

Symantec Enterprise Security Manager™ Modules for Oracle Databases User's Guide

Release 2.7 for Symantec ESM 6.0, 6.1, and 6.5.x

For Solaris, AIX, HP-UX, and RHEL



Symantec Enterprise Security Manager™ Oracle Databases Release 2.7

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 ©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

As part of Symantec Security Response, the Symantec Global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- n A range of support options that gives you the flexibility to select the right amount of service for any size organization
- n Telephone and Web support components that provide 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 from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- n Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, that offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features that are available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.htm, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

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

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

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

- 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 performed prior to contacting Symantec
 - n Recent software configuration changes and/or network changes

Customer Service

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

- 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 on product updates and upgrades
- n Information on upgrade insurance and maintenance contracts
- n Information on Symantec Value License Program
- n Advice on Symantec's technical support options
- n Nontechnical presales questions
- n Missing or defective CD-ROMs or manuals

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: 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 ESM modules for Oracle Databases	
	Installing ESM modules for Oracle Databases	15
	Before you install	16
	System requirements	18
	Installing the modules	19
	About using alternate account	26
	About registering agents	27
	About customizing checks	27
	Customizing SIDs	27
	Customizing .m files	28
	Uninstalling ESM modules for Oracle Databases	29
Chapter 2	Oracle accounts	
	Establishing a baseline snapshot	31
	Automatically update snapshots	31
	Editing default settings	31
	Reporting operating system access	32
	Users to skip in OS DBA groups	32
	Users in OS DBA groups	32
	OS authenticated users	33
	Reporting user roles	33
	Roles	33
	Grantable roles	33
	Directly-granted roles	34
	New directly-granted roles	34
	Deleted directly-granted roles	35
	Reporting user privileges	35
	Privileges	35
	Grantable privileges	35
	Directly-granted privileges	36
	New directly-granted privileges	36
	Deleted directly-granted privileges	37
	Reporting user accounts	37
	Database accounts	37
	New database accounts	38

Active database accounts	38
Inactive database accounts	38
Deleted database accounts	39
Reporting account changes	39
Database account tablespace changed	39
Database account creation date changed	40
Reporting account defaults	40
Password-protected default role	40
Active default accounts	41
Users to check	41
Granted prohibited roles	41

Chapter 3 Oracle auditing

Establishing a baseline snapshot	43
Automatically update snapshots	43
Editing default settings	43
Reporting audit status and access	44
Audit trail enabled	44
Audit trail protection	44
Audit reporting methods	45
Reporting statement audits	45
Auditing options	45
Statement auditing	46
New statement auditing	46
Deleted statement auditing	47
Changed statement auditing	47
Reporting object audits	48
Auditing objects	49
Object auditing	49
New object auditing	49
Deleted object auditing	50
Changed object auditing	50
Reporting privilege audits	51
Auditing privileges	51
Privilege auditing	51
New privilege auditing	52
Deleted privilege auditing	52
Changed privilege auditing	53

Chapter 4 Oracle configuration

Editing default settings	55
Automatically update snapshots	55

Oracle system identifiers (SIDs)	55
Reporting Oracle version information	55
Oracle server	56
Oracle components	56
Trace files	56
Trace file size	56
Alert file	57
List SID:HOME (oracle.dat)	57
List SID:HOME (oratab)	57
Reporting link password encryption	57
DB link encrypted password	57
Reporting operating system account prefixes	58
Prefix for OS account	59
Table-level SELECT privileges	59
Restrictions on system privileges	59
Reporting parameter values	60
Remote login password file	60
UTL_FILE accessible directories	60
Oracle configuration watch	61
Oracle configuration watch template	61
Redo log files	63
New redo log files	64
Deleted redo log files	65
Control files	65
New control files	66
Deleted control files	66

Chapter 5 Oracle networks

Editing default settings	67
Oracle system identifiers (SIDs)	67
Reporting SID configuration status	68
SID configuration	68
Reporting net configuration violations	68
Oracle net configuration watch	68
Creating a new Oracle Net Watch template	69

Chapter 6 Oracle objects

Editing default settings	75
Oracle system identifiers (SIDs)	75
Reporting table privileges	75
Access to SYS.ALL_SOURCE	76
Table privileges	76

Object name	76
Grantors	76
Grantable privilege	76
Directly granted privilege	77

Chapter 7 Oracle passwords

Editing default settings	79
Oracle system identifiers (SIDs)	79
Users to check	79
Account status	80
Password display	80
Specifying check variations	80
Reverse order	80
Double occurrences	80
Plural	80
Prefix	81
Suffix	81
Comparing passwords to word lists	81
Password = wordlist word	81
Password = username	82
Password = any username	82
Detecting well-known passwords	83
Well-known passwords	83

Chapter 8 Oracle patches

Editing default settings	85
Oracle Home Paths	85
Template files	85
Oracle patches	86
Patch information	86
Opatch Tool	86
Installed Patches	87
Creating a new Patch template	87

Chapter 9 Oracle profiles

Establishing a baseline snapshot	89
Automatically update snapshots	89
Editing default settings	89
Oracle system identifiers (SIDs)	89
Reporting profiles and their limits	90
Profile enforcement	90
Profiles	90

New profiles	90
Deleted profiles	92
Profile resources	92
Changed resource limits	93
Reporting CPU limit violations	93
Oracle profiles	93
Sessions per user	93
CPU time per session	94
CPU time per call	94
Connection time	95
Idle time	95
Reporting password violations	95
Failed logins	96
Password grace time	96
Password duration	96
Password lock time	97
Password reuse max	97
Password reuse time	98
Password verify function	98
Invalid profiles	99

Chapter 10 Oracle roles

Establishing a baseline snapshot	101
Automatically update snapshots	101
Editing default settings	101
Oracle system identifiers (SIDs)	101
Reporting roles	102
Roles	102
New roles	102
Deleted roles	103
Reporting role privileges	103
Privileges	103
New privileges	104
Deleted privileges	104
Grantable privileges	105
Reporting nested roles	105
Nested roles	105
New nested roles	106
Deleted nested role	106
Grantable nested role	107
Reporting role access	107
Password-protected default role	107
DBA equivalent roles	108

Granted Oracle DBA role	108
Roles without passwords	108
PUBLIC role access	109

Chapter 11 Oracle tablespace

Creating a baseline snapshot	111
Automatically update snapshots	111
Editing default settings	111
Oracle system identifiers (SIDs)	111
Reporting tablespaces	112
Tablespaces	112
New tablespaces	112
Deleted tablespaces	113
Reporting tablespace datafiles	113
Tablespace datafiles	113
New tablespace datafiles	114
Deleted tablespace datafiles	114
Reporting SYSTEM tablespace information	115
Objects in SYSTEM tablespace	115
SYSTEM tablespace assigned to user	115
Reporting DBA tablespace quotas	117
Oracle tablespaces	117
MAX_BYTES in DBA_TS_QUOTAS	117
MAX_BLOCKS in DBA_TS_QUOTAS	117

Introducing Symantec ESM modules for Oracle Databases

This chapter includes the following topics:

- [Installing ESM modules for Oracle Databases](#)
- [About using alternate account](#)
- [About registering agents](#)
- [About customizing checks](#)
- [Uninstalling ESM modules for Oracle Databases](#)

Installing ESM modules for Oracle Databases

You can install the following Symantec Enterprise Security Manager (ESM) modules for Oracle on Solaris, HP-UX, and AIX platforms:

- [Oracle accounts](#)
- [Oracle auditing](#)
- [Oracle configuration](#)
- [Oracle networks](#)
- [Oracle objects](#)
- [Oracle passwords](#)
- [Oracle patches](#)
- [Oracle profiles](#)

- [Oracle roles](#)
- [Oracle tablespace](#)

Before you install

To install the modules, you need the following:

- **CD-ROM access**
At least one computer on your network must have a CD-ROM drive.
- **Account privileges**
You must have access to an account with superuser privileges on each computer where you plan to install the modules.
- **Connection to the manager**
Verify that the Symantec ESM enterprise console can connect to the Symantec ESM manager.
- **Agent and manager**
The Symantec ESM agent must be running and registered to at least one Symantec ESM manager.

Note: Real Application Clustering (RAC) is supported on only Oracle 10.x.

Minimum account privileges

The following minimum privileges for logon accounts are needed to perform ESM security checks on Oracle Server:

sys.dba_data_files
sys.dba_indexes
sys.dba_obj_audit_opts
sys.dba_priv_audit_opts
sys.product_component_version
sys.dba_profiles
sys.dba_role_privs
sys.dba_roles
sys.dba_stmt_audit_opts
sys.dba_sys_privs

sys.dba_tab_privs
sys.dba_tables
sys.dba_tablespaces
sys.dba_ts_quotas
sys.dba_users
sys.user\$\br/>v\$controlfile
v\$instance
v\$logfile
v\$parameter
v\$version

System requirements

Table 1-1 lists the operating systems that support the ESM Application modules for Oracle, and the installation file required for the Oracle versions.

Table 1-1 Supported operating systems for ESM modules on Oracle

Supported operating systems	Supported OS versions	Supported Oracle versions	Installation file (.tpi)
AIX (RS6k)	4.3.3 and later	8.1.x, 9.0.1, 9.2.0.x, 10.1.0.x, 10.2.0	esmora5.tpi, esmora7.tpi
AIX (PPC64 64-bit)	5.3	9.2.0.x, 10.1.0.x, 10.2.0	esmora6.tpi, esmora7.tpi
HP-UX	11 and later	8.1.x, 9.0.1, 9.2.0.x, 10.1.0.x, 10.2.0	esmora5.tpi, esmora7.tpi
HP-UX	11 and later	9.2.0.x, 10.1.0.x, 10.2.0	esmora6.tpi, esmora7.tpi
Solaris	2.7 and later	8.1.x, 9.0.1, 9.2.0.x, 10.1.0.x, 10.2.0	esmora5.tpi, esmora7.tpi
Solaris	2.7 and later	9.2.0.x, 10.1.0.x, 10.2.0	esmora6.tpi, esmora7.tpi
Red Hat Enterprise Linux (32-bit)	ES 3, ES 4	9.2.0.x, 10.1.0.x, 10.2.0	esmora6.tpi, esmora7.tpi

To install Symantec ESM modules for Oracle Databases, you must have the following free disk space:

Table 1-2 Disk space requirements

Agent operating system	Disk space
AIX 4.3.3 and later (RS6k)	25 MB
AIX 5.3	25 MB
HP-UX 11 and later	25 MB
Solaris 2.7 and later	25 MB
Linux x86	70 MB

Installing the modules

The modules are stored in an installation package named `esmora7.tpi`, which is supported on Red Hat Enterprise Linux ES 3 and ES 4, Solaris, AIX, and HP-UX.

See [Table 1-1, “Supported operating systems for ESM modules on Oracle,”](#) on page 18.

If you are installing the modules using an older `tpi`, note the following:

- For Red Hat Enterprise Linux ES 3 and ES 4 and Solaris, the installation package is named `esmora6.tpi`.
- For AIX, HP-UX, and Solaris, the installation package is named `esmora5.tpi`.

The package does the following:

- Extracts and installs module executables, configuration (`.m`) files, and template files.
- Registers the `.m` and template files using your agent’s registration program.
- Creates the `ESMDBA` account when the `esmora7.tpi` is run to configure a SID. The password of `ESMDBA` account is 12 characters long and is generated randomly. The password is encrypted by using a proprietary encryption function and is stored in the following file:
`/esm/config/oracle.dat`

- Changes the `ESMDBA` account password according to the period that is specified by the parameter "PassChangedPeriod" in the `/esm/config/oraenv.dat` file. The default days of "PassChangedPeriod" is 35 days. In ESM modules for Oracle, the password must contain at least one upper-case, one lower-case, one number (0-9), and one special character. The default special characters are:

```
_+ -= <> ? ( ) * > % & # ! ~ { }
```

This is the character set that is used if the config `PassSpecString` entry is not defined in the `/esm/config/oraenv.dat` file.

To use another set of special characters, you must add a "config `PassSpecString $#_`" entry into the `/esm/config/oraenv.dat` file before running the `tpi` or `esmora7.tpi` program.

For more information on the `oraenv.dat` file, see [Using the oraenv.dat file](#).

- Grants the following privileges:
 - For Oracle 8.X: `SELECT_CATALOG_ROLE`;
 - For Oracle 9.X and 10.X: `SELECT ANY DICTIONARY`;
 The `ESMDBA` account has the read-only privilege. During the policy runs, the `ESMDBA` account does not create any object in the database.

Using the oraenv.dat file

The oraenv.dat file is a configuration file that stores the configuration parameters, which control certain functions of the ESM modules for Oracle.

To specify the parameters, create the oraenv.dat file in the /esm/config directory.

You can specify the following parameters in the oraenv.dat file:

SHELL	<p>Set an environment variable during an ESM Oracle module policy run.</p> <p>For example, to set the SHELL environment variable to /bin/bash, add the following entry to the oraenv.dat file:</p> <p>set SHELL /bin/bash</p>
ORA_LANG	<p>Unset an environment variable during an ESM Oracle module policy run.</p> <p>For example, to unset the ORA_LANG environment variable, add the following entry to the oraenv.dat file:</p> <p>unset ORA_LANG</p>
DebugFlag	<p>Configure debug level.</p> <p>To configure the debug level, add the following entry to the oraenv.dat file:</p> <p>config DebugFlag 1</p> <p>The default debug level is 0.</p>
PassCreationLog	<p>Configure the logging level for password creation.</p> <p>To configure the logging level for password creation, add the following entry to the oraenv.dat file:</p> <p>config PassCreationLog 1</p> <p>The default logging level is 0.</p>
PassSpecString	<p>Configure the special characters for password.</p> <p>For example, to configure the different set of special characters for the password, add the following entry to the oraenv.dat file:</p> <p>config PassSpecString \$#_</p> <p>The default special characters are as follows:</p> <p><code>_+--<>()*%&#!~{}</code></p>

PassChangePeriod Configure the period to change the password .

For example, to change the password change period value to 60, add the following entry to the oraenv.dat file:

config PassChangePeriod 60

The default value is 35.

