

Symantec™ Enterprise Security Manager 6.5.3 Service Pack 2 Release Notes



Symantec™ Enterprise Security Manager™ 6.5.3 Service Pack 2 Release Notes

The software 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 6.5.3 Service Pack 2 (SP2)

Legal Notice

Copyright ©2007 Symantec Corporation.

All Rights Reserved.

Symantec, the Symantec Logo, LiveUpdate, Symantec Enterprise Security Architecture, Enterprise Security Manager, and NetRecon are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

<http://www.symantec.com>

Technical support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product feature and function, installation, and configuration. The Technical Support group also authors content for our online 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 and Symantec Security Response to provide alerting services and virus definition updates.

Symantec technical support offerings include the following:

- n A range of support options that give you the flexibility to select the right amount of service for any size organization
- n A telephone and web-based support that provides rapid response and up-to-the-minute information
- n Upgrade insurance that delivers automatic software upgrade protection
- n Content Updates for virus definitions and security signatures that ensure the highest level of protection
- n Global support that is available 24 hours a day, 7 days a week worldwide. Support is provided in a variety of languages for those customers that are enrolled in the Platinum Support program
- n Advanced features, including Technical Account Management

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Select your country or language under Global Support. The specific features that are available may vary based on the level of maintenance that was purchased and the specific product that you are using.

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/techsupp/

Select your region or language under Global Support.

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to recreate the problem.

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

- n Product release level
- n Hardware information

- n Available memory, disk space, NIC information
- n Operating system
- n Version and patch level
- n Network topology
- n Router, gateway, and IP address information
- n Problem description
 - n Error messages/log files
 - n Troubleshooting that was performed before contacting Symantec
 - n Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/

Select your region or language under Global Support, and then select the Licensing and Registration page.

Customer Service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Select your country or language under Global Support.

Customer Service is available to assist with the following types of issues:

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

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

- n Asia-Pacific and Japan: contractsadmin@symantec.com
- n Europe, Middle-East, and Africa: semea@symantec.com
- n North America and Latin America: [supportolutions@symantec.com](mailto:supportsolutions@symantec.com)

Additional Enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively. Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring and management capabilities, each focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

<http://www.symantec.com>

Select your country or language from the site index.

Contents

Chapter 1	Introducing Symantec Enterprise Security Manager 6.5.3 Service Pack 2	
	About Symantec Enterprise Security Manager 6.5.3 Service Pack 2	9
	Enhancements	10
	How Symantec ESM 6.5.3 Service Pack 2 is organized	13
Chapter 2	Upgrading to Symantec Enterprise Security Manager 6.5.3 Service Pack 2	
	About upgrading to Symantec ESM 6.5.3 Service Pack 2	15
	About the RenameAgentFolder utility	16
	Before you upgrade to Symantec ESM 6.5.3 Service Pack 2	17
	System requirements	18
	Software requirements	18
	Hardware requirements	20
	Upgrading on Windows	25
	Installing Symantec ESM 6.5.3 SP2 agents using MSI installer	26
	Running the RenameAgentFolder utility on Windows	27
	Upgrading on UNIX	28
	Running the RenameAgentFolder utility on UNIX	29
Chapter 3	Upgrading to Symantec Enterprise Reporting for ESM 6.5.3 Service Pack 2	
	About Symantec Enterprise Reporting for ESM 6.5.3 Service Pack 2	31
	Before upgrading to Symantec Enterprise Reporting for ESM 6.5.3 Service Pack 2	32
	System requirements	32
	Upgrading to Symantec Enterprise Reporting for ESM 6.5.3 Service Pack 2	33
Chapter 4	Symantec ESM 6.5.3 Service Pack 2 Resolved Issues and Enhancements	
	I18n issues resolved in Symantec ESM 6.5.3 Service Pack 2	39
	Enhancements in Symantec ESM 6.5.3 Service Pack 2	40
	Issues resolved in Symantec ESM 6.5.3 Service Pack 2	40

Chapter 5	Symantec ESM 6.5.3 Service Pack 2 Known Issues	
	I18n issues known in Symantec ESM 6.5.3 Service Pack 2	44
	Issues known in Symantec ESM 6.5.3 Service Pack 2	44
Chapter 6	Related Service Pack: Symantec ESM 6.5.3 Service Pack 1	
	Symantec ESM 6.5.3 Service Pack 1 enhancements and new features	47
	Symantec ESM 6.5.3 Service Pack 1 resolved issues and enhancements ...	50
	Symantec ESM 6.5.3 Service Pack 1 known issues	52

Introducing Symantec Enterprise Security Manager 6.5.3 Service Pack 2

This chapter includes the following topics:

- n [About Symantec Enterprise Security Manager 6.5.3 Service Pack 2](#)
- n [How Symantec ESM 6.5.3 Service Pack 2 is organized](#)

About Symantec Enterprise Security Manager 6.5.3 Service Pack 2

The Symantec Enterprise Security Manager (ESM) 6.5.3 Service Pack 2 (SP2) release is a maintenance release of Symantec ESM 6.5.3. This release also includes the fixes and enhancements that were a part of the ESM 6.5.3 Service Pack 1 (SP1) release.

For information on the ESM 6.5.3 SP1 release, see [“Related Service Pack: Symantec ESM 6.5.3 Service Pack 1”](#) on page 47.

The ESM 6.5.3 SP2 release provides the following:

- n Cumulative bug fixes
- n Internationalization (I18n) bug fixes
- n Enhancements to the various ESM components that enhance security, stability, and performance

Enhancements

Symantec ESM 6.5.3 SP2 release includes the following enhancements:

Internationalization of ESM

ESM has been internationalized to support the following languages:

- n German (Germany)
- n Spanish (Spain)
- n French (France)
- n Italian (Italy)
- n English (US)

See “[I18n issues resolved in Symantec ESM 6.5.3 Service Pack 2](#)” on page 39 for information on I18n issues that are resolved in ESM.

See “[I18n issues known in Symantec ESM 6.5.3 Service Pack 2](#)” on page 44 for information on I18n issues that are known in ESM.

New manager platform support

The Symantec ESM 6.5.3 SP2 release provides manager support on Solaris 10 SPARC (64-bit) operating system on local and global zones.

New command-line interface options

The following new parameters have been added to the delete job command:

n **-r**

Previously, the sumfinal records of a job were retained after the job was deleted using the delete job command.

You can now specify **-r** with the delete job command to delete a job with its sumfinal records.

Use the following format:

delete job -r <job_id>

n **-i**

Previously, you could specify only a single job with the delete job command.

You can now create a .csv file and list the job IDs, which need to be deleted, in the file. Using the **-i** parameter with the delete job command, you can specify the name of this file, and delete multiple jobs simultaneously.

Use the following format:

delete job -i <filename>

The following conditions apply to this file:

- n It should be a text file.
- n A non-digit character should be used to separate the job IDs in the file. The recommended format for this file is Comma Separated Values (CSV).

New option in the ciffix utility

The ciffix utility creates a backup file for every .dat file that has either corrupted or deleted records. Previously, with every subsequent run on a .dat file, the ciffix utility overwrote the backup file that it created in the last run. As a result, the backup history was lost.

A new option -p has now been added to the ciffix utility to preserve the backup data. If you use this option while running the ciffix utility, it appends the timestamp to the extension of the backup file as follows:

agent.bak<YYYY_MM_DD_HH_mm_SS>

YYYY, MM, and DD specify the year, month, and day respectively. HH, mm, and SS specify the hour (in 24-hour format), minutes, and seconds respectively.

