

Symantec Enterprise Security Manager™ Security Update 24 Release Notes

Symantec ESM 6.0, 6.1.1, and 6.5

For Windows, UNIX, and Linux modules

Symantec ESM Security Update 24 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.
050929

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 <https://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”, “ACCEPT” 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”, “I DO NOT ACCEPT” 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 the number of copies of the Software as have been licensed to You by Symantec under a License Module. If the Software is part of a suite containing multiple Software titles, the number of copies You may use may not exceed the aggregate number of copies indicated in the License Module, as calculated by any combination of licensed Software titles. Your License Module shall constitute proof of Your right to make such copies. 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 computer;
- 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 on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;
- D. use the Software in accordance with any written agreement between You and Symantec; and
- E. 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 in writing to the terms of this license.

You may not:

- A. copy the printed documentation that accompanies the Software;
- B. 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;
- C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
- D. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
- E. 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;
- F. 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 permission in a License Module; nor
- G. 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: antispam software utilize updated antispam rules; antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; policy compliance software utilize updated policy compliance updates; and vulnerability assessment products utilize updated vulnerability signatures; 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 thirty (30) 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:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. Licensee agrees to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in

connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

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 Customer Service Center, PO BOX 5689, Dublin 15, Ireland , or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

8. Additional Uses and Restrictions:

A. Required Software Installation and Activation: There may be technological measures in this Software that are designed to prevent unlicensed or illegal use of the Software. You agree that Symantec may use these measures. You must register the Software functions and any associated maintenance and support that are controlled by these technological measures through the use of the Internet. Symantec cannot guarantee that use of the Internet will be uninterrupted. Symantec will maintain your registration details.

B. If the Software You have licensed is Symantec Enterprise Security Manager, notwithstanding any of the terms and conditions contained herein, the following additional terms apply to the Software:

1. Permission to use the software to assess Desktop, Server, or Network devices does not constitute permission to make additional copies of the Software.

2. You may use the Software to assess up to the number of Desktop computers, on which a host-based agent is installed, as set forth under a License Module.. "Desktop" means a computer for a single end user.

3. You may use the Software to assess up to the number of Servers, on which a host-based agent is installed, as set forth under a License Module.. "Server" means a computer that is used to provide services to other computers via a network.

4. You may use the Software to assess up to the number of Virtual Machines, on which a host-based agent is installed, as set forth under a License Module.. "Virtual Machine" means a machine completely defined and implemented in software rather than hardware. Virtual Machines are run on a hosting Server and can function as a Server or Desktop.

5. You may use the Software to assess up to the number of unique Network Devices set forth under a License Module, which can be assessed by a network scan agent. "Network Devices" means an interconnected system of computers and devices.

C. If the Software you have licensed includes Cognos® Report Studio You may use the single (1) user license of Cognos Report Studio that is received with the Software only. Additional Cognos Report Studio licenses must be purchased separately.

Symantec ESM Security Update Release Notes

Security Update 24	3
New supported operating system	4
Changed messages	4
Account Integrity (Solaris)	4
Backup Integrity (Windows 2000/ 2003)	5
ICE (All)	6
Object Integrity (Solaris 10)	9
Password Strength (UNIX)	11
Startup (UNIX)	12
Resolved issues	12
System requirements	14

Symantec ESM Security Update Release Notes

These Symantec ESM Security Update Release Notes describe the security updates for Symantec Enterprise Security Manager 6.0, 6.1.1, and 6.5 that have been released since the latest Symantec Enterprise Security Manager Security Update user guides were published. Security updates will be added to the Symantec 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 24

The following are new in SU 24:

- Support for the following operating system:
 - Red Hat Enterprise Linux 4 ES (x86)
- Twelve new checks
- One new option
- Eighteen new messages
- Two changed messages
- Three new templates

New supported operating system

SU 24 includes the following newly-supported platform:

- Red Hat Enterprise Linux 4 ES (x86)

Changed messages

The Account Information module contains two messages that were reformatted in SU 24. This modification only affects Windows 2000/ 2003 agents that are running on domain controllers. See [“Account Information \(Widows 2000/ 2003\)”](#) on page 12.

Account Integrity (Solaris)

SU 24 includes two new checks, one new option, three new messages, and one new template in the Account Integrity module.

Role based access (Solaris)

This new check reports when the users, roles, or profiles on the agent do not match the template definition. Use the template list to include role based access templates.

[Table 3-1](#) shows the new message for the Role based access check.