To run the installation program and register the files

- 1 At the command prompt, type **su** or **logon** to access the root directory.
- 2 Type **cd <path>** to open the directory that corresponds to your vendor/operating system/architecture, where <path> is one of the following:
 - /hp/hpux/parisc/esmora
 - /sun/solaris/sparc/esmora
 - /ibm/aix/rs6k/esmora
- 3 Type **./esmora7.tpi**.
 For older versions of ESM modules for Oracle, do one of the following:
 - Type **./esmora6.tpi** for Red Hat Enterprise Linux ES 3 and ES 4, and Solaris.
 - Type **./esmora5.tpi** for AIX, HP-UX, and Solaris.
 See [Table 1-1, “Supported operating systems for ESM modules on Oracle,”](#) on page 18.
- 4 Type a **1** or a **2** to select an option:
 - Option 1 Displays the contents of the package. To install the module, rerun the tpi and select option 2.
 - Option 2 Displays a list of files that will be installed and the modules or templates that they belong to. Register template and .m files only once for agents that use the same manager on the same operating system.
- 5 Do one of the following:
 - If the template files are not registered with the manager, type **Y**.
 - If the template files have already been registered, type **N**.
- 6 Type the name or IP address of the manager to which the agent is registered.
- 7 Type the logon name for the manager.
- 8 Type the agent name as it is registered to the manager.
- 9 Type the password to log on to the manager.

- 10 Type the port number that the manager uses.
- 11 Do one of the following:
 - If the displayed information is correct, type **Y**.
File names are displayed as they are extracted.
 - If the information is not correct, type **N**.
The command line is returned.
- 12 When the extraction is complete, the installation program asks if you want to add configuration records to enable security checking for the oracle database. Do one of the following:
 - To continue the installation and connect to the current SID, type **Y**.
 - To end the installation without adding the security checks, type **N**.
- 13 Do one of the following:
 - Type **A** to connect using "SYSTEM" account.
 - Type **B** to connect using "/as sysdba" method.
- 14 If you chose option A, see [To add security checking using the default SYSTEM account](#). If you chose option B, see [To add security checking using the "/as sysdba" method](#).

To add security checking using the default SYSTEM account

- 1 Type the Oracle Home path, or press **Enter** to accept the default path.
- 2 Type the SYSTEM account password.
- 3 Retype the password.
- 4 Type the name of the temporary tablespace for the ESMDBA user or press **Enter** to accept the default name.
- 5 Type the name of the default tablespace for the ESMDBA user, or press **Enter** to accept the default name.
- 6 Type the name of the profile for the ESMDBA user or press **Enter** to accept the default name.
- 7 Review the summary information that the installation program displays. Type **Y** to begin the installation.
Symantec ESM does the following:
 - Verifies the password
 - Connects you to the database as a SYSTEM user
 - Creates an ESMDBA user account in your Oracle database with privileges to perform security checks

The SYSTEM account password is not stored. The ESMDBA user account is used to perform security checks.

If an ESMDBA account already exists, Symantec ESM drops it, then recreates it.

- Finds the next SID in the oratab file and prompts you to continue
- 8 Do one of the following:
 - To add security checking for the next SID, type **Y**.
 - To continue without adding security checks to the next SID, type **N**.
 - 9 Repeat steps 3 through 10 until you have installed the security checks or skipped the installation on every SID in your oratab file.
 Do not change the privileges or password of the ESMDBA account. Drop this account only if you uninstall the agent from the computer.

Any time after installation, you may add or update a pre-created Oracle account, from the command line, to perform the ESM security checks, instead of the default SYSTEM account.

To add security checking using the "/as sysdba" method

- 1 Type the Oracle Home path, or press **Enter** to accept the default path.
- 2 Type **Y** to add security checking for the designated SID.
- 3 Type the name of the temporary tablespace for the ESMDBA user or press **Enter** to accept the default name.
- 4 Type the name of the default tablespace for the ESMDBA user, or press **Enter** to accept the default name.
- 5 Type the name of the profile for the ESMDBA user or press **Enter** to accept the default name.
- 6 Do one of the following:
 - To configure the next SID, type **Y**.
 - To continue without configuring the next SID, type **N**.
- 7 Repeat steps 4 through 9 until you have installed the security checks or skipped the installation on every SID in your oratab file.
 Do not change the privileges or password of the ESMDBA account. Drop this account only if you uninstall the agent from the computer.

Note: The "/as sysdba" method for configuring the SIDs is available only in esmora7.tpi.

Note: The following procedure must be used to support RAC clustering. You must have a pre-created oracle account to run the ESM security checks in RAC clustering mode. ESMDBA user accounts are not created for RAC clustering.

To add security checking using a pre-created account

- 1 When the extraction is complete, the installation program asks if you want to add configuration records to enable security checking for the oracle database.
 - To continue the installation and connect to the current SID, type **Y**.
 - To end the installation without adding the security checks, type **N**.
- 2 Type **Y** to configure the designated SID for security checking.
- 3 Type the Oracle Home path, or press **Enter** to accept the default path.
- 4 Type the pre-created Oracle account name.

A pre-created Oracle account, used to perform the security checks, will be checked for CONNECT and SELECT privileges instead of the default SYSTEM account.
- 5 Type the pre-created Oracle account password.
- 6 Retype the password.
- 7 The installation program asks if you want to add security checking for SID ESM. Type **Y** or **N**.

Repeat steps 3 through 7 until you have installed the security checks or skipped the installation on every SID in your oratab file.

If you configure an instance that is mounted in RAC cluster database mode, you must use a pre-created account. Otherwise, the esmorasetup program displays the following message:

```
The <SID> instance is mounted in cluster database mode.  
To prevent conflicting password for the ESMDBA account,  
You need to provide a pre-created logon account to be used  
by the ESM Modules for Oracle Database security checks.  
Failed to configure Oracle SID <SID>.
```

To add or update a pre-created Oracle account

- ◆ At the command prompt, type the following:

```
esmorasetup -a {SID} [-A {ACCOUNT}] [-P {PASSWORD}] [-H {ORAHOME}] [-Q]
```

-A {Account} Predefined Oracle database logon account

-P {Password} Predefined Oracle database logon account password

- H {OraHome} Oracle home directory
- Q Silent install, does not prompt for confirmation

Silently installing the modules

You can install the ESM Modules for Oracle and configure the SIDs in a single step by doing a silent install. The modules can be silently installed only using `esmora7.tpi`.

You can use the following options while silently installing the ESM modules for Oracle:

- d Display the description and contents of this Tune-up/third-party installation package
- i Install this Tune-up/third-party installation package
- U Specify ESM access record name
- P Specify ESM access record password
- p Specify the TCP Port to use
- m Specify the ESM manager name
- t Connect to the ESM manager using TCP
- x Connect to the ESM manager using IPX (for Windows only)
- g Specify the ESM agent name to use for reregistration
- N Do not update the report content file on the ESM manager
- Y Update the report content file on the ESM manager
- K Do not prompt for and do the re-registration of agents
- A Specify the Oracle SYSTEM user
- C Specify the password for Oracle SYSTEM user
- T Specify the temporary tablespace.
This option is used by the ESMDBA users. The default value is TEMP.
- S Specify the default tablespace.
This option is used by the ESMDBA users. The default value is USERS.
- W Specify the user's profile.
This option is used by the ESMDBA users. The default value is DEFAULT.
- h Display help on the usage of options that can be used for silent installation

To silently install the ESM modules for Oracle

- ◆ At the command prompt, type the following:
`./esmora7.tpi {-it} {-m} {-U} {-p} {-P} {-g} {Y}`

The above command only installs the ESM modules for Oracle. To configure the SIDs for security checking, run `esmorasetup`, which is located in the `/esm/bin/<platform>` directory.

To silently install the ESM modules for Oracle and configure all SIDs

- ◆ At the command prompt, type the following:
`./esmora7.tpi {-it} {-m} {-U} {-p} {-P} {-g} {Y} {-A} {-C} [-T] [-S] [-W]`

About using alternate account

Initially, to install the ESM modules for Oracle and configure the SIDs on the databases, a user was required to log on to the computer as SYSTEM.

An alternate method `"/as sysdba"` has been introduced in the ESM modules for Oracle. Using the `"/as sysdba"` method, a user can log on to the Oracle server without providing a user name and password, and configure all SIDs.

The superuser needs to change the ownership of the `tpi` to enable the other users to do the installation.

To use the alternate account

- 1 Log on to the computer as the superuser.
- 2 Copy `esmora7.tpi`.
- 3 Change the ownership of `esmora7.tpi` by typing the following command:
chown root: oinstall esmora7.tpi
The users of the `oinstall` group get the superuser privileges to use `esmora7.tpi`.
- 4 Apply sticky bit to `esmora7.tpi` by typing the following command:
chmod 4750 esmora7.tpi
- 5 Log on to the Oracle server as an Oracle account.
- 6 Run the `tpi` and configure the SIDs.
See [“Installing the modules”](#) on page 19.
See [“Silently installing the modules”](#) on page 25.

About registering agents

Each agent must reregister with a manager. The `esm3rd.tpi` program prompts you for the required information when the agent is installed with new modules.

To manually reregister an agent to additional managers, use the `esmsetup` program. See your *Symantec ESM Installation Guide* for information about accessing and running the `esmsetup` program.

If connection errors are reported while running security checks, examine the `/esm/config/manager.dat` file on the agent. You can add the manager's fully-qualified name to the file or if the file is missing, manually reregister the agent to the manager.

About customizing checks

After installation, you can change the configuration of SIDs and security checks in the `.m` files.

Customizing SIDs

You can change the Oracle instances that are included in security checks by using the `esmorasetup` program that is installed in the `/esm` directory.

Table 1-3 SID customization options

To do this	Type
Configure a new SID	<code>esmorasetup -a <sid_name></code>
Configure all SIDs	<code>esmorasetup -a ALL [-f <file_name>]</code>
Configure a new SID using a specified oratab file	<code>esmorasetup -a <sid_name> -f <file name></code>
Display Help	<code>esmorasetup</code>
Perform the above tasks interactively	<code>esmorasetup -a <SID_name></code>
Register an Oracle Home into Symantec ESM modules for Oracle Databases	<code>esmorasetup -H <OraHome></code>
Remove (delete) a SID	<code>esmorasetup -d <SID_name></code>
Remove (delete) all SIDs (both using the SYSTEM account and “/as sysdba” method)	<code>esmorasetup -d all</code>
Remove a registered Oracle Home from Symantec ESM modules for Oracle Databases	<code>esmorasetup -R <OraHome></code>

Table 1-3 SID customization options

To do this	Type
Specify an Oracle database SYSTEM password	<code>esmorasetup -a <SID_name> [-f file name>] -P <password> [-H <OraHome>]</code>
Update Oracle home for all registered SIDs	<code>esmorasetup -U all [-f <file name>]</code>
Update Oracle home for one registered SID	<code>esmorasetup -U <SID_name> [-f <file name>] [-H <OraHome>]</code>

For example, to specify an oratab on a SID, with a password, and using the interactive mode, type the following:

```
./esmorasetup <-a|-d> <sid_name|all> [-P <SYS_PASSWORD>]
[-f <file_name>]
```

You can silently change the Oracle instances that are included in security checks by using the `esmorasetup` program that is installed in the `/esm` directory.

Table 1-4 Silent SID customization options

To do this	Type
Configure an SID silently by connecting to the database as SYSTEM account	<code>esmorasetup -a <SID_name> [-f <file_name>] -A <account_name> -P <password> [-H <OraHome>] [-T <Temp>] [-S <Users>] [-W <Default>] -Q</code>
Configure an SID silently by connecting to the database by using the “/as sysdba” method	<code>esmorasetup -a <SID_name> [-f <file_name>] -A <account_name> -P <password> [-H <OraHome>] [-T <Temp>] [-S <Users>] [-W <Default>] -Q</code>
Configure all SIDs silently by connecting to the database as SYSTEM account	<code>esmorasetup -a ALL -A SYSTEM -P <password> [-T <Temp>] [-S <Users>] [-W <Default>] -Q</code>
Configure all SIDs silently by connecting to the database by using the “/as sysdba” method	<code>esmorasetup -a ALL -A <oracle_owner> [-T <Temp>] [-S <Users>] [-W <Default>] -Q</code>

Customizing .m files

Module configuration (.m) files contain the messages that report security check results.

The .m files reside in the agent’s `/esm/register/<os>` directory.

The .m files consist of ASCII text that you can edit with a text editor. Individual lines of text should not exceed 128 characters. Some lines of text in a .m file start with directives. Directives classify information and are:

- Preceded by a dot or period character (.)
- Followed by data or descriptive text
- Not case-sensitive

To edit a .m file

- 1 Select an agent with an operating system of the type that reports the security messages you want to edit.
Use a text editor to modify the security messages.
- 2 Verify that the customized directive in each modified message has been changed to .customized 1. Otherwise, whenever you update an agent, the .m file changes will be overwritten.
Changes to the messages are saved in the manager database.
- 3 Register the agent that contains the customized .m files to all the managers that run policies on the agent.
- 4 Verify that the modified messages appear on the manager systems in the default location that is shown in Table 1.2. You can relocate this file.

Table 1-5 Default message.dat file location

System	Directory
UNIX	Symantec ESM creates a symbolic link: /esm/system/<system name>/db/message.dat

For more information about .m file directives, see the *Symantec ESM Security Update User’s Guide for UNIX Modules*.

Uninstalling ESM modules for Oracle Databases

Uninstalling the ESM modules for Oracle databases includes the following:

- Deleting the logon account
- Uninstalling the ESM agent on which the module is installed

To delete the logon account for Oracle 2.6.0 and before

- 1 Change to the /esm/bin/<platform> directory.
- 2 Run the esmorasetup utility as follows:

./esmorasetup -d all

- 3 Type **Y** to confirm the deletion of the security checking for the specified SID.
- 4 Type the password for the SYSTEM account.
- 5 Type **Y** to continue deleting the security checking for the SID.
- 6 Repeat steps 3 through 5 to delete the security checking for other SIDs that are configured.

To delete the logon account for Oracle 2.7

- 1 Change to the /esm/bin/<platform> directory.
- 2 Run the esmorasetup utility as follows:
./esmorasetup -d all
- 3 Do one of the following:
 - Type **1** to connect as SYSTEM.
 - Type **2** to connect using “/as sysdba”.
- 4 Type **Y** to confirm the deletion of the security checking for the specified SID.
- 5 Type the password for the SYSTEM account if you chose option 1 in step 3.
- 6 Type **Y** to continue deleting the security checking for the SID.
- 7 Repeat steps 3 through 5 to delete the security checking for other SIDs that are configured.

