

# Symantec Enterprise Security Manager™ Security Update 19.01 Release Notes

Symantec ESM 6.0, and 5.5

For Windows, UNIX, and Linux modules

# Symantec ESM Security Update 19.01 Release Notes

The software that is described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.  
040719

## Copyright Notice

Copyright © 2004 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, and Windows NT 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 and security alerts.

Symantec technical support offerings include:

- A range of support options that gives you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, that offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features that are available may vary based on the level of support purchased and the specific product that you are using.

## Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at [www.symantec.com/certificate](http://www.symantec.com/certificate). Alternatively, you may go to [www.symantec.com/techsupp/ent/enterprise.htm](http://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](http://www.symantec.com/techsupp).

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at [www-secure.symantec.com/platinum/](http://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](http://www.symantec.com), select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

# Symantec Software License Agreement

## Symantec Enterprise Security Manager

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

### 1. License:

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

#### You may:

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

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

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

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

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

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

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

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

#### You may not:

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

### 2. Content Updates:

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

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

### 3. Limited Warranty:

Syantec 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

Security Update 19.01 .....	13
Security Update 19 .....	14
Account Integrity (Windows) .....	14
Disabled/expired/locked accounts (Windows) .....	15
Account Integrity (UNIX) .....	15
Duplicate IDs (UNIX) .....	15
Reserved UID/GID (UNIX) .....	16
Reserved UID ranges (UNIX) .....	16
Reserved GID ranges (UNIX) .....	16
Account Integrity (Windows/UNIX) .....	17
Automatically update snapshots (Windows/UNIX) .....	17
Active Directory (Windows) .....	17
Enforce user logon restrictions (Windows 2000/2003) .....	17
Maximum lifetime for service ticket (Windows 2000/2003) .....	18
Maximum lifetime for user ticket (Windows 2000/2003) .....	18
Maximum lifetime for user ticket renewal (Windows 2000/2003) .....	19
Maximum tolerance for computer clock synchronization (Windows 2000/2003) .....	19
File Attributes (Windows/UNIX) .....	20
Automatically update snapshots (Windows NT/UNIX) .....	20
File Attributes (Windows) .....	20
File template (Windows) .....	20
File Attributes (UNIX) .....	21
New File template (UNIX) .....	21
File Find (UNIX) .....	22
Automatically update snapshots (UNIX) .....	22
Directories/files/types excluded (UNIX) .....	22
Excluding by file type enhancement (UNIX) .....	23
File Content Search template (UNIX) .....	24
File Watch (Windows/UNIX) .....	25
Keywords list (Windows/UNIX) .....	25
File Watch template (Windows/UNIX) .....	25
File Watch template (Windows 2000/XP/2003/UNIX) .....	25
Login Parameters (Windows) .....	26
Account lockout threshold (Windows) .....	26
Network Integrity (Windows/UNIX) .....	26
Automatically update snapshots (Windows/UNIX) .....	26

Network Integrity (Windows) .....	27
IP Security Policies (Windows XP/2000/2003) .....	27
Object Integrity (UNIX) .....	28
Automatically update snapshots (UNIX) .....	28
OS Patches (AIX) .....	28
Patch template (AIX) .....	28
OS Patches (Solaris/HP-UX) .....	29
Patch template (Solaris/HP-UX) .....	29
Password Strength (Windows) .....	30
Display name as distinguished name (Windows 2000/XP/2003) .	30
Password stored using reversible encryption (Windows 2000/XP/2003)	31
Registry (Windows) .....	32
Automatically update snapshots (Windows NT) .....	32
Registry template (Windows XP/2003) .....	32
Startup Files (Windows/UNIX) .....	33
SU 19 includes one new option and message. ....	33
Automatically update snapshots (Windows/UNIX) .....	33
Known issues .....	33
Resolved issues .....	34
System requirements .....	35
Security Update 18 .....	37
SUSE LINUX .....	37
Account Integrity (Windows) .....	37
Group member watch (Windows 2000/XP/2003) .....	37
Group Member Watch template .....	38
File Attributes (Windows/UNIX) .....	40
Automatically update snapshots (Windows 2000/XP/2003/UNIX)	40
File Attributes (Windows) .....	40
File and folder attributes .....	40
File and folder ownership .....	41
File template .....	41
File Keywords template .....	42
File Attributes (UNIX) .....	42
Keywords list .....	42
New File template .....	43
Permissions .....	45
User ownership .....	45
Group ownership .....	45
File Find (UNIX) .....	46
File Watch (Windows/UNIX) .....	47
Automatically update snapshots (Windows 2000/XP/2003/UNIX)	47
Login Parameters (UNIX) .....	48