For example, for a file named job.dat, the backup file is created as job.bak2007_10_03_12_30_15.

In this way, ciffix utility makes sure that the previous backup files are retained, if required.

Use the following format to use the -p option with the ciffix utility:

ciffix -p <file>

<file> specifies the relative path of the .dat file on which you want to run the ciffix utility.

The usage of -p is optional.

Fixed value for yellow custom messages in the database

All custom messages, after being processed by the ESM manager, are assigned the severity levels of 0 through 2. The levels 0, 1, and 2 represent green, yellow, and red colors respectively in the ESM proprietary data system.

The Reporting Database link (RDL), after importing these custom messages from the ESM manager, remaps them using its own grading system of 0 through 4. The messages are remapped to 0, 2, and 4 levels that indicate green, yellow, and red colors respectively. Due to this difference in the grading systems of the RDL and ESM manager, the original values of yellow messages cannot be restored in the relational database, if they get any value from 1 through 3. Hence, all yellow custom messages are now set to a value of 2 in the relational database.

Console support for Windows Vista

The ESM console can now be installed on Windows Vista (32-bit). Before you upgrade to the ESM 6.5.3 SP2 console on Windows Vista, you need to install the ESM 6.5.3 console from the May 2007 release. The same holds true for upgrading to ESM 6.5.3 SP1 console also.

To install the ESM 6.5.3 console on Windows Vista

- 1 From the CD 1 of the May 2007 release of ESM 6.5.3, copy the ESMSuiteInstaller folder to a local directory.
- 2 Right-click setupwin32.exe.
- 3 Click **Properties**.
- 4 Click the Compatibility tab.
- 5 Check **Run this program in compatibility mode for:**.
- 6 Select Windows 2000 from the drop-down box.
- 7 Click **OK**.

To upgrade the ESM 6.5.3 console to ESM 6.5.3 SP2

- 1 From the ESM 6.5.3 SP2 CD, copy the ESMSuiteInstaller folder to a local directory.
- 2 Repeat steps 2 through 7 of [To install the ESM 6.5.3 console on Windows Vista](#).

How Symantec ESM 6.5.3 Service Pack 2 is organized

Table 1-1 lists the contents of Symantec ESM 6.5.3 SP2.

Table 1-1 ESM 6.5.3 SP2 Contents

CD Image Name	Contents
Symantec_Enterprise_Security_Manager_6.5.3SP2_CD1	<p>Symantec ESM installation files for the following Windows operating systems:</p> <ul style="list-style-type: none"> n Manager, agent, and console on Windows Server 2003 (32-bit) n Manager, agent, and console on Windows 2000 n Agent on Windows XP n Agent on Windows Server 2003 (64-bit) n MSI Agent Installer and the associated files <p>The following documents are also included:</p> <ul style="list-style-type: none"> n <i>Symantec ESM 6.5.3 SP2 Release Notes</i> n <i>Symantec ESM 6.5.3 SP2 Rollback Guide</i>
Symantec_Enterprise_Security_Manager_6.5.3SP2_CD2	<p>Symantec ESM installation files for the following UNIX operating systems:</p> <ul style="list-style-type: none"> n Manager and agent on AIX n Manager and agent on HP-UX n Manager and agent on Solaris n Agent on Red Hat Linux n Agent on SUSE Linux
Symantec_Enterprise_Security_Manager_6.5.3SP2_CD3	Remote upgrade packages for agents on Windows
Symantec_Enterprise_Security_Manager_6.5.3SP2_CD4	Remote upgrade packages for agents on HP and Solaris
Symantec_Enterprise_Security_Manager_6.5.3SP2_CD5	Remote upgrade packages for agents on Linux
Symantec_Enterprise_Security_Manager_6.5.3SP2_CD6	Remote upgrade packages for agents on AIX PPC64

Table 1-1 ESM 6.5.3 SP2 Contents

CD Image Name	Contents
Symantec_Enterprise_Security_Manager_6.5.3SP2_CD7	Remote upgrade packages for agents on AIX RS6k
Symantec_Enterprise_Security_Manager_6.5.3SP2_CD8	The following are included: <ul style="list-style-type: none"><li data-bbox="606 461 1120 513">n Installers for Reporting Database Link (RDL) and database foundation on Windows and Solaris<li data-bbox="606 522 1120 574">n SQL scripts to create/upgrade the Oracle and SQL Server databases

Upgrading to Symantec Enterprise Security Manager 6.5.3 Service Pack 2

This chapter includes the following topics:

- n [About upgrading to Symantec ESM 6.5.3 Service Pack 2](#)
- n [Before you upgrade to Symantec ESM 6.5.3 Service Pack 2](#)
- n [System requirements](#)
- n [Upgrading on Windows](#)
- n [Upgrading on UNIX](#)

About upgrading to Symantec ESM 6.5.3 Service Pack 2

You can use the Symantec ESM 6.5.3 SP2 release to upgrade the following Symantec ESM components:

- n Symantec ESM 6.5.3 or 6.5.3 SP1 managers on supported Windows and UNIX computers
- n Symantec ESM 6.5.3 or 6.5.3 SP1 agents on supported Windows and UNIX computers

- n Symantec ESM 6.5.3 or 6.5.3 SP1 consoles on supported Windows computers

You can upgrade to ESM 6.5.3 SP2 in the following ways:

- n Upgrade the installed ESM components to ESM 6.5.3 SP2 on your Windows/UNIX computers from the CD
- n Remotely upgrade the installed ESM agents to ESM 6.5.3 SP2

Note: ESM no longer supports the IPX protocol.

About the RenameAgentFolder utility

ESM stores the results of the policy run on an agent in a folder on the manager. This folder has the same name as that of the agent. For agent names that exceed eight characters, ESM used an algorithm to truncate the name to eight characters for naming the folder. This process could result in a common folder name for agents with similar names, and affect their policy run data.

To avoid this conflict, ESM now uses the agent's complete name that is registered with the manager to name the folder. The RenameAgentFolder utility renames the existing folders using the agent's complete name, and preserves their historical data.

The RenameAgentFolder utility runs in the background during the ESM 6.5.3 SP2 installation, and updates the required files on the manager. If the utility generates an error, you can manually run the utility at the command prompt after completing the ESM 6.5.3 SP2 installation.

ESM creates a log file at the following location after the RenameAgentFolder utility is run:

On UNIX: <esm_install_directory>/esm/system/<manager_name>

On Windows: <esm_install_directory>\esm\system\<manager_name>

See [“Running the RenameAgentFolder utility on Windows”](#) on page 27.

See [“Running the RenameAgentFolder utility on UNIX”](#) on page 29.

Before you upgrade to Symantec ESM 6.5.3 Service Pack 2

Before upgrading to ESM 6.5.3 SP2, you need to complete the following tasks:

- n Make sure that one of the following is installed on Windows computers:
 - n Symantec ESM 6.5.3 May 2007 release
 - n Symantec ESM 6.5.3 SP1
- n Make sure that one of the following is installed on UNIX computers:
 - n Symantec ESM 6.5.3 March 2007 release
 - n Symantec ESM 6.5.3 SP1

Note: The ESM 6.5.3 May 2007 release does not include updates to UNIX.

