

Symantec Enterprise Security Manager Security Update 15 Release Notes

Release for Symantec ESM 5.1 and 5.5
NetWare/NDS Modules



Symantec ESM Security Update 15 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.

Documentation version: SU15

Copyright Notice

Copyright © 2003 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, 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. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.htm, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

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

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

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

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
 - Error messages/log files
 - Troubleshooting performed prior to contacting Symantec
 - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

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

SYMANTEC CORPORATION SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("LICENSOR") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR THE COMPANY OR LEGAL ENTITY THAT WILL BE UTILIZING PRODUCT AND THAT YOU REPRESENT AS AN EMPLOYEE OR AUTHORIZED AGENT ("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 CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "I DO AGREE" OR "YES" BUTTON OR LOADING THE PRODUCT, 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 AND DO NOT USE THE SOFTWARE.

1. LICENSE TO USE

Licensor grants You a non-exclusive, non-transferable license (the "License") for the use of the number of licenses of Licensor's software in machine readable form, and accompanying documentation (the "Product"), on Your machines for which You have been granted a license key and for which You pay the License fee and applicable tax. The License governs any releases, revisions or enhancements to the Product that Licensor may furnish to You.

2. RESTRICTIONS

Product is copyrighted and contains proprietary information and trade secrets belonging to Licensor and/or its licensors. Title to Product and all copies thereof is retained by Licensor and/or its licensors. You will not use Product for any purpose other than for Your own internal business purposes or make copies of the software, other than a single copy of the software in machine-readable format for back-up or archival purposes. You may make copies of the associated documentation for Your internal use only. You shall ensure that all proprietary rights notices on Product are reproduced and applied to any copies. You may not modify, decompile, disassemble, decrypt, extract, or otherwise reverse engineer Product, or create derivative works based upon all or part of Product. You may not transfer, lease, assign, make available for timesharing or sublicense Product, in whole or in part. No right, title or interest to any trademarks, service marks or trade names of Licensor or its licensors is granted by this License.

3. LIMITED WARRANTY

Licensor will replace, at no charge, defective media and product materials that are returned within 30 days of shipment. Licensor warrants, for a period of 30 days from the shipment date, that Product will perform in substantial compliance with the written materials accompanying the Product on that hardware and operating system software for which it was designed, as stated in the documentation. Use of Product with hardware and/or operating system software other than that for which it was designed and voids this applicable warranty. If, within 30 days of shipment, You report to Licensor that Product is not performing as described above, and Licensor is unable to correct it within 30 days of the date You report it, You may return Product, and Licensor will refund the License fee. If You promptly notify Licensor of an infringement claim based on an existing U.S. patent, copyright, trademark or trade secret, Licensor will indemnify You and hold You harmless against such claim, and shall control any defense or settlement. This warranty is null and void if You have modified Product, combined the Product with any software or portion thereof owned by any third party that is not specifically authorized or failed promptly to install any version of Product provided to You that is non-infringing. If commercially reasonable, Licensor will either obtain the

right for You to use the Product or will modify Product to make it non-infringing. The remedies above are Your exclusive remedies for Licensor's breach of any warranty contained herein.

4. LIMITATION OF REMEDIES

THE WARRANTIES IN THIS AGREEMENT ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OF ANY PRODUCT OR ITS DOCUMENTATION. THE LIABILITY OF LICENSOR HEREUNDER FROM ANY CAUSE OF ACTION WHATSOEVER WILL NOT EXCEED THE AGGREGATE LICENSE FEE PAID BY LICENSEE FOR THE PRODUCT. IN NO EVENT WILL LICENSOR OR ITS AUTHORIZED REPRESENTATIVES BE LIABLE FOR LOST PROFITS OR SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF, OR INABILITY TO USE, THE PRODUCT OR LOSS OF OR DAMAGE TO DATA, EVEN IF LICENSOR OR ITS AUTHORIZED REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. LICENSOR AND ITS AUTHORIZED REPRESENTATIVES WILL NOT BE LIABLE FOR ANY SUCH CLAIMS BY ANY OTHER PARTY. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. No action or claim arising out of or relating to this Agreement may be brought by You more than one (1) year after the cause of action is first discovered.

