snapshots (Windows/UNIX)

Enable this option to automatically update snapshots with current agent information.

When snapshots are automatically updated, Snapshot updated is reported in the Updateable/Correctable field of the console grid. The type of change is described in the Information field.

[Table 1-54](#) lists the message that is reported when automatic updates fail.

Table 1-54 Automatic snapshot update message

Message name	Title	Severity
AUTO_UPDATE_FAILED	Automatic update failed	Green

Active Directory (Windows)

SU 19 includes five new checks and eight new messages that verify and report Kerberos Policy settings.

Enforce user logon restrictions (Windows 2000/2003)

This check reports when the Enforce user logon restrictions setting in the Kerberos Policy is not enabled.

When user logon restrictions are not enforced, session tickets can be granted for unauthorized services.

If the computer being checked is not a domain controller, this check is ignored

[Table 1-55](#) lists the message for this check.

Table 1-55 Enforce user logon restrictions message

Message name	Title	Severity
ESM_LOG_RESTRICT_DISABLED	User logon restrictions not enforced	Yellow

To protect your computers

- ◆ Enable the Enforce user logon restrictions setting in the Kerberos policy.

Maximum lifetime for service ticket (Windows 2000/2003)

This check reports when the Maximum lifetime for service ticket setting in the Kerberos Policy is set higher than the default setting of 600 minutes.

When the value for this setting is too high, user accounts that have been disabled might be able to access network services by using valid service tickets that were issued before the accounts were disabled. Or, they might be able to access network resources outside of logon hours.

If the computer being checked is not a domain controller, this check is ignored.

[Table 1-56](#) lists the messages for the Maximum lifetime for service ticket check.

Table 1-56 Maximum lifetime for service ticket messages

Message name	Title	Severity
ESM_SERV_TICK_LIFE_TOO_HIGH	Service ticket lifetime too high	Yellow
ESM_SERV_TICK_LIFE_NOT_SET	Service ticket lifetime not set	Red

To protect your computers

- ◆ Set the Maximum lifetime for service ticket setting in the Kerberos Policy to 600 minutes or less.

Maximum lifetime for user ticket (Windows 2000/2003)

This check reports when the Maximum lifetime for user ticket setting in the Kerberos Policy is set higher than the default setting of ten hours.

When the value for this setting is too high, user accounts that have been disabled could be used to access network services by using valid service tickets that were issued before the accounts were disabled. Or, they could be used to access network resources outside of logon hours.

If the computer being checked is not a domain controller, this check is ignored.

Table 1-57 Maximum lifetime for user ticket messages

Message name	Title	Severity
ESM_USER_TICK_LIFE_TOO_HIGH	User ticket lifetime too high	Yellow
ESM_USER_TICK_LIFE_NOT_SET	User ticket lifetime not set	Red

To protect your computers

- ◆ Set the Maximum lifetime for user ticket setting in the Kerberos Policy to ten hours or less.

Maximum lifetime for user ticket renewal (Windows 2000/2003)

This check reports when the Maximum lifetime for user ticket renewal setting in the Kerberos Policy is set higher than the default setting of seven days.

When the value for this setting is too high, users might be able to renew very old user tickets.

If the computer being checked is not a domain controller, this check is ignored.

[Table 1-58](#) lists the messages for this check.

Table 1-58 Maximum lifetime for user ticket renewal messages

Message name	Title	Severity
ESM_USER_TICK_RENEW_TOO_HIGH	User ticket renewal lifetime too high	Yellow
ESM_USER_TICK_RENEW_NOT_SET	User ticket renewal lifetime not set	Red

To protect your computers

- ◆ Set the Maximum lifetime for user ticket renewal setting in the Kerberos Policy to seven days or less.

Maximum tolerance for computer clock synchronization (Windows 2000/2003)

This check reports a problem when the Maximum tolerance for computer clock synchronization setting in the Kerberos Policy is set higher than the default setting of five minutes.

When the value for this setting is too high, the possibility of a successful “replay attack” increases.

If the computer being checked is not a domain controller, this check is ignored.

[Table 1-59](#) lists the message for this check.

Table 1-59 Maximum tolerance for computer clock synchronization message

Message name	Title	Severity
ESM_CLOCK_SYNCH_TOO_HIGH	Clock synchronization tolerance too high	Yellow

To protect your computers

- ◆ Set the Maximum tolerance for computer clock synchronization setting in the Kerberos Policy to five minutes or less.

File Attributes (Windows/UNIX)

SU 19 includes one new option and message.

Automatically update snapshots (Windows NT/UNIX)

Enable this option to automatically update snapshots with current agent information.

When snapshots are automatically updated, Snapshot updated is reported in the Updateable/Correctable field of the console grid. The type of change is described in the Information field.

[Table 1-60](#) lists the message that is reported when automatic updates fail.

Table 1-60 Automatic snapshot update message

Message name	Title	Severity
AUTO_UPDATE_FAILED	Automatic update failed	Green

File Attributes (Windows)

SU 19 includes enhancements to the File template.

File template (Windows)

You can now enter more than one value in the Owner field of the File template by separating values with a comma (,).

If the owner of the file or directory being checked matches any of the owners listed, Symantec ESM does not report ownership problems.

If any owner in the list is a privileged account, the entire template item is considered privileged. This means that when the Allow any privileged account check is enabled and a privileged account is in the list of users or groups, Symantec ESM does not report.

File Attributes (UNIX)

SU 19 includes enhancements to the New File template

New File template (UNIX)

Multiple values in User and Group fields

You can now enter more than one value in the User and Group fields of the New File template by separating values with a comma (,).

If the owner of the file or directory being checked matches any of the users or groups listed, Symantec ESM does not report ownership problems.

If any user or group in the list is a privileged account, the entire template item is considered privileged. This means that if the Allow any privileged account check is enabled and a privileged account is in the list of users or groups, Symantec ESM does not report.

Depth field

The Depth field, introduced to the New File template in SU 18, has been modified to include a new option, Current level only.

Select one of the following to specify the maximum search depth for files that are specified with wildcard characters:

Traverse all levels	This option searches all directories and subdirectories starting from the last directory separator (/). For example, if the wildcard path is /sbin/rc*, any file or directory below /sbin that matches the wildcard is reported. There is no limit to the number of subdirectories that can be searched.
Current level only	This option searches one level starting from the last directory separator. For example, if the wildcard path is /sbin/rc*, only the first file or directory below /sbin that matches the wildcard character is reported. For example /sbin/rc_d is reported, but /sbin/rc_d/file is ignored.
Traverse 1 level	This option searches two levels starting from the last directory separator. For example, if the wildcard path is /sbin/rc*, then /sbin/rc_d, /sbin/rc_d/file, and /sbin/rc_d/newdir are all reported but /sbin/rc_d/newdir/newfile is ignored because it is at the third level.
Traverse 2 levels through Traverse 9 levels	Specify the number of levels that you want to search from the last directory separator. To search deeper, use All or change the wildcard characters that you use.

File Find (UNIX)

SU 19 includes one new option and message, enhancements to seven checks, enhancements to the File Content Search template, and one renamed option.

Automatically update snapshots (UNIX)

Enable this option to automatically update snapshots with current agent information.

When snapshots are automatically updated, Snapshot updated is reported in the Updateable/Correctable field of the console grid. The type of change is described in the Information field.

