

Symantec Enterprise Security Manager™ Application Modules

Getting Started Guide

Symantec ESM for Databases

Symantec ESM for Firewalls

Symantec ESM for Web Servers

Symantec ESM for Antivirus

Symantec ESM for HIPAA

Symantec ESM for CIS



Application Modules Getting Started Guide

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 1.2

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, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. Enterprise Security Manager, LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or U.S. registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

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.

Understanding Symantec ESM application modules

This section includes:

- What's in the box
- What's on the CD
- Best practice policies
- Industry research sources
- Installation

Note: In the PDF version of this document, you can click a topic in the list above to go directly to that topic. Similarly, you can click an item in the Contents or Index, or a cross-reference that contains a page number.

Application modules that are designed by the Symantec Security Response team extend Symantec ESM security assessments to specific operating system and application combinations. They include best practice policies that are based on ISO 17799 and other industry standards, regulations, and best practices.

What's in the box

This guide is packaged in a box that includes a CD for one of the following products:

- Symantec Enterprise Security Manager for Databases
- Symantec Enterprise Security Manager for Firewalls
- Symantec Enterprise Security Manager for Web Servers
- Symantec Enterprise Security Manager for Routers
- Symantec Enterprise Security Manager for Antivirus
- Symantec Enterprise Security Manager for HIPAA

If the CD is defective, use the CD Replacement Form at the end of this guide to order a replacement.

An order form for the latest Symantec ESM Security Update CD is also enclosed in the box. Order this CD if you are unable to obtain Security Updates through LiveUpdate or if you are unable to download them from the Symantec Security Response Web site at <http://securityresponse.symantec.com>.

The enclosed Symantec Corporation Software License Agreement sets forth the licensing terms and conditions for the products that you have purchased. It is the same agreement that is used for Symantec ESM.

What's on the CD

The CD includes folders for software and documentation.

Software

Software files are named by architectural structure. For example, in Symantec ESM for Databases, the TPI executable for Oracle on a Solaris Sparc machine is: `oracle_tpi3\solaris-sparc-806\esmora3.tpi`.

The Symantec ESM Best Practice Policy for HIPAA on Windows 2000 is `BestPractice_Windows_2000_HIPAA_<date>`.

Documentation

Documentation includes PDF files for Best Practice Policy Manuals for each application and operating system combination. The document file names indicate the operating system and the standard applied. For example, the PDF file

name of the *Symantec ESM Best Practice Policy for HIPAA* for Windows is win-hipaa.pdf. For UNIX, it is unix-hipaa.pdf.

Some application modules also have User's Guides, such as the *Symantec ESM Modules for Oracle User's Guide*. You can also obtain information about module security checks in Symantec ESM Security Update User's Guides, which can be downloaded at <http://securityresponse.symantec.com>.

Best practice policies

Symantec ESM best practice policies are configured by the Symantec Security Response team to detect vulnerabilities that could compromise the confidentiality, integrity and/or availability of data stored and transmitted on your computer.

Some best practice policies are designed for operating system versions. Others are designed for specific application and operating system combinations. Some best practice policies require the installation of additional modules.

ISO/IEC standard

ISO-based best practice policies assess compliance with the common best practices that are described in the ISO/IEC 17799 international standard, "Information technology - Code of practice for information security management," and defined by trusted security experts and clearing houses.

Note: Symantec ESM best practice policies are based on sections of the ISO 17799 standard that address logical access controls and other security issues pertaining to electronic information systems. Symantec recommends that you review the ISO 17799 standard in its entirety to identify all issues that need to be addressed in your organization's information policy.

Other standards and regulations

The information in this guide also applies to Symantec ESM best practice policies that will be released as new products to assess compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLB), and the Center for Internet Security (CIS) benchmarks.

How best practice policies differ from default policies

The Phase 1, 2, and 3 default policies that are installed with Symantec ESM and Security Updates are intended to be modified by users. This lets you create relaxed, cautious, and strict security policies for your specific network environment.

Best practice policies are installed as read-only policies. They use Security Update modules and templates and may also introduce new modules and templates.

To customize a best practice policy, copy and rename it, then edit the copy. This preserves the original policy and protects your policy from being overwritten by updates to the best practice policy.

How base policies differ from high-level policies

Symantec ESM best practice policies are configured as base policies, as high-level policies, or as a set that includes one base policy and one high-level policy.