5. CONFIDENTIALITY

You agree that Product and all information relating to the Product is confidential property of the Licensor ("Proprietary Information"). You will not use or disclose any Proprietary Information except to the extent You can document that any such Proprietary Information is in the public domain and generally available for use and disclosure by the general public without any charge or license. Use by persons to which You have contracted any of Your data processing services is permitted only if each contractor (and its associated employees) is subject to a valid written agreement prohibiting the reproduction or disclosure to third parties of software products and associated documentation to which they have access and such prohibitions apply to the Product. You recognize and agree that there is no adequate remedy at law for a breach of this Section, that such a breach would irreparably harm the Licensor and that the Licensor is entitled to equitable relief (including, without limitation, injunctive relief) with respect to any such breach or potential breach, in addition to any other remedies available at law.

6. EXPORT REGULATION

You agree to comply strictly with all US export control laws, including the US Export Administration Act and its associated regulations and acknowledge Your responsibility to obtain licenses to export, re-export or import Product. Export or re-export of Product to Cuba, North Korea, Iran, Iraq, Libya, Syria or Sudan is prohibited.

7. US GOVERNMENT RESTRICTED RIGHTS

If You are licensing Product or its accompanying documentation on behalf of the US Government, it is classified as "Commercial Computer Product" and "Commercial Computer Documentation" developed at private expense, contains confidential information and trade secrets of Licensor and its licensors, and is subject to "Restricted Rights" as that term is defined in the Federal Acquisition Regulations ("FARs"). Contractor/Manufacturer is: Symantec Corporation, and its subsidiaries, Cupertino, California, USA.

8. MISCELLANEOUS

This License is made under the laws of the State of California, USA, excluding the choice of law and conflict of law provisions. Product is shipped FOB origin. This License is the entire License between You and Licensor relating to Product 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 communication between the parties during the term of this License. Notwithstanding the foregoing, some Products or products of Licensor may require Licensee to agree to additional terms through Licensor's on-line "click-wrap" license, and such terms shall supplement this Agreement. If any provision of this License is held invalid, all other provisions shall remain valid unless such validity would frustrate the purpose of this License, and this License shall be enforced to the full extent allowable under applicable law. Except for additional terms that may be required through Licensor's on-line "click-wrap" license, no modification to this License is binding, unless in writing and signed by a duly authorized representative of each party. The License granted hereunder shall terminate upon Your breach of any term herein and You shall cease use of and destroy all copies of Product. Duties of confidentiality, indemnification and the limitation of liability shall survive termination or expiration of this Agreement. Any Product purchased by You after the purchase of Product which is the subject of this License shall be subject to all of the terms of this License. All of Symantec Corporation's and its subsidiaries' licensors are direct and intended third-party beneficiaries of this License and may enforce it against You. Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). Licensee may obtain Content Updates for any period for which Licensee has purchased Upgrade Insurance for the Software, entered into a maintenance agreement with Symantec that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates.

Contents

Technical support	3
Licensing and registration 3	
Contacting Technical Support	4
Customer Service	4

Release Notes

New features and enhancements	9
Novell Yes, Tested and Approved certification	10
File Attributes module	10
File Information module	10
Startup Files module	10
File Access module	11
Object Integrity module	11
New check and option names	12
Known restrictions	16
IPX/SPX communications and NetWare 6.x	16
NDS 8.x incompatibilities	16
System Auditing module on NetWare 6.x	16
Operating requirements	17
Supported operating systems	17
Memory and disk space requirements	17
Frequently asked questions	18
Helpful hints	18
Preserving user data	18

Release Notes

This document describes Security Update 15 for Symantec Enterprise Security Manager (Symantec ESM). Use this release to update Symantec ESM 5.1 and 5.5 managers and agents that are running on supported NetWare/NDS platforms. See “Supported operating systems” on page 17.