[Table 1-61](#) lists the message that is reported when automatic updates fail.

Table 1-61 Automatic snapshot update message

Message name	Title	Severity
AUTO_UPDATE_FAILED	Automatic update failed	Green

Directories/files/types excluded (UNIX)

The Directories/files option is now called Directories/files/types because of the file type enhancement described below.

Excluding by file type enhancement (UNIX)

Using new functionality in the File Find module, you can exclude file types in addition to specific directories and files.

File types must be preceded by the pipe character (|). Valid entries are |CHAR, |FIFO, |BLOCK, and |SOCK.

This enhancement is included in the following checks:

- Directories/files/types excluded
Valid entries are |CHAR, |FIFO, |BLOCK, and |SOCK.
- Sticky files
Valid entries are |CHAR, |FIFO, |BLOCK, and |SOCK.
- Device files not in /dev
Valid entries are |CHAR, and |BLOCK.
- World writable files
Valid entries are |CHAR, |FIFO, |BLOCK, and |SOCK.
- Group writable files
Valid entries are |CHAR, |FIFO, |BLOCK, and |SOCK.
- Uneven file permissions
Valid entries are |CHAR, |FIFO, |BLOCK, and |SOCK.
- Unowned directories/files
Valid entries are |CHAR, |FIFO, |BLOCK, and |SOCK.

File Content Search template (UNIX)

The drop-down list in the Type field of the Conditions sublist in the File Content Search template, includes three new options.

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:

Key	Value	Explanation
I	Inetd	Verify that inetd service exists
i	No Inetd	Verify that inetd service does not exist
P	Process	Verify that process is running
p	No Process	Verify that process is not running
F	File	Verify that file exists
f	No File	Verify that file does not exist

- 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**.

File Watch (Windows/UNIX)

SU 19 includes one new option plus wildcard character and keyword support for File Watch templates.

Keywords list (Windows/UNIX)

Use this option to enable or disable File Keywords template files that File Watch templates use to locate file paths. File Watch templates locate file paths according to keyword values that correspond to registry locations (Windows) or folder/directory paths (Windows, UNIX).

File Watch template (Windows/UNIX)

In the File/Directory field of the File Watch template and the File/Directory to exclude field of the Excludes sublist, you can now use keywords that correspond to entries in the File Keywords template.

File Watch template (Windows 2000/XP/2003/UNIX)

Wildcard characters * and ? are supported for both directory and file names in the File Watch template.

The following examples illustrate how to use these characters with directory and file names.

Example	Description
usr or ?home/	Wildcard characters in the first position are not supported on UNIX. In this example, the File Watch module could not determine the root directory or know where to begin the scan. An Unexpected system error message would be reported in the audit results.
:\Windows C?\Windows or C:	Wildcard characters are not supported before the first “\” on Windows. In this example, the File Watch module could not determine the root directory and would not know where to begin the scan. An Unexpected system error message would be reported in the audit results.
C:\Windows\system*	Matches all files and directories that begin with system and reside in C:\Windows. All files in c:\Windows\system32 and c:\Windows\system directories and subdirectories would be processed.

Example	Description
C:\Windows\system*\	Matches c:\Windows\system32\ and c:\Windows\system\. This directory and all of its sub-directories would be processed. Symantec ESM would not process the files in those directories.
C:\Windows\system??\ C:\Windows\system??	Matches only the c:\Windows\system32\ directory. Symantec ESM would not process the files in the directory.
C:*.txt	Matches and process every .txt file on the C drive.

Login Parameters (Windows)

SU 19 includes enhancements to one check.

Account lockout threshold (Windows)

This check reports only if the Windows account lockout threshold is set higher than that set in the check. Previously, this check reported when the Windows account lockout threshold was different than that set in the check.

Network Integrity (Windows/UNIX)

SU 19 includes one new option and message.

Automatically update snapshots (Windows/UNIX)

Enable this option to automatically update snapshots with current agent information.

When snapshots are automatically updated, Snapshot updated is reported in the Updateable/Correctable field of the console grid. The type of change is described in the Information field.

[Table 1-62](#) lists the message that is reported when automatic updates fail.

Table 1-62 Automatic snapshot update message

Message name	Title	Severity
AUTO_UPDATE_FAILED	Automatic update failed	Green

Network Integrity (Windows)

SU 19 includes one new check and four new messages.

IP Security Policies (Windows 2000/2003)

This check reports IP Security Policies that exist for Active Directory on domain controllers. The check reports if the policy is assigned, if IP Security Rules exist but are not selected, and if the Check for policy changes text box is set to greater than four minutes.

[Table 1-63](#) lists the messages for this check.

Table 1-63 IP Security Policy message

Message name	Title	Severity
ESM_IP_SECPOLICY_DEFAULT	IP Security Policy is not assigned	Red
ESM_IP_SECURITY_POLICY_DEFAULT	IP Security Policy is assigned	Green
ESM_IP_SECURITY_RULE_NOT_SELECTED	IP Security Policy Rule is not selected	Yellow
ESM_IP_SECURITY_REFRESH	Check for policy changes setting is set too high	Yellow

To protect your computers

- ◆ Always assign IP Security Policies on Domain Controllers, remove rules that are not intended for use rather than leave them unchecked, and set the Check for policy changes text box to four minutes or less to ensure that all computers on Domain Controllers are using current Policy settings.

Object Integrity (UNIX)

SU 19 includes one new option and message.

Automatically update snapshots (UNIX)

Enable this option to automatically update snapshots with current agent information.

When snapshots are automatically updated, Snapshot updated is reported in the Updateable/Correctable field of the console grid. The type of change is described in the Information field.

[Table 1-64](#) lists the message that is reported when automatic updates fail.

Table 1-64 Automatic snapshot update message

Message name	Title	Severity
AUTO_UPDATE_FAILED	Automatic update failed	Green

OS Patches (AIX)

SU 19 includes an enhancement to the AIX Patch template.

Patch template (AIX)

The AIX Patch template now includes a new Description field option in the Superseded sublist. The new Maintenance option can only be used on AIX computers.

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.
 - **Maintenance.** The patch specified in the Template Editor row will be superseded by the listed AIX maintenance release. This option works only on AIX computers.

- 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**.

OS Patches (Solaris/HP-UX)

SU19 includes enhancements to Solaris and HP-UX Patch templates.

Patch template (Solaris/HP-UX)

Patch template files for Solaris (patch.ps6 and patch.pso) and HP-UX (patch.ph1) can now identify mandatory patches that are included in add-on packages before checking for a specific patch.

Select Package in the Type field of the Conditions sublist in the Patch template and specify the patch-id for Solaris or the fileset name for HP-UX in the Name field.

The fileset name for HP-UX can be further configured with the specific version. Separate the fileset name and the version number with a colon. for example, OS-Core.UX-CORE:1.2.

Symantec ESM checks for the patch only if the specified package exists.

To add a row to the Conditions sublist

- 1 In the Template Editor, select the Conditions field of the row that you are editing.
- 2 In the Template Sublist Editor, click **Add Row**.
- 3 In the Type field, select one of 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.
 - **Package - Check for existing installed package**

Symantec ESM only checks the patch if the named package exists. This option is only valid on Solaris and HP-UX.

- 4 In the Name field, 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, or a package that must be installed 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**.