Base policies apply the 80-20 rule of security, which states that 80 percent of a successful compromise comes from 20 percent of a system's vulnerabilities or misconfiguration.

Base policies are configured to:

- Check for critical security vulnerabilities.
- Identify unneeded services.
- Identify missing OS and application patches.
- Assess compliance with password strength rules.

High-level policies include checks for additional best practices from the ISO 17799 standard. These practices are recommended by vendors and other trusted information security experts.

Industry research sources

As you develop your organization's information security policy, you may want to consult some of the following organizations that serve as security information clearing houses, publishing security advisories on the Internet. Acknowledgement of these organizations does not imply their endorsement of Symantec ESM best practice policies.

For more information about creating a security policy and Internet links to standards and regulations that many enterprise customers and government agencies are required to adhere to, see the article, "Importance of Corporate Security Policy" at: <http://securityresponse.symantec.com/avcenter/security/Content/security.articles/corp.security.policy.html>.

International Organization for Standardization (ISO/IEC) 17799

ISO/IEC 17799 is an international standard for electronic information systems that was released in 2000.

The predecessor of the ISO/IEC standard is the British Standard 7799 (BS 7799). See <http://emea.bsi-global.com/InformationSecurity/Overview/WhatisBS7799.xalter>.

Australian and New Zealand 4444 standards (AS 4444 and NZS 4444) have also been replaced by ISO/IEC 17799.

A helpful Internet address for ISO/IEC 17799 is <http://www.iso-17799.com>.

Center for Internet Security (CIS)

CIS is a worldwide consortium of companies, educational organizations, government and law enforcement agencies, professional associations, and individuals that are concerned about electronic information security.

The center operates by consensus. Members "identify security threats of greatest concern, then participate in development of practical methods to reduce the threats."

The center's foundational standards are:

- ISO 17799
- BS 7799 of the British Standards Institute (BSI)
- Internet Engineering Task Force (IETF)
- COBIT of the Information Systems Audit and Control Association (ISACA)

- Federal Information System Controls Audit Manual (FISCAM)
- Generally Accepted System Security Principles (GASSP) sponsored by the International Information Security Foundation
- National Institute of Standards and Technology (NIST)
- SysTrust Principles and Criteria for Systems Reliability (AICPA)

Members of the center have agreed on “security configuration specifications” called benchmarks “that represent a prudent level of due care.” You can download benchmarks and scoring tools from the Internet. The center is now working on best-practice configurations for computers that are connected to the Internet.

The Internet address of CIS Benchmarks and Scoring Tools is:
<http://www.cisecurity.org>.

CERT Coordination Center (CERT/CC)

CERT/CC is a center of Internet security expertise at the Software Engineering Institute, which is a federally-funded research and development center that is operated by Carnegie Mellon University.

“We study Internet security vulnerabilities, handle computer security incidents, publish security alerts, research long-term changes in networked systems, and develop information and training to help you improve security at your site.”

The Internet address of CERT/CC is http://www.cert.org/nav/index_main.html.

Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA standard was established by United States federal law in 1996 for the U. S. health care industry. Developed by the Department of Health and Human Services, HIPAA defines security and electronic signature standards to protect the confidentiality, integrity, and availability of individual health information.

Health care providers, health care clearing houses, and health plans that electronically maintain or transmit health information will have to comply with this security standard.

A helpful Internet address for HIPAA regulations is:
<http://www.hipaadvisory.com/regs/securityandelectronicsign/subpartc.htm>.
The U.S. Department of Health and Human Services also has a Security and Privacy Web site with a section devoted to HIPAA at:
<http://aspe.hhs.gov/admsimp/bannerps.htm#security>.

Gramm-Leach-Bliley Act (GLB)

The Gramm-Leach-Bliley Act of 1999, also known as the Financial Services Modernization Act, requires financial institutions to employ measures designed to detect any actual or attempted attacks or intrusions on customer information systems.

For information about the Gramm-Leach-Bliley Act, go to <http://rr.sans.org/legal/gramm.php>.

System Administration, Networking and Security (SANS)

The SANS Institute is a cooperative research and education organization on behalf of security practitioners in government agencies, corporations, and universities. It publishes news digests, research summaries, security alerts and papers on the Internet.

The SANS Institute and the National Infrastructure Protection Center (NIPC) publish the SANS/FBI Top Twenty list of critical internet security vulnerabilities. The list includes steps to remedy weaknesses.