To uninstall the ESM agent on which the module is installed

- 1 Change to the /esm directory.
- 2 Run the esmdeinstall utility as follows:
./esmdeinstall
- 3 Type **Y** to continue.

Note: Uninstalling the ESM agent on which the ESM module for Oracle Databases is installed also uninstalls the module.

Oracle accounts

This chapter includes the following topics:

- [Establishing a baseline snapshot](#)
- [Editing default settings](#)
- [Reporting operating system access](#)
- [Reporting user roles](#)
- [Reporting user privileges](#)
- [Reporting user accounts](#)
- [Reporting account changes](#)
- [Reporting account defaults](#)

Establishing a baseline snapshot

To establish a baseline snapshot file, run the Symantec ESM module for Oracle accounts once. Periodically rerun the module to detect changes and update the snapshot when appropriate.

Automatically update snapshots

Enable this option to update snapshots automatically with current information.

Editing default settings

The module for Oracle accounts includes one option, that you can use to edit default settings for all security checks in the module.

Use the name lists in the Oracle system identifiers (SIDS) option to specify Oracle system identifiers (SIDs) that are to be examined by module checks. By

default, the module examines all SIDs that are specified when you configure Symantec ESM modules for Oracle Databases. The configuration file for Symantec ESM modules for Oracle Databases is stored in `/esm/config/oracle.dat`.

Reporting operating system access

Users who can access the database as OS administrators have exceptional privileges. Users who can access the database directly from the operating system do so without the protection of Oracle authentication. Both groups of users should be monitored to ensure your systems are protected. The following checks monitor for these users.

Users to skip in OS DBA groups

You can use the name lists in this option to specify users who are to be excluded for Users in OS DBA groups. By default, all users in each group are included.

Users in OS DBA groups

This check reports users who can connect to a database as INTERNAL, SYSDBA, or SYSOPER. The check also reports users who connect as members of DBA, OPER, OSDBA, and OSOPER groups.

You can use the Users to skip in OS DBA groups check to specify which users are to be excluded for the check (usually administrators). You can also use the check's name list to specify OS database administrator groups and users to be included for the check.

Table 2-1 User in OS DBA groups message

Message name	Title	Severity
UNAUTHORIZED_INTERNAL	User in OS DBA group	Red (4)

To protect your computers

- ◆ Drop unauthorized users from OS DBA groups.

OS authenticated users

This check reports users who are authenticated only by the operating system, without Oracle authentication.

The user can log in to Oracle without providing a user name and password. This method of authentication may be appropriate for development or testing environments, but it should not be permitted in production environments.

Table 2-2 OS authenticated user message

Message name	Title	Severity
USER_AUTHORIZED_EXTERNAL	User authenticated by OS only	Yellow (1)

You can use the check's name list to specify users who are to be excluded for the check.

To protect your computers

- ◆ Do the following
 - Change the user's password authentication from external to local.
 - Require Oracle authentication to add another level of security.

Reporting user roles

These checks report roles that have been directly granted to users or revoked from users and the associated user names. Nested roles are not reported.

For checks that report role definitions, see [“Oracle roles”](#) on page 101.

Roles

Use the name lists in this option to specify roles that are to be included or excluded for the Directly-granted roles and Grantable roles checks.

Grantable roles

This check reports usernames with permissions to grant roles to other users.

Use the check's name list to specify users who are to be excluded for the check.

Table 2-3 Grantable role message

Message name	Title	Severity
GRANTABLE_ROLE	Grantable role	Yellow (1)

To protect your computers

- ◆ Do the following:
 - Revoke the grantable roles from any user who is not authorized to grant it.
 - Periodically review all users with grantable roles to ensure that they are currently authorized to grant their grantable roles.

Directly-granted roles

This check reports roles that have been directly granted to users. Roles that were nested in directly-granted roles were also deleted, but they are not reported.

Use the check’s name list to specify users who are to be excluded for the check.

Table 2-4 Role directly-granted to user message

Message name	Title	Severity
PRIVILEGE_LIST_ROLES	Role directly-granted to user	Green (0)

To protect your computers

- ◆ Periodically review this check to ensure that users with directly-granted roles are authorized, and then revoke inappropriately directly-granted roles.

New directly-granted roles

This check reports user names with roles that were directly granted to them after the last snapshot update. Roles that are nested in directly-granted roles are not reported.

Use the check’s name list to specify users who are to be excluded for the check.

Table 2-5 New directly-granted role message

Message name	Title	Severity
USER_ROLE_ADDED	New role granted to user	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the user is authorized for this role, update the snapshot.
 - If the user is not authorized for this role, revoke it from the user.

Deleted directly-granted roles

This check reports user names with directly-granted roles that were revoked or dropped after the last snapshot update. Roles that are nested within the directly-granted role are also deleted or revoked, but are not reported.

Use the check's name list to specify users who are to be excluded for the check.

Table 2-6 Deleted directly-granted role

Message name	Title	Severity
USER_ROLE_DELETED	Role deleted from user	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the deletion is authorized, update the snapshot.
 - If the deletion is authorized, restore the role to the user.

Reporting user privileges

These checks report users with grantable privileges and privileges that have been directly granted to users or revoked from users.

Privileges

Use the name lists in this option to specify system privileges that are to be included or excluded for grantable and directly-granted privileges checks.

Grantable privileges

This check reports users with the privileges that they can directly grant.

Use the check's name list to specify users who are to be excluded for the check.

Table 2-7 Grantable privilege message

Message name	Title	Severity
GRANTABLE_PRIV	Grantable privilege	Green (0)

To protect your computers

- ◆ Do the following:
 - Revoke the privilege from any user who is not authorized to grant it.
 - Periodically review grantable privileges to ensure that users are currently authorized to grant their grantable privileges.

Directly-granted privileges

This check reports users with system privileges that have been directly granted to them. To simplify maintenance, privileges are usually granted in roles.

Use the check’s name list to specify users (SIDs) that are to be excluded for the check.

Table 2-8 Directly-granted privilege

Message name	Title	Severity
PRIVILEGE_LIST_DIRECT	Privilege directly-granted	Green (0)

To protect your computers

- ◆ Revoke the privilege from any user who is not authorized for it.

New directly-granted privileges

This check reports users with privileges that were directly granted to them after the last snapshot update. To simplify maintenance, privileges are usually granted in roles.

Use the check’s name list to specify users who are to be excluded for the check.

Table 2-9 New granted privilege message

Message name	Title	Severity
USER_PRIV_ADDED	New privilege granted to user	Yellow (1)

To protect your computers

- If the user is authorized for this privilege, update the snapshot.
- If the user is not authorized for this privilege, revoke the privilege.

Deleted directly-granted privileges

This check reports users with directly-granted privileges that were revoked or dropped after the last snapshot update.

Use the check's name list to specify users who are to be excluded for the check.

Table 2-10 Directly-granted privilege deleted message

Message name	Title	Severity
USER_PRIV_DELETED	Privilege deleted from user	Yellow (1)

To protect your computers

- 1 If the deletion is authorized, update the snapshot.
- 2 If the deletion is not authorized, restore the privilege.

Reporting user accounts

These checks report current, new, active, inactive, and deleted database accounts.

Database accounts

This check reports user accounts, their tablespaces, and account creation dates.

Use the check's name list to specify users who are to be excluded for the check.

Table 2-11 Database account message

Message name	Title	Severity
USER_ACCT	Database account	Green (0)

To protect your computers

- ◆ Do the following:
 - Delete unauthorized or out-of-date accounts.
 - Periodically review database accounts to ensure that they and their tablespaces are currently authorized.

New database accounts

This check reports user accounts that were added to the database after the last snapshot update.

Use the check's name list to specify users who are to be excluded for the check.

Table 2-12 New database account message

Message name	Title	Severity
USER_ACCT_ADDED	New database account	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the new account is authorized, update the snapshot.
 - If the new account is not authorized, delete it.

Active database accounts

This check reports active user accounts with their tablespaces, profile, and account creation date. You should review user accounts periodically to verify that they are current and authorized.

Table 2-13 Active database accounts message

Message name	Title	Severity
ACTIVE_USER_ACCT	Active database account	Green (0)

Inactive database accounts

This check reports inactive user accounts with their inactive status, date, and account creation date. You should review user accounts periodically to verify that they are current and authorized.

Table 2-14 Inactive database accounts message

Message name	Title	Severity
INACTIVE_USER_ACCT	Inactive database account	Green (0)

Deleted database accounts

This check reports user accounts that were deleted after the last snapshot update.

Use the check's name list to specify user accounts that are to be excluded for the check.

Table 2-15 Deleted database account message

Message name	Title	Severity
USER_ACCT_DELETED	Deleted database account	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the deletion is authorized, update the snapshot.
 - If the deletion not is authorized, restore the account.

Reporting account changes

These checks report changes to tablespace assignments and creation dates.

Database account tablespace changed

This check reports database accounts that changed after the last snapshot update. The user account has been deleted and recreated. When a user account is deleted, all data associated with it can also be deleted.

Use the check's name list to specify users who are to be excluded for the check.

Table 2-16 Changed tablespace message

Message name	Title	Severity
USER_ACCT_TABLESPACE	Database account tablespace changed	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the change is authorized, update the snapshot.
 - If the change is not authorized, restore the tablespace.

Database account creation date changed

This check reports database accounts with creation dates that changed after the last snapshot update. This indicates that the user account has been deleted and recreated. When a user account is deleted, all data that is associated with it can also be deleted.

Use the check's name list to specify users who are to be excluded for the check.

Table 2-17 Changed creation date message

Message name	Title	Severity
USER_ACCT_CREATION	Database account creation date changed	Green (0)

To protect your computers

- ◆ Do one of the following:
 - If the change is authorized, update the snapshot.
 - If the recreated account is not authorized, drop the account.

Reporting account defaults

These checks report password-protected roles that are used as default roles and default accounts with default passwords.

Password-protected default role

This check reports users who have been granted password-protected roles as default roles.

Default roles do not require passwords. Password-protected roles typically include privileges or roles that require authorization. Users who have password-protected default roles do not have to use passwords to use those roles.

Use the check's name list to specify users who are to be excluded for the check.

Table 2-18 Password protected role as default message

Message name	Title	Severity
DEFAULT_ROLE_WITH_PASSWORD	Default role with password protection	Yellow (1)

To protect your computers

- ◆ If the user is not authorized to use this role without typing a password, do one of the following:

- Assign a different default role to the user.
- Remove password protection from the role.
Users who have the role will not be required to type passwords to use it.

Active default accounts

This check reports default accounts that are available on your system.

The check's name list should include all Oracle default accounts. Intruders can use default accounts to access your database.

Table 2-19 Active default account message

Message name	Title	Severity
ACTIVE_DEFAULT_ACCT	Active default account	Yellow (1)

To protect your computers

- ◆ Remove, lock, or disable the account to prevent intruders from using it to access your database.

Users to check

You can use the name lists in this option to specify which users are to be included or excluded for Granted prohibited roles.

Granted prohibited roles

This check reports users who have been granted prohibited roles.

Use the check's name list to specify the prohibited roles that are to be included or excluded for the check.

Note: A few default Oracle roles the DBA (database administrator) role and the connect role should never be directly granted to users.

Table 2-20 Prohibited role granted message

Message name	Title	Severity
ROLE_GRANTED	Prohibited role granted	Yellow (1)

To protect your computers

- ◆ Drop the prohibited role.

Oracle auditing

This chapter includes the following topics:

- [Establishing a baseline snapshot](#)
- [Editing default settings](#)
- [Reporting audit status and access](#)
- [Audit reporting methods](#)
- [Reporting statement audits](#)
- [Reporting object audits](#)
- [Reporting privilege audits](#)

Establishing a baseline snapshot

To establish a baseline, run the Symantec ESM module for auditing Oracle databases. This creates a snapshot of current audit information that you can update when you run checks for new, deleted, or changed information.

Automatically update snapshots

Enable this option to update snapshots automatically with current information.

Editing default settings

The Auditing module for Oracle databases includes one option that you can use to edit default settings for all security checks in the module.

You can use the name lists in this option to specify Oracle system identifiers (SIDs) that are to be examined by module checks. By default, the module examines all SIDs that are specified when you configure Symantec ESM modules

for Oracle Databases. The configuration file? for Symantec ESM modules for Oracle Databases is stored in /esm/config/oracle.dat.

Reporting audit status and access

These checks report whether auditing is enabled and who has access to the audit trail database.

Audit trail enabled

This check reports whether an audit trail is available for the SID.

You can use the check's name list to specify the users who are to be excluded for the check.

Table 3-1 Auditing not enabled message

Message name	Title	Severity
AUDIT_DISABLE	Auditing not enabled for the SID	Red (4)

To protect your computers

- ◆ In a production environment, ensure that the audit trail is enabled by setting the AUDIT-TRAIL parameter to DB or OS.

Audit trail protection

This check reports users and roles that have privileges that allow them to make changes or deletions to the audit trail database.

You can use the check's name list to specify the users who are to be excluded for the check.

Table 3-2 Audit trail protection message

Message name	Title	Severity
AUDIT_PROTECTION	Audit trail protection	Yellow (2)

To protect your computers

- ◆ Do the following
 - Grant access to the audit trail database only to administrators or users with administrator roles.
 - If the user is not authorized to access the audit trail database, drop the role from the user.

- Drop the privilege of an inappropriately defined role.
- Ensure that the auditing options of DEL, INS, and UPD for SYS.AUD\$ are set properly to A/A in dba_obj_audit_opts.

Audit reporting methods

The success or failure of an audited operation is identified by the following codes, separated by the forward slash (/) character:

- A indicates reporting is BY ACCESS.
- S indicates reporting is BY SESSION.

Table 3-3 Reporting methods

Method	Description of report
A/A	Every successful and failed operation
A/S	Every successful operation, but only sessions in which failed operations occur
S/S	Every session in which successful and failed operations occur
S/A	Every session in which an operation was successful and every failed operation

Reporting statement audits

The Auditing module for Oracle databases reports SQL statements that are audited. Security checks report statements that were set or removed for auditing and statements with success or failure reporting methods that changed after the last snapshot update.