Note: In the PDF version of this document, you can click cross-references such as the one above to go directly to that topic.

New features and enhancements

New features and enhancements in Security Update 15 include:

- Novell Yes Certification
- New File Templates
- Changed check and message names

Novell Yes, Tested and Approved certification



Symantec ESM Security Update 15 is a Novell certified **Yes, Tested and Approved** product.

See http://developer.novell.com/nss/nss_profile.jsp?product_key=87616 for more information.

File Attributes module

Security Update 15 for NetWare/NDS installs new File Templates. Before, the .nw4 File Templates were used for all NetWare/NDS versions. Now, each major NetWare/NDS version (4.x, 5.x, and 6.x) each has unique File Templates with distinct file extensions (.nf4, .nf5, and .nf6). Symantec ESM continues to support .nw4 File Templates on any system that has not yet registered the Security Update 15 File Attributes .m file.

Also, the previous release of NetWare/NDS modules had distinct template files, for example system.nw4, login.nw4 and public.nw4. Now these template files have been combined into one File Template for each NetWare version: nw42.nf4, nw5.nf5, and nw6.nf6.

File Information module

The Server module: Consider objects X levels above server option has been changed to Server module: All objects in the tree will be considered. This change reflects the removal of an older and slower effective rights algorithm. The newer and faster algorithm, available since Security Update 2, is now the only one used by Symantec ESM.

Startup Files module

The Server module: Consider objects X levels above server option has been changed to Server module: All objects in the tree will be considered. This change reflects the removal of an older and slower effective rights algorithm. The newer and faster algorithm, available since Security Update 2, is now the only one used by Symantec ESM.

File Access module

The Server module: Consider objects X levels above server option has been changed to Server module: All objects in the tree will be considered. This change reflects the removal of an older and slower effective rights algorithm. The newer and faster algorithm, available since Security Update 2, is now the only one used by Symantec ESM.

Object Integrity module

The following Object Integrity message names have changed.

Table 2-1 Changes to NetWare/NDS message names

Title	Old name	New name
File server removed from system	F_SERVER_SNAP	F_SERVER_REMOVED
Print queue directory trustee added	PQ_ACCESS_SNAP	PQ_TRUSTEE_ADDED
Print queue directory trustee removed	PQ_ACCESS_USERS	PQ_TRUSTEE_REMOVED
Print queue operator added	PQ_OPERATOR_OBJ	PQ_OPERATOR_ADDED
Print queue operator removed	PQ_OPERATOR_SNAP	PQ_OPERATOR_REMOVED
Print queue server added	PQ_SERVER_OBJ	PQ_SERVER_ADDED
Print server removed from print queue	PQ_SERVER_SNAP	PQ_SERVER_REMOVED
Print queue user removed	PQ_USER_OBJ	PQ_USER_REMOVED
Print queue user added	PQ_USER_SNAP	PQ_USER_ADDED
Print server operator added	PS_OPERAT_OBJ	PS_OPERAT_ADDED
Print server operator removed	PS_OPERAT_SNAP	PS_OPERAT_REMOVED
Print server user added	PS_USERS_OBJ	PS_USERS_ADDED
Print server user removed	PS_USERS_SNAP	PS_USERS_REMOVED
Snapshot file cannot be created on server	SIF_CREATE	SIF_CREATE_FAILED
Server added to network	SNAP_NETW_GONE	SERVER_ADDED

Table 2-1 Changes to NetWare/NDS message names

Title	Old name	New name
Print server added	SNAP_PSERV_GONE	PS_ADDED

New check and option names

Symantec has changed many NetWare/NDS check names. The checks function the same; only the names have changed. Many of the changes are only to capitalization. For example, the Accounting Events Enabled check has been renamed Accounting events enabled. Other changes remove unnecessary verbs. For example, the List Security Equivalences check has been renamed Security equivalences. A few changes are more significant and aim to better reflect the functionality of the check. For example, the Perform Checksum Check (CRC/MD5) check has been renamed Changed files (signature).