Warning banners .....	48
Network Integrity (UNIX) .....	49
Anonymous FTP shell .....	49
Network Integrity (Windows) .....	49
NetBIOS info via SNMP .....	49
Anonymous SID/name translation (Windows 2003) .....	50
Password Strength (Windows) .....	50
Password stored with reversible encryption (Windows 2000/XP/2003)	
50	
Registry (Windows) .....	51
Automatically update snapshots (Windows 2000/XP/2003) .....	51
Registry template .....	51
Startup Files (UNIX) .....	51
Services template .....	51
System Auditing (Windows) .....	52
Application event log size .....	52
System event log size .....	53
Guest access to event logs .....	53
Resolved issues .....	54
Documentation updates .....	55
System requirements .....	56
Frequently asked questions .....	58



# Symantec ESM Security Update Release Notes

This document describes security updates for Symantec Enterprise Security Manager, 6.0, and 5.5 that have been released since the latest *Symantec Enterprise Security Manager Security Update User's Guides* were published. Additional security updates will be added to this document until the next version of Symantec ESM is released. At that time, the contents of this document will be moved into new Security Update User's Guides.

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 19.01

In Security Update 19 a keyword template is shared between the File Watch and the File Attributes modules. The Symantec ESM template database can only associate one module to each template. As a result, whichever module registers first loses its association with the keyword template when the second module registers.

Any policies that exist at the time of updating to SU 19 that include the File Attributes module will not be associated with the correct File Attributes Keyword template.

---

**Note:** If you install Security Update 19.01 on top of SU 18 or earlier, you will not experience the template problem. This problem only applies to customers that have upgraded to SU 19.

---

The following is a resolution to the template problem:

- The version of fileatt.m was increased to force a register (in case the File Attributes module lost its association)
- A new template extension (.fk2) was created and added to the fwatch\*.m files
- A new association was made in fwatch\*.m between the check and the template named File Watch Keywords to avoid the conflict from fileatt.m's File Keywords. See [To repair these policies](#).
- The version of each fwatch\*.m was changed.
- All manifest.xml files are updated to include the new MD5 sums of the changed files.

#### **To repair these policies**

- 1 Open the policy to edit.
- 2 Note the enabled checks in the File Watch module.
- 3 Remove the File Watch module from the policy.
- 4 Click OK.
- 5 Open the same policy again.
- 6 Add the File Watch module to the policy and enable the checks.
- 7 Click OK.

## **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.

The check returns the following message:

Disabled/expired/locked accounts message

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

## Account Integrity (UNIX)

SU 19 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.

The check returns the following messages:

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)**

This option lets you 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.

A message is reported when automatic updates fail.

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.

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.

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.

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.

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.

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.

A message is reported when automatic updates fail

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.

A message is reported when automatic updates fail.

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.

A message is reported when automatic updates fail.

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 XP/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.

The check returns the following messages:

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.

A message is reported when automatic updates fail.

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)

SU 19 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 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/XP/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/XP/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 with 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.

---

Reversible password encryption message

Message name	Title	Severity
REVERSIBLE_ENCRYPTION	Password stored with 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.

A message is reported when automatic updates fail.

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.

A message is reported when automatic updates fail.

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

SU 19 supports the following operating systems

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:

SU 19 agent disk space requirements

<b>Agent operating system</b>	<b>SU 18</b>
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 RedHat 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.

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 console 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 39.

---

**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 39.

---

**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.

A new message is reported when automatic updates fail

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.

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.

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.

The following examples illustrate how to use wildcard characters for directory and file names.