Audits at the statement level can require considerable resources. BY ACCESS (A) reporting consumes more resources than BY SESSION (S) reporting.

Auditing options

You can use the name lists in this option to specify options to be included or excluded for Statement auditing and New/Deleted/Changed statement auditing checks.

Statement auditing

This check reports user SQL statements that are audited and the Success/Failure reporting methods that are used.

You can use the check's name list to specify the users who are to be excluded for the check.

Table 3-4 Statement auditing message

Message name	Title	Severity
STMT_AUDITING	Statement auditing	Green (0)

To protect your computers

- ◆ Do the following:
 - Remove unauthorized or out-of-date statements.
 - Ensure that reporting methods are appropriate for the available resources and perceived risks.

New statement auditing

This check reports SQL statements that were set for auditing after the last snapshot update, and the Success/Failure reporting methods that are used.

Use the check's name list to specify the users who are to be excluded for the check.

Table 3-5 New statement auditing message

Message name	Title	Severity
NEW_STMT_AUDITING	New statement auditing	Yellow (1)

To protect your computers

- ◆ Do the following:
 - Remove unauthorized or out-of-date statements.
 - If auditing of the statement is authorized and the reporting methods are correct, update the snapshot.
 - If auditing of the statement is not authorized, deactivate the audit.
 - If the reporting methods are not appropriate for available resources and perceived risks, change the reporting methods.

Deleted statement auditing

This check reports user statements that were removed from auditing after the last snapshot update.

You can use the check's name list to specify the users who are to be excluded for the check.

Table 3-6 Deleted statement auditing message

Message name	Title	Severity
DELETED_STMT_AUDITING	Deleted statement auditing	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the statement deletion is authorized, update the snapshot.
 - If the statement deletion is not authorized, restore the audit setting.

Changed statement auditing

This check reports audited user statements with Success/Failure reporting methods that changed after the last snapshot update.

You can use the check's name list to specify the users who are to be excluded for the check.

Table 3-7 Changed statement auditing message

Message name	Title	Severity
CHANGED_STMT_AUDITING	Statement auditing changed	Yellow (1)

- ◆ Do the following:
 - If the change is authorized, update the snapshot.
 - If the change is not authorized, restore the previous statement settings.

Reporting object audits

The first check of this group reports objects that are audited. The second and third checks report objects that were set for auditing and removed from auditing after the last snapshot update. The fourth check reports objects with reporting methods that were changed after the last snapshot update.

There are 16 options for audited objects.

Table 3-8 Audited object options

	Option	Description
1	ALT	ALTER
2	AUD	AUDIT
3	COM	COMMENT
4	DEL	DELETE
5	GRA	GRANT
6	IND	INDEX
7	INS	INSERT
8	LOC	LOCK
9	REN	RENAME
10	SEL	SELECT
11	UPD	UPDATE
12	REF	REFER
13	EXE	EXECUTE
14	CRE	CREATE
15	REA	READ
16	WRI	WRITE

Unavailable and unaudited options appear as -/-.

For example, with A/A in the fourth position, every auditable DEL operation is recorded as successful or failed. A/S reports every auditable DEL operation that is successful, but only sessions that contain one or more failed operations.

Auditing objects

You can use the name lists in this option to specify tables and views that are to be included or excluded for object auditing checks.

Object auditing

This check reports user objects that are audited and the Success/Failure reporting methods that are used.

You can use the check's name list to specify the users who are to be excluded for the check.

Table 3-9 Object auditing message

Message name	Title	Severity
OBJ_AUDITING	Object auditing	Green (0)

To protect your computers

- ◆ Do the following:
 - Remove unauthorized or out-of-date statements from auditing.
 - Periodically review audited objects to ensure that the audit is currently authorized and that reporting methods are appropriate for available resources and perceived risks.

New object auditing

This check reports user objects that were set for auditing after the last snapshot update, and the Success/Failure reporting methods that are used.

See “[Audited object options](#)” on page 48 for options that can be reported for audited objects.

You can use the check's name list to specify the users who are to be excluded for the check.

Table 3-10 New object auditing message

Message name	Title	Severity
NEW_OBJ_AUDITING	New object auditing	Yellow (1)

To protect your computers

- ◆ Do the following:
 - If auditing of the object is authorized, update the snapshot.
 - If the reporting methods are not correct, correct them.
 - If auditing of the object is not authorized, remove the object from auditing.

Deleted object auditing

This check reports user objects and object options that were removed from auditing after the last snapshot update.

See [“Audited object options”](#) on page 48 for object options available for auditing.

You can use the check’s name list to specify the users who are to be excluded for the check.

Table 3-11 Deleted object auditing message

Message name	Title	Severity
DELETED_OBJ_AUDITING	Deleted object auditing	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the deletion is authorized, update the snapshot.
 - If the deletion is not authorized, restore audit of the object.

Changed object auditing

This check reports changes to the reporting methods of audited objects after the last snapshot update.

See [“Audited object options”](#) on page 48 for object options that are available for auditing.

You can use the check’s name list to specify the users who are to be excluded for the check.

Table 3-12 Changed object auditing message

Message name	Title	Severity
CHANGED_OBJ_AUDITING	Object auditing changed	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the change is authorized, update the snapshot.
 - If the change is not authorized, restore the previous settings.

Reporting privilege audits

The first of these checks reports privileges that are audited. The second and third checks report privileges that were set for auditing and removed from auditing after the last snapshot update. The fifth check reports privileges with reporting methods that were changed after the last snapshot update.

Auditing privileges

You can use the name lists in this option to specify privileges that are to be included or excluded for privilege option checks.

Privilege auditing

This check reports user privileges that are audited, and the Success/Failure reporting methods that are used.

You can use the check's name list to specify the users who are to be excluded for the check.

Table 3-13 Privilege auditing message

Message name	Title	Severity
PRIV_AUDITING	Privilege auditing	Green (0)

To protect your computers

- ◆ Do the following:
 - Periodically review privilege auditing to ensure that the audits are currently authorized and that the reporting methods are appropriate for available resources and perceived risks.

New privilege auditing

This check reports user privileges that were set for auditing after the last snapshot update and the Success/Failure reporting methods that are used.

You can use the check's name list to specify the users who are to be excluded for the check.

Table 3-14 New privilege auditing message

Message name	Title	Severity
NEW_PRIV_AUDITING	New privilege auditing	Green (0)

To protect your computers

- ◆ Do the following:
 - If the new privilege and its reporting methods are authorized, update the snapshot
 - If the new privilege is authorized, but its reporting methods are not correct, change them.
 - If the user is not authorized for the privilege, drop it from the user.

Deleted privilege auditing

This check reports user privileges that were removed from auditing after the last snapshot update.

You can use the check's name list to specify the users who are to be excluded for the check.

Table 3-15 Deleted privilege auditing message

Message name	Title	Severity
DELETED_PRIV_AUDITING	Deleted privilege auditing	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the deletion is authorized, update the snapshot.
 - If the deletion is not authorized, restore the user privilege to auditing.

Changed privilege auditing

This check reports audited user privileges with Success/Failure reporting methods that changed after the last snapshot update.

You can use the check's name list to specify the users who are to be excluded for the check.

Table 3-16 Changed privilege auditing message

Message name	Title	Severity
CHANGED_PRIV_AUDITING	Privilege auditing changed	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the change is authorized, update the snapshot.
 - If the change is not authorized, restore the previous audit settings.

Oracle configuration

This chapter includes the following topics:

- [Editing default settings](#)
- [Reporting Oracle version information](#)
- [Reporting link password encryption](#)
- [Reporting operating system account prefixes](#)
- [Reporting parameter values](#)

Editing default settings

The Oracle Configuration module includes two options that you can use to edit default settings for all security checks in the module.

Automatically update snapshots

Enable this option to update snapshots automatically with current information.

Oracle system identifiers (SIDs)

You can use the name lists in this option to specify Oracle system identifiers (SIDs) that are to be examined by module checks. By default, the module examines all SIDs that are specified when you configure Symantec ESM modules for Oracle Databases. The configuration for Symantec ESM modules for Oracle Databases is stored in `/esm/config/oracle.dat`.

Reporting Oracle version information

These checks report Oracle version, status, trace, and alert log file information. Versions 8i through 9.2.x are supported.

For the location of USER_DUMP_DEST files, use Trace file.

For the maximum size of trace files, specified by MAX_DUMP_FILE_SIZE, use Trace file size.

Oracle server

This check reports the version number and status of the Oracle server.

Table 4-1 Oracle server version and status message

Message name	Title	Severity
SERVER_VERSION	Oracle server version	Green (0)

Oracle components

This check reports the version number and status of all Oracle components, including the version and status of the Oracle server.

Table 4-2 Oracle component version and status message

Message name	Title	Severity
PRODUCT_COMPONENT_VERSION	Oracle product component version	Green (0)

Trace files

This check reports the location of the trace files that are specified by USER_DUMP_DEST.

Table 4-3 Trace file location message

Message name	Title	Severity
TRACE_FILE_DEST	Location of trace files	Green (0)

Trace file size

This check reports the maximum sizes of trace files that are specified by MAX_DUMP_FILE_SIZE.

Table 4-4 Trace file size message

Message name	Title	Severity
MAX_DUMP_FILE_SIZE	Maximum size for trace files	Green (0)

Alert file

This check reports the location of debugging trace files for background processes such as LGWR and DBWR. The Alert_[SID].log file at this location contains information for global and instance operations.

Table 4-5 Alert file path message

Message name	Title	Severity
ALERT_FILE_DEST	Directory path for alert files	Green (0)

List SID:HOME (oracle.dat)

This check reports all the SIDs and their Oracle homes from the oracle.dat file. The configuration information of the Symantec ESM modules for Oracle is stored in oracle.dat, which is located in the /esm/config directory.

Table 4-6 List SID:HOME (oracle.dat) message

Message name	Title	Severity
SID_HOME_DATFILE	Oracle.dat file information	Green (0)

List SID:HOME (oratab)

This check reports all the SIDs and their Oracle homes from the oratab file. The oratab file is created during the installation of Oracle server.

Table 4-7 List SID:HOME (oratab) message

Message name	Title	Severity
SID_HOME_DATFILE	Oratab file information	Green (0)

Reporting link password encryption

The DB link encrypted password check reports whether encryption is required for database link passwords.

DB link encrypted password

This check reports whether encrypted passwords are required to connect to other Oracle servers through database links. The check examines the DBLINK_ENCRYPT_LOGIN setting.

The first attempt to connect to another Oracle server always sends encrypted passwords. If the reported setting is TRUE, a failed connection will not be retried. If FALSE, Oracle reattempts the connection with an unencrypted version of the password. TRUE settings provide the best protection for your database.

Table 4-8 Password encrypting for links message

Message name	Title	Severity
DBLINK_ENCRYPT	Connect to database with encrypted password	Green (0)

Reporting operating system account prefixes

These checks report prefixes for operating system accounts and whether SELECT and SYSTEM privileges are required to change table column values.

Prefix for OS account

This check reports the characters that are attached to the beginning of account names that operating systems authenticate.

The default OPS\$ prefix gives you access to a database from the operating system by typing a slash (/) instead of the username/password string.

Table 4-9 OS account prefix message

Message name	Title	Severity
OS_AUTHENT_PREFIX	Prefix for OS account	Green (0)

Table-level SELECT privileges

This check reports whether SELECT privileges are required to update or delete table column values.

If TRUE is reported in the Info field, table-level SELECT privileges are required to update or delete table column values. If FALSE, SELECT privileges are not required. SQL92_SECURITY specifies the setting.

Table 4-10 SELECT privileges at the table level message

Message name	Title	Severity
SQL92_SECURITY	Table-level SELECT privileges	Green (0)

Restrictions on system privileges

This check, which is used for migration from Oracle7 to any later version of Oracle, reports whether access to objects in the SYS schema is allowed (Oracle7 behavior).

If FALSE is reported in the Info field, system privileges that allow access to objects in any schema do not allow access to objects in the SYS schema. If TRUE, access to objects in the SYS schema is allowed (Oracle7 behavior).

7_DICTIONARY_ACCESSIBILITY specifies the setting.

Table 4-11 Restrictions on system privileges message

Message name	Title	Severity
O7_DICTIONARY_ACCESSIBILITY	Restrictions on system privileges	Green (0)

Reporting parameter values

Remote login password file

This check reports whether the value of REMOTE_LOGIN_PASSWORDFILE conforms to the conditions that you specify in the check's Parameter Value field.

You can specify values that are to be accepted or not accepted for the check in the check's list name.

The default value is None.

Table 4-12 Remote login password file

Message name	Title	Severity
REMOTE_LOGIN_PASSWORDFILE	Remote login password file	Yellow (3)

To protect your computers

- ◆ Change the value of the REMOTE_LOGIN_PASSWORDFILE parameter to conform to your security policy.

UTL_FILE accessible directories

This check reports whether the value of UTL_FILE_DIR complies with the conditions that you specify in the check's Parameter Value field.

You can use UTL_FILE_DIR to specify one or more directories that Oracle can use for PL/SQL file I/O. The exclude tag of the parameter value specifies acceptable values and the include tag specifies unacceptable values.

Table 4-13 UTL_FILE accessible directories

Message name	Title	Severity
UTL_FILE_DIR	UTL_FILE accessible directories	Yellow (3)

To protect your computers

- ◆ Do one of the following:
 - If the location of the UTL_FILE_DIR is not authorized, change the configuration of the SID's UTL_FILE_DIR parameter to specify an authorized location.
 - If the location is correct, update the template.

Oracle configuration watch

This check lets you enable or disable templates that specify initialization and configuration parameters that should be watched.

Table 4-14 Oracle configuration watch messages

Message name	Title	Severity
ORC_RUNTIME_RED	Red level condition	Red -4
ORC_RUNTIME_YELLOW	Yellow level condition	Yellow-1
ORC_RUNTIME_GREEN	Green level condition	Green-0
ORC_INITFILE_RED	Red level condition	Red-4
ORC_INITFILE_YELLOW	Yellow level condition	Yellow-1
ORC_INITFILE_GREEN	Green level condition	Green-0
ORC_PARAMETER_NOT_FOUND	Required Oracle parameter not found	Green-0

Oracle configuration watch template

You should not edit the Oracle Configuration Watch template that is installed with the modules. Instead, you can create a new template by copying and renaming the Oracle Configuration Watch template, and then specifying the required parameters and new parameter values.