Password Strength (Windows)

SU 19 includes one new option and one renamed check with updated information.

Display name as distinguished name (Windows 2000/2003)

Enable this option to have password checks report users' distinguished names in the console's Name field (e.g., "/UserName1/Users/company/corp/com").

Disable this option to have password checks report users' logon names in the console's Name field.

Password stored using reversible encryption (Windows 2000/2003)

The Password stored with reversible encryption check, introduced with SU 18, is now called Password stored using reversible encryption, making the check name more consistent with the Microsoft setting.

This check reports domain accounts with passwords that are stored using reversible encryption.

Note: This check does not report the domain level or local Security Settings/Password Policy/Store password using reversible encryption for all users in the domain setting.

[Table 1-65](#) lists the message for this check.

Table 1-65 Password stored using reversible encryption message

Message name	Title	Severity
REVERSIBLE_ENCRYPTION	Password stored using reversible encryption	1

To protect your computers

- 1 Disable the Store password using reversible encryption setting in Users Properties for each user and then reset the user's password.
- 2 Disable the reversible encryption setting in the local and domain Password Policy.

Registry (Windows)

SU 19 includes one new option and message, and enhancements to the Registry template.

Automatically update snapshots (Windows NT)

Enable this option to automatically update snapshots with current agent information.

When snapshots are automatically updated, Snapshot updated is reported in the Updateable/Correctable field of the console grid. The type of change is described in the Information field.

[Table 1-66](#) lists the message that is reported when automatic updates fail.

Table 1-66 Automatic snapshot update message

Message name	Title	Severity
AUTO_UPDATE_FAILED	Automatic update failed	Green

Registry template (Windows XP/2003)

Registry templates registry.rs6, registry.rwx, and registry_ADS.rs6 have been enhanced to verify and report Software Restriction Policies that include Certificate Rule, Hash Rule, Internet Zone (UrlZone) Rule, and Path Rule.

The following registry keys are reported:

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer

Startup Files (Windows/UNIX)

SU 19 includes one new option and message.

Automatically update snapshots (Windows/UNIX)

Enable this option to automatically update snapshots with current agent information.

When snapshots are automatically updated, Snapshot updated is reported in the Updateable/Correctable field of the console grid. The type of change is described in the Information field.

[Table 1-67](#) lists the message that is reported when automatic updates fail.

Table 1-67 Automatic snapshot update message

Message name	Title	Severity
AUTO_UPDATE_FAILED	Automatic update failed	Green

Known issues

The %ORACLE_HOME% keyword has essentially been reserved to indicate the Oracle home directory in a Symantec ESM environment that has Symantec ESM Modules for Oracle Databases installed. If you don't have Symantec ESM Modules for Oracle Databases installed and you want to use a keyword to indicate the Oracle home directory, you must use a different keyword.

Resolved issues

The following issues have been resolved:

Account Integrity (UNIX)	<p>The message reported for the User shell compliance check has been changed from a severity of Green to Yellow.</p> <p>The Everyone group can now be successfully added to the include and exclude name lists in this module.</p>
ICE (Windows/UNIX)	<p>Previous versions of the ICE template failed to execute script parameters. This has now been resolved.</p>
File Attributes (Windows/UNIX)	<p>Template files in the File Attributes module no longer check checksums on passwd or shadow files, preventing Symantec ESM from reporting each time users change their passwords.</p>
Login Parameters (UNIX)	<p>The Login retries check reports on AIX computers and on HP-UX and Digital UNIX (Tru64) computers that are running in trusted mode.</p>
Network Integrity (UNIX)	<p>The NFS exported directory root access by any host check was reported to work only on Digital UNIX (Tru64) operating systems. This check has been verified to work on all UNIX versions.</p>
Network Integrity (Windows)	<p>The block characters displayed in the console grid when reporting trusted domain names are no longer displayed.</p>
Password Strength (Windows/UNIX)	<p>The Minimum password age check can now be set to 0.</p>

System requirements

[Table 1-68](#) lists the supported operating systems for SU 19 .

Table 1-68 SU 19 supported operating systems

Agent operating system	Versions
AIX	4.2.1, 4.33, 5.1, 5.2
HP-UX	10.20, 11, 11.11
Red Hat Linux	6.2, 7.x, 8, 9
Red Hat Linux Enterprise Server (ES) (x86)	2.1, 3.0
Solaris	2.5.1, 2.6, 2.7, 2.8, 2.9
SUSE LINUX Standard Server	8
Windows 2000 Professional and Server (Intel)	All
Windows NT Workstation and Server (Intel)	4.0 SP6a
Windows Server 2003	All
Windows XP Professional (Intel)	All

SU 19 may run on newer versions of the supported operating systems, but Symantec reserves the right to certify the Security Update on the new versions before officially supporting them.

The LiveUpdate installation of SU 19 on all supported operating systems requires approximately 560 MB on each Symantec ESM manager.

The amount of disk space required by each agent depends on its operating system.

[Table 1-69](#) lists the agent disk space requirements.

Table 1-69 SU 19 agent disk space requirements

Agent operating system	SU 18
AIX	92 MB
HP-UX	72 MB
Red Hat Linux	36 MB
Red Hat Linux Enterprise Server (ES)	36 MB
Solaris	58 MB
SUSE LINUX Standard Server 8	36 MB
Windows 2000 Professional or Server (Intel)	31 MB
Windows NT (Intel)	31 MB
Windows Server 2003	31 MB
Windows XP Professional (Intel)	31 MB

Security Update 18

The following are new in SU 18:

- Support for SUSE LINUX Standard Server 8

Note: Systems installed from the SUSE CD1 are supported. Systems installed from a UnitedLinux CD1 are not supported.

- Support for Red Hat Enterprise Server (ES) 2.1 and 3.0
- One new template and enhancements to four others
- Eight new checks and eleven messages
- Documentation updates and resolved issues

SUSE LINUX

To install the SUSE Standard Server 8 agent

- 1 Download Symantec ESM 6.0 SUSE Linux Standard Server 8 Agent Setup to save esmsuse.tar on your computer.
- 2 Copy esmsuse.tar to your setup files directory.
- 3 Run tar -xvf esmsuse.tar to extract the setup files.
- 4 Follow the instructions for installing Symantec ESM on a local computer in the *Symantec Enterprise Security Manager Installation Guide*.

Installation of Symantec ESM agents for SUSE LINUX does not include Patch templates for SUSE LINUX. Use the latest OS Patch policy to obtain current SUSE LINUX patches.

Account Integrity (Windows)

SU 18 includes one new check, two new messages, and one new template.

Group member watch (Windows 2000/XP/2003)

This check reports groups with prohibited members (users and groups) and groups in prohibited groups.

Use the Members and Member Of sublists in the Group Member Watch template to designate prohibited members and groups.

For example, in the Members sublist, if the GUESTS group prohibits all members (the Members sublist is empty), but the check detects one or more members in the GUEST group, Prohibited member is reported.

If, in the Member Of sublist, the GUESTS group is prohibited from the ADMINISTRATORS group, but the check detects the GUESTS group in the ADMINISTRATORS group, Prohibited member of is reported.

Use the name list to specify template files that are to be used.

[Table 1-70](#) lists the messages for the Group member watch check.