- n Make sure that each selected computer satisfies the minimum operating system, memory, free disk space, swap, and platform requirements. See [“System requirements”](#) on page 18.
- n On UNIX computers, make sure that you log on as the superuser.
- n For UNIX installations, if you are not installing from the CD, you must identify one of the following:
 - n The special-device file name of the drive containing the ESM media
 - n The full path name of the ESM tar file that is located on the disk

You can remotely upgrade the following versions of the installed agents to ESM 6.5.3 SP2:

- n 6.5.3 March 2007 release
- n 6.5.3 March 2007 release with Mini Update applied
- n 6.5.3 May 2007 release (Windows only)
- n 6.5.3 SP1

Note: Remote installation of ESM 6.5.3 SP2 is not supported.

Note: You can remotely upgrade only the ESM 6.5.2 Windows Vista (32-bit/64-bit) and SUSE 9 Linux Enterprise Server on IBM PPC e-Server agents to ESM 6.5.3 SP2.

System requirements

Make sure that the computers meet the software and hardware requirements.

Software requirements

The operating systems or software platforms support the following Symantec ESM 6.5.3 SP2 components:

- n Symantec ESM managers
- n Symantec ESM agents
- n Symantec ESM console

Table 2-1 lists the operating systems supported by ESM 6.5.3 SP2 managers.

Table 2-1 Manager operating systems for ESM 6.5.3 SP2

Manager operating system	Versions supported by ESM 6.5.3 SP2
AIX (RS6K)	5.1, 5.2
HP-UX (PA-RISC)	11, 11.11
Sun Solaris (SPARC)	2.7, 2.8, 2.9, 2.10**
Windows 2000 Professional, Server, or Advanced Server	SP2 or later
Windows Server 2003 Standard and Enterprise Editions	All

Note: Symantec ESM 6.5.3 SP2 Managers can be installed only on 32-bit Windows operating systems.

** To upgrade to the ESM 6.5.3 SP2 manager on Solaris 10 SPARC, do the following:

- n Download the ESM manager for Solaris 10 SPARC (64-bit) from the following Web site:
<https://fileconnect.symantec.com/>
- n Install the manager.
- n Upgrade to ESM 6.5.3 SP2.

The ESM 6.5.3 SP2 manager is supported on Solaris 10 SPARC (64-bit) on both global and local zones.

[Table 2-2](#) lists the operating systems supported by ESM 6.5.3 SP2 agents.

Table 2-2 Agent operating systems for ESM 6.5.3 SP2

Agent operating system	Versions supported by 6.5.3 SP2
AIX (32-bit)	5.2
AIX (64-bit)	5.2, 5.3
HP-UX (PA-RISC)	11.11
HP-UX (Itanium)	11.23
Red Hat Enterprise Linux ES (Intel x86)	3.0, 4.0, 5.0
Red Hat Enterprise Linux WS and AS (Opteron)	3.0, 4.0, 5.0
Red Hat Enterprise Linux AS and ES (Itanium)	3.0, 4.0, 5.0
Sun Solaris (SPARC)	2.8, 2.9, 2.10
Sun Solaris (x86)	2.10
SUSE Linux Enterprise Servers	9, 10**
SUSE Linux Enterprise Server (Itanium)	9
SUSE Linux Enterprise Server on IBM PPC e-Server	9
Windows 2000 Professional and Server (x86)	All
Windows Server 2003 (x86, Itanium, and Opteron)	All
Windows Vista (32-bit and 64-bit)	All
Windows XP Professional (x86)	SP2
Windows 2008 (x86, x64, IA64) Core and GUI	SP1, SP2
Windows 2008 R2 (x64, IA64) Core and GUI	*
Windows 7 (x86, x64)	*

* ESM 6.5.3 SP2 supports the base versions of Windows 2008 R2 and Windows 7.

** Install the SUSE Linux Enterprise Server 9 agent on SUSE Linux Enterprise Server 10.

[Table 2-3](#) lists the operating systems supported by ESM 6.5.3 SP2 consoles.

Table 2-3 Console operating systems for ESM 6.5.3 SP2

Console operating system	Versions supported by ESM 6.5.3 SP2
Windows 2000 Professional, Server, or Advanced Server	SP2 or later
Windows Server 2003 (x86)	All
Windows XP Professional	SP2 or later
Windows Vista (32-bit)**	All

** See [“Console support for Windows Vista”](#) on page 12 for information on upgrading the ESM console to Windows Vista.

Hardware requirements

The amount of additional disk space that is required by the Symantec ESM 6.5.3 SP2 agents depends on the operating system.

[Table 2-4](#) lists the agent additional disk space requirements for the ESM 6.5.3 SP2 agents.

Table 2-4 Agent minimum disk space requirements for ESM 6.5.3 SP2

Agent operating system	Disk space required	Additional disk space required for SP2	Total disk space required
AIX /RS 6000	109 MB	134 MB	243 MB
AIX (PPC, 64-bit)	109 MB	120 MB	229 MB
HP-UX	47 MB	63 MB	110 MB
HP-UX (Itanium)	47 MB	50 MB	97 MB
Red Hat Enterprise Linux ES (Intel x86)	42 MB	46 MB	88 MB
Red Hat Enterprise Linux WS and AS (Opteron)	42 MB	26 MB	68 MB
Red Hat Enterprise Linux AS and ES (Itanium)	42 MB	46 MB	88 MB

Table 2-4 Agent minimum disk space requirements for ESM 6.5.3 SP2

Agent operating system	Disk space required	Additional disk space required for SP2	Total disk space required
Sun Solaris (SPARC)	43 MB	48 MB	91 MB
Sun Solaris (x86)	19 MB	23 MB	42 MB
SUSE Linux Enterprise Servers	42 MB	46 MB	88 MB
SUSE Linux Enterprise Server (Itanium)	42 MB	46 MB	88 MB
Windows 2000 Professional and Server (Intel)	39 MB	56 MB	95 MB
Windows Server 2003 (Intel)	39 MB	56 MB	95 MB
Windows Server 2003 (Itanium and Opteron)	39 MB	56 MB	95 MB
Windows XP Professional (Intel)	39 MB	56 MB	95 MB
Windows 2008, Windows 2008 SP1/SP2 (x86, x64, IA64) Core and GUI	-	-	82 MB
Windows 2008 R2 (x64, IA64) Core and GUI	-	-	92 MB
Windows 7 (x86, x64)	-	-	59 MB

[Table 2-5](#) lists the disk space requirements to remotely upgrade the ESM 6.5.3 SP2 agent.

Table 2-5 Disk space requirements to remotely upgrade the ESM 6.5.3 SP2 agents

Agent operating system	Disk space required	Additional disk space	Total disk space required
Windows	39 MB	54 MB	93 MB
AIX (PPC, 64-bit)	109 MB	152 MB	261 MB
AIX (RS 6k)	109 MB	152 MB	261 MB
HP-HPPA	47 MB	65 MB	112 MB
HP-UX (IA 64)	47 MB	65 MB	112 MB
Red Hat Enterprise Linux ES (Intel x86)	42 MB	60 MB	102 MB
Red Hat Enterprise Linux ES (IA-64)	41 MB	59 MB	100 MB
Sun Solaris (SPARC)	43 MB	61 MB	104 MB
Sun Solaris (x86)	19 MB	28 MB	47 MB

The total disk space that is required on the manager for remotely upgrading the agents to ESM 6.5.3 SP2 is 1.5 GB.