To add a new Oracle Configuration Watch template

- 1 In the console tree, right-click **Templates**, and then click **New**.
- 2 In the Create New Template dialog box, select **Oracle Configuration Watch - all**.
- 3 Type a new template name of no more than eight characters without an extension.
- 4 Press **Enter**.
Symantec ESM automatically adds the .ocw extension.

To specify parameters for the New Oracle Configuration Watch template

- 1 In the Template Editor, click **Add Row**.
- 2 In the Description and Parameter fields, replace <NEW> with the appropriate information. Parameters are case sensitive.
- 3 Do one of the following:

- To examine runtime values, leave the Runtime Value check box checked.
 - To exclude runtime values, uncheck the check box.
- 4 Click **Init File Value** (initially Optional), and then select one of the following:
 - **Optional**
Report parameter values that violate the value that is defined in init<SID>.ora.
 - **Required**
Report a violation if the parameter is not defined in init<SID>.ora.
 - **Skipped**
Ignore the parameter value that is defined in init<SID>.ora.
 - 5 Specify parameter values.
See [“To specify parameter values”](#) on page 62.
 - 6 Click **Severity** (initially Green), and then select one of the following severity levels to be reported when the parameter value is violated:
 - Green
 - Yellow
 - Red
 - 7 In the Oracle Version field, replace <NEW> with the version that the parameter applies to. The following values are valid:
 - [Empty]
All version numbers
 - 8.1.5 for 8.1.5.x
 - 9.0 for 9.0.x
 - 7 for 7.x
 - +8 for 8.x and later
 - -9.2 for 9.2.x and earlier
 - +10
 - 8 Click **Save**.
 - 9 To add another parameter, repeat steps 1-8.
 - 10 Click **Close**.

To specify parameter values

- 1 In the Template Editor, click the Parameters Values field (initially 0).
- 2 In the Template Sublist Editor, click **Add Row**.

- 3 Do one of the following:
 - To designate the value as prohibited, leave the Prohibited Value check box checked.
 - To designate the value as acceptable, uncheck the check box.
- 4 In the Value field, replace <NEW> with a parameter value expressed as a regular expression or as a numeric comparison.
The following special cases can also be used:

+	'+' character
NULL or null	empty string

If the value begins with one of the following numeric comparison operators, a numeric comparison is performed:

=	equal to
<	less than
>	greater than
!=	not equal to
<=	less than or equal to
>=	greater than or equal to

- 5 Click **Apply**.
- 6 To add another parameter value, repeat steps 2-5.
- 7 Click **Close**.

Redo log files

This check reports the locations of the SID's redo log files, violations of redo log file permissions, discrepancies in redo log file ownerships, and file status.

If you specify 0 in the check's Permission field, the location and status of the SID's redo log file is reported in the Info field.

If you specify a permission value that is more restrictive than the SID's redo log file permission, a problem is reported.

If the SID's redo log file ownership (UID/GID) does not match the ownership that is specified in the Oracle database, a problem is reported.

Specify permission values as three-digit octal numbers.

You can use the check's name list to specify the file statuses that are to be included or excluded by the check.

Table 4-15 Redo log files message

Message name	Title	Severity
REDOLOGFILE	Redo log file	Green (0)
REDOLOGFILE_PERM	Redo log file permission	Yellow (2)

To protect your computers

- ◆ Do the following:
 - Periodically review the redo log file location to ensure that it is in a secure, authorized location.
 - If the file's permissions are excessive, reset the redo log file's permission to conform to your security policy.
 - If the owner of the redo log file is not authorized for the file, immediately take ownership of the file and review it for possible tampering.

New redo log files

This check reports redo log files that were added after the last snapshot update, their locations, and the status of the files.

You can use the check's name list to exclude redo log file status reporting by the check.

Table 4-16 New redo log files message

Message name	Title	Severity
ADDED_REDOLOGFILE	New redo log file	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the addition is authorized, update the snapshot.
 - If the addition is not authorized, delete the new redo log file.

Deleted redo log files

This check reports redo log files that were deleted after the last snapshot update.

Table 4-17 Deleted redo log files message

Message name	Title	Severity
DELETED_REDOLOGFILE	Deleted redo log file	Yellow (1)

To protect your computers

- ◆ Do one of the following
 - If the deletion is authorized, update the snapshot.
 - If the deletion is not authorized, restore the file.

Control files

This check reports the locations of the SID's control files and violations of control file permissions in the Info field.

If you specify 0 in the check's Permission field, only the locations of the SID's control files are reported.

If you specify a permission value that is more restrictive than the SID's control file permission, a violation is reported.

Specify permission values as three-digit octal numbers.

Table 4-18 Control files message

Message name	Title	Severity
CONTROLFILE	Control file	Green (0)
CONTROLFILE_PERM	Control file permission	Yellow (2)

To protect your computers

- ◆ Do the following:
 - Periodically review control file locations to ensure that they are in secure, authorized locations.
 - If the file's permissions are excessive, reset the control file's permission to conform to your security policy.

New control files

This check reports control files that were added after the last snapshot update.

Table 4-19 New control files message

Message name	Title	Severity
ADDED_CONTROLFILE	New control file	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the addition is authorized, update the snapshot.
 - If the addition is not authorized, delete the new control file.

Deleted control files

This check reports control files that were deleted after the last snapshot update.

Table 4-20 Deleted control files message

Message name	Title	Severity
DELETED_CONTROLFILE	Deleted control file	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the deletion is authorized, update the snapshot.
 - If the deletion is not authorized, restore the control file.

Oracle networks

This chapter includes the following topics:

- [Editing default settings](#)
- [SID configuration](#)
- [Reporting net configuration violations](#)

Editing default settings

The Symantec ESM module for Oracle networks includes one option that you can use to edit default settings for all security checks in the module.

Oracle system identifiers (SIDs)

You can use the name lists in this option to specify Oracle system identifiers (SIDs) that are to be examined by module checks. By default, the module examines all SIDs that are specified when you configure Symantec ESM modules for Oracle Databases. The configuration for Symantec ESM modules for Oracle Databases is stored in `/esm/config/oracle.dat`.

Reporting SID configuration status

SID configuration

This check reports SIDs that are not configured for Symantec ESM modules for Oracle Databases. If an oratab file resides in a different location than /etc/oratab or /var/opt/oracle/oratab, change the value in the oratab file field to specify the full path.

The check returns the following message:

Table 5-1 SID configuration message

Message name	Title	Severity
UNCONFIG_SID	SID not configured for modules	Yellow (3)

Reporting net configuration violations

Oracle net configuration watch

This check reports Oracle Listener, Sqlnet, and Names configuration parameter values that violate conditions of the corresponding Oracle Net Watch template parameters.

You can use the check's name lists to enable and disable template files for the check.

The check returns the following messages:

Table 5-2 Net configuration messages

Message name	Title	Severity
ORC_NETCONFIG_RED	Red level condition	Red (4)
ORC_NETCONFIG_YELLOW	Yellow level condition	Yellow (1)
ORC_NETCONFIG_GREEN	Green level condition	Green (0)
ORC_NETCONFIG_PARA_MISSING	Required parameter not found	Yellow (3)

Creating a new Oracle Net Watch template

You should not edit the Oracle Net Watch template that is installed with the modules. Instead, create your own template by copying and renaming the Oracle Net Watch template, and then specifying the required parameters and new parameter values in the new template.

To add a new Oracle Net Watch template

- 1 In the console tree, right-click **Templates**, and then click **New**.
- 2 In the Create New Template dialog box, click **Oracle Net Watch - all**.
- 3 Type a new template name of no more than eight characters without an extension.
- 4 Press **Enter**.
Symantec ESM automatically adds the .onw extension.

To specify parameters for the Oracle Net Watch template

- 1 In the Template Editor, click **Add Row**.
- 2 In the Description field, replace <NEW> with explanatory or descriptive information.
- 3 In the Parameter field, replace <NEW> with the name of a configuration value. Examples of valid entries include the following:

Table 5-3 Examples of valid configuration parameters

Parameter type	Oracle file	Examples of valid parameters
Listener Control Parameter	listener.ora	ADMIN_RESTRICTIONS LOG_FILE PASSWORDS SAVE_CONFIG_ON_STOP STARTUP_WAIT_TIME TRACE_DIRECTORY, TRACE_FILE
Sqlnet Profile Parameter	sqlnet.ora	BEQUEATH_DETACH DAEMON.TRACE_DIRECTORY DISABLE_OOB LOG_DIRECTORY_CLIENT LOG_DIRECTORY_SERVER NAMES.CONNECT_TIMEOUT

Table 5-3 Examples of valid configuration parameters

Parameter type	Oracle file	Examples of valid parameters
Oracle Names Parameter	names.ora	NAMES.ADDRESSES NAMES.ADMIN_REGION NAMES.AUTHORITY_REQUIRED NAMES.CONFIG_CHECKPOINT_FILE NAMES.DOMAIN_HINTS NAMES.LOG_FILE

See your Oracle documentation for detailed descriptions of listener.ora, sqlnet.ora, and names.ora configuration parameters.

- 4 Click **Parameter Type** (initially Listener Address), and then select one of the following:
 - Listener Control Parameter (listener.ora)
 - Sqlnet Profile Parameter (sqlnet.ora)
 - Oracle Names Parameter (names.ora)
- 5 Do one of the following:
 - If the parameter is required, leave the Required Parameter check box checked.
Symantec ESM reports if this parameter is not found and if the parameter is found but fails the comparison with template values.
 - If the parameter is not required, uncheck the check box.
Symantec ESM reports only if this parameter is found and fails the template comparison.
- 6 Specify parameter values.
See [“To specify parameter values”](#) on page 71.
- 7 Click **Severity** (initially Green), and then select one of the following severity levels to be reported when the parameter value is violated:
 - Green
 - Yellow
 - Red
- 8 In the Oracle Version field, replace <NEW> with the version to which the parameter applies.
- 9 Click **Save**.
- 10 To add another parameter, repeat steps 1-9.

11 Click Close.**To specify parameter values**

- 1** In the Template Editor, click **Parameter Values** (initially 0).
- 2** In the Template Sublist Editor, click **Add Row**.
- 3** Do one of the following:
 - To designate the value as prohibited, leave the Prohibited Value check box checked.
 - To designate the value as allowed, uncheck the check box.
- 4** In the Value field, replace <NEW> with a parameter value that is expressed as a regular expression or as a numeric comparison.
The following special cases can also be used:

+ '+' character

NULL or empty string
null

If the value begins with one of the following numeric comparison operators, a numeric comparison is performed:

= equal to

< less than

> greater than

!= not equal to

<= less than or equal to

>= greater than or equal to

- 5** Click **Apply**.
- 6** To add another parameter value, repeat steps 2-5.
- 7** Click **Close**.

Example: Editing the Oracle Net Watch template

Your company might have the following password security policy:

Every defined listener in the \$ORACLE_HOME/network/admin/listener.ora file must have a password of at least seven characters in a combination of a-z A-Z, 0-9, and _ characters.

The following example shows how to add configuration parameters to the Oracle Net Watch template to implement this security policy.

To implement a password security policy

- 1 Add a new Oracle Net Watch template.
See [“To add a new Oracle Net Watch template”](#) on page 69.
- 2 In the Description field, replace <NEW> with a description of your security policy.
For example, type Password security for listeners.
- 3 In the Parameter field, replace <NEW> with **PASSWORDS**.
The PASSWORDS parameter of the listener.ora file stores passwords for listeners.
- 4 In the Parameter Type field, click **Listener Control Parameter**.
When you select Listener Control Parameter, Symantec ESM compares the values in the Oracle Net Watch template with the parameter values in the listener.ora file.
- 5 In the Required Parameter field, leave the check box checked.
Symantec ESM reports listeners with passwords that fail to match the values of this template entry and reports listeners that have no configured PASSWORDS parameter.
- 6 In the Prohibited Value field of the Parameter Values template sublist editor, uncheck the check box.
Symantec ESM reports passwords that do not match the entry of the Value field of the Parameter Values template sublist editor.
- 7 In the Value field of the Parameter Values template sublist editor, type the following:
[a-zA-Z0-9_]{6}[a-zA-Z0-9_]+
Parameter values must be expressed as a regular expression or as a numeric comparison.
See [“To specify parameter values”](#) on page 71.
- 8 In the Severity field, select the severity level that you want reported when the parameter value is violated.

- 9 In the Oracle Version field, replace <NEW> with the version to which the parameter applies.

Oracle objects

This chapter includes the following topics:

- [Editing default settings](#)
- [Reporting table privileges](#)

Editing default settings

The Symantec ESM modules for Oracle Databases includes one option that you can use to edit default settings for all security checks in the module.

Oracle system identifiers (SIDs)

You can use the name lists in this option to specify the Oracle system identifiers (SIDs) that are to be examined by module checks. By default, the module examines all SIDs that are specified when you configure Symantec ESM modules for Oracle Databases. The configuration for Symantec ESM modules for Oracle Databases is stored in `/esm/config/oracle.dat`.

Reporting table privileges

The following checks report entities that can:

- Access `SYS.ALL_SOURCE`
- Grant privileges to Oracle objects such as tables, indexes, and views
- Have directly granted table privileges to Oracle objects

Access to SYS.ALL_SOURCE

This check reports roles, accounts, and synonyms that have access privileges to the SYS.ALL_SOURCE system table. The ALL_SOURCE table contains the source code for user-defined objects in all schemas of the SID. Verify that the entity's direct access to SYS.ALL_SOURCE is authorized.

Table 6-1 Access to SYS.ALL_SOURCE

Message name	Title	Severity
ACCESS_ALL_SOURCE	Access to SYS.ALL_SOURCE	Yellow (3)

Table privileges

You can use this option to specify table privileges that are to be included or excluded for grantable and directly granted privilege checks.

Object name

You can use this option to specify object names that are to be included or excluded for grantable and directly granted privilege checks.

Grantors

You can use this option to specify grantors that are to be included or excluded for grantable and directly granted privilege checks.

Grantable privilege

This check reports roles, accounts, or synonyms that have grantable table privileges to Oracle objects.

You can use the name list to specify grantees that are to be included or excluded for the check.