Table 3-1 Role based access messages

Message name	Title	Severity
SKU_RBAC_MANDATORY_ATTRIB	Mandatory attribute not found	Red-4
STKU_RBAC_MANDATORY_ATTRIB	Forbidden attribute found	Red-4
STKU_RBAC_ABSENT_ATTRIB	Attribute not listed in template	Yellow-1

Role based access con't (Solaris)

Use the include/ exclude list in this new option to define the users, roles, and profiles that you want the Role based access check to audit.

Rbac attributes not in template (Solaris)

Use this new check to enable reporting of users, roles, and profiles that are found on the agent but are not listed in the template. Use the include/ exclude

list to define the users, roles, and profiles that should be reported as missing in the template.

Rbac template

Use the Add Attribute button in this new template to add user, role, and profile definitions. You may also add to the template subordinate roles or profiles assigned to the initial users, roles, or profiles using the depth options in the Add Attribute feature. The template contains four columns: Type, Name, Comment, and Attributes.

Type	Specify the type of attribute: User (u), Role (r), Profile (p).
Name	Type the name of the attribute. If you type ALL, all the users, roles, and profiles will be added.
Comment	Type the comment that you want to display in the info field of reported messages.
Attributes	List the mandatory/ forbidden/ optional attributes owned by the user, role, or profile.

Backup Integrity (Windows 2000/ 2003)

SU 24 includes three new checks and three new messages in the Backup Integrity module. These three new checks extend ESM integration to Veritas' Backup Exec product.

Backup Exec last backup status (Windows 2000/ 2003)

This new check reports Veritas Backup Exec jobs that complete their last run with an error or unsuccessful status. Use the include/ exclude name list to define the Backup Exec job runs that you want ESM to audit.

[Table 3-2](#) shows the new message for the Backup Exec last Backup Status check.

Table 3-2 Backup Exec last Backup Status message

Message name	Title	Severity
ESM_LAST_BACKUP_FAILED	Last backup job failed	Red-4

Backup Exec backup frequency (Windows 2000/ 2003)

This new check reports Veritas Backup Exec jobs that have a longer time interval between backups than what is specified in the template. This time

interval is the length of time between the end of the previous run and the beginning of the next scheduled run. Jobs not listed in the templates will not be reported.

[Table 3-3](#) shows the new message for the Backup Exec backup frequency check.

Table 3-3 Backup Exec backup frequency message

Message name	Title	Severity
ESM_BACKUP_ FREQUENCY	Job run interval too long	Red-4

Backup Exec Version (Windows 2000/ 2003)

This new check reports if the installed version of Veritas Backup Exec is earlier than the version that is specified in the value field. The version must be formatted as: <major version>.<minor version>. If only the major version is specified, the minor version is assumed to be zero.

[Table 3-4](#) shows the new message for the Backup Exec Version check.

Table 3-4 Backup Exec Version message

Message name	Title	Severity
ESM_BACKUP_VERSION	Backup Exec version out of date	Red-4

ICE (All)

SU 24 includes two new checks, three new messages, and one new template in the ICE module. Use the template load feature (Add Script button) in the template editor to add files to the ICE Scripts template.

To ensure that your system is as secure as possible when running these checks, you should define user permissions and ownership security settings within the template. When the template is created, you can define the path where the script should be written, the owner and group that is assigned to the file after transfer (UNIX only), and permissions that are assigned to the file after transfer (in the form rwxrwxrwx). Also, the checksum is used to make sure that the script has not been tampered with since it was imported into the template.

To further enhance the security of your system, you should use ESM Access Records to define separation of duties among ESM users. For more information on creating and using ESM Access Records see “Administering user accounts” on page 57 of the Symantec Enterprise Security Manager 6.5 Administrator’s Guide.

Following is an example of possible ESM user roles that illustrates how you could implement separation of duties using the ESM Access Records:

- **Super User Role**
Default ESM install user with all access rights. This role should be used to create accounts and modify other ESM users' access records.
- **Template Management Role**
This role should provide access rights to create and edit templates only. Assign TEMPLATES access rights to view, create, and modify templates.
- **Policy Management Role**
This role should provide access rights to create and edit policies only. Assign POLICIES access rights to view, create, and modify policies. Assign TEMPLATES access rights to view templates.
- **Policy Run/ Domain Management Role**
This role should provide access rights to run policies and manage domains only. Assign TEMPLATES access rights to view templates. Assign POLICIES access rights to run and view policies. Assign DOMAINS access rights to view, modify, and run policies, capture snapshot updates, and create domains.

