Symantec™ Enterprise Security Manager Modules for Oracle Databases User Guide for Windows

Release 5.0 for Symantec ESM 9.0 and 10.0 For Windows 2003, 2008

Symantec™ Enterprise Security Manager Modules for Oracle Databases User Guide for Windows

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 5.0

Legal Notice

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
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates 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's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

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

www.symantec.com/business/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 replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

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

Support agreement resources

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

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

Contents

Chapter 1

Introducing Symantec ESM modules for Oracle Databases

This chapter includes the following topics:

About the Symantec ESM modules for Oracle Databases

The Symantec Enterprise Security Manager (ESM) modules for Oracle databases extend the Symantec ESM protection to your databases. These modules implement the checks and options that are specific to Oracle databases, to protect them from exposure to known security problems. The modules may be installed locally on the Symantec ESM agent that is installed on the same computer where the Oracle database resides. You can use the Symantec ESM modules for Oracle database in the same way that you use for other Symantec ESM modules.

What you can do with the Symantec ESM modules for Oracle databases

You can use the ESM Application modules to scan the Oracle databases for reporting vulnerabilities, such as weak passwords, patches update, and so on.

You can perform the following tasks using the ESM console:

- Create a policy.
- Configure the policy.
- Create a rules template.
- Run the policy.
- Review the policy run.
- Correct security problems from the console.
- Create reports.

Templates

Several of the documented modules use templates to store the Oracle database parameters and object settings. Differences between the current settings and template values are reported when the modules run. Modules use templates to store Oracle database parameters and object settings.

Table 1-1 Template name

Module	Check name	Template name	Predefined template
Oracle Auditing	Audit settings	Oracle Auditing	oraaudit.oad
Oracle Configuration	Oracle configuration watch	Oracle Configuration Watch	NA
Oracle Networks	Oracle net configuration watch	Oracle Net Configuration Watch	NA
Oracle Objects	Oracle Critical objects	Oracle Critical Object	oraclecritical objects.rco
Oracle Objects	Object Privileges	Oracle Object Privileges	oracleobject privileges.oop
Oracle Patches	Oracle Template files	Oracle Patch	orawinpatch.orp

Table 1-1 Template name *(continued)*

Module	Check name	Template name	Predefined template
Oracle Patches	Oracle Template files	Oracle Patch	ora_cpu_psu.orp
Oracle Roles	Granted privileges	Oracle System Privileges	NA
Oracle Roles	Granted roles	Oracle Roles	NA
Oracle Profiles	Profile settings	Oracle Profiles	NA

Where you can get more information

For more information about Symantec ESM modules and Security Updates, see the latest versions of the *Symantec Enterprise Security Administrator's Guide* and the *Symantec ESM Security Update User's Guide*.

For more information on Symantec Enterprise Security Manager (ESM), Symantec ESM Security Updates, and Symantec ESM support for database products, see the Symantec Security Response Web site at the following URL: Security Response Web site

About the Logging functionality on the Oracle database modules

A Logging feature has been introduced on the Oracle database modules that enables ESM to log the information, such as errors and exceptions, that a module generates at the runtime.

About the log levels of the messages

The log level specifies the type and criticality of a message. You can manually create a configuration file and specify the log level of the messages that you want to be logged.

ESM checks the log level that you set in the configuration file and stores only the qualifying messages in the log file.

You can specify the following log levels:

ESMNOLOG	Disable logging for the module

ESMCRITICALFAILURES	All critical failures are logged. ESM always logs all critical failures irrespective of the log level that you specify in the configuration file. However, if ESMNOLOG is specified in the configuration file, ESM does not log the critical failures. ESMCRITICALFAILURES is the default log level and you need not explicitly specify it in the configuration file.
ESMERRORS	All errors are logged. The following are some examples of the errors: ■ Template file not found ■ Configuration file not found
ESMEXCEPTIONS	All exceptions are logged.
ESMWARNINGS	All warnings are logged.
ESMINFORMATION	All information messages are logged. The information that is gathered during a policy run is also logged at this level. **Note:** Enabling this level may affect the performance of the module since all the information messages get logged.
ESMTRACE	All debug information is logged.
ESMPERFMANCETIMING	All time-consuming operations are logged.
ESMAUDIT	All audit information is logged. This level covers the data modification operations such as Correction and Update.
ESMMAXIMUM	Includes all log levels except ESMNOLOG.

You specify the log level using the LogLevel parameter of the configuration file. For example, to log the messages that are related to critical failures, specify the log level as follows:

[<module>_LogLevel]= ESMCRITICALFAILURES

You can also specify multiple log levels by separating them with a pipe (|) character as follows:

[<module>_LogLevel]= ESMCRITICALFAILURES|ESMPERFMANCETIMING

You can use log levels for specific operations as follows:

For regular policy runs	ESMCRITICALFAILURES and ESMERRORS
To generate detailed logs for policy failure	ESMCRITICALFAILURES, ESMERRORS, ESMTRACE, and ESMINFORMATION

Creating the configuration file

You must create a configuration file named esmlog.conf in the <esm_install_dir>/config folder and specify the values that ESM uses to store the logs of a module.

To create the configuration file

1. Change to the <esm_install_dir>/config folder.
2. Create a new text file and specify the parameters and their values.
3. Save the text file as `esmlog.conf`.

The following is an example of the entries in the configuration file:

```
[MaxFileSize] = 1024

[NoOfBackupFile] = 20

[LogFileDirectory] = <esm_install_dir>\system\agentname\logs

[password_LogLevel] = ESMINFORMATION|ESMTRACE

[pwdll_LogLevel] = ESMMAXIMUM
```

Note: No default configuration file is shipped with the current release. You need to manually create the file and specify the parameters in it.

Parameters of the configuration file

Table 1-2 lists the parameters that you need to specify in the configuration file.

Table 1-2 Configuration file parameters

Parameter name	