Table 1-70 Group member watch messages

Name	Title	Class
INVALID_MEMBER	Prohibited member	1
INVALID_MEMBER_OF	Prohibited member of	1

Note: If you enable Group member watch but do not create a Group Member Watch template, no messages are reported.

Group Member Watch template

A sample Group Member Watch template is not included in SU 18. You must create your own.

To add a Group Member Watch template

- 1 In the enterprise tree, right-click **Templates**, and then click **New**.
- 2 In the Create New Template dialog box, click **Group Member Watch - all**. The template type determines the file extension of the new template file.
- 3 In the Template file name field, type a template name. Symantec ESM automatically adds the .gmw extension.
- 4 In the Group Name field, replace <NEW> with the name of the group that is to be watched.
- 5 Add entries to the Members sublist (initially 0). See [“To add a row to the Members sublist”](#) on page 99.

Note: If you do not add one or more entries to the Members sublist, all group members are prohibited.

- 6 In the Comments for Members field, replace <NEW> with text that you want to display with the Prohibited member message.
- 7 Add entries to the Member Of sublist (initially 0). See [“To add a row to the Member Of sublist”](#) on page 99.

Note: If you do not add one or more entries to the Members sublist, all group memberships are permitted.

- 8 In the Comments for Member Of field, replace <NEW> with text that you want to display with the Prohibited member of message.
- 9 Click **Save**.
- 10 To add another group, repeat steps 3–8.
- 11 Click **Close**.

To add a row to the Members sublist

- 1 In the Template Editor, click the **Members** field (initially 0) in the row that you are editing.
- 2 Click **Add Row**.
- 3 Do one of the following:
 - To prohibit the member, check Prohibited member.
 - To permit the member, uncheck Prohibited member.
- 4 In the Member Name field, replace <NEW> with the member’s name.
- 5 Click **Apply**.
- 6 To add another member, repeat steps 2–5.
- 7 Click **Close**.

To add a row to the Member Of sublist

- 1 In the Template Editor, click the **Member Of** field (initially 0) in the row that you are editing.
- 2 Click **Add Row**.
- 3 Do one of the following:
 - To designate the group as prohibited, check Prohibited group.
 - To designate the group as permitted, uncheck Prohibited group.
- 4 In the Group Name field, replace <NEW> with the group’s name.
- 5 Click **Apply**.
- 6 To add another Member Of entry, repeat steps 2–5.

- 7 Click **Close**.

File Attributes (Windows/UNIX)

SU 18 includes one new option and message (Automatic update failed).

Automatically update snapshots (Windows 2000/XP/2003/UNIX)

Enable this option to automatically update snapshots with current information.

When snapshots are automatically updated, Snapshot updated is reported in the Updateable/Correctable field. The type of change is described in the message Info field.

[Table 1-71](#) lists the new message that is reported when automatic updates fail.

Table 1-71 Automatic snapshot update messages

Name	Title	Class
AUTO_UPDATE_FAILED	Automatic update failed	0

File Attributes (Windows)

SU 18 renames two checks and adds two new messages, wildcard support and examination of ACL executable code in the File template, and the ability to associate variable keywords with directories in the File Keywords template.

File and folder attributes

This check, previously named File attributes, now also reports a folder attributes message.

[Table 1-72](#) lists the message for this check

Table 1-72 Folder attributes message

Name	Title	Code	Class
FOLDER_ATTRIB_MISMATCH	Different folder attributes	TU / C	1

To protect your computers

- ◆ Do one of the following:
 - If the folder attribute is authorized, update the template manually.

- If the folder attribute is not authorized, use the Correct feature in the console grid to revert the attribute to the setting that is specified in the template.

File and folder ownership

This check, previously named File ownership, now also reports changed folder ownership.

[Table 1-73](#) lists the messages for the File and folder ownership check.

Table 1-73 Folder ownership messages

Name	Title	Code	Class
FILEAT_OWNER_MMAT	Different file ownership	TU / C	1
FOLDERAT_OWNER_MMAT	Different folder ownership	TU / C	1

To protect your computers

- ◆ Do one of the following:
 - If the folder owner is authorized, update the template manually.
 - If the folder owner is not authorized, use the Correct feature in the console grid to revert the folder to the owner that is specified in the template.

File template

SU 18 includes wildcard support in the File template and examination of all executable code in %systemroot%\system32 and %systemroot%\drivers.

Wildcard support

Wildcard characters are supported for both directory and file names.

[Table 1-74](#) provides examples that illustrate how to use wildcard characters for directory and file names.

Table 1-74 Wildcard functionality

Example	Description/Examples
C:\Win*\temp	Matches all files and directories named temp in any directory that begins with C:\Win.
	Matches C:\Win\temp, C:\Windows\temp, C:\Win32\temp
	Does not match C:\Wendows\temp, C:\Windows\temp\otherdir

Table 1-74 Wildcard functionality

Example	Description/Examples
C:\Win*\tim?	Matches all files and directories that begin with tim, end with any single character, and are in any directory that begins with C:\Win.
	Matches C:\Win\timp, C:\Windows\time, C:\Win32\tims
	Does not match C:\Won\timp, C:\Windows\timber, C:\Windows\tim, C:\Windows\time\otherdir
C:\Windows\sys*	Matches all files and directories that begin with sys and reside in C:\Windows.
	Matches C:\Windows\sys, C:\Windows\system.ini, C:\Windows\system32
	Does not match C:\Windows\sy, C:\Windows\sistem
C:\Windows\sy*.i*	Matches all files and directories that begin with sy, contain .i, and reside in C:\Windows
	Matches C:\Windows\sy.i, C:\Windows\system.ini, C:\Windows\sysfiles.inf
	Does not match C:\Windows\si.i, C:\Windows\system.exe

Executable code

The module examines all executable code in %systemroot%\system32 and %systemroot%\drivers as well as specified files.

File Keywords template

You can associate keywords with directories as well as with registry key values.

- In the Keyword Value field, do one of the following:
 - If you intend to associate a keyword with a directory, replace <NEW> with the directory's full path.
 - If you intend to associate a keyword with a registry key value, replace <NEW> with the value's full path.
- In the Keyword Type field, select one of the following values:
 - Registry
 - Directory

File Attributes (UNIX)

SU 18 includes a new option, two new fields and wildcard support in the New File template, and one new message for two existing checks.

Keywords list

Use this option to specify Keywords template files that are to be included or excluded for the New File template.

New File template

SU 18 includes two new fields, Depth and Item, and wildcard support for both directories and files.

Depth

Select one of the following to specify the maximum search depth for files that are specified with wildcard characters:

Traverse all levels	This option searches all directories and subdirectories starting from the last directory separator (/). For example, if the wildcard path is /sbin/rc*, any file or directory below /sbin that matches the wildcard is reported. There is no limit to the number of subdirectories that can be searched.
Traverse 1 level	This option searches one level starting from the last directory separator. For example, if the wildcard path is /sbin/rc*, only the first file or directory below /sbin that matches the wildcard character is reported. For example /sbin/rc_d is reported, but /sbin/rc_d/file is ignored.
Traverse 2 levels	This option searches two levels starting from the last directory separator. For example, if the wildcard path is /sbin/rc*, /sbin/rc_d, /sbin/rc_d/file, and /sbin/rc_d/newdir are all reported but /sbin/rc_d/newdir/newfile is ignored because it is at the third level.
Traverse 3 levels through Traverse 9 levels	Specify the number of levels that you want to search from the last directory separator. To search deeper, use All or change the wildcard characters that you use.