Table 6-2 Grantable privilege message

Message name	Title	Severity
GRANTABLE	Grantable table privilege	Yellow (3)

Directly granted privilege

This check reports roles, accounts, or synonyms that have directly granted table privileges to Oracle objects.

You can use the check's name list to specify entities that are to be included or excluded for the check.

Table 6-3 Directly granted privilege message

Message name	Title	Severity
DIRECT_GRANTED	Directly granted table privilege	Yellow (3)

Oracle passwords

This chapter includes the following topics:

- [Editing default settings](#)
- [Specifying check variations](#)
- [Comparing passwords to word lists](#)
- [Detecting well-known passwords](#)

For password restrictions such as failed login attempts, lock time, grace time, and so forth, see [Reporting password violations](#).

Editing default settings

The Symantec ESM module for Oracle passwords includes four options that you can use to edit default settings for all security checks in the module.

Oracle system identifiers (SIDs)

Use the name lists in this option to specify Oracle system identifiers (SIDs) that are to be examined by module checks. By default, the module examines all SIDs that are specified when you configure Symantec ESM modules for Oracle Databases. The configuration for Symantec ESM modules for Oracle Databases is stored in `/esm/config/oracle.dat`.

Users to check

Use this option to specify users that are to be included or excluded for the checks.

Account status

Use this option to specify statuses that are to be included or excluded for the checks.

Password display

Enable this option to display passwords that are matched in Password = checks in the format: User <name>: Password is <first character>*<last character>. Disable the option to display matched passwords in the format: User <name>: <password>.

Specifying check variations

This module contains three checks: Password = wordlist word, Password = username, and Password = any username.

You can also compare passwords to word list words spelled backward or doubled, in plural form, or with prefixes or suffixes.

You can display the results with or without the first and last characters of the password.

Reverse order

Enable this option to have Password = checks report passwords that match the backward spelling of user names or common words. For example, in Password = wordlist word, password flog matches the word golf.

Double occurrences

Enable this option to have Password = checks report passwords are user names or common words spelled twice. For example, in Password = wordlist word, password golfgolf matches the word golf.

Plural

Enable this option to have Password = checks report passwords are plural forms of user names or common words. For example, in Password = wordlist word, password golfs matches the word golf.

Prefix

Enable this option to have Password = checks report passwords which have prefixes at the beginning of user names or common words. For example, if you specify in the check's Prefixes to Use list, and golf is a wordlist word, Password = wordlist word reports progolf is a weak password.

Suffix

Enable this option to have Password = checks report passwords which have suffixes at end of user names or common words. For example, if you specify pro in the check's Suffixes to Use list, and golf is a wordlist word, Password = wordlist word reports golfpro is a weak password.

Comparing passwords to word lists

Three checks compare passwords to words that are found in word lists and/or user names. Any matched word is a weak password and should be changed immediately.

Password = wordlist word

This check compares the encrypted version of user passwords to the encrypted version of words in files of common words and names and reports matches. You can specify the word and name files that you want to check.

You can use the check's name list to specify word files that are to be used for the check.

The reported password matches a word or a variation of a word in a selected word file. It is a weak password.

Table 7-1 Password / word list messages

Message name	Title	Severity
PASS_GUESSED	Weak user password	Red (4)
NO_WORDS	No word files specified	Red (4)

To protect your computers

- ◆ Do the following:
 - Do not use common words or names as passwords.
 - Assign a more secure password immediately. Instruct the user to log in with the more secure password and change the password again.
A secure password has six to eight characters, including at least one non-alphabetic character, is not be found in any dictionary, and does not match an account name.

Password = username

This check reports users who use their own user names as passwords. The check is not as thorough as Password = any username. However, if Password = any username takes too much time or consumes too much CPU, use Password = username daily and Password = any username on weekends.

The reported password matches the user account name or a variation of that name. Passwords that closely resemble account names are easily guessed.

Table 7-2 Password / user name message

Message name	Title	Severity
PASS_GUESSED	Weak user password	Red (4)

To protect your computers

- ◆ Assign a more secure password immediately. Instruct the user to log in with the more secure password and change the password again.
A secure password has six to eight characters, including at least one non-alphabetic character, is not be found in any dictionary, and does not match an account name.

Password = any username

This check reports users whose passwords also exist as user names in the database.

The reported password matches a user account name or a variation of that name. Passwords that closely resemble account names are easily guessed.

Table 7-3 Password / any user name message

Message name	Title	Severity
PASS_GUESSED	Weak user password	Red (4)

To protect your computers

- ◆ Assign a more secure password immediately. Then instruct the user to log in with the more secure password and change the password again.
A secure password has six to eight characters, including at least one non-alphabetic character, is not be found in any dictionary, and does not match an account name.

Detecting well-known passwords

Oracle products ship with default, or sample, accounts and passwords that are widely known. These passwords should be changed as soon as they are installed. Otherwise, unauthorized users can log in as SYS or SYSTEM with administrator privileges.

Well-known passwords

This check reports well known account/password combinations that you specify in the name list and default Oracle account/password combinations such as scott/tiger. You should not allow well known account/password combinations.

You can use the check's name list to specify account and password combinations that are to be included for the check.

Table 7-4 Well known password message

Message name	Title	Severity
DEFAULT_PASSWORD	Well known account/password found	Red (4)

To protect your computers

- ◆ Do the following:
 - Do not use common words or names as passwords.
 - Assign a more secure password immediately. Instruct the user to log in with the more secure password and change the password again.
A secure password has six to eight characters, including at least one non-alphabetic character, is not be found in any dictionary, and does not match an account name.

Oracle patches

This chapter includes the following topics:

- [Editing default settings](#)
- [Oracle patches](#)

Editing default settings

The Symantec ESM module for Oracle Patches includes two options that you can use to edit default settings for all security checks in the module.

Oracle Home Paths

Use this option to specify the Oracle home paths that need to be examined for module checks. By default, the module examines all Home paths that are specified to be examined when you configure the Symantec ESM Modules for Oracle Databases. The configuration for Symantec ESM Modules for Oracle Databases is stored in the `oracle.dat` file that is located in the `/esm/config/` folder.

Template files

You can use this option to specify template files that are to be included for the checks.

Oracle Patch template files are identified by `.orp` file extensions.

Oracle patches

Patch information

This check reports information about patches that have been released within the number of days that you specify in the check. The information includes patch type and number, ID number, patch release date, and description.

You can use the check's name list to specify template files that are to be included for the check.

You should verify that all current patches are installed on your Oracle clients and servers.

Table 8-1 Patch information messages

Message name	Title	Severity
PATCH_AVAILABLE	Patch available	Yellow (1)
PATCHSET_AVAILABLE	Patchset available	Yellow (1)

To protect your computers

- ◆ Verify that your Oracle server and components have the current applicable patches.

You can download patch updates by using LiveUpdate.

Opatch Tool

Symantec ESM incorporates the Opatch tool to determine which Oracle patches are installed. The Opatch Tool check supplies Symantec ESM with information on the location of the Opatch tool. To use the check, you must type the path to the location where you have the Opatch application. This application can be downloaded from the following URL:

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

Table 8-2 Opatch Tool messages

Message name	Title	Severity
OPATCH_INFO	Opatch Information	Green (0)

Installed Patches

This check reports patches that are currently installed on your computers.

Table 8-3 Patch information messages

Message name	Title	Severity
INSTALLED_PATCH	Installed patches	Green (0)

Creating a new Patch template

You can create a new Oracle Patch template by copying and renaming the old one, then adding the parameters and parameter values that are required.

To add a new patch template

- 1 In the Templates branch of the console tree, right-click **Oracle Patch - all (orapatch.orp)**.
- 2 Click **Add Patch**.
- 3 Scroll to the bottom of the table.
- 4 In the Version field, replace <NEW> with the patch version number.
- 5 Click **Platform** (initially ALL), and then select one of the following platforms:
 - ALL for all platforms
 - aix-rs6k
 - hpux-hppa
 - hpux-hppa/HP-UX 10.20
 - solaris-sparc
 - windows 2003
- 6 In the Product, ID, Patch ID, and Date fields, replace <NEW> with the appropriate information.
- 7 Click **Architecture** (initially ALL), and then select one of the following options:
 - ALL
 - 32 bits
 - 64 bits
- 8 In the Description field, type a description of the patch.
- 9 Click **Patch Set** (initially Yes), and then select Yes or No.

- 10 Add merged patch entries if applicable. See [“To add a merged patch entry”](#) on page 88.
- 11 Click **Save**.
- 12 Click **Close**.

To add a merged patch entry

- 1 In the Patches Template Editor, click **Merged Patches**.
- 2 Click **Add New Row**.
- 3 In the Patch ID field, replace <NEW> with the ID of the patch that you want to merge.
- 4 To add another row, click **Apply**, and then repeat steps 2 and 3.
- 5 Click **Close**.

Oracle profiles

This chapter includes the following topics:

- [Establishing a baseline snapshot](#)
- [Editing default settings](#)
- [Reporting profiles and their limits](#)
- [Reporting CPU limit violations](#)
- [Reporting password violations](#)

Establishing a baseline snapshot

To establish a baseline, run the Profiles module. This creates a snapshot of current account information that you can update when you run checks that report new, deleted, or changed information.

Automatically update snapshots

Enable this option to update snapshots automatically with current information.

Editing default settings

The Profiles module includes one option that you can use to edit default settings for all security checks in the module.

Oracle system identifiers (SIDs)

You can use the name lists in this option to specify Oracle system identifiers (SIDs) that are to be examined by module checks. By default, the module examines all SIDs that are specified when you configure Symantec ESM modules

for Oracle Databases. The configuration for Symantec ESM modules for Oracle Databases is stored in /esm/config/oracle.dat.

Reporting profiles and their limits

These checks report existing, new, and deleted profiles and their resource limits.

Profile enforcement

This check reports SIDs that do not enforce profiles.

Table 1-1 Profiles not enabled message

Message name	Title	Severity
PROFILE_NOT_ENABLED	Profiles are not enabled	Red (4)

To protect your computers

- ◆ In the database's parameter file, change the value of the RESOURCE_LIMIT parameter from FALSE to TRUE so that profiles are enforced.

Profiles

This check reports all profiles that are defined in the database.

You Can use the check's name list to specify profiles that are to be excluded for the check.

Table 1-2 Existing profiles message

Message name	Title	Severity
PROFILE_LIST	Existing profiles	Green (0)

New profiles

This check reports all profiles that were defined in the database after the last snapshot update.

You can use the check's name list to specify profiles that are to be excluded for the check.

Table 1-3 New profile message

Message name	Title	Severity
PROFILE_ADDED	New profile	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the addition is authorized, update the snapshot.
 - If the addition is not authorized, delete the profile.

Deleted profiles

This check reports all profiles that were deleted from the database after the last snapshot update.

You can use the check's name list to specify profiles that are to be excluded for the check.

Table 1-4 Deleted profile message

Message name	Title	Severity
PROFILE_DELETED	Deleted profile	Green (0)

To protect your computers

- ◆ Do one of the following:
 - If the deletion is authorized, update the snapshot.
 - If the deletion is not authorized, restore the profile.

Profile resources

This check reports profile resource limits.

You can use the check's name list to specify profiles that are to be excluded for the check.

Table 1-5 Profile resource message

Message name	Title	Severity
PROFILE_LIMIT_LIST	Profile resource limits	Green (0)

To protect your computers

- ◆ Ensure that the profile resource limits conform to company security policies.

Changed resource limits

This check reports profile resource limits that changed after the last snapshot update.

You can use the check's name list to specify profiles that are to be excluded for the check.

Table 1-6 Changed profile resource limit message

Message name	Title	Severity
PROFILE_LIMIT_CHANGED	Changed profile resource limits	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the change is authorized, update the snapshot.
 - If the change is not authorized, restore the previous limit.

Reporting CPU limit violations

These checks report the CPU resource limits.

Oracle profiles

You can use this option to specify Oracle profiles that are to be included or excluded for the following resource checks.

Sessions per user

This check reports profiles that allow more concurrent sessions per user than the number that you specify in the check.

Specify the maximum number of simultaneous sessions per user in resource parameter `SESSIONS_PER_USER`.

Table 1-7 Simultaneous sessions per user message

Message name	Title	Severity
PROFILE_SESSIONS_PER_USER	Sessions per user too high	Yellow (1)

To protect your computers

- ◆ Specify a maximum number of simultaneous sessions per user to prevent a small number of users from denying access to other users by using an excessive number of connections simultaneously.

CPU time per session

This check reports profiles that allow more CPU time per session than the amount that you specify in the check.

Specify the maximum amount of time that is allowed per session in hundredths of a second.

Table 1-8 CPU time per session message

Message name	Title	Severity
PROFILE_CPU_PER_SESSION	CPU time per session exceeds limit	Yellow (1)

To protect your computers

- ◆ Specify a maximum CPU time per session limit that lets users perform their duties without frequent logging in and out and prevents a small number of users from denying service to others by using excessive CPU resources.

CPU time per call

This check reports profiles that allow more CPU time for each call, such as fetch, execute, and parse, than the amount of time that you specify in the check.

Specify the maximum amount of time that is allowed per call in hundredths of a second.

Table 1-9 Time per call message

Message name	Title	Severity
PROFILE_CPU_PER_CALL	CPU time per call exceeds limit	Yellow (1)

To protect your computers

- ◆ Specify a maximum CUP time per call limit that lets users perform their duties and that prevents a small number of users from denying service to others by using excessive CPU resources.

Connection time

This check reports profiles that allow more elapsed connection time for an account than the number of minutes that you specify in the check.

Table 1-10 Connection time message

Message name	Title	Severity
PROFILE_CONNECT_TIME	Connect time exceeds limit	Yellow (1)

To protect your computers

- ◆ Specify a realistic limit that allows users to perform their duties and that prevents a few connections from denying service to others by using excessive CPU resources.

Idle time

This check reports profiles that allow more idle time before a process is disconnected than the number of minutes that you specify in the check.

Connections that are idle for a long period may indicate that the machine is unattended.

Table 1-11 Idle time message

Message name	Title	Severity
PROFILE_IDLE_TIME	Idle time exceeds limit	Yellow (1)

To protect your computers

- ◆ Specify a realistic amount of time before an inactive process is disconnected.

Reporting password violations

These checks report profiles with settings for the number of failed login attempts, password grace time, password duration, password lock time, and password reuse requirements that violate your security policy.