The following table lists all check name changes, except for those with changes to capitalization only.

Table 2-2 Changes to NetWare/NDS check and option names

Module	Old name	New name
Account Integrity	Accounts w/o Expiration Dates	Accounts without expiration dates
	Check Expiration Time	Expiration time
	Accounts w/o a Home Directory	Accounts without home directory
	Accounts w/o Login Time Restrictions	Accounts without login time restrictions
	Check for New, Changed, and Deleted Users	New, changed, and deleted users
	Check for New, Changed, and Deleted Groups	New, changed, and deleted groups
Account Information	List Group Membership	Group membership
	List Security Equivalences	Security equivalences
	List Account Login Status	Account login status
	List User Information	User information
	List Directory Trustees	Directory trustees

Table 2-2 Changes to NetWare/NDS check and option names

Module	Old name	New name
	List User Information (cont'd)	User information (cont'd)
	List Directory Trustees (cont'd)	Directory trustees (cont'd)
System Auditing	Files and Directories Flagged for Auditing	Files/directories for auditing
	Users Flagged for Auditing	Users for auditing
File Access	Server module: Consider objects X levels above server	Server module: All objects in the tree will be considered
	Check Access to ESM Files	Access to ESM files
	Check for Excessive File Access	Excessive file access
	List System Directories with Non-recommended Rights Mask	System directories with non-recommended rights mask
File Attributes	Check File Attributes	File attributes
	Check File Creation Time	Changed files (creation time)
	Check File Ownership	File ownership
	Perform Checksum Check (CRC/MD5)	Changed files (signature)
	Check Inherited Rights Mask	Inherited rights mask
	Check File Modification Time	Changed files (modification time)
	Check File Size	Changed files (size)
File Find	Find Hidden and System Files	Hidden and system files
	Find Duplicate System Files	Duplicate system files
	Find Duplicate Non-System Files	Duplicate non-system files
File Information	Server module: Consider objects X levels above server	Server module: All objects in the tree will be considered
	Check Directories Only	Directories only

Table 2-2 Changes to NetWare/NDS check and option names

Module	Old name	New name
Login Parameters	List Disabled Accounts	Disabled accounts
	List Locked Accounts	Locked accounts
	List Unused Accounts	Unused accounts
	List Inactive Accounts	Inactive accounts
Network Integrity	Check Disk Space Limits	Disk space limits
Object Integrity	List Excessive ACL Access	Excessive ACL access
	List Subordinates of Stealth Objects	Subordinates of stealth objects
	List Server Console Operators	Server console operators
	Check ESM Object's Access to Agent's Contexts	ESM object's access to agent's contexts
	List ACLs of Stealth Objects	ACLs of stealth objects
	Check for Missing Object Properties	Missing object properties
	List NetWare Server Equivalences	NetWare server equivalences
	Check for Missing Object Properties (cont'd)	Missing object properties (cont'd)
	Check for New, Changed, and Deleted Print Servers	New, changed, and deleted print Servers
	Check for New, Changed, and Deleted Print Queues	New, changed, and deleted print queues
	Check for New, Changed, and Deleted File Servers	New, changed, and deleted file servers
	Check for Stealth Objects	Stealth objects
	Password Strength	List Accounts Without Passwords
Check Password Length Restrictions		Password length restrictions

Table 2-2 Changes to NetWare/NDS check and option names

Module	Old name	New name
Startup Files	Server module: Consider objects X levels above server	Server module: All objects in the tree will be considered
	List NLMs currently loaded on server	NLMs currently loaded on server
	List NLMs added since snapshot	NLMs added since snapshot
	List NLMs removed since snapshot	NLMs removed since snapshot
	List NLMs changed since snapshot	NLMs changed since snapshot
	Check Access to Files Loaded by AUTOEXEC.NCF	Access to files loaded by AUTOEXEC.NCF
	Check NetWare Console Parameters	NetWare console parameters
	Check for REMOVE DOS	REMOVE DOS
	Check for SECURE CONSOLE	SECURE CONSOLE
	Check for ALLOW UNENCRYPTED PASSWORDS = ON	ALLOW UNENCRYPTED PASSWORDS = ON
Check for LOAD REMOTE with Unencrypted Password	LOAD REMOTE with unencrypted password	
User Files	Check Access to DOS Bindery Login Scripts	Access to DOS bindery login scripts
	Check Access to NDS Login Scripts	Access to NDS login scripts