Additional hardware requirements for Windows computers

Computers that install Symantec ESM 6.5.3 SP2 must meet the minimum hardware requirements.

[Table 2-6](#) lists the requirements for Windows computers running ESM 6.5.3 SP2.

Table 2-6 Minimum CPU and RAM requirements for Windows computers

ESM components	CPU	RAM
Manager and agent	1 GHz	256 MB
Agent only	550 MHz	128 MB

[Table 2-7](#) lists the additional disk space requirements for ESM 6.5.3 SP2 managers and consoles.

Table 2-7 Manager and console minimum disk space requirements for ESM 6.5.3 SP2 on Windows

ESM component	Disk space required
Manager	85 MB
Console	210 MB

Additional hardware requirements for UNIX computers

UNIX computers must meet the minimum hardware requirements for running ESM 6.5.3 SP2.

[Table 2-8](#) lists the requirements for UNIX computers running ESM 6.5.3 SP2.

Table 2-8 Minimum CPU, RAM, and swap requirements for UNIX computers

ESM components	CPU	RAM	Swap
Manager and agent	1 GHz	256 MB	1 GB
Agent only	250 MHz	128 MB	256 MB

[Table 2-9](#) lists the additional disk space requirements for ESM 6.5.3 SP2 manager and agent.

Table 2-9 Manager and agent additional disk space requirements for ESM 6.5.3 SP2 on UNIX

Manager and agent operating system	Disk space required
AIX	320 MB
HP-UX	127 MB
Sun Solaris	112 MB

Virtualization support for ESM

The ESM components are currently supported on VMWARE virtualized environment for Windows.

ESM managers on Solaris 10 are supported on both local and global zones. However, the agents should be installed in the local zone.

The following are not supported:

- n ESM agents on Linux in XEN virtualization environment
- n AIX micro-partitions
- n Microsoft Virtual Server

The agent support for VMWARE ESX servers is planned to be provided in the future ESM release.

Virtual environments use more system resources than the physical environments do. If significant performance degradation occurs in a virtualized environment, try to recreate the issue in a physical environment. Doing so provides a benchmark for the performance.

If you face any issue while using ESM on VMWARE, recreate that issue on a physical computer. If the issue cannot be recreated on a physical computer, contact the VMWARE Technical Support.

For more information and help, contact the ESM Technical Support.

Upgrading on Windows

On computers running supported Windows operating systems, you should begin the installation of Symantec ESM components by starting the Symantec ESM Suite installer.

The Autorun feature automatically launches the Symantec ESM Suite installer. You can also start the installer manually.

ESM creates a backup of all the existing files that get replaced when you upgrade to ESM 6.5.3 SP2. The files are backed up in a folder named backup that is located in the \ESM directory. If you want to roll back to the previous version from ESM 6.5.3 SP2, you can restore the files from the backup folder.

See *ESM6.5.3SP2RollbackGuide.pdf* for information on manually rolling back from ESM 6.5.3 SP2 on Windows and UNIX.

To start the installer with the Autorun feature

- 1 Log on as administrator to the computer on which you are installing the Symantec ESM component.
- 2 Insert the Symantec ESM installation CD-ROM in the CD-ROM drive.
- 3 In the Important panel, click **OK**.
- 4 In the Welcome panel, click **Next**.
- 5 In the Overview panel, click **Next**.
- 6 In the Software License Agreement panel, read the license agreement and click **I accept the terms of the license agreement**, and click **Next**.
- 7 Type the user name and password to establish a connection with the ESM manager. Make sure that this user account has at least the read-only privileges on all the policies.
- 8 In the Summary Information panel, click **Install**.
- 9 Respond to the prompts from the installation wizard.

To start the installer manually

- 1 Log on as administrator to the computer on which you are installing the Symantec ESM component.
- 2 Change to the \ESMSuiteInstaller folder on the installation CD-ROM or the network installation directory, if you copied the files to a hard disk.
- 3 Double-click setupwin32.exe.
- 4 In the Important panel, click **OK**.

- 5 In the Welcome panel, click **Next**.
- 6 In the Overview panel, click **Next**.
- 7 In the Software License Agreement panel, read the license agreement and click **I accept the terms of the license agreement**, and click **Next**.
- 8 Type the user name and password to establish a connection with the ESM manager. Make sure that this user account has at least the read-only privileges on all the policies.
- 9 In the Summary Information panel, click **Install**.
- 10 Respond to the prompts from the installation wizard.

Installing Symantec ESM 6.5.3 SP2 agents using MSI installer

The MSI installer provides an alternate method of installing Symantec ESM agents on Windows operating systems on local computers.

About MSI installer

The MSI installer can only be used on a local computer.

The MSI installer is not compatible with the components that are installed using the ESM Suite installer and has the following limitations:

- n You cannot use the MSI installer to install an ESM agent on a computer that has a Symantec ESM manager installed.
- n You cannot install an ESM manager on a computer that hosts a Symantec ESM agent that was installed by the MSI installer.

Supported operating systems

The MSI installer is supported on the following Windows operating systems:

- n Windows 2000 Professional and Server (Intel)
- n Windows Server 2003 (x64 -Xeon/Opteron)
- n Windows Server 2003 (Intel)
- n Windows Server 2003 (Itanium)
- n Windows XP Professional (Intel)
- n Windows 2008 or Windows 2008 SP1 or SP2 (x86, x64, IA64) Core and GUI
- n Windows 2008 R2 (x64, IA64) Core and GUI
- n Windows 7 (x86, x64)

To install a Symantec ESM agent using the MSI installer

- 1 Log on as administrator to the computer on which you are installing the Symantec ESM agent.
- 2 Change to the \AgentMSIInstall\ESMMSIInstall folder on the installation CD 1. If you copied the files to a hard disk, change to the network installation directory.
- 3 Double-click setup.exe.
- 4 In the Welcome panel, click **Next**.
- 5 In the License Agreement panel, read the license agreement and click **I accept the terms in the license agreement**, and click **Next**.
- 6 In the Install Wizard completed panel, click **Finish**.

Running the RenameAgentFolder utility on Windows

If the RenameAgentFolder utility fails while upgrading to ESM 6.5.3 SP2, you can run the utility manually.

To run the RenameAgentFolder utility on Windows

- 1 Stop the Enterprise Security Manager service.
- 2 Change to the \ESM\system\\reports directory.
- 3 Back up the reports folder.
- 4 Change to the \ESM\bin folder.
- 5 Execute the RenameAgentFolder utility.
- 6 Type the user name of the ESM account that has at least the read-only privileges on all the policies.
- 7 Type the password of the ESM account.
- 8 Type the manager's port number.
- 9 Type **Y** if you want to exit the utility and take a backup.
- 10 Type **Y** if you want the utility to continue processing other agents, should any failure occur while processing an agent.
- 11 If the agents are successfully renamed, the following output is displayed:
 Rename Agent folders completed successfully
 Hit ENTER to continue...
- 12 Make sure that the Enterprise Security Manager service is running. If it is not running, start the service manually.

Upgrading on UNIX

On computers running UNIX operating systems, you can install the Symantec ESM manager and ESM agent.

ESM creates a backup of all the existing files that get replaced when you upgrade to ESM 6.5.3 SP2. The files are backed up in a folder named backup that is located in the /esm directory. If you want to roll back to the previous version from ESM 6.5.3 SP2, you can restore the files from the backup folder.