Password strength checks, which compare passwords to common words and user names, are documented in chapter 7.

Failed logins

This check reports profiles that allow more failed login attempts than the number that you specify in the check.

Table 1-12 Failed logins message

Message name	Title	Severity
PROFILE_FAILED_LOGIN_ATTEMPTS	Failed login attempts exceed limit	Red (4)

To protect your computers

- ◆ Restrict the number of permitted failed login attempts to minimize the likelihood of break-ins by intruders who attempt to guess user names and passwords.

Password grace time

This check reports profiles that have more than or fewer than the number of password grace days that you specify in the check. This number specifies the number of days that a warning may be issued before a password expires.

Table 1-13 Different password grace time message

Message name	Title	Severity
PROFILE_PASS_GRACE_TIME	Password grace time differs from limit	Yellow (1)

To protect your computers

- ◆ Specify a realistic number of days for a user to change a password after being warned that it is about to expire.

Password duration

This check reports profiles that permit a password to be used for more days than the number that you specify in the check,

Table 1-14 Password duration message

Message name	Title	Severity
PROFILE_PASS_LIFE_TIME	Password duration too high	Red (4)

To protect your computers

- ◆ Require password changes often enough to minimize the possibility that an intruder will discover passwords but not so often that users have difficulty remembering their passwords.

Password lock time

This check reports profiles that lock accounts for fewer days than the number that you specify in the check. Accounts are locked after the number of failed login attempts that you specify in the `FAILED_LOGIN_ATTEMPTS` parameter of the profile. `PASSWORD_LOCK_TIME` specifies the number of days that an account is locked.

Table 1-15 Password lock time message

Message name	Title	Severity
PROFILE_PASS_LOCK_TIME	Password lock time too low	Yellow (1)

To protect your computers

- ◆ Change the resource parameter `PASSWORD_LOCK_TIME` setting to conform to your security policy.

Password reuse max

This check reports profiles that require fewer password changes before a password can be reused than the number that you specify in the check.

Note: If you set a `PASSWORD_REUSE_MAX` value, `PASSWORD_REUSE_TIME` must be `UNLIMITED`.

Table 1-16 Password reuse message

Message name	Title	Severity
PROFILE_PASS_REUSE_MAX	Password reuse time too low	Yellow (1)

To protect your computers

- ◆ Change the resource parameter `PASSWORD_REUSE_TIME` to require a realistic number of times that a password must be changed before it can be reused.

Password reuse time

This check reports profiles that require fewer days before a password can be reused than the number that you specify in the check.

Note: If this setting has a value, `PASSWORD_REUSE_TIME` must be `UNLIMITED`. If you set a `PASSWORD_REUSE_TIME` value, `PASSWORD_REUSE_MAX` must be `UNLIMITED`.

Table 1-17 Password reuse message

Message name	Title	Severity
<code>PROFILE_PASS_REUSE_TIME</code>	Password reuse time too low	Yellow (1)

To protect your computers

- ◆ Change the resource parameter `PASSWORD_REUSE_TIME` to require a realistic amount of time that must pass before it can be reused.

Password verify function

This check reports profiles that do not use one or more of the password complexity functions that you specify in the name list.

Note: Password complexity functions are specified in the resource parameter `PASSWORD_VERIFY_FUNCTION`.

You can use the check's name list to specify functions that are to be included for the check.

Table 1-18 Password verification function message

Message name	Title	Severity
<code>PROFILE_PASS_VERIFY_FUNCTION</code>	Password verify function	Yellow (1)

To protect your computers

- ◆ Immediately assign a more secure password, and then instruct the user to log in with the more secure password and change the password again.

Invalid profiles

This check reports users that are assigned to profiles that fail one or more of the enabled resource limitation checks.

You can use the check's name list to specify users that are to be excluded for the check.

Table 1-19 Invalid profile message

Message name	Title	Severity
INVALID_PROFILE_ASSIGNED	Invalid profile assigned	Yellow (3)

Oracle roles

This chapter includes the following topics:

- [Establishing a baseline snapshot](#)
- [Editing default settings](#)
- [Reporting roles](#)
- [Reporting role privileges](#)
- [Reporting nested roles](#)
- [Reporting role access](#)

Establishing a baseline snapshot

To establish a baseline, run the Roles module. This creates a snapshot of current role information that you can update when you run checks for new, deleted, or changed information.

Automatically update snapshots

Enable this option to update snapshots automatically with current information.

Editing default settings

The Roles module includes one option that you can use to edit default settings for all security checks in the module.

Oracle system identifiers (SIDs)

You can use the name lists in this option to specify Oracle system identifiers (SIDs) that are to be examined by module checks. By default, the module examines all SIDs that are specified when you configure Symantec ESM modules

for Oracle Databases. The configuration for Symantec ESM modules for Oracle Databases is stored in `/esm/config/oracle.dat`.

Reporting roles

These checks report existing roles and roles that have been added or deleted since the last snapshot update.

Roles

This check reports roles that are defined in the database.

You can use the check's name list to specify roles that are to be excluded for the check.

Table 2-1 Roles message

Message name	Title	Severity
EXISTING_ROLES	Defined role	Green (0)

To protect your computers:

- ◆ Do the following:
 - Drop any roles that are not authorized or are out of date.
 - Periodically review roles to ensure that they are currently authorized.

New roles

This check reports roles that were added to the database after the last snapshot update.

You can use the check's name list to specify roles that are to be excluded for the check.

Table 2-2 New role message

Message name	Title	Severity
ADDED_ROLES	New role	Yellow (1)

To protect your computers

- ◆ Do the following:
 - If the new role is authorized, update the snapshot.
 - If the new role is not authorized, drop the role.

Deleted roles

This check reports roles that have been deleted from the database since the last snapshot update.

You can use the check's name list to specify roles that are to be excluded for the check.

Table 2-3 Deleted role message

Message name	Title	Severity
DELETED_ROLES	Deleted role	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the deletion is authorized, update the snapshot.
 - If the deletion is not authorized, restore the role.

Reporting role privileges

These checks report role privileges, privileges that were granted to or dropped from roles after the last snapshot update, and grantable role privileges.

Privileges

This check reports privileges that have been granted to roles.

You can use the check's name list to specify roles that are to be excluded for the check, and add or revoke privileges as appropriate.

Table 2-4 Role privilege message

Message name	Title	Severity
ROLE_PRIVILEGE	Role privilege	Green (0)

- ◆ Do the following:
 - Add or drop privileges for roles as appropriate.
 - Periodically review roles to ensure that the privileges granted to them are consistent with current user duties.

New privileges

This check reports privileges that were directly granted to roles after the last snapshot update.

You can use the check's name list to specify roles that are to be excluded for the check.

Table 2-5 New privilege message

Message name	Title	Severity
ADDED_ROLE_PRIVILEGE	New role privilege	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the new privilege is authorized for the role, update the snapshot.
 - If the new privilege is not authorized for the role, drop the privilege from the role.

Deleted privileges

This check reports privileges that were dropped from listed roles after the last snapshot update.

You can use the check's name list to specify roles that are to be excluded for the check.

Table 2-6 Deleted privilege message

Message name	Title	Severity
DELETED_ROLE_PRIVILEGE	Deleted role privilege	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the deletion is authorized for the role, update the snapshot.
 - If the deletion is not authorized for the role, restore the privilege.

Grantable privileges

This check reports role privileges that can be granted to other users by users who are assigned the role.

You can use the check's name list to specify roles that are to be excluded for the check.

Table 2-7 Grantable privilege

Message name	Title	Severity
GRANTABLE_ROLE_PRIVILEGE	Grantable role privilege	Green (0)

To protect your computers

- ◆ Do the following:
 - Periodically review all grantable role privileges to ensure that the grantable privilege is appropriate for the role.
 - Revoke grantable role privileges from users who are not authorized to grant them.

Reporting nested roles

These checks report existing nested roles and nested roles that have been added to or dropped from their parent roles since the last snapshot update.

Nested roles

This check reports roles and the nested roles that they contain.

You can use the check's name list to specify roles that are to be included or excluded for the check.

Table 2-8 Nested role message

Message name	Title	Severity
ROLE_ROLE	Nested role	Green (0)

To protect your computers

- ◆ Do one of the following:
 - If the deletion is authorized, update the snapshot.
 - If the deletion is not authorized, restore the nested role.

New nested roles

This check reports roles that were directly granted to other roles after the last snapshot update.

You can use the check's name list to specify roles that are to be included or excluded for the check.

Table 2-9 New nested role message

Message name	Title	Severity
ADDED_ROLE_ROLE	New nested role	Yellow (1)

To protect your computers

- If the change is authorized, update the snapshot.
- If the change is not authorized, drop the nested role.

Deleted nested role

This check reports nested roles that were removed from parent roles since the last snapshot update.

You can use the check's name list to specify roles that are to be included or excluded for the check.

Table 2-10 Deleted nested role message

Message name	Title	Severity
DELETED_ROLE_ROLE	Nested role deleted	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the deletion is authorized, update the snapshot.
 - If the deletion is not authorized, restore the nested role.

Grantable nested role

This check reports nested roles that can be granted to other roles or users.

You can use the check's name list to specify roles that are to be excluded for the check.

Table 2-11 Grantable nested role message

Message name	Title	Severity
GRANTABLE_ROLE_ROLE	Grantable nested role	Green (0)

To protect your computers

- ◆ Periodically review grantable nested roles to ensure that they are currently authorized for the roles where they reside and that the roles are currently authorized to grant the nested roles.

Reporting role access

These checks report password-protected roles that are used as default roles, directly granted DBA roles, roles without password protection, and tables accessed by the public role.

Password-protected default role

This check reports password-protected roles that are assigned to users as default roles.

Default roles do not require passwords. Password-protected roles normally contain privileges and/or roles that require authorization. Users who have password-protected default roles are not required to type passwords to use the roles.

Table 2-12 Password protected default role message

Message name	Title	Severity
DEFAULT_ROLE_PASS_REQUIRED	Default role requires password	Yellow (1)

To protect your computers

- ◆ If the user is not authorized to use this role without typing a password, do one of the following:
 - Assign a different default role to the user.
 - Remove password protection from the role.

Users who have the role will not be required to type passwords to use it.

DBA equivalent roles

You can use this option to specify roles that are to be examined for the Granted Oracle DBA role.

Granted Oracle DBA role

This check reports users and roles that have been directly granted to an Oracle database administrator (DBA) role or equivalent.

You can use the check's name list to specify users that are to be excluded for the check.

Table 2-13 Oracle DBA role message

Message name	Title	Severity
DBA_ROLE_USERS	User granted Oracle DBA role	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - Revoke DBA roles from unauthorized users.
 - Tightly control database administrator rights.

Roles without passwords

This check reports roles that do not require a password.

You can use the check's name list to specify roles that are to be excluded for the check.

Table 2-14 Role without passwords message

Message name	Title	Severity
ROLE_PASSWORD	Password not required for role	Yellow (1)

To protect your computers

- ◆ Do the following:
 - If the role could be exploited to give users access to security-related information, require a password for the role.
 - Control permissions that are granted to roles that do not require passwords.

PUBLIC role access

This check reports tables that users can access with a PUBLIC role and the privileges that are used.

Table 2-15 Publicly accessible table message

Message name	Title	Severity
PUBLIC_ACCESS	Table accessible to PUBLIC	Green (0)

To protect your computers

- ◆ Control permissions that are granted to the PUBLIC role.
The preferred method of granting access is to give EXECUTE to the procedures.

Oracle tablespace

- [Creating a baseline snapshot](#)
- [Editing default settings](#)
- [Reporting tablespaces](#)
- [Reporting tablespace datafiles](#)
- [Reporting SYSTEM tablespace information](#)
- [Reporting DBA tablespace quotas](#)

Creating a baseline snapshot

To establish a baseline, run the Tablespace module. This creates a snapshot of current account information that you can update when you run checks that report new, deleted, or changed information.

Automatically update snapshots

Enable this option to update snapshots automatically with current information.

Editing default settings

The Symantec ESM module for Oracle tablespaces includes one option that you can use to edit default settings for all security checks in the module.

Oracle system identifiers (SIDs)

You can use the name lists in this option to specify Oracle system identifiers (SIDs) that are to be examined by module checks. By default, the module examines all SIDs that are specified when you configure Symantec ESM modules

for Oracle Databases. The configuration for Symantec ESM modules for Oracle Databases is stored in `/esm/config/oracle.dat`.

Reporting tablespaces

These checks report existing tablespaces and tablespaces that have been added or deleted since the last snapshot update.

Tablespaces

This check reports all tablespaces that have been created in the Oracle database. You can use the check's name list to specify authorized tablespaces that are to be excluded for the check.

Table 3-1 Tablespaces message

Message name	Title	Severity
TABLESPACE	Oracle tablespace	Green (0)

To protect your computers

- ◆ Periodically review tablespaces to ensure that they are all authorized.

New tablespaces

This check reports tablespaces that were created in the Oracle database after the last snapshot update.

You can use the check's name list to specify authorized tablespaces that are to be excluded for the check.

Table 3-2 New tablespace message

Message name	Title	Severity
ADDED_TABLESPACE	New Oracle tablespace	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the addition is authorized, update the snapshot.
 - If the addition is not authorized, delete the new tablespace.

Deleted tablespaces

This check reports tablespaces that were deleted from the Oracle database after the last snapshot update.

You can use the check's name list to specify tablespaces that are to be excluded for the check.

Table 3-3 Deleted tablespace message

Message name	Title	Severity
DELETED_TABLESPACE	Deleted Oracle tablespace	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the deletion is authorized, update the snapshot.
 - If the deletion is not authorized, restore the tablespace.

Reporting tablespace datafiles

These checks report existing datafiles and datafiles that were added to or dropped from the database after the last snapshot update.

Tablespace datafiles

This check reports the locations of all tablespace datafiles if the Permission setting is 0. Otherwise, the check reports either tablespace datafiles that have file permissions which are less restrictive than you specify in the Permission field, or tablespace datafiles that have UID/GIDs which do not match the corresponding UID/GIDs in the Oracle database.

In the check's Tablespaces to Skip field, specify tablespaces that are to be excluded for the check.

In the check's Permission field, specify a permission value as a three-digit octal number.