SANS also includes Incidents.org, a virtual organization of intrusion detection analysts, forensics experts, and incident handlers. The Storm Center of Incidents analyzes data from thousands of firewalls and intrusion detection systems, then issues alerts and postings.

The Internet address of the SANS Top Twenty list is <http://www.sans.org/top20.htm>.

The Storm Center is at www.incidents.org.

Installation

Some application modules require only the installation of policy executable files. Others also require the installation of module TPI files.

All Symantec ESM best practice policies require the installation of compatible core products and current Security Update modules.

Module TPIs

The following released and planned application modules require the installation of their own TPI executables.

- Symantec ESM for Databases 2.0
- Symantec ESM for Databases 3.0
- Symantec ESM for Firewalls 1.0
- Symantec ESM for Firewalls 2.0
- Symantec ESM for Routers 1.0

Installation procedures for TPI files vary according to product and operating system. See the Best Practice Policy Manual that accompanies each policy.

Symantec ESM best practice policies for Web servers and future standards-based policies such as HIPAA, GLB, and CIS do not require their own TPI executables.

Prerequisites

Before you install a best practice policy, do the following:

- Make sure that the Java 2 Runtime Environment is installed on your system.
- Make sure that all managers and agents that use best practice policies run Symantec ESM version 5.1 or later.
- Upgrade the modules on all managers and agents that use best practice policies to the current Security Update.
- Identify the account name, password, and communication port for each agent that connects to each manager.
- Install the application module TPI executable (if applicable). See the product's User's Guide or Best Practice Policy Manual.

Policy installation

To install best practice polics

- 1** Run the BestPractice_<application>_<platform>executable file that is on your CD from a Windows NT, Windows 2000, or Windows XP Professional system that has network access to the manager that you want to install.
- 2** Click **Next** to close the InstallShield Welcome dialog box.
- 3** Click **Yes** to start installing the best practice policies.
- 4** Enter the requested manager information.
- 5** Click **Next**.
- 6** Click **Finish**.

Installing application modules

This chapter includes the following topics:

- Before installing the application modules
- Installation

Symantec ESM application modules are stored in a third-party installation (.tpi) file that:

- Extracts and installs module executables, configuration (.m) files, and template files.
- Registers the .m and template files using the Symantec ESM register.exe program.
- Performs application-specific functions such as configuring tablespaces for database applications.

Before installing the application modules

To get ready to install the modules

- 1 Make sure that the Java 2 Runtime Environment is installed on your system.
- 2 Upgrade all managers and agents that use best practice policies to Symantec ESM version 5.1 or later.
- 3 Upgrade the modules on all managers and agents that use best practice policies to the current Security Update.
- 4 Install modules for the application that you want to protect on all managers and agents that use best practice policies. The .tpi file that installs these modules is on your CD in a directory that is identified by application/product/modules/operating system/platform.
- 5 Identify the account name, password, and communication port for each agent that connects to each manager.

Note: Symantec best practice policies for Web servers and standards-based policies such as HIPAA, GLB, and CIS provide (or will provide) templates, word lists, register keys, and patches that run with the Symantec ESM executables. Separate executables are not required for these policies.

Installation

Module executables

The following released and planned products require the installation of their own TPI executables.

- Symantec ESM for Databases 2.0
- Symantec ESM for Databases 3.0
- Symantec ESM for Firewalls 1.0
- Symantec ESM for Firewalls 2.0
- Symantec ESM for Routers 1.0

Installation procedures vary according to application and operating system combinations. See the product's User Guide or Best Practice Policy Manual.

Not all policies require their own executables.

Policy installation

All Symantec ESM best practice policies in application modules can be installed in the following manner.

To install a product application module policy

- 1** Run the BestPractice_<application>_<platform>executable file that is on your CD from a Windows NT, Windows 2000, or Windows XP Professional system that has network access to the manager that you want to install.
- 2** Click **Next** to close the InstallShield Welcome dialog box.
- 3** Click **Yes** to start installing the best practice policies.
- 4** Enter the requested manager information, then click **Next**.
- 5** Click **Finish**.