To install Symantec ESM components

- 1 Use su, or log on to root on the computer on which you are installing the Symantec ESM component.
- 2 Mount the Symantec ESM installation CD-ROM on the host computer. Type one of the following commands to mount a CD-ROM on a UNIX computer:

For AIX:

Type **mount -v cdrfs -r /device /cdrom** or use smit to mount the CD-ROM.

For HP-UX:

Type **mount -F cdrfs -o cdcase /dsk/device /cdrom**.

For Solaris:

Insert the CD-ROM. The vold daemon will mount it. If the vold daemon is not running, type **mount -F hsfs -r /device /cdrom**.

- 3 Change to the /ESM65 directory.
- 4 Type **./esmsetup653sp2**.
- 5 Do one of the following:
 - n Type **1** to view the license agreement.
 - n Type **2** to start the installation.
- 6 Read the license agreement, and type **A** to agree.
- 7 Type the complete path name of the ESM 6.5.3 SP2 tar/tgz file that is located on the disk.
- 8 Type the user name and password to establish a connection with the ESM manager. Make sure that this user account has at least the read-only privileges on the policies.
The setup continues with the installation and exits after upgrading the ESM components to ESM 6.5.3 SP2.

Note: If you run the `pkgsetup` for installing ESM 6.5.3 SP2 on Solaris operating systems, the setup only asks for the user name and password of an account that has at least read-only privileges on the policies.

To uninstall ESM

- 1 Use `su`, or log on to root on the computer on the Symantec ESM components are installed.
- 2 Change to the `/ESM65` directory.
- 3 Type `./esmdeinstall`.

Running the RenameAgentFolder utility on UNIX

If the `RenameAgentFolder` utility fails while upgrading to ESM 6.5.3 SP2, you can run the utility manually.

To install the RenameAgentFolder utility on UNIX

- 1 Stop the ESM daemons on the ESM manager.
- 2 Change to the `<esm_install_directory>/esm/system/<manager_name>/reports` directory.
- 3 Back up the reports folder.
- 4 Change to the `/esm/bin` folder.
- 5 Execute the `RenameAgentFolder` utility.
- 6 Type the user name of the ESM account that has at least the read-only privileges on all the policies.
- 7 Type the password of the ESM account.
- 8 Type the manager's port number.
- 9 Type **Y** for if you want to exit the utility and take a backup.
- 10 Type **Y** if you want the utility to continue processing other agents, if any failure occurs while processing an agent.
- 11 If the agents are successfully renamed, the following output is displayed:
Rename Agent folders completed successfully
Hit ENTER to continue...
- 12 Make sure that the ESM daemons are running. If they are not running, start the daemons manually.

Upgrading to Symantec Enterprise Reporting for ESM 6.5.3 Service Pack 2

This chapter includes the following topics:

- n [About Symantec Enterprise Reporting for ESM 6.5.3 Service Pack 2](#)
- n [Before upgrading to Symantec Enterprise Reporting for ESM 6.5.3 Service Pack 2](#)
- n [System requirements](#)
- n [Upgrading to Symantec Enterprise Reporting for ESM 6.5.3 Service Pack 2](#)

About Symantec Enterprise Reporting for ESM 6.5.3 Service Pack 2

The Symantec Enterprise Reporting release for Symantec Enterprise Security Manager 6.5.3 SP2 includes enhancements and updates to the Symantec Enterprise Reporting Database Link (RDL).

Before upgrading to Symantec Enterprise Reporting for ESM 6.5.3 Service Pack 2

If you are installing Symantec Enterprise Reporting for the first time, refer to the *Symantec Enterprise Security Manager Reporting Implementation Guide* for installation procedures.

If you are upgrading from Symantec Enterprise Reporting 6.5/6.1.1, or have ESM Reporting installed with Symantec ESM 6.5.3, do the following to upgrade the application:

- n Make sure that each selected computer satisfies the minimum operating system, memory, free disk space, swap, and platform requirements.
- n On UNIX computers, obtain an account with superuser privileges.

To use the jtds drivers for upgrading the Symantec Enterprise Reporting Database Link (RDL), do the following:

- n Log on to http://sourceforge.net/project/showfiles.php?group_id=33291 and download `jtds-1.2-dist.zip`.
- n Copy `jtds-1.2-dist.zip`.
- n Change to `<Drive_name>:\Program Files\Java\jre<version>\lib\` directory, and paste `jtds-1.2-dist.zip`.
- n Unzip `jtds-1.2-dist.zip`.

System requirements

Table 3-1 describes the Symantec Enterprise Reporting configurations that are supported by the Symantec Enterprise Reporting release for ESM 6.5.3 SP2.

Each row of the table represents one possible configuration. You must use the indicated combination of the Reporting Database Link platform and database platform.

Table 3-1 Configurations supported by ESM Reporting for ESM 6.5.3 SP2

Reporting Database Link Platforms	Database Platform
Windows 2000 Server	MSSQL Server 2000 with SP4, MSSQL Server 2005
Windows Server 2003	MSSQL Server 2000 with SP4, MSSQL Server 2005
Solaris 8/9	Oracle version 9.0.2x, 10.1.0.x, and 10.2.0
Solaris 10 SPARC	

For more system requirements see “Planning to install Symantec Enterprise Reporting” in the *Symantec Enterprise Reporting Implementation Guide*, version 6.5.

Upgrading to Symantec Enterprise Reporting for ESM 6.5.3 Service Pack 2

The Symantec Enterprise Reporting Database Link versions that ship with Symantec Enterprise Reporting versions 6.1.1 are incompatible with Symantec ESM 6.5.3 SP2 managers. For ESM 6.5.3 and 6.5.3 SP2 managers on Windows, Solaris, and AIX computers, you must install the RDL that ships with Symantec ESM 6.5.3 or ESM 6.5.3 SP2.

If you have the RDL from the ESM 6.5.3 release installed, you should upgrade to the latest RDL from the Symantec Enterprise Reporting release for ESM 6.5.3 SP2.

When you make changes to the RDL, you must clear the cache by stopping and restarting the Symantec ESM Reporting Database Link service.

You must upgrade the Symantec Enterprise Reporting components in the following order:

- n The Symantec Enterprise Reporting Database Foundation
- n The Symantec Enterprise Reporting Database Link (RDL)

For more information about upgrading or installing, see “Planning to install Symantec Enterprise Reporting” and “Installing Symantec Enterprise Reporting” in the *Symantec Enterprise Security Manager Reporting Implementation Guide*, version 6.5.

Upgrading the Symantec Enterprise Reporting components on Windows

Upgrade the following Symantec Enterprise Reporting components on Windows:

- n Database foundation
- n Reporting Database Link

To upgrade the database foundation

- 1 Change to \database_foundation\windows directory.
- 2 Double-click install.exe.
- 3 In the Welcome panel, click **Next**.

- 4 In the License Agreement panel, read the agreement and click **I accept the terms in the license agreement**, and then click **Next**.
- 5 Select **Upgrade Schema**, and then click **Next**.

If you have an earlier version of the Symantec Enterprise Reporting Database Foundation installed and you select Default MS SQL Server or Import Data, the installation cannot complete and you must do either of the following:

 - n Return to the previous window and change your selection.
 - n End and restart the installation of the Symantec Enterprise Reporting Database Foundation.
- 6 Select the type of database that you are using for your Symantec Enterprise Reporting database, and then click **Next**.
- 7 Select the appropriate executable file from the list that is provided to execute database scripts, and then click **Next**.

