

Symantec Enterprise Security Manager™ Modules for Oracle Databases Release Notes

Maintenance Release 3.0 for Symantec ESM 6.0, 6.1, and 6.5.x
For Red Hat Enterprise Linux, HP-UX, AIX, Windows, and Solaris



Symantec Enterprise Security Manager™ Modules for Oracle 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.

Legal Notice

Copyright ©2008 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>
Third Party Legal Notices

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Code of Use Documentation accompanying this Symantec product for more information on the Third Party Programs.

Privacy; Data Protection:

Symantec may collect and store certain non-personally identifiable information for product administration and analysis. Symantec may disclose the collected information if asked to do so by a law enforcement official as required or permitted by law or in response to a subpoena or other legal process. In order to promote awareness, detection and prevention of Internet security risks, Symantec may share certain information with research organizations and other security software vendors. Symantec may also use statistics derived from the information to track and publish reports on security risk trends. By using the Licensed Software, You acknowledge and agree that Symantec may collect, transmit, store, disclose and analyze such information for these purposes. From time to time, the Licensed Software will collect certain information from the computer on which it is installed, which may include: (a) Information regarding installation of the WebClient Installer including username and password which should not be personally identifiable if You have chosen an alias to protect Your identity. (b) Information collected by the WebClient Profile such as mandatory user/employee information including, name, e-mail address, title, position, physical address and use ID/employee ID as well as IP address and username. (c) Other information including username, user events and IP addresses which is used for product administration and analysis. All of the above information is collected and stored on the Your side and is not transferred to Symantec. Consult Your company's privacy policy for further information.

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:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- A telephone and web-based support that provides rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support 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
- 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:

- Product release level
- Hardware information

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

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

- Asia-Pacific and Japan: contractsadmin@symantec.com
- Europe, Middle-East, and Africa: semea@symantec.com
- North America and Latin America: 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

Release Notes for Symantec ESM modules for Oracle Release 3.0

What's new in this release	9
New platform support	9
256-bit AES encryption	10
New check in the Oracle Objects module	10
Configuration log	10
Resolved issues	10
Known issues	11

Release Notes for Symantec ESM modules for Oracle Release 3.0

This document summarizes Symantec ESM modules for Oracle Databases in the Maintenance release 3.0. Full documentation is included in the current *Symantec ESM Modules for Oracle Databases (Windows) User's Guide* and *Symantec ESM Modules for Oracle Databases (UNIX) User's Guide*.

What's new in this release

The following are new in this release of Symantec ESM Modules for Oracle Databases:

- [New platform support](#)
- [256-bit AES encryption](#)
- [New check in the Oracle Objects module](#)
- [Configuration log](#)

New platform support

The Symantec ESM Modules for Oracle Databases 3.0 release supports installation of the modules with all supported features on the following operating systems:

- Windows 2000
- Windows Server 2003

256-bit AES encryption

The encryption method that is used to encrypt the credentials in Symantec ESM Modules for Oracle Databases has been enhanced to use the OpenSSL's 256-bit AES encryption algorithm.

New check in the Oracle Objects module

A new check has been added in the Oracle Objects module.

Critical objects

The Critical objects check works if the Grantable privilege check or the Directly granted privilege check is enabled. This check iterates through all objects and reports critical objects in Red on ESM console when an object matches a word in the template. For example, sys.kupw\$wor, sys.dbms_ddl, and so on.

Configuration log

After configuring the SIDs, logs are created in the /esm/system/<system name> directory. The log file name is EsmOraConfig.log.

Resolved issues

The following issues are resolved in ESM modules for Oracle 3.0 (UNIX):

Configuration	<p>The configuration used to fail when the permissions of the /esm directory were manually changed from the default 770 to 700, which allowed only the root user, and not the members of the root group, to access the directory.</p> <p>This issue is now resolved and the configuration now succeeds.</p>
Policy runs	<p>The policy runs used to fail when the permissions of the /esm directory were manually changed from the default 770 to 700, which allowed only the root user, and not the members of the root group, to access the directory.</p> <p>This issue is now resolved and the policy runs now succeed.</p>
Oracle Passwords (AIX)	<p>The status of the Oracle Passwords module is no longer incorrectly reported as complete even when the module is in a running state.</p>

Oracle Tablespace (HP-UX)	The “Tablespace datafiles” check reports the permissions of the datafile correctly even when the size of the datafile is greater than 2 GB.
Oracle Patches (UNIX)	The Oracle Patches module now correctly reports the patches on a computer that has multiple Oracle homes.

Known issues

The following issues are known in ESM modules for Oracle 3.0 (UNIX):

Policy runs	If the first configured SID in the oracle.dat file is not running, the policy runs might fail to report on the other SIDs even when they are running.
Oracle Patches	The “Opatch tool” check does not report the opatch version and installed patches correctly if the opatch path contains spaces.
Oracle Accounts	The format of the time that is displayed in the Information field of the messages has been changed from HH:MM:SS to HH-MM-SS. If any messages with the HH:MM:SS format were suppressed earlier, they will reappear with the new time format.
Configuration	Configuration does not work if the Oracle server is installed on a mounted file system with the “nosuid” option set.

The following issues are known in ESM modules for Oracle 3.0 (Windows):

Oracle Patches	The Oracle Patches module is not supported on Oracle 8i.
----------------	--

Known issues

Policy runs and Configuration of SIDs (Oracle 8i)

Policy runs and configuration of the SIDs by using the “as SYSDBA” method are successful only if the following are true:

- The `sqlnet.authentication_services` parameter in the `sqlnet.ora` file is set to NTS
- The agent service is running in the context of administrator

Policy runs fail if `sqlnet.authentication_services` is set to NTS and the agent service is running in the context of the local system.

To resolve this issue, do one of the following:

- Set the value of `sqlnet.authentication_service` to NONE.
- Run the agent service in the context of administrator.

Configuration of the SIDs by using the “as SYSDBA” method fails if `sqlnet.authentication_services` is set to NONE.

To resolve this issue, do one of the following:

- Set the value of `sqlnet.authentication_service` to NTS.
- Configure the SIDs by using the SYSTEM account

Configuration of SIDs using the “as SYSDBA” method (Oracle 8i)

You cannot configure the SIDs by using the “as SYSDBA” method if you are connected to the Oracle server by using Microsoft Remote Desktop Connection (RDC).

To resolve this issue, use the SYSTEM account to configure the SIDs.

Configuration of SIDs (Oracle 8i)

You cannot configure the SIDs if the following are true:

- The SID names and databases names do not match
- You are connected to the Oracle server by using Microsoft RDC

To resolve this issue, do the following:

- For every database that you configure, type the following at the command prompt:
set Local = <database_name>

Configuration of all SIDs

You can use only the SYSTEM account to configure all SIDs by using the `-a ALL` silent configuration command. Pre-created accounts cannot be used for the same.