As an added precaution, scripts can be pushed only to the ESM installation directory structure on the agent. This allows only users with permission to this folder to access the files. However, scripts pushed to these folders have no inherent restrictions on which files or folders they can modify. Sensitive files that are pushed to the agent should be deleted when they are no longer needed.

Note: When using the template load feature, #esm is prepended to the target destination listed in the template. #esm refers to the installation directory and must not be modified.

Copy scripts (All)

This new check copies the ICE scripts that are encoded in the enabled templates to the agents. When this check is enabled, the enabled templates are audited for template entries that have OS/Rev sublists that apply to the current agent. If the OS/Rev matches, the module writes the file to the location specified in the template.

Overwrite scripts (All)

This new check overwrites existing file signatures with the new one if the file signatures are different. When the Overwrite scripts check is disabled, it reports the ESMM_FILEEXISTS message if the file signature exists and is different.

Table 3-5 shows the new message for the Overwrite scripts check.

Table 3-5 Overwrite scripts messages

Message name	Title	Severity
ESMM_FILECOPIED	File copied successfully	Green-0
ESMM_FILEEXISTS	File exists	Yellow-2
ESMM_FILEBAD	Could not copy script	Red-4

ICE scripts template

Use this new template to add script files to a specific agent. The template contains nine columns: Path, Permissions, Owner, Group, CheckSum, Checksum hash, Comment, OS/ Rev, and File Data.

Path	Specify the path and filename where the script should be written. This path should begin with #esm.
Permissions	Specify the permissions to be assigned to the file after transfer. These should be in the form rwxrwxrwx.
Owner	Specify the owner to be assigned to the file after transfer. A user name or uid can be used. This applies to UNIX only.
Group	Specify the group to be assigned to the file after transfer. A group name or gid can be used. This applies to UNIX only.
CheckSum	Select the type of checksum to use for verification: None (-), CRC (C), MD5 (M), and CRC +MD5 (A).
Checksum hash	Specify the hash to be used to verify the file's integrity after transfer.
Comment	Type a comment for the file.
OS/ Rev	Specify the operating systems and versions to which this file should be transferred.
File Data	This is not a user-entry field. This column contains the data from the script, that is stored in the template. The contents of the script are inserted into the template, but they are base 64 encoded, so they cannot be edited within the template. This encoding allows binary files to be inserted into the template and copied to the agent.

To add files to the ICE scripts template

- 1 In the ICE scripts template editor, click the Add Script button.
- 2 In the drop-down menu of registered agents, select the agent from which you want to load script files.
- 3 Specify the name of the script.

Note: The path of the script is relative to the ESM directory. For example, to select the following file: C:\Program Files\esm\bin\testscript.exe
type: bin\test script.exe in the Add Script dialog.

- 4 Click OK.

Object Integrity (Solaris 10)

SU 24 includes three new checks and three new messages in the Object Integrity module.

List Solaris zones (Solaris 10)

This new check reports each zone that is found on the agent. You can use the include/ exclude name list to define the zones that you want to list. Zones can also be included or excluded based on status. In the name list, type a pipe character followed by the status of the zone. For example, a status of either |installed or |configured refers to zones where the setup process has been initiated, but not completed. |running refers to zones that are completely set up and running. All status filters (|installed, |configured, |running, etc.) can be included in the same name list. The status of a zone can be checked using the 'zoneadm list-civ' command. This check runs from the global zone only.

[Table 3-6](#) shows the new message for the List Solaris zones check.

Table 3-6 List Solaris zones message

Message name	Title	Severity
STKU_ZONE	Solaris zone	Yellow-2

List running Solaris zones without ESM (Solaris 10)

This new check reports each zone that does not have ESM installed in the /esm directory. You can use the include/ exclude name list to define the zones that you want to list. Zones can also be included or excluded based on status. In the name list, you can type a pipe character followed by the status of the zone. For example, a status of either |installed or |configured refers to zones where the

setup process has been initiated, but not completed. |running refers to zones that are completely set up and running. All status filters (|installed, |configured, |running, etc.) can be included in the same name list. The status of a zone can be checked using the 'zoneadm list-civ' command. This check runs from the global zone only.

[Table 3-7](#) shows the new message for the List running Solaris zones without ESM check.

Table 3-7 List running solaris zones without ESM message

Message name	Title	Severity
STKU_ZONE_WITHOUT_ESM	Solaris zone without ESM	Red-4

Solaris user stack protection (Solaris 10)

This new check reports if the user stack protection is not enabled on the system.