Item Type

Select one of the following to specify the scope of wildcard searches:

Files and Directories	This option searches for directories and for files that match the wildcard entry.
Files Only	This option searches only for files that match the wildcard entry.
Directories Only	This option searches only for directories that match the wildcard entry.

Wildcard support

Wildcard characters are supported for both directory and file names.

[Table 1-75](#) lists the wildcard character functionality.

Table 1-75 Wildcard character functionality

Example	Description/Examples
/usr*/temp	Matches all files and directories named temp in any directory that begins with usr.
	Matches /usr/temp, usrs/temp, /usrbin/temp
	Does not match /user/temp, /usrbin/temp/otherdir
/usr*/tim?	Matches all files and directories that begin with tim, end with any single character, and are in any directory that begins with usr.
	Matches /usrs/timp, /usrbin/time, /usr/tims
	Does not match /user/timp, /usrbin/timber, /usrbin/tim, /usrbin/time/otherdir
/sbin/rc*	Matches all files and directories (all the way to leaf nodes) that begin with rc in the /sbin directory. Files and directories in the first level of subdirectories of /sbin that begin with rc are also matched.
	Matches /sbin/rc, /sbin/rcedit, /sbin/rcdir/file.txt, /sbin/rcdir/otherdir
	Does not match /rbin/rc, /sbin/rcredit
/sbin/rc*.d*	Matches all files and directories (to leaf nodes) that begin with rc, contain .d, and are in the /sbin directory. Files and directories in the first level of subdirectories of /sbin that begin with rc and contain .d are also matched.
	Matches /sbin/rc.d, /sbin/rcedit.d, /sbin/rcdir.d/file.txt, /sbin/rcdir.dt/otherdir
	Does not match /rbin/rc.d, /sbin/rcredit.d, /sbin/rcedit.e/file.txt

Permissions

[Table 1-76](#) lists the new directory permissions message for this check.

Table 1-76 Directory permissions message

Name	Title	Code	Class
STKU_DIFFPERM_DIR	Different directory permissions	TU	1

To protect your computers

- ◆ Do one of the following:
 - If the directory permission is authorized, update the template.
 - If the directory permission is not authorized, correct the directory ownership manually.

User ownership

[Table 1-77](#) lists the new directory permissions message for this check.

Table 1-77 Directory permissions message

Name	Title	Code	Class
STKU_DIFFOWN_DIR	Different directory ownership	TU	1

To protect your computers

- ◆ Do one of the following:
 - If the directory owner is authorized, update the template.
 - If the directory owner is not authorized, correct the directory ownership manually.

Group ownership

[Table 1-78](#) lists the new directory permissions message for this check.

Table 1-78 Directory permissions message

Name	Title	Code	Class
STKU_DIFFOWN_DIR	Different directory ownership	TU	1

To protect your computers

- ◆ Do one of the following:
 - If the directory owner is authorized, update the template.

- If the directory owner is not authorized, correct the directory ownership manually.

File Find (UNIX)

SU 18 includes numeric comparison functionality to the File Content Search template.

In the 2nd Pattern field of the File List sublist, replace <NEW> with a numeric comparison or regular expression to narrow the range of the text pattern that is specified in the Pattern field. The File content search check reports the first variable/value combination that matches the template.

File Watch (Windows/UNIX)

SU 18 includes one new check and message (Automatic update failed).

Automatically update snapshots (Windows 2000/XP/2003/UNIX)

Enable this option to automatically update snapshots with current agent information.

When snapshots are automatically updated, Snapshot updated is reported in the Updateable/Correctable field of the updateable messages that are listed above. The type of change is described in the message Info field.

[Table 1-79](#) lists the message for this check.

Table 1-79 Automatic snapshot update messages (Windows)

Name	Title	Code	Class
AUTO_UPDATE_FAILED	Automatic update failed		0

Login Parameters (UNIX)

SU 18 includes one check enhancement.

Warning banners

[Table 1-80](#) lists the following actions that this check now performs.

Table 1-80 New Warning banners actions

Platform	Action
AIX	Searches for a specified string in the herald line of the default stanza in <code>/etc/security/login.cfg</code> .
HP-UX	Examines <code>/etc/inetd.conf</code> to determine if telnetd is configured to display banners using the <code>-b</code> option. The check parses the file and searches for matching strings.
Linux	Examines <code>/etc/issue.net</code> in addition to <code>/etc/issue</code> .
OSF1/Tru64	Examines <code>/etc/gettydefs</code> for default banner information. If the default banner information is found, the check searches for string matches. If the check doesn't find a matching string but does find <code>%v</code> or <code>%h</code> , the check uses <code>popen</code> to run <code>uname -a</code> . Then the check parses the output for the matching string. Examines <code>/etc/issue.net</code> as well as <code>/etc/issue</code> .
Solaris	Parses <code>/etc/default/telnetd</code> and <code>/etc/default/ftpd</code> to match string expressions in the line <code>BANNER=</code> . Sends the parsed line to the shell for evaluation. Searches the operating system output for strings that match the expressions that you entered in the template.

Network Integrity (UNIX)

SU 18 includes one new check and message.

Anonymous FTP shell

This security check reports shells that are being used by anonymous FTP accounts.

Table 1-81 Anonymous FTP shell message

Name	Title	Class
STKU_ANONSHELL	Anonymous FTP shell	1

To protect your computers

- ◆ Ensure that valid shells are not used for anonymous FTP accounts.

Network Integrity (Windows)

SU 18 includes two new checks and messages.

NetBIOS info via SNMP

This check reports a problem if NetBIOS information is available through SNMP.

[Table 1-82](#) lists the message for this check.

Table 1-82 NetBIOS information message

Name	Title	Code	Class
NETBIOS_VIA_SNMP	NetBIOS info via SNMP	C	3

To protect your computers

- ◆ Do the following:
 - If a private community is reported, use the Correct feature in the console grid to change the Private value of HKEY_LOCAL_MACHINE\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities to 1.
 - If a public community is reported, use the Correct feature in the console grid to change the Public value of HKEY_LOCAL_MACHINE\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities to 1.

Anonymous SID/name translation (Windows 2003)

This check reports Group Policy settings that allow anonymous SID/name translation.

An anonymous user who knows an administrator's SID can use the SID to obtain the administrator's name.

[Table 1-83](#) lists the message for this check.

Table 1-83 Anonymous SID/name translation message

Name	Title	Code	Class
ANONYMOUS_SID_NAME_TRANSLATION	Anonymous SID/name translation allowed	SU	3

To protect your computers

- ◆ Disable Local Policies/Security Options/Network Access: Allow anonymous SID/Name translation.

Password Strength (Windows)

SU 18 includes one new check and message.

Password stored with reversible encryption (Windows 2000/XP/2003)

This check reports domain accounts with passwords that are stored with reversible encryption.

[Table 1-84](#) lists the message for this check.

Table 1-84 Reversible password encryption message

Name	Title	Class
REVERSIBLE_ENCRYPTION	Password stored with reversible encryption	1

To protect your computers

- ◆ Disable Local Policies/Account Policies/Password Policy/Store password using reversible encryption for all users in the domain.