Table 3-4 Tablespace datafile messages

Message name	Title	Severity
DATAFILE	Tablespace file	Green (0)
DATAFILE_PERM	Tablespace file permission	Yellow (2)

To protect your computers

- ◆ Do the following:
 - If the file permissions are less restrictive than your security policy, specify a permission value for the datafile that conforms to your security policy.
 - Periodically review tablespace datafiles to ensure that they are authorized, and that their file permissions conform to your security policy.

New tablespace datafiles

This check reports datafiles that were added to tablespaces after the last snapshot update.

You can use the check's name list to specify tablespaces that are to be excluded for the check.

Table 3-5 New tablespace datafile message

Message name	Title	Severity
ADDED_DATAFILE	New tablespace datafile	Yellow (1)

To protect your computers

- ◆ Do one of the following:
 - If the addition is authorized, update the snapshot.
 - If the addition is not authorized, drop the datafile from the tablespace.

Deleted tablespace datafiles

This check reports datafiles that were deleted after the last snapshot update.

You can use the check's name list to specify tablespaces that are to be excluded for the check.

Table 3-6 Deleted tablespace datafile message

Message name	Title	Severity
DELETED_DATAFILE	Deleted tablespace datafile	Yellow (1)

To protect your computers

- If the deletion is authorized, update the snapshot.
- If the deletion is not authorized, restore the datafile.

Note: The Deleted tablespace datafiles check reports messages only if the New tablespace datafiles check is enabled.

Reporting SYSTEM tablespace information

These checks report objects in the SYSTEM tablespace and users whose default or temporary tablespace is the SYSTEM tablespace.

Objects in SYSTEM tablespace

This check reports tables and indexes that are in the SYSTEM tablespace.

You can use the check's name list to specify users (owners) that are to be excluded for the check.

Table 3-7 SYSTEM tablespace objects message

Message name	Title	Severity
TAB_IN_SYS_TABLESPACE	Object defined in SYSTEM tablespace	Green (0)

To protect your computers

- ◆ Ensure that only authorized objects reside in the SYSTEM tablespace.

SYSTEM tablespace assigned to user

This check reports users whose default and/or temporary tablespaces are the SYSTEM tablespace.

You can use the check's name list to specify users that are to be excluded for the check.

Table 3-8 SYSTEM tablespace user message

Message name	Title	Severity
USER_USING_SYS_TABLESPACE	SYSTEM tablespace user	Green (0)

To protect your computers

- ◆ Ensure that only authorized users have access to the SYSTEM tablespace.

Reporting DBA tablespace quotas

These checks report violations of MAX_BYTES and MAX_BLOCKS tablespace quotas.

Oracle tablespaces

You can use this option to specify tables that are to be included or excluded for MAX_BYTES in DBA_TS_QUOTAS and MAX_BLOCKS in DBA_TS_QUOTAS.

MAX_BYTES in DBA_TS_QUOTAS

This check reports users with resource rights to tablespaces whose MAX_BYTES values exceed the value that you specify in the check. For an unlimited number of bytes, specify -1 in the MAX_BYTES field.

You can use the check's name list to specify authorized users that are to be excluded for the check.

Table 3-9 MAX_BYTES message

Message name	Title	Severity
MAX_BYTES_QUOTA	MAX_BYTES per tablespace exceeded	Yellow (1)

To protect your computers

- ◆ Drop the user or change the user's MAX_BYTES setting for the tablespace.

MAX_BLOCKS in DBA_TS_QUOTAS

This check reports users with resource rights to tablespaces whose MAX_BLOCKS values exceed the value that you specify in the check. For an unlimited number of bytes, specify -1 in the MAX_BLOCKS field.

You can use the check's name list to specify authorized users that are to be excluded for the check.

Table 3-10 MAX_BLOCKS message

Message name	Title	Severity
MAX_BLOCKS_QUOTA	MAX_BLOCKS per tablespace exceeded	Yellow (1)

To protect your computers

- ◆ Drop the user or change the user's MAX_BLOCKS setting for the tablespace.

Symbols

- .m files
 - editing 24, 25
 - installing 18

Numerics

- 7_DICTIONARY_ACCESSIBILITY 54

A

- Access to SYS.ALL_SOURCE 72
- Account status option 76
- accounts
 - Access to SYS.ALL_SOURCE 72
 - Active default accounts 37
 - creation date 33
 - Database account tablespace changed 35
 - Database accounts 33
 - deleted 35
 - New database accounts 34
 - Prefix for OS account 54
 - user 33
- Active default account 37
- agents
 - connection error 23
 - reregister 23
- Alert file 53
- auditing
 - Audit trail enabled 40
 - Audit trail protection 40
 - reporting methods 41
 - See also* Auditing objects
 - See also* Object auditing
 - See also* Privilege auditing
 - See also* Statement auditing
 - users and roles with privileges 40
- Auditing objects 45
 - Deleted object auditing 46
 - New object auditing 45
- Auditing options 41
- Auditing privileges option 47

B

- background processes alert file 53
- BY ACCESS 41
- BY SESSION 41

C

- Changed object auditing 46
- Changed privilege auditing 49
- Changed resource limits 89
- Changed statement auditing 43
- column values 54
- connections
 - Connection time 91
 - errors 23
 - idle 91
- Control files 60
 - Deleted control files 61
 - New control files 61
- CPU sessions per user 89
- CPU time per call 90
- CPU time per session 90

D

- Database accounts 33
 - Database account creation date changed 36
 - Database account tablespace changed 35
 - DB link encrypted password 53
 - Deleted database accounts 35
 - New database accounts 34
- DBA equivalent roles option 104
- DBA roles granted 104
- DBA users 28
- DBLINK_ENCRYPT_LOGIN 53
- debugging
 - alert file location 53
 - trace file location 52
 - trace file size 52
- default accounts 37
- Deleted control files 61
- Deleted database accounts 35
- Deleted directly granted privileges (users) 33
- Deleted directly granted roles 31
- Deleted nested role 102
- Deleted object auditing 46
- Deleted privilege auditing 48
- Deleted privileges 100
- Deleted profiles 88
- Deleted redo log files 60
- Deleted roles 99
- Deleted statement auditing 43
- Deleted tablespace datafiles 110
- Deleted tablespaces 108
- Directly granted privilege (objects) 73

- Directly granted privileges (users) 32
 - Deleted directly granted privileges 33
 - New directly granted privileges 32
- Directly granted roles 30
 - Deleted directly granted roles 31
 - New directly granted roles 30
- directory access, UTL_FILE 55
- Double occurrences 76

E

- editing .m files 24
- ESMDBA tablespaces 18
- ESMDBA user account 20
- esmora3.tpi 18
- esmora75.tpi 18
- esmorasetup
 - add SID 23
 - change SID 23
 - delete SID 24
 - help 23
 - interactive 24
 - oratab 23
- expiration warning (passwords) 92

F

- Failed logins 92
 - Password lock time 93

G

- global operations 53
- grace time (passwords) 92
- Grantable nested role 103
- Grantable privilege (objects) 72
- Grantable privileges 31
- Grantable privileges (roles) 101
- Grantable roles 29
- Granted Oracle DBA role 104
- Granted prohibited roles 37
- Grantors option 72

I

- Idle time 91
- installation
 - before you install 16
 - esmora2.tpi installation package 18
- Invalid profiles 95

L

logins

- failed 92
- OS authentication 29
- Password lock time 93

M

MAX_BLOCKS in DBA_TS_QUOTAS 112

MAX_BYTES in DBA_TS_QUOTAS 112

MAX_DUMP_FILE_SIZE 52

message.dat file location 25

modules

- installation 18
- Oracle Accounts 27
- Oracle Auditing 39
- Oracle Configuration 51
- Oracle Networks 63
- Oracle Objects 71
- Oracle Passwords 75
- Oracle Patches 81
- Oracle Profiles 85
- Oracle Roles 97
- Oracle Tablespace 107

N

Nested roles 101

- Deleted nested role 102
- Grantable nested roles 103
- New nested roles 102

New control files 61

New database accounts 34

New directly granted privilege 32

New directly granted privileges (users) 32

New directly granted roles 30

New nested roles 102

New object auditing 45

New privilege auditing 48

New privileges 100

New profiles 86

New redo log files 59

New roles 98

New statement auditing 42

New tablespace datafiles 110

New tablespaces 108

O

Object auditing 45

- Auditing objects 45
 - Changed object auditing 46
 - Deleted object auditing 46
 - New object auditing 45
 - reporting methods 44, 45
- Object name option 72
- Oracle Accounts module 27
- Oracle Auditing module 39
- Oracle components 52
- Oracle Configuration module 51
- Oracle configuration watch option 56
- Oracle Net Watch template 65
- Oracle Networks module 63
- Oracle Objects module 71
- Oracle Passwords module 75
- Oracle Patches module 81
- Oracle Profiles module 85
- Oracle profiles option 89
- Oracle Roles module 97
- Oracle server 52
- Oracle system identifiers (SIDs) option 51, 63, 75, 81, 85, 97, 107
- Oracle Tablespace module 107
- Oracle tablespaces option 112
- Oracle versions 16
 - Oracle components 52
 - Oracle server 52
- Oracle7 migration 54
- oratab file 21, 23
- OS accounts, prefix 54
- OS authenticated users 28, 29

P

- Password = any username 78
- Password = username 78
- Password = wordlist word 77
- Password display option 76
- Password duration 92
- Password grace time 92
- Password lock time 93
- Password protected default role (accounts) 36
- Password protected default role (roles) 103
- Password reuse max 93
- Password reuse time 94
- Password verify function 94
- passwords
 - compare to all user names 78
 - compare to user name 78
 - compare to word list 77
 - complexity 94

- DB link encrypted password 53
- default role (accounts) 36
- default role passwords 103
- doubled spelling 76
- grace time 92
- lock time 93
- logins failed 92
- OS authentication 29
- plural spelling 76
- remote login password file 55
- reuse 93
- reversed order 76
- roles without 104
- well known 79
- with prefix 77
- with suffix 77
- Patch information 82
- Patch template 83
- Plural 76
- Prefix 77
- Prefix for OS account 54
- Privilege auditing 47
 - Changed privilege auditing 49
 - Deleted privilege auditing 48
 - New privilege auditing 48
- Privileges 99
 - Access to ALL_SOURCE 72
 - Deleted directly granted privileges 33
 - Deleted privileges 100
 - Directly granted privileges 32
 - Grantable privileges (accounts) 31
 - Grantable privileges (roles) 101
 - New directly granted privilege 32
 - New directly granted privileges (users) 32
 - New privileges 100
 - Restrictions on system privileges 54
 - See also* Privilege auditing
- Privileges option 31
- Profile enforcement 86
- Profile resources 88
- Profiles 86
 - Changed resource limits changed 89
 - Connection time 91
 - Deleted profiles 88
 - Invalid profiles 95
 - New profiles 86
 - Profile enforcement 86
 - profile resources 88
- prohibited roles 37

PUBLIC role access 105

Q

quotas

MAX_BLOCKS in DBA_TS_QUOTAS 112

MAX_BYTES in DBA_TS_QUOTAS 112

R

Redo log files 58

Deleted redo log files 60

locations and permissions 58

New redo log files 59

registering files 18

Remote login password file 55

reregister agent 23

RESOURCE_LIMIT 86

resources

changed limits 89

concurrent sessions per user 89

Connection time 91

CPU time per call 90

CPU time per session 90

idle time 91

MAX_BLOCKS in DBA_TS_QUOTAS 112

MAX_BYTES in DBA_TS_QUOTAS 112

profile resources 88

profile violations 95

Restrictions on system privileges 54

reuse passwords 93

Reverse order 76

Roles 29, 98

Deleted directly granted roles 31

Deleted nested role 102

Deleted privileges 100

Deleted roles 99

Directly granted roles 30

Grantable nested roles 103

Grantable privileges 101

Grantable roles 29

Granted Oracle DBA role 104

Granted prohibited roles 37

Nested roles 101

New directly granted roles 30

New nested roles 102

New privileges 100

New roles 98

Password protected default role 103

Password protected default role (accounts) 36

- Privileges 99
- PUBLIC role access 105
- Roles without passwords 104

S

- SELECT privileges for column values 54
- sessions

- CPU time 90
 - simultaneous 89

- Sessions per user 89

- SID

- change 23
 - configure 23
 - delete 24

- SQL statements. See Statement auditing

- Statement auditing 42

- Changed statement auditing 43
 - Deleted statement auditing 43
 - New statement auditing 42

- Suffix 77

- SYS

- default password 79
 - schema and system privileges 54

- SYSTEM default password 79

- system privilege restrictions 54

- system requirements 18

- SYSTEM tablespace

- objects 111
 - user 111

T

- table privileges

- Access to ALL_SOURCE 72
 - Directed granted privilege 73
 - Grantable privilege (objects) 72

- Table privileges option 72

- Table-level SELECT privileges 54

- Tablespaces 108

- Database accounts 33
 - Deleted tablespace datafiles 110
 - Deleted tablespaces 108
 - ESMDBA 18
 - MAX_BLOCKS in DBA_TS_QUOTAS 112
 - MAX_BYTES in DBA_TS_QUOTAS 112
 - New Tablespace datafiles 110
 - New tablespaces 108
 - Objects in SYSTEM tablespace 111
 - SYSTEM tablespace assigned to user 111

- Tablespace datafiles 109
- Tablespace file permission 109
- Template files option 81
- templates
 - Oracle Net Watch 65
- time
 - connection time 91
 - idle 91
 - lockout 93
 - password duration 92
 - password grace time 92
 - password reuse 94
 - per call limit 90
 - per session limit 90
- Trace file size 52
- Trace files 52

U

- user accounts 33
 - creation date changed 36
 - deleted 35
 - new 34
 - tablespace changed 35
- user authentication 28
- user privileges
 - Deleted directly granted privileges 33
 - Directly granted privileges 32
 - New directly granted privileges 32
- user roles
 - deleted directly granted 31
 - directly granted 30
 - new directly granted 30
- USER_DUMP_DEST 52
- Users in OS DBA groups 28
- Users to check option 37, 75
- Users to skip in OS DBA groups option 28
- UTL_FILE accessible directories 55

W

- Well known passwords 79
- word lists
 - doubled spelling 76
 - plural spelling 76
 - reversed spelling 76
 - with prefix 77
 - with suffix 77