If you are unsure about which file to select, or if you need to use an executable that is not listed, you should verify the file information. See “Installing Symantec Enterprise Reporting” in the *Symantec Enterprise Security Manager Reporting Implementation Guide*.
- 8 Type the name of the Symantec Enterprise Reporting database, and then click **Next**.

If you did not use the default name of ESM, you must type the name that you used during the original installation of Symantec Enterprise Reporting.
- 9 Type the information for the JDBC drivers, and then click **Next**. See the information on drivers in “Installing Symantec Enterprise Reporting” in the *Symantec Enterprise Security Manager Reporting Implementation Guide*.
- 10 Type the information for the database connection, and then click **Next**.

This information must be identical to the information that was used in the original installation of Symantec Enterprise Reporting. See “Installing Symantec Enterprise Reporting” in the *Symantec Enterprise Security Manager Reporting Implementation Guide* for more information.
- 11 Type the user name for the Symantec Enterprise Reporting Database Link and the user name for the Symantec Enterprise Reporting Account, and then click **Next**.

These user names must match the ones that you used during the original installation. The user accounts must have the privileges that are specified in the installation window.
- 12 Review the information in the Pre-Install Summary window, and then click **Install**.

13 Click Done.

To upgrade the Symantec Enterprise Reporting Database Link

- 1 Change to \database_link\windows directory.
- 2 Double-click install.exe.
- 3 In the Welcome panel, click **Next**.
- 4 In the License Agreement panel, read the agreement and click **I accept the terms in the license agreement**, and then click **Next**.
- 5 Select **Upgrade Installation**, and then click **Next**. Other options do not install the upgrade.
- 6 Type the path to the original installation of the Symantec Enterprise Reporting Database Link. Click **Choose** to select a path other than the default path. Click **Next**.
- 7 Select the type of database that you are using as your Symantec Enterprise Reporting Database, and then click **Next**.
- 8 For MS SQL Server 2000, enter the JDBC driver information as follows:
 - n Type the following in the JDBC Driver Class field:
net.sourceforge.jtds.jdbc.Driver
 - n Type the following path in the JDBC Classpath field:
<Drive_name>:\Program Files\Java\<jre_version>\lib\jtds-1.2.jar
 - n Leave the JDBC Library path field blank.
 - n Retain the value present in the SQL Dialect field or leave it blank.If you used another driver for your initial installation, you must use a compatible driver to upgrade the Symantec Enterprise Reporting Database Link.
- 9 Click **Next**.
- 10 Type the database connection information, and click **Next**.
This information must match the information that you used in the initial installation.
For MS SQL Server, do the following:
 - n Type the following in the URL field:
jdbc:jtds:sqlserver://<database_hostname>:1433/
ESM;sendStringParametersAsUnicode=false
 - n Type **sa** in the User field and the SQL administrator password in the Password field.
- 11 Type the information that is required for any new manager connections and click the arrow to add the new manager connection to the list of existing

manager connections. To remove managers, select a manager from the list and click **Remove**. Click **Next**.

- 12 Review the information that is listed in the Pre-Installation Summary window, and then click **Install**.
- 13 Click **Done**.

Upgrading the Symantec Enterprise Reporting components on Solaris

Upgrade the following Symantec Enterprise Reporting components on UNIX:

- n Database foundation
- n Reporting Database Link

To upgrade the database foundation

- 1 On the computer where Oracle is installed, access the Symantec ESM Reporting Solaris CD.
- 2 At the command prompt, type the following:
setup.sh
- 3 In the left pane of the Symantec ESM 6.5.3 SP2 Reporting CD, click **Database Foundation**.
- 4 In the right pane, do the following:
 - n Review the information.
 - n Complete the installation prerequisites.
 - n Click **Execute the Database Foundation Installer**.
- 5 In the Introduction panel, click **Next**.
- 6 In the License Agreement panel, click **I accept the terms of the License Agreement**, and then click **Next**.
- 7 Select **Upgrade Schema**, and then click **Next**.
- 8 Select the type of database that you are using for the Symantec Enterprise Reporting database, and then click **Next**.
- 9 Type the name of the Symantec Enterprise Reporting database, and then click **Next**.
If you did not use the default name of ESM, you must type the name that you used during the original installation of Symantec Enterprise Reporting.
- 10 In the JDBC Driver panel, do the following:
 - n Specify the default values for the JDBC Driver Class, JDBC Classpath, and JDBC Library Path.

n Click **Next**.

- 11 Type the information for the database connection.
This information must be identical to the information that was used in the original installation of Symantec Enterprise Reporting.
- 12 Type the user name for the Symantec Enterprise Reporting Database Link and the Symantec Enterprise Reporting Account, and then click **Next**.
These user names must match the user names that you specified during the original installation. The user accounts must have the privileges that are specified in the installation window.
- 13 Review the information in the Pre-Install Summary window, and then click **Install**.
- 14 Click **Done**.

To upgrade the Symantec Enterprise Reporting Database Link

- 1 On the computer where you are upgrading the Symantec ESM Reporting Database Link, access the Symantec ESM Reporting Solaris CD.
- 2 At the system command prompt, type the following:
setup.sh
- 3 In the left pane of the Symantec ESM 6.5.3 SP2 Reporting CD panel, click **Database Link**.
- 4 Click **Execute the Database Link Installer**.
- 5 In the Introduction panel, click **Next**.
- 6 In the License Agreement panel, click **I accept the terms of the License Agreement**, and then click **Next**.
- 7 Select **Upgrade Installation**, and then click **Next**.
- 8 In the Choose Install Folder panel, select the default location, and then click **Next**.
- 9 In the Database Type Selection panel, select **Oracle**, and then click **Next**.
- 10 In the JDBC Driver Information panel, do one of the following tasks:
 - n Specify the default JDBC Driver Class, JDBC Classpath, JDBC Library Path, and SQL Dialect, click **Next**.
 - n Specify another JDBC Driver Class, JDBC Classpath, JDBC Library Path, and SQL Dialect, type the information in the respective text boxes, and then click **Next**.
- 11 In the Database Connection panel, do one of the following:

- n Specify the default database URL, type the user name and password of the Oracle account in the respective text boxes, and then click **Next**.
 - n Specify another database URL, user name, and password, type the information in the respective text boxes, and then click **Next**.
- 12** In the ESM Manager Connection panel, do the following:
- n Type the name of the Symantec ESM Manager.
 - n Type the user name of an account on the manager that has the manage user rights and read only access rights to all domains, policies, and templates.
 - n Type the password of the manager account.
 - n Specify the port number of the manager.
 - n Add the manager to the list.
- You can repeat these steps for connecting the Symantec ESM Reporting Database Link with another ESM Manager.
- 13** In the Pre-Install Summary panel, click **Install**.
- 14** Click **Done**.

Symantec ESM 6.5.3 Service Pack 2 Resolved Issues and Enhancements

This chapter includes the following topics:

- n [I18n issues resolved in Symantec ESM 6.5.3 Service Pack 2](#)
- n [Enhancements in Symantec ESM 6.5.3 Service Pack 2](#)
- n [Issues resolved in Symantec ESM 6.5.3 Service Pack 2](#)

I18n issues resolved in Symantec ESM 6.5.3 Service Pack 2

[Table 4-1](#) lists the I18n issues that have been resolved in Symantec ESM 6.5.3 SP2.