Registry (Windows)

SU 18 includes one new option and a new template field.

Automatically update snapshots (Windows 2000/XP/2003)

Enable this option to automatically update snapshots with current agent information.

When snapshots are automatically updated, snapshot-updateable (SU) messages display Snapshot updated in the Updateable/Correctable field and report the type of change in the message Info field.

[Table 1-85](#) lists the new message that is reported when automatic updates fail.

Table 1-85 Automatic snapshot update messages

Name	Title	Code	Class
AUTO_UPDATE_FAILED	Automatic update failed		0

Registry template

Use the Report once on wildcarded mandatory keys check box to specify whether to report one message or multiple messages for missing mandatory keys that use wildcard characters.

Do one of the following:

- Check the Report once on wildcarded mandatory keys check box to report only one message for all missing mandatory keys that use wildcard characters.
- Uncheck the check box to report messages for every possible wildcard expansion of missing mandatory keys.

Startup Files (UNIX)

SU 18 includes a template enhancement.

Services template

The Services template in SU 18 includes a new field where you can specify whether to report only running services, services in inetd/xinetd, or both.

- ◆ Click the Source field, then select one of the following:

Either Report either inetd/xinetd or running processes

Process Report only running processes

Inetd Report only inetd/xinetd services

System Auditing (Windows)

SU 18 includes three new checks and messages.

Application event log size

This check reports a problem when the maximum size (kilobytes) of the application event log is less than the size that you specified in the check.

[Table 1-86](#) lists the message for this check.

Table 1-86 Application event log size message

Name	Title	Code	Class
APP_LOG_SIZE_SMALL	Application event log size is too small	C	1

To protect your computers

- ◆ Use the Correct feature in the console grid to increase the agent's setting for maximum size of the application event log to match the template setting.

System event log size

This check reports a problem when the maximum size (kilobytes) of the system event log is less than the size that you specified in the check.

[Table 1-87](#) lists the message for this check.

Table 1-87 System event log size message

Name	Title	Code	Class
SYS_LOG_SIZE_SMALL	System event log size is too small	C	1

To protect your computers

- ◆ Use the Correct feature in the console grid to increase the agent's setting for maximum size of the system event log to match the template setting.

Guest access to event logs

This check reports application, system, or security event logs that the Guest account can access.

[Table 1-88](#) lists the message for this check.

Table 1-88 Guest access to event log message

Name	Title	Code	Class
EVENTLOG_RESTRICT_ACCESS	Guest can access event log	C	1

To protect your computers

- ◆ Use the Correct feature in the console grid to set the RestrictGuestAccess value of the Application, System, and Security registry keys in HKEY_LOCAL_MACHINE\CurrentControlSet\Services\Eventlog to 1. If the key does not exist, it will be created with a RestrictGuestAccess value of 1. This prevents Guest access to event log files.

Resolved issues

The following issues have been resolved:

Disk Quota (Windows 2000)	<p>When the operating system's default setting for new users on the volume is No Limit, the Info field of the Tracked quotas not enforced message now reports default volume limit: No limit. Tracked quotas not enforced is reported by Volume quota not enforced.</p> <p>The severity level of Tracked quotas not enforced is now green (0).</p>
File Attributes (UNIX)	<p>UIDs 0-99 are now considered privileged users on all UNIX platforms. GIDs 0-99 are for privileged groups, except on Linux platforms, where 0-499 are privileged.</p>
File Attributes (Solaris)	<p>Exclude decreased permissions does not disregard permissions that have increased for file owners.</p>
File Find (UNIX)	<p>Setgid files no longer reports File is setgid when file locking is used.</p>
File Watch (Windows)	<p>Removed files now consistently reports files that have been removed based on the Depth level that is specified in the File Watch template.</p>
Login Parameters (UNIX)	<p>When sulog is examined for Inactive accounts, the Inactive accounts message now also reports the year that the user last logged in.</p>
Network Integrity (Windows)	<p>When only RRAS enabled is enabled, two system errors are no longer improperly reported:</p> <p>The specified service does not exist as an installed service.</p> <p>Error trying to determine if the LANMan server service is running.</p>
Network Integrity (UNIX)	<p>Anonymous FTP enabled now also detects anonymous FTP user entries in <code>/etc/ftpusers</code>.</p> <p>FTP session logging disabled now correctly interprets <code>syslog.conf</code> files that contain daemon info fields after the file name in the configuration file (<code>syslog.conf</code>).</p>
OS Patches (Windows)	<p>When Registry keys is the only check or option enabled in the module, Registry checking cannot be performed on file-only patch is reported.</p>

OS Patches (Windows NT)	The current Patch template now contains file versions. This eliminates false reports of Cannot determine patch status messages with No Version information supplied, unable to do version check in the Info field.
OS Patches (HP-UX)	When Superseded is disabled and a superseding patch is installed, the module no longer reports superseded patches.
Password Strength (AIX)	Maximum password age and Minimum password age no longer report password age violations for locked or disabled accounts.

Documentation updates

The following installation information supersedes Table 3-2 on pages 56-57 of the *Symantec Enterprise Security Manager Installation Guide* v. 6.0.

[Table 1-89](#) lists the minimum free disk space requirements.

Table 1-89 Free disk space computer resources

Platforms	Manager and agent	Agent
AIX	148 MB	125 MB
HP-UX	132 MB	112 MB
Red Hat Linux	Not supported	49 MB
SGI Irix	Not supported	140 MB
Solaris	114 MB	97 MB
Tru/OSF1	Not supported	140 MB

System requirements

SU 18 adds support for Red Hat Linux Enterprise Server and SUSE LINUX Standard Server.

[Table 1-90](#) lists the supported operating systems for SU 18.

Table 1-90 SU 18 supported operating systems

Agent operating system	Versions
AIX	4.2.1, 4.33, 5.1, 5.2
HP Tru64/OSF1	4.0D to 5.1A
HP-UX	10.20, 11, 11.11
Red Hat Linux	7x
Red Hat Linux Enterprise Server (ES) (x86)	2.1, 3.0
Solaris	2.5.1, 2.6, 2.7, 2.8, 2.9
SUSE LINUX Standard Server	8
Windows 2000 Professional and Server (Intel)	SP1+
Windows NT	4.0 SP6a
Windows Server 2003	All
Windows XP Professional (Intel)	All

SU 18 may run on newer versions of the supported operating systems, but Symantec reserves the right to certify the Security Update on the new versions before officially supporting them.

The LiveUpdate installation of SU 18 on all supported operating systems requires approximately 560 MB on each Symantec ESM manager.

The amount of disk space required by each agent depends on its operating system.

[Table 1-91](#) lists the agent disk space requirements.

Table 1-91 SU 18 agent disk space requirements

Agent operating system	SU 18
AIX	92 MB
HP Tru64/OSF1	67 MB
HP-UX	72 MB

Table 1-91 SU 18 agent disk space requirements

Agent operating system	SU 18
Red Hat Linux	36 MB
Red Hat Linux Enterprise Server (ES)	36 MB
Solaris	58 MB
SUSE LINUX Standard Server 8	36 MB
Windows 2000 Professional or Server (Intel)	31 MB
Windows NT (Intel)	31 MB
Windows Server 2003	31 MB
Windows XP Professional (Intel)	31 MB

Frequently asked questions

The following information applies to all Security Updates.