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
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\temp, C:\Windows\time, C:\Win32\tims
	Does not match C:\Won\temp, C:\Windows\timber, C:\Windows\tim, C:\Windows\time\otherdir

### Wildcard functionality

Example	Description/Examples
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.

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

This check now also reports a directory permissions message.

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

This check now also reports a directory permissions message.

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

This check now also reports a directory permissions message.

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.

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

This check now also performs the following actions.

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.

Anonymous FTP shell message

Name	Title	Class
STKU_ANONHELL	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.

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 KEY\_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.

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.

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.

A new message is reported when automatic updates fail.

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.

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.

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.

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.

The computers must meet the minimum free disk space requirements in Table 3-2.

**Table 3-2** 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.

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:

SU 18 agent disk space requirements

Agent operating system	SU 18
AIX	92 MB
HP Tru64/OSF1	67 MB
HP-UX	72 MB
Red Hat Linux	36 MB
Red Hat Linux Enterprise Server (ES)	36 MB

## SU 18 agent disk space requirements

<b>Agent operating system</b>	<b>SU 18</b>
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 *Symantec ESM Security Update User's Guides*.

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 *Symantec ESM Security Update User's Guides*.

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

## A

- Account Integrity (UNIX) module
  - Duplicate IDs 15
  - Privileged users and groups 16
  - Reserved GID ranges 16
  - Reserved UID ranges 16
  - Reserved UID/GID 16
  - resolved issue 34
- Account Integrity (Windows) module
  - Disabled/expired/locked accounts 15
  - Group member watch 37
- Account Integrity (Windows) templates
  - Group Member Watch 38
- Account Integrity (Windows/UNIX) module
  - Automatically update snapshots 17
- Account lockout threshold
  - Login Parameters (Windows) module 26
- Active Directory (Windows) checks
  - Enforce user logon restrictions 17
  - Maximum lifetime for service ticket 18
  - Maximum lifetime for user ticket 18
  - Maximum lifetime for user ticket renewal 19
  - Maximum tolerance for computer clock synchronization 19
- Anonymous FTP shell
  - Network Integrity (UNIX) module 49
- Anonymous SID/name translation
  - Network Integrity (Windows) module 50
- Application event log size
  - System Auditing (Windows) module 52
- Automatically update snapshots
  - Account Integrity (Windows/UNIX) module 17
  - File Attributes (UNIX) module 40
  - File Attributes (Windows) module 40
  - File Attributes (Windows/UNIX) module 20
  - File Find (UNIX) module 22
  - File Watch (Windows) module 47
  - Network Integrity (Windows/UNIX) module 26
  - Object Integrity (UNIX) module 28
  - Registry (Windows) module 32, 51
  - Startup Files (Windows/UNIX) module 33

## D

- Directories/files/types excluded
  - File Find (UNIX) module 22
- Disabled/expired/locked accounts
  - Account Integrity (Windows) module 15
- Disk Quota (Windows 2000) module
  - resolved issue 54
- Display name as distinguished name
  - Password Strength (Windows) module 30
- Duplicate IDs
  - Account Integrity (UNIX) module 15

## E

- Enforce user logon restrictions
  - Active Directory (Windows) module 17
- executable code
  - File Attributes (Windows) module 42

## F

- File and folder attributes
  - File Attributes (Windows) module 40
- File and folder ownership
  - File Attributes (Windows) module 41
- File Attributes (Solaris) module
  - resolved issue 54
- File Attributes (UNIX) module
  - Automatically update snapshots 40
  - Group ownership 45
  - Keywords list 42
  - Permissions 45
  - resolved issue 54
  - User ownership 45
- File Attributes (UNIX) templates
  - New File 21, 43
- File Attributes (Windows) module
  - executable code 42
  - File and folder attributes 40
  - File and folder ownership 41
- File Attributes (Windows) options
  - Automatically update snapshots 40