Table 4-1 Symantec ESM 6.5.3 SP2 I18n resolved issues

Defect ID	Description
1127708	esmc.exe does not support input in the HI-ASCII format
1127229	Domain names that contain HI-ASCII characters appear garbled at the command line
1053335	The agent name appears garbled if the host name contains HI-ASCII characters
1079510	ESM console ignores the locale settings while displaying the date/time

Table 4-1 Symantec ESM 6.5.3 SP2 I18n resolved issues

Defect ID	Description
1083792	ESM console incorrectly displays the names containing HI-ASCII characters
1084943	ESM improperly handles the HI-ASCII characters on AIX agents and reports incorrect results for them
1120630	Policies with HI-ASCII characters in their names generate errors when they are executed

Enhancements in Symantec ESM 6.5.3 Service Pack 2

[Table 4-2](#) lists the enhancements in Symantec ESM 6.5.3 SP2.

Table 4-2 Symantec ESM 6.5.3 SP2 enhancements

Defect ID	Description
1073208	Add an option for the CLI delete job command to remove the sumfinal data
1037764	The ciffix utility overwrites the suppression .bak files
1077101	ESMC should be able to execute remote upgrade of an agent
1087422	When an agent is removed from a domain, the audit log displays the necessary information about the deleted agent

Issues resolved in Symantec ESM 6.5.3 Service Pack 2

[Table 4-3](#) lists the issues that are resolved in Symantec ESM 6.5.3 SP2.

Table 4-3 Symantec ESM 6.5.3 SP2 resolved issues

Defect ID	Description
1140577	The 'audit_successful' status flag (in table ESMDB10.ESM_AUDIT_AGENT) in RDL is set to zero
1050287	The Show access command does not work properly

Table 4-3 Symantec ESM 6.5.3 SP2 resolved issues

Defect ID	Description
1097148	RDL fails to recover from the ArrayIndexOutOfBounds error in Connection pool
881706	Policy name gets truncated while scheduling policy runs
964539	Remote upgrade of HPUX and Solaris agents to ESM 6.5.3 from older versions generates errors
1061849	Upgrade of ESM agents using the latest windows code fails
1116145	Errors in the esmmodd.log and esmmodd.err files
877559	ESM process spikes up when a new zone is created on Solaris 10
1039173	RDL hangs while importing data from the manager
877753	The 6.5 ESMC does not recognize %s syntax in the message.dat file
878221	Error retrieving the policy run while updating a 6.5 manager from the SU24 CD

Symantec ESM 6.5.3 Service Pack 2 Known Issues

This chapter includes the following topics:

- n [118n issues known in Symantec ESM 6.5.3 Service Pack 2](#)
- n [Issues known in Symantec ESM 6.5.3 Service Pack 2](#)

I18n issues known in Symantec ESM 6.5.3 Service Pack 2

[Table 5-1](#) lists the I18n issues that are known in Symantec ESM 6.5.3 SP2.

Table 5-1 Symantec ESM 6.5.3 SP2 I18n known issues

Operating system	Description
All Windows and UNIX	Currently, ESM supports only the following international languages: <ul style="list-style-type: none">n German (Germany)n Spanish (Spain)n French (France)n Italian (Italy)n English (US) Refer the Knowledge Base article titled <i>How to modify the cs.tbl file to support international languages in ESM on UNIX</i> at the following Symantec Web site: http://www.symantec.com/enterprise/support/overview.jsp?pid=51911
All Windows and UNIX	ESM does not support HI-ASCII characters in the user names and passwords that you use to access various components.
Windows	The ESM 6.5.3 SP2 installation fails if you specify a user name that contains non-ASCII characters.

Note: The I18n known issues will be addressed in the ensuing release of ESM.

Issues known in Symantec ESM 6.5.3 Service Pack 2

[Table 5-2](#) lists the issues that are known in Symantec ESM 6.5.3 SP2.

Table 5-2 Symantec ESM 6.5.3 SP2 known issues

Operating system	Description
All Windows	When you uninstall an ESM manager or agent, warning messages that ask you to confirm the deletion of certain ESM files are displayed. Click Yes on the warning messages for a successful uninstallation.

Table 5-2 Symantec ESM 6.5.3 SP2 known issues

Operating system	Description
All Windows	If an agent is installed using the MSI installer and you try to re-register the agent with its manager, no error message is displayed informing that the agent is already registered with that manager.
All Windows and UNIX	If ESM is unable to resolve the agent's IP address, FQDN, or NetBIOS name when you re-register an agent, ESM creates an additional record for that agent.
All Windows and UNIX	The Symantec Enterprise Reporting Database Link (RDL) does not put the version information of the various ESM components in the database.
All Windows and UNIX	If you upgrade an agent to ESM 6.5.3 SP2 by using an on-the-top installation, the agent's properties on the console do not show the updated version. Instead, the release date is displayed. To resolve this issue, re-register the agent with its manager.
All Windows and UNIX	If you upgrade a manager to ESM 6.5.3 SP2, the manager's properties on the console do not show the updated version. To resolve this issue, close the console and restart it.
Windows Vista (32-bit, 64-bit)	The members of the administrators group can run register.exe only if the administrator sets the privilege level of this file. To set the privilege level of register.exe for all users in the administrators group, do the following: <ul style="list-style-type: none"> n Log on as the BUILTIN administrator to the computer where the agent is installed. n Locate register.exe and right-click it. n Click Properties. n Click the Compatibility tab. n Click Show settings for all users. n Select Run this program as administrator under Privilege level.

Related Service Pack: Symantec ESM 6.5.3 Service Pack 1

This chapter includes the following topics:

- n [Symantec ESM 6.5.3 Service Pack 1 enhancements and new features](#)
- n [Symantec ESM 6.5.3 Service Pack 1 resolved issues and enhancements](#)
- n [Symantec ESM 6.5.3 Service Pack 1 known issues](#)

Symantec ESM 6.5.3 Service Pack 1 enhancements and new features

The following were new in Symantec ESM 6.5.3 SP1 release:

New agent platform support

The Symantec ESM 6.5.3 SP1 release provides agent support on the following operating systems:

- n Windows Vista (32-bit/64-bit)
- n SUSE 9 Linux Enterprise Server on IBM PPC e-Server
- n Red Hat Enterprise Linux 5

New database support for Reporting Database Link

The Reporting Database Link (RDL) for Symantec ESM 6.5.3 SP1 is now supported on the following databases:

- n Oracle 10g (10.1.0.x and 10.2.0) (32-bit/64-bit)
- n Microsoft SQL Server 2005 (32-bit/64-bit)

Roll back from ESM 6.5.3 SP1

The ESM 6.5.3 SP1 release provides a new feature that lets you manually roll back to the previous ESM version. The previous ESM version is one from which you upgraded to ESM 6.5.3 SP1.

See *ESM6.5.3SP1RollbackGuide.pdf* for information on how to manually roll back from ESM 6.5.3 SP1 on Windows and UNIX.

Symantec ESM 6.5.3 SP1 includes the following enhancements:

Encryption and security

On Windows operating systems, RDL can now communicate with the database server using Internet Protocol Security (IPSec). IPSec creates an encrypted channel between RDL and the database server. This communication is independent of ESM.