- | | |
|---|---|
| Do the security checks in new Security Updates replace the security checks on my agent systems? | Yes. |
| How can I preserve my customized settings? | Template file settings are retained. Template data is stored in the /esm/template directory.
Policy settings such as identification of enabled security checks and related name lists are retained.
Changes to message text in .m files are retained only if you also change the message's .customized directive to 1.
See the <i>Symantec ESM Security Update User's Guides</i> .
All other .m file changes are overwritten. |
| How do I install the Security Update release? | The standard method is to use the LiveUpdate feature in the Symantec ESM console.
You can also use files from a CD or the Internet to install the update manually. See the <i>Symantec ESM Security Update User's Guides</i> . |
| How can I be notified when new Symantec offerings or updates are available? | Subscribe to the Symantec Enterprise Security Manager technical support bulletin at: http://www.symantec.com/techsupp/bulletin/index.html .
You will be notified by e-mail when new products, Symantec ESM versions, Security Updates, OS Patch Policies, OS and Regulatory Policies, and Response Policies are released. |

Index

Numerics

- 9 PAM functionality
 - Password Strength (Solaris) module 30

A

- Account Integrity (UNIX) module
 - Duplicate IDs 75
 - Privileged users and groups 75
 - Reserved GID ranges 76
 - Reserved UID ranges 76
 - Reserved UID/GID 75
 - resolved issue 71, 94
- Account Integrity (Windows) module
 - Disabled/expired/locked accounts 73
 - Group member watch 97
- Account Integrity (Windows) templates
 - Group Member Watch 98
- Account Integrity (Windows/UNIX) module
 - Automatically update snapshots 77
- Account lockout threshold
 - Login Parameters (Windows) module 86
- Account Policies - Account Lockout Policy 22
- Account Policies - Password Policy
 - Group Policy (Win2S, Win3S) module 21
- Active Directory (Windows) checks
 - Enforce user logon restrictions 77
 - Maximum lifetime for service ticket 78
 - Maximum lifetime for user ticket 78
 - Maximum lifetime for user ticket renewal 79
 - Maximum tolerance for computer clock synchronization 79
- Active Directory Services (Windows) module
 - Security Options 39
- Anonymous FTP shell
 - Network Integrity (UNIX) module 110
- Anonymous SID/name translation
 - Network Integrity (Windows) module 111
- Application event log size
 - System Auditing (Windows) module 113
- Approved Wrappers
 - Startup Files (UNIX) module 70

- Auditing ACL
 - Auditing ACL 14
- Auditing permissions
 - Auditing permissions 15
- Automatically update snapshots
 - Account Integrity (Windows/UNIX) module 77
 - File Attributes (UNIX) module 100
 - File Attributes (Windows) module 100
 - File Attributes (Windows/UNIX) module 80
 - File Find (UNIX) module 82
 - File Watch (Windows) module 108
 - Network Integrity (Windows/UNIX) module 86
 - Object Integrity (UNIX) module 88
 - Registry (Windows) module 92, 112
 - Startup Files (Windows/UNIX) module 93

C

- Conditions sublist
 - File Content Search template 51

D

- Directories/files/types excluded
 - File Find (UNIX) module 82
- Disabled/expired/locked accounts
 - Account Integrity (Windows) module 73
- Disallow services cont
 - Startup (Windows2000/ NT/ XP/ 2003) module 31
- Disk Quota (Windows 2000) module
 - resolved issue 115
- Display name as distinguished name
 - Password Strength (Windows) module 90
- Duplicate IDs
 - Account Integrity (UNIX) module 75

E

- Enforce user logon restrictions
 - Active Directory (Windows) module 77
- Event Log
 - Group Policy (Win2S, Win3S) module 25

Event Log Info

File Attributes (Windows) module 43

File Watch (Windows) module 56

Excessive failed su attempts for users

Login Parameters (UNIX) module 59

Excessive successful su attempts for users

Login Parameters (UNIX) module 61

executable code

File Attributes (Windows) module 102

F

File ACL

File Attributes (Windows) module 14

File and folder attributes

File Attributes (Windows) module 100

File and folder ownership

File Attributes (Windows) module 101

File Attributes (LINUX) module 20

File Attributes (Solaris) module

resolved issue 115

File Attributes (SUSE ES) module

SUSE ES templates 41

File Attributes (UNIX) module

Automatically update snapshots 100

Group ownership 106

Keywords list 103

NFS exported files 41

Permissions 106

resolved issue 115

Specifying files to check 42

User ownership 106

File Attributes (UNIX) templates

New File 81, 103

File Attributes (Windows) module 14

Event Log Info 43

executable code 102

File ACL 14

File and folder attributes 100

File and folder ownership 101

File Version 42

File Attributes (Windows) options

Automatically update snapshots 100

File Attributes (Windows) templates

File 80, 101

File Keywords 102

File Attributes (Windows/UNIX) module

Automatically update snapshots 80

resolved issue 71, 94

File Attributes (WinNT, Win2K, Win3S,

WinXP)module

file version field 20

File Content Search template,

Conditions sublist 51

File List sublist 47

File Find (UNIX) module

Automatically update snapshots 82

Directories/files/types excluded 82

excluding by file type 83

resolved issue 115

File Find (UNIX) templates

File Content Search 84, 107

File Find (Windows) module

FileFind keywords 44

Windows file content search 44

File List sublist

File Content Search template 47

File System

Group Policy (Win2S, Win3S) module 28

File System Auto-Protected

Symantec Product Information (All

Windows) 33

File Version

File Attributes (Windows) module 42

File Watch (All) module

Ignore Directories 20

File Watch (Linux) module

Filter changed device ownership/

permissions 57

File Watch (Windows) checks

Automatically update snapshots 108

File Watch (Windows) module

Event Log Info 56

resolved issue 115

File Watch (Windows/UNIX) checks

Keywords list 85

File Watch (Windows/UNIX) module

Keywords list 84

File Watch (Windows/UNIX) templates

File Watch 85

FileFind keywords

File Find (Windows) module 44

Filter 32

Filter changed device ownership/permissions

File Watch (Linux) module 57

Filter disallow services not running

Startup (Windows 2000/ NT/ XP/ 2003)

module 32

Find File (UNIX) module

- Unprintable characters in file names 20
- folder ownership (Windows)
 - changed 101
- FX/path directives
 - System Mail (UNIX) module 34

G

- Group member watch
 - Account Integrity (Windows) module 97
- Group Member Watch (Windows) template
 - Member Of sublist 99
 - Members sublist 99
- Group ownership
 - File Attributes (UNIX) module 106
- Group Policy (Win2S, Win3S) module
 - Account Policies - Account Lockout Policy
 - Group Policy (Win2S, Win3S) module 22
 - Account Policies - Kerberos Policy 23
 - Account Policies - Password Policy 21
 - Event Log 25
 - File System 28
 - Local Policies - Audit Policy 23
 - Local Policies - Security Options 24
 - Local Policies - User Rights Assignment 24
 - Registry 27
 - Restricted Groups 26
 - System Services 26
- Guest access to event logs
 - System Auditing (Windows) module 114