- File Attributes (Windows) templates
  - File 20, 41
  - File Keywords 42
- File Attributes (Windows/UNIX) module
  - Automatically update snapshots 20
  - resolved issue 34
- File Find (UNIX) module
  - Automatically update snapshots 22
  - Directories/files/types excluded 22
  - excluding by file type 23
  - resolved issue 54
- File Find (UNIX) templates
  - File Content Search 24, 46
- File Watch (Windows) checks
  - Automatically update snapshots 47
- File Watch (Windows) module
  - resolved issue 54
- File Watch (Windows/UNIX) checks
  - Keywords list 25
- File Watch (Windows/UNIX) module
  - Keywords list 24
- File Watch (Windows/UNIX) templates
  - File Watch 25
- folder ownership (Windows)
  - changed 41

**G**

- Group member watch
  - Account Integrity (Windows) module 37
- Group Member Watch (Windows) template
  - Member Of sublist 39
  - Members sublist 39
- Group ownership
  - File Attributes (UNIX) module 45
- Guest access to event logs
  - System Auditing (Windows) module 53

**I**

- ICE (Windows/UNIX) module
  - resolved issue 34
- IP Security Policies
  - Network Integrity (Windows) module 27

**K**

- Keywords list
  - File Attributes (UNIX) module 42
  - File Watch (Windows/UNIX) module 24, 25

- Known issues, SU 19 33

## L

- Login Parameters (UNIX) module
  - resolved issue 34, 54
  - Warning banners 48
- Login Parameters (Windows) checks
  - Account lockout threshold 26

## M

- Maximum lifetime for service ticket
  - Active Directory (Windows) module 18
- Maximum lifetime for user ticket
  - Active Directory (Windows) module 18
- Maximum lifetime for user ticket renewal
  - Active Directory (Windows) module 19
- Maximum tolerance for computer clock
  - synchronization
    - Active Directory (Windows) module 19

## N

- NetBIOS info via SNMP
  - Network Integrity (Windows) module 49
- Network Integrity (UNIX) checks
  - Anonymous FTP shell 49
- Network Integrity (UNIX) module
  - resolved issue 34, 54
- Network Integrity (Windows) module
  - Anonymous SID/name translation 50
  - IP Security Policies 27
  - NetBIOS info via SNMP 49
  - resolved issue 34, 54
- Network Integrity (Windows/UNIX) module
  - Automatically update snapshots 26

## O

- Object Integrity (UNIX) module
  - Automatically update snapshots 28
- OS Patches
  - SUSE LINUX 37
  - Windows NT 55
- OS Patches (AIX) templates
  - Patches 28
- OS Patches (Solaris/HP-UX) templates
  - Patches 29
- OS Patches (Windows) module
  - resolved issue 54

**P**

- Password stored with reversible encryption
  - Password Strength (Windows) module 31, 50
- Password Strength (AIX) module
  - resolved issue 55
- Password Strength (Windows) module
  - Display name as distinguished name 30
  - Password stored with reversible encryption 31, 50
- Password Strength (Windows/UNIX) module
  - resolved issue 34
- Permissions
  - File Attributes (UNIX) module 45
- Privileged users and groups
  - Account Integrity (UNIX) module 16

**R**

- Registry (Windows) module
  - Automatically update snapshots 32, 51
- Registry (Windows) templates
  - Registry 32, 51
- Reserved GID ranges
  - Account Integrity (UNIX) module 16
- Reserved UID ranges
  - Account Integrity (UNIX) module 16
- Reserved UID/GID
  - Account Integrity (UNIX) module 16

**S**

- Startup Files (UNIX) templates
  - Services 51
- Startup Files (Windows/UNIX) module
  - Automatically update snapshots 33
- SUSE LINUX Standard Server 8 37
  - installation 37
- System Auditing (Windows) module
  - Application event log size 52
  - Guest access to event logs 53
  - System event log size 53
- System event log size
  - System Auditing (Windows) module 53
- System requirements, SU19 35

**T**

- templates
  - File (Windows) 20, 41
  - File Content Search (UNIX) 24, 46

- File Keywords (Windows) 42
- File Watch (Windows/UNIX) 25
- Group Member Watch (Windows) 38
- New File (UNIX) 21, 43
- Patches (AIX) 28
- Patches (Solaris/HP-UX) 29
- Registry (Windows) 32, 51
- Services (UNIX) 51

**U**

- User ownership
  - File Attributes (UNIX) module 45

**W**

- Warning banners
  - Login Parameters (UNIX) module 48