[Table 3-8](#) shows the new message for the Solaris user stack protection check.

Table 3-8 Solaris user stack protection message

Message name	Title	Severity
STKU_SOLARIS_STACK	User stack protection not enabled	Red-4

Password Strength (UNIX)

SU 24 includes one new check, three new messages, and one new template in the Password Strength module.

Password requirements (UNIX)

This new check reports password options that do not match those found in the enabled templates. One of three messages is reported when a password option that is on the agent does not match the values defined in the template.

[Table 3-9](#) shows the new message for the Password requirements check.

Table 3-9 Password requirements messages

Message name	Title	Severity
STKU_PASSWORD_REQUIREMENT_GREEN	Password option does not match template	Green-1
STKU_PASSWORD_REQUIREMENT_YELLOW	Password option does not match template	Yellow-2
STKU_PASSWORD_REQUIREMENT_RED	Password option does not match template	Red-4

Password requirements template

Use this new template to add password settings. By defining password settings in the template you are able to control how users set their passwords. These settings are enabled/ disabled in the `/etc/default/passwd` file.

The template contains six columns: File Name, Parameter Name, Comment, Severity Level, Parameter Values, and OS/ Rev.

File Name	Type the name of the file where the setting is contained.
Parameter Name	Type the name of the setting.
Comment	Type the comment that you want to display in the info field of reported messages.
Severity Level	Specify the severity level used by the message regarding this setting: Green (G), Yellow (Y), Red (R).
Parameter Values	Specify the valid and invalid values for this setting. This may also include valid or invalid patterns.
OS/ Rev	Specify the operating systems that are affected by this setting.

Startup (UNIX)

SU 24 includes one new check and three new messages in the Startup module.

Syslog (UNIX)

This new check reports any forbidden combinations, as specified in the template, that are found in /etc/syslog.conf, as well as any mandatory combinations, as specified in the template, that are also not found. One of three message severities is reported according to the severity level that is defined in the template.

[Table 3-10](#) shows the new messages for the Syslog check.

Table 3-10 Syslog messages

Message name	Title	Severity
STKU_SYSLOG_GREEN	Syslog configuration does not match template	Green-0
STKU_SYSLOG_YELLOW	Syslog configuration does not match template	Yellow-2
STKU_SYSLOG_RED	Syslog configuration does not match template	Red-4

Resolved issues

The following issues are resolved in SU 24:

Account Information (Widows 2000/ 2003)	The messages in the Security groups and their users check and the Users and their security groups check in the Account Information module have been reformatted. These message changes only affect Windows 2000 and 2003 agents running on domain controllers. When the checks run on a domain controller, the information field contains a fully qualified distinguished name format for user and group information rather than a path.
Account Integrity (AIX)	invscout has been added to the list of default system users/groups for AIX 5.3.
Account Integrity (HP-UX)	The Account disabled check now detects accounts that have been locked using the system command on HP-UX trusted mode.

Account Integrity (Windows)	The New Users check and the Deleted Users check in the Account Integrity module have been enhanced to prevent reporting of false positives for new users.
File Watch (UNIX)	<p>The snapshot format for the File Watch module has changed. When you upgrade to SU 24, the File Watch module automatically detects snapshot files previous to SU 24.</p> <p>When you run the module for the first time after upgrading to SU 24, you will receive the following message: Obsolete snapshot file '<old snapshot file name>' has been renamed to '<new snapshot file name>' for backup purposes.</p> <p>ESM renames the old fwatch.dat snapshot file to fwatch.dat.old and regenerates it.</p>
OS Patches (UNIX)	The OS Patch template allows non-root user processes to be checked. You may now specify the user name and the process separated by a #, , or @. By default, ESM will check the root user.
Password Strength (AIX)	The Login requires password check in the Password Strength module is compatible with AIX 5.2 and later.
System Mail (AIX, Solaris)	The System Mail module does not run the requested checks when the sendmail service is not running and the sendmail configuration file does not exist.
System Mail (UNIX)	The System Mail module no longer reports false positives when sendmail.cf parameters are followed by #.
User Files (UNIX)	The exclude list has been changed to an include/ exclude list in the UMASK check.

System requirements

[Table 3-11](#) lists the supported operating systems for SU 24.