TPI installation log

The following log shows how the third-party installation (TPI) installs on agent GS1100 and registers the modules to manager GS1001 using the register account, the account password, port 5600, and the TCP communications protocol:

```
Symantec Tune-up/3rd Party Installation package
```

```
Select an option:
```

- 1) Display description and contents of Tune-up/3rd Party...
- 2) Install this Tune-up/3rd Party Installation package on...

```
Enter option number [1]: 2
```

```
Installing tune-up package: ksysmod
```

```
This tune-up pack includes the following template and/or ".m"  
file(s):
```

```
File: C:\Program Files\Symantec\ESM\register\ win2000\account...
```

```
Description: ESM "Account Integrity" module definition file
```

```
.  
.
```

```
Template or *.m files need to be re-registered only once from the  
same type of agents with the same manager. If you have already re-  
registered this tune-up pack for the other agents of this same type  
of Operating System with the same manager you can skip this step.
```

```
Do you wish to re-register the template or .m files at this time  
[no]? yes
```

```
Enter the ESM manager that this agent is registered to:
```

```
GS1001
```

```
Enter the ESM access name to login to the ESM manager [ESM]:
```

```
<manager_name>
```

```
Enter the ESM password to use to login to the ESM manager.
```

```
Password: *****
```

Enter the network protocol used to contact the ESM manager.

1) IPX

2) TCP

Enter 1 or 2 [2]: **2**

Enter the port to contact the ESM manager [5600]? **5600**

Enter the name of this agent as it is registered to the ESM manager:
GS1100

ESM Manager: **GS1001**

ESM user name: **register**

Protocol: **TCP**

Port: **<5600>**

ESM agent: **GS1100**

Is this information correct? [yes] **yes**

Extracting C:\...\ESM\bin\w2k-ix86\mtpkreg.exe.gz...

Extracting C:\...\ESM\bin\w2k-ix86\account.exe.gz...

.

.

Extracting C:\...\ESM\template\win2000\patch.pw5.gz...

Extracting C:\...\ESM\template\win2000\patch.ps5.gz...

Re-registering modules/template files... Please wait...

 updating: Account Integrity

 updating: Account Information

.

.

 updating template patch.ps5 (Patch - Windows 2000...)

 updating template registry.rs5 Registry - Windows...

End of installation.

Registering the modules

Each time you run a .tpi file, you will be asked if you want to re-register the module and .m files. You only need to register the files once for each manager. However, if an agent is registered to multiple managers, re-run the .tpi file on the agent to register the modules with each manager. Re-register each module to any other previously-registered managers.

Note: Do not register agents that use different versions to the same manager. This can cause manager database errors.

You can continue to use earlier version agents with an upgraded manager, but you should upgrade agents to the same version as the manager as soon as feasible.

Resolving connection errors

If you get a connection error while running security checks, check the \esm\config\manager.dat file on the agent.

To resolve connection errors, add the manager's fully-qualified name to this file. If the file is missing, run setup.exe to re-register the agent to the manager.

Service and support solutions

You can reach Customer Service and Technical Support for Symantec Enterprise Security Manager and add-on products on the Internet or by telephone.

- Before contacting technical support
- Service and support Web site
- Service and support offices

Before contacting technical support

Before contacting technical support

- 1 Use online Help to look up the information you need.
- 2 Read the relevant portions of this guide and your *Symantec Enterprise Security Manager User Manual*. This guide is available as a .pdf file on the product CD.
- 3 Consult the product's release notes for the version you are using at <http://www.symantec.com/techsupp/>.

4 Gather the following information:

Category	Information	Source
Console	Machine type	Windows: System properties
	OS level	System properties
	Version	Help > About
	Date	Help > About
Manager	Machine type	UNIX: uname -a NT/2000: System properties
	OS level	UNIX: uname -a NT/2000: System properties NetWare: version
	Version and date	Manager properties
Agent	Machine type	UNIX: uname -a NT/2000: System properties NetWare: version
	OS level	UNIX: uname -a NT/2000: System properties NetWare: version
	Version and date	Agent properties
Network	Protocol vendor and version	
Problem	Symptoms	
	Steps to reproduce	
	Error message text (all characters)	
	System log file text	

Service and support Web site

The award-winning Symantec Service and Support Web site provides a wide variety of methods to help you solve your enterprise technical issues. Point your browser at <http://www.symantec.com/techsupp/>.

Knowledge Base

Search the Symantec Enterprise Security Manager Knowledge Base to find answers to common problems and questions. The Symantec Knowledge Base contains 90% of all known issues with accompanying solutions.

Often this is the fastest way to get the information that you are looking for.

If you do not use Microsoft Internet Explorer, you may have to go first to <http://www.msn.com>, then to <http://www.symantec.com/techsupp/>

Releases and updates

Download new products and Security Updates using LiveUpdate or from the Symantec Security Response Web site at <http://securityresponse.symantec.com>.