Known restrictions

IPX/SPX communications and NetWare 6.x

The Symantec ESM 5.5 manager does not support SPX. Any attempt to use IPX/SPX to communicate to 5.5 managers will fail.

NetWare 6.x is certified to use the 5.51 agent. Therefore, NetWare 6.x will not register to a 5.1 or 5.0 manager with IPX/SPX, even though these managers do support IPX/SPX communications. The NetWare 6.x Symantec ESM agent will not be able to communicate through IPX/SPX.

The current agent for NetWare 5.x and NetWare 4.x is already certified, can communicate with 5.1 managers using IPX/SPX, and does not need to be replaced.

NDS 8.x incompatibilities

Due to incompatibilities between Security Update 15 and NDS 8.x, password cracking checks (Password = username, Password = any username, Password = wordlist word) will only run in Bindery mode. In addition, the Stealth objects check (Object Integrity module) will not work on systems using NDS 8.x.

System Auditing module on NetWare 6.x

The System Auditing module is not supported on NetWare 6.x. The checks in this module correspond to functionality that is no longer available in NetWare 6.x.

Operating requirements

Supported operating systems

Use this release to upgrade Symantec ESM 5.1 and 5.5 agents on the following platforms:

Table 2-3 Supported operating systems

Operating system	Versions
NetWare	4.2, 5.0, 5.1, 6.x

This security update 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.

Memory and disk space requirements

Resource requirements for security updates are the same as the requirements for the core products that you are upgrading.

Table 2-4 Memory and disk space requirements

CPU	RAM	Free disk space
P120	16 MB	135 MB

Frequently asked questions

- Do the security checks in new Security Updates replace the security checks on the agent systems?
Yes.
- Where can I find the Security Update software?
You can download the appropriate software for your system architectures by using LiveUpdate or going to the Symantec Web site at:
<http://securityresponse.symantec.com/>
- How do I install the Security Update release?
See Chapter 2 in the *Symantec ESM Security Update 15 User's Guide* for NetWare/NDS for installation prerequisites and instructions.
- How can I be notified when new Security Update releases or Response policies become available?
Symantec notifies subscribers of the Symantec ESM newsletter by e-mail when new response templates become available. To subscribe, visit the Symantec Web site at <http://www.symantec.com/techsupp/bulletin/index.html>.

Helpful hints

Preserving user data

Symantec ESM preserves user customized data while upgrading from one version of modules to a newer version. This data includes user modifications to policies, templates, and customized messages from the .m (dot-m) files.

During the upgrade process:

- Symantec ESM stores template data in the /esm/template directory. During an upgrade, Symantec ESM preserves any modifications to the template files while it merges the new template information that is contained in the upgrade version.
- Symantec ESM saves any changes that customize the policy database. These changes identify the security checks that are currently enabled in the security modules, as well as any changes to the related name lists.
- Symantec ESM preserves any changes to the message database that result from user changes to the .m files, if the customized value in the modified messages is set to 1.

Customized protection applies only to messages in the .m files. Security option information, such as the names of the security checks and the on-line help, have neither a customized flag nor the same protection.

- Symantec ESM overwrites the .m files. This does not affect any customized messages because they are protected in the message database. However, you do lose the source of the customized messages.

You can save the modified .m files in a backup directory. However, you must not replace the upgraded .m files with the modified .m files, because this causes errors. Instead, you should manually change the messages in the upgraded .m files using the procedures described in the *Symantec ESM Security Update 15 User's Guide*.