Table 3-11 SU 24 supported operating systems

Agent operating system	Supported versions on 6.0	Supported versions on 6.5
AIX /RS 6000	4.2.1, 4.33, 5.1	5.1, 5.2
AIX (PPC)	5.2, 5.3	5.2, 5.3
HP-UX	10.20, 11, 11.11, 11.23	11, 11i, 11.23
HP-UX (Itanium®)	11i	11i
Red Hat Linux	7.x, 8, 9	N/A
Red Hat Enterprise Linux ES (Intel x86)	2.1, 3.0	3.0, 4.0
Red Hat Enterprise Linux WS and AS (AMD64)	3.0	3.0
Red Hat Enterprise Linux AS (Itanium®)	3.0	3.0
Red Hat Enterprise Linux WS and AS (EM64T)	3.0	3.0
Sun Solaris	2.5.1, 2.6, 2.7, 2.8, 2.9, 2.10	2.8, 2.9, 2.10
SUSE LINUX Standard Server	8	8, 9
SUSE LINUX Enterprise Server	8, 9	8, 9
SUSE LINUX Enterprise Server (Itanium®)	9	9
Windows 2000 Professional and Server (Intel)	All	All
Windows Server 2003 (Intel)	All	All
Windows Server 2003 (Itanium®)	All	All
Windows XP Professional (Intel)	SP2	SP2

Symantec reserves the right to certify the Security Update on the new versions of these operating systems before officially supporting them.

The LiveUpdate installation of SU 24 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 3-12](#) lists the agent disk space requirements for the ESM 6.5 agent.

Table 3-12 SU 24 agent disk space requirements

Agent operating system	SU 24
AIX /RS 6000	204 MB
AIX 5.3 (PPC)	204 MB
HP-UX	131 MB
HP-UX (Itanium®)	157 MB
Red Hat Linux	132 MB
Red Hat Enterprise Linux ES (Intel x86)	132 MB
Red Hat Enterprise Linux WS and AS (AMD64)	87 MB
Red Hat Enterprise Linux AS (Itanium®)	133 MB
Red Hat Enterprise Linux WS and AS (EM64T)	90 MB
Sun Solaris (2.7)	99 MB
Sun Solaris (10)	105 MB
SUSE LINUX Standard Server 8	75 MB
SUSE LINUX Enterprise Server 9	75 MB
SUSE LINUX Enterprise Server 9 (Itanium®)	94 MB
Windows 2000 Professional and Server (Intel)	80 MB
Windows Server 2003 (Intel)	85 MB
Windows Server 2003 (Itanium®)	149 MB
Windows XP Professional (Intel)	84 MB

A

- Account Integrity (UNIX) module
 - Rbac attributes not in template 4
 - Rbac template 5
 - Role based access 4
 - Role based access con't 4

B

- Backup Exec backup frequency
 - Backup Integrity (Windows 2000, XP, 2003) module 5
- Backup Exec last Backup Status
 - Backup Integrity (Windows 2000, XP, 2003) module 5
- Backup Exec Version
 - Backup Integrity (Windows 2000, XP, 2003) module 6
- Backup Integrity (Windows 2000, XP, 2003) module
 - Backup Exec backup frequency 5
 - Backup Exec last Backup Status 5
 - Backup Exec Version 6
 - Last backup status 4

C

- Copy scripts
 - ICE (All) module 7

I

- ICE (All) module
 - Copy scripts 7
 - ICE scripts template 8
 - Overwrite scripts 8
- ICE scripts template
 - ICE (All) module 8

L

- Last backup status
 - Backup Integrity (Windows 2000, XP, 2003) module 4
- List running solaris zones without ESM
 - Object Integrity (Solaris) module 9
- List solaris zones
 - Object Integrity (Solaris) module 9

N

- Newly-supported operating systems, SU 24 4

O

- Object Integrity (Solaris) module
 - List running solaris zones without ESM 9
 - List solaris zones 9
 - Solaris user stack protection 10
- Overwrite scripts
 - ICE (All) module 8

P

- Password requirements
 - Password Strength (UNIX) module 11
- Password Strength (UNIX) module
 - Password requirements 11

R

- Rbac attributes not in template
 - Account Integrity (UNIX) module 4
- Rbac template
 - Account Integrity (UNIX) module 5
- Resolved issues, SU 24 12
- Role based access
 - Account Integrity (UNIX) module 4
- Role based access con't
 - Account Integrity (UNIX) module 4

S

- Solaris user stack protection
 - Object Integrity (Solaris) module 10
- Startup (UNIX) module
 - Syslog 11
- Syslog
 - Startup (UNIX) module 11
- System requirements, SU 24 14