Manuals and documentation

Download current user's guides, installation guides, and other documentation in .pdf format. Most .pdf documents can be found on the product CD.

Web support

Log questions or problems for Technical Support. You can also create a case, add notes to a case, check the status of a case, and close a case.

Email support

Email pre-sales or non-technical questions to Customer Service for service options.

Symantec ESM news bulletins

Subscribe to this product specific mailing list for:

- Timely notification of product upgrades and security upgrades
- Product-specific information
- Alerts for security threats
- New product announcements
- Latest offerings from Technical Support
- Product tips and tricks

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

<http://www.symantec.com/>

Argentina and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

<http://service.symantec.com/mx>
+54 (11) 5382-3802

Asia/Pacific Rim (APAC)

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

<http://service.symantec.com/br>
+55 (11) 5189-6300
Fax: +55 (11) 5189-6210

Europe, Middle East, and Africa (EMEA)

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Mexico

Symantec Mexico
Blvd Adolfo Ruiz Cortines,
No. 3642 Piso 14
Col. Jardines del Pedregal
Ciudad de México, D.F.
C.P. 01900
México

<http://service.symantec.com/mx>
+52 (5) 661-6120

Other Latin American Countries

Symantec Corporation
9100 South Dadeland Blvd.
Suite 1810
Miami, FL 33156
U.S.A.

<http://www.service.symantec.com/mx>

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

June 2002

Symantec ESM for _____ v _____

CD Replacement Form

CD REPLACEMENT

After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return this form with your damaged CD and your payment (see pricing below, add sales tax if applicable), to the address below. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer to receive CD replacements.

CUSTOMER INFORMATION

Name _____ Company _____

Street address (no P.O. boxes please) _____

City _____ State _____ ZIP or other postal code _____

Country* _____ Daytime phone _____ Software purchase date _____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

Briefly describe the problem: _____

CD replacement price \$ 10.00

Sales tax (see table) \$ _____

Shipping & handling \$ 9.95

TOTAL DUE \$ _____

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT (CHECK ONE)

Check payable to Symantec Amount enclosed \$ _____ Visa MasterCard AMEX

Credit card number _____ Expires _____

Name on card (please print) _____ Signature _____

**U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.

MAIL YOUR CD REPLACEMENT ORDER TO

Symantec Corporation
Attention: Order Processing
555 International Way
Springfield, OR 97477
(800) 441-7234

Please allow 2-3 weeks for delivery within the U.S.

Symantec and Enterprise Security Manager are trademarks of Symantec Corporation.
Other brands and products are trademarks of their respective holders.
© 2002 Symantec Corporation. All rights reserved. Printed in the U.S.A.



Symantec ESM Security Update

CD Request Form

Symantec ESM 5.x and the Symantec ESM Application Modules require recent Security Updates (SUs), which most registered Symantec ESM 5.5 or later customers download with LiveUpdate.

Customers can also download the SUs at the Symantec Security Response Web site:

<http://securityresponse.symantec.com> > Security Updates: Enterprise Security Manager > ESM Security Updates

CD ORDERING

If you are a registered Symantec ESM customer and need a CD of the latest SUs, complete this form and send it with your payment to the address below.

CUSTOMER INFORMATION

Name _____ Company _____

Street address (no P.O. boxes please) _____

City _____ State _____ ZIP or other postal code _____

Country* _____ Daytime phone _____ Software purchase date _____

*This offer limited to U.S. and Canada. Customers outside the U.S. and Canada, please contact your local Symantec office or distributor.

CD price	No charge
Sales tax	None
Shipping & handling	\$ 9.95 USD
TOTAL DUE	\$ 9.95 USD

FORM OF PAYMENT (CHECK ONE)

Amount enclosed \$ _____ Visa MasterCard AMEX

Credit card number _____ Expires _____

Name on card (please print) _____ Signature _____

MAIL YOUR CD REPLACEMENT ORDER TO

Symantec Corporation

Attention: Enterprise Customer Service

555 International Way

Springfield, OR 97477

Email: custservcorporate@symantec.com

(800) 721-3934

Please allow 2-3 weeks for delivery within the U.S.

Symantec and Enterprise Security Manager are trademarks of Symantec Corporation.
Other brands and products are trademarks of their respective holders.
© 2002 Symantec Corporation. All rights reserved. Printed in the U.S.A.



PN: 10025180

08/02