New command-line interface options

The following new command-line interface (CLI) options have been introduced in ESM 6.5.3 SP1:

set luagent	This option enables or disables LiveUpdate for an agent. Use the following format: set luagent <agent_name> on/off
set password	This option changes the password of the specified user name. Use the following format: set password <user_name> <new_password>
set access	This option enables or disables an account. Use the following format: set access -e/d <account_name>

Customizable default suppression expiration date

You can now customize the default expiration date of a suppression.

To customize the default expiration date of a suppression

- 1 On the computer where the ESM console is installed, log on as the administrator.

- 2 Create a system environment variable called ESM_DEFAULT_SUPPR_EXPIRATION_DELAY.
- 3 Assign one of the following values to the variable:
 - n “Never”
 - n Number of days that have passed since the suppression was created; for example, 30.
- 4 Restart the console.

If you do not create the ESM_DEFAULT_SUPPR_EXPIRATION_DELAY environment variable, ESM considers the default value of 180 days for the expiration of the suppression.

Version information for ESM components

You can determine the current version of the installed ESM components in the following ways:

- n [Viewing the properties of the manager and agent executable](#)
- n [Using the console](#)
- n [Running a domain report](#)

Viewing the properties of the manager and agent executable

To check the current version of ESM in the esmmanager.exe and esmagent.exe files, do the following:

- n Right-click the file, and click **Properties**.
- n On the **Properties** window, click the **Version** tab.
- n Check the **File Version**.

Using the console

The ESM version information for the managers and agents is also displayed in their properties on the console. This feature is available for the following ESM versions of the console, manager, and agent:

Console	ESM 6.5.3 SP1
Manager	ESM 6.0 to ESM 6.5.3 SP1
Agent	ESM 5.5 to ESM 6.5.3 SP1

The properties of the agents display the version of the latest patch that has been applied on the agents. For example, if the Signature Fix was applied on the agent, its properties display the ESM version as 6.5 Signature Fix.

Running a domain report

You can also generate a domain report on the console to check the versions of all the agents that are registered to a manager.

To run a domain report, do the following:

- n On the console, right-click the domain for which you need to generate the domain report.
- n Click **Domain Report**.
- n On the Report Options window, click **OK**.
A domain report is generated in the HTML format.
- n Click **All Agents** in the left pane of the report.
ESM Version is displayed in the right pane of the report.

Agent re-registration

ESM no longer allows multiple instances of an agent registered with a manager.

For example, if you try to re-register an agent that is already registered with its IP address, FQDN, or NetBIOS name, ESM does not create a duplicate entry for that agent, and does the following:

- n Displays a message stating that the agent is already registered using a particular name
- n Re-registers the agent with its existing name

JRE version changes

Symantec ESM 6.5.3 SP1 now includes the following JRE versions:

- n JRE 1.5.0_12 for managers, agents, and console on Windows
- n JRE 1.4.2_15 for RDL on Windows and UNIX

Symantec ESM 6.5.3 Service Pack 1 resolved issues and enhancements

[Table 6-1](#) lists the issues that were resolved in Symantec ESM 6.5.3 SP1.

Table 6-1 Symantec ESM 6.5.3 SP1 resolved issues

Defect ID	Description
878247	Suppressions do not work when the ownership of the suppression file is changed

Table 6-1 Symantec ESM 6.5.3 SP1 resolved issues

Defect ID	Description
880065	Installation overwrites the RDL files
880284	ESM manager does not resolve the DNS
881906	Agents register to one report directory
895591	Agent re-registered to the same manager with IP address as well as Net-Bios name
914100	Console crashes when a policy is run with large number of messages
933678	Communication of the RDL with the manager causes a frozen fin_wait_2 connection
937257	After reconnecting, it takes several minutes to expand the "Domains" tree node.
1001912	Client warning banner longer than ESMCheckNameValue table size limitation
1002840	Re-registration of the agent fails after remotely upgrading it from 6.0 to 6.5.3 using the agent registration wizard
1025088	In ESM 6.5.3, the registered agent is not replaced if you upgrade from ESM 6.0
1028394	Scheduler service fails with the Error 33 on 5 different managers / DST ESM 6.5.2 Manager
1029357	ESM 6.5.3 Console crashes upon startup with the Rich Content pane
1033264	The version.dat file does not get updated when you upgrade from ESM 6.0 (with signature fix) to ESM 6.5.3
1036376	Keyring.dat corruption when cdb record length reaches 1,400
1038355	Some types of port scans can send 6.5.3 managers and agents on Windows in an infinite loop
1040047	ESM Agent Segmentation Fault
1070248	ESM 6.5.3 uninstall does not leave system clean
1072620	Error 1720 when performing 6.5.3 agent installation
1074740	Failed to register ESM agent with TCP/IP after installing ESM agent with MSI installer

[Table 6-2](#) lists the enhancements in Symantec ESM 6.5.3 SP1.

Table 6-2 Symantec ESM 6.5.3 SP1 enhancements

Defect ID	Description
876443	CLI option required for setting LiveUpdate to Enabled/Disabled
881786	Need the Symantec Enterprise Reporting to be supported on Oracle 10g
971435	New CLI commands are required
1019012	The correct ESM Manager version needs to be displayed in the console
1051552	Console needs to display the version of the installed ESM components
1060919	ESM manager/agent binaries should contain the appropriate file version

Symantec ESM 6.5.3 Service Pack 1 known issues

[Table 6-1](#) lists the issues were known in Symantec ESM 6.5.3 SP1.

Table 6-3 Symantec ESM 6.5.3 SP1 known issues

Operating system	Description
All Windows and UNIX	If ESM is unable to resolve the agent's IP address, FQDN, or NetBIOS name when you re-register an agent, ESM creates an additional record for that agent.
All Windows and UNIX	If you upgrade the ESM manager and agent to ESM 6.5.3 SP1 on the same computer, the properties of the agent in the console do not display the version as ESM 6.5.3 SP1. To resolve this issue, re-register the agent with its manager.
All Windows and UNIX	The Symantec Enterprise Reporting Database Link (RDL) does not put the version information of the various ESM components in the database.
All Windows	When you uninstall an ESM manager or agent, warning messages that ask you to confirm the deletion of certain ESM files are displayed. Click Yes on the warning messages for a successful uninstallation.

Table 6-3 Symantec ESM 6.5.3 SP1 known issues

Operating system	Description
All Windows	<p>If an agent is installed using the MSI installer and you try to re-register the same agent with the same manager, no error message is displayed informing that the agent is already registered with that manager.</p>
Windows Vista (32-bit, 64-bit)	<p>You cannot remotely upgrade an ESM 6.5.2 agent to ESM 6.5.3 SP1 on Windows Vista if the agent was silently installed.</p> <p>To resolve this issue, do the following:</p> <ul style="list-style-type: none"> n Open the liveupdate.dat file that is located in the \ESM\config folder on the computer where agent is installed. n Delete the IP address of the manager to which the agent is registered. n Remotely upgrade the agent again.
Windows Vista (32-bit, 64-bit)	<p>The members of the administrators group can run register.exe only if the administrator sets the privilege level of this file.</p> <p>To set the privilege level of register.exe for all users in the administrators group, do the following:</p> <ul style="list-style-type: none"> n Log on as the BUILTIN administrator to the computer where the agent is installed. n Locate register.exe and right-click it. n Click Properties. n Click the Compatibility tab. n Click Show settings for all users. n Select Run this program as administrator under Privilege level.

54 | Related Service Pack: Symantec ESM 6.5.3 Service Pack 1
Symantec ESM 6.5.3 Service Pack 1 known issues