I

- ICE (Windows/UNIX) module
 - resolved issue 71, 94
- ICMP messages
 - ICMP messages 15
- ICS exposed network services
 - Network Integrity (Windows 2003/XP)
 - module 65
- Ignore Directories
 - File Watch (All) module 20
- Inactive accounts with unchanged passwords
 - Login Parameters (UNIX) module 59
 - Login Parameters (Windows) module 58
- Internet 63
- Internet Connection Sharing
 - Network Integrity (Windows 2003/XP)
 - module 64
- IP Security Policies

- Network Integrity (Windows) module 87
- IPv6 Protocol
 - Network Integrity (Windows 2003/XP)
 - module 62

K

- Key permissions
 - Registry (Windows) module 15
- Keywords list
 - File Attributes (UNIX) module 103
 - File Watch (Windows/UNIX) module 84, 85
- Known issues, SU 19 93
- Known issues, SU 21 34

L

- Local Policies - Audit Policy
 - Group Policy (Win2S, Win3S) module 23
- Local Policies - Security Options
 - Group Policy (Win2S, Win3S) module 24
- Local Policies - User Rights Assignment
 - Group Policy (Win2S, Win3S) module 24
- Login Parameters (UNIX) module
 - Excessive failed su attempts for users 59
 - Excessive successful su attempts for users 61
 - Inactive accounts with unchanged
 - passwords 59
 - resolved issue 71, 94, 115
 - Warning banners 109
- Login Parameters (Windows) checks
 - Account lockout threshold 86
- Login Parameters (Windows) module
 - Inactive accounts with unchanged
 - passwords 58

M

- Maximum lifetime for service ticket
 - Active Directory (Windows) module 78
- Maximum lifetime for user ticket
 - Active Directory (Windows) module 78
- Maximum lifetime for user ticket renewal
 - Active Directory (Windows) module 79
- Maximum tolerance for computer clock
 - synchronization
 - Active Directory (Windows) module 79

N

- NetBIOS info via SNMP

- Network Integrity (Windows) module 110
- Network (WinNT, Win2K, Win3S, WinXP) module
 - Shared folders giving all users Full Control 29
- Network Integrity (Solaris, HP-UX, AIX, RedHat) module
 - Promiscuous mode 29
- Network Integrity (UNIX) checks
 - Anonymous FTP shell 110
- Network Integrity (UNIX) module
 - Exported non-secure exclude list
 - Network Integrity (UNIX) module 69
 - resolved issue 94, 115
 - SNMP config file path 67
 - SNMP default community strings 68
 - SNMP v3 encryption 69
 - SNMP version 69
 - SNMP write access 68
- Network Integrity (Windows 2003/XP) module
 - ICS exposed network services 65
 - Internet Connection Sharing 64
 - IPv6 Protocol 62
- Network Integrity (Windows XP/2003) module 15
- Network Integrity (Windows) module
 - Anonymous SID/name translation 111
 - IP Security Policies 87
 - NetBIOS info via SNMP 110
 - resolved issue 94, 115
- Network Integrity (Windows/UNIX) module
 - Automatically update snapshots 86
- NFS exported files
 - File Attributes (UNIX) module 41

O

- Object Integrity (UNIX) module
 - Automatically update snapshots 88
- OS Patches
 - SUSE LINUX 97
 - Windows NT 116
- OS Patches (AIX) templates
 - Patches 88
- OS Patches (Solaris/HP-UX) templates
 - Patches 89
- OS Patches (SUSE ES 8) module
 - Patch.psl template 70
- OS Patches (Windows) module
 - resolved issue 115

P

- Password stored with reversible encryption
 - Password Strength (Windows) module 91, 111
- Password Strength (AIX) module
 - resolved issue 116
- Password Strength (Solaris) module
 - 9 PAM functionality 30
- Password Strength (UNIX) module
 - Repeating characters 15
- Password Strength (Win2k, 3s) module
 - Passwords stored using reversible encryption 31
- Password Strength (Windows) module
 - Display name as distinguished name 90
 - Password stored with reversible encryption 91, 111
- Password Strength (Windows/UNIX) module
 - resolved issue 94
- Passwords stored using reversible encryption
 - Password Strength (Win2k, 3s) module 31
- Patch.psl template
 - OS Patches (SUSE ES 8) 70
 - OS Patches (SUSE ES8) module 70
- Permissions
 - File Attributes (UNIX) module 106
- Privileged users and groups
 - Account Integrity (UNIX) module 75
- Promiscuous mode
 - Network Integrity (Solaris, HP-UX, AIX, RedHat) module 29

R

- Registry
 - Group Policy (Win2S, Win3S) module 27
- Registry (Windows) module 15
 - Automatically update snapshots 92, 112
 - Key permissions 15
- Registry (Windows) templates
 - Registry 92, 112
- Repeating characters
 - Password Strength (UNIX) module 15
- Reserved GID ranges
 - Account Integrity (UNIX) module 76
- Reserved UID ranges
 - Account Integrity (UNIX) module 76
- Reserved UID/GID
 - Account Integrity (UNIX) module 75
- Resolved issues, SU 21 36

Resolved issues, SU 22 16
 Restricted Groups
 Group Policy (Win2S, Win3S) module 26

S

Security Options
 Active Directory Services (Windows)
 module 39
 SESE ES templates
 File Attributes (SUSE ES) module 41
 Shared folders giving all users Full Control
 Network (WinNT, Win2K, Win3S, WinXP)
 module 29
 SNMP config file path
 Network Integrity (UNIX) module 67
 SNMP default community strings
 Network Integrity (UNIX) module 68
 SNMP v3 encryption
 Network Integrity (UNIX) module 69
 SNMP version
 Network Integrity (UNIX) module 69
 SNMP write access
 Network Integrity (UNIX) module 68
 Specifying files to check
 Files Attributes (UNIX) module 42
 Startup (Windows 2000/ NT/ XP/ 2003) module
 Filter disallow services not running 32
 Startup (Windows2000/ NT/ XP/ 2003) module
 Disallow services cont. 31
 Startup Files (UNIX) module
 Approved Wrappers 70
 Startup Files (UNIX) templates
 Services 112
 Startup Files (Windows/UNIX) module
 Automatically update snapshots 93
 SUSE LINUX Standard Server 8 97
 installation 97
 Symantec Product Information (All Windows)
 File System Auto-Protected 33
 System Auditing (Windows) module
 Application event log size 113
 Guest access to event logs 114
 System event log size 114
 System event log size
 System Auditing (Windows) module 114
 System Mail (UNIX) module
 FX/path directives 34
 System requirements
 SU19 95

System requirements, SU 21 38
 System requirements, SU 22 17
 System Services
 Group Policy (Win2S, Win3S) module 26

T

templates
 File (Windows) 80, 101
 File Content Search (UNIX) 84, 107
 File Keywords (Windows) 102
 File Watch (Windows/UNIX) 85
 Group Member Watch (Windows) 98
 New File (UNIX) 81, 103
 Patches (AIX) 88
 Patches (Solaris/HP-UX) 89
 Registry (Windows) 92, 112
 Services (UNIX) 112
 tpk
 Update Report Content 19

U

Unprintable characters in file names
 Find File (UNIX) module 20
 Update Report Content
 tpk 19
 User ownership
 File Attributes (UNIX) module 106

W

Warning banners
 Login Parameters (UNIX) module 109
 Windows file content search
 File Find (Windows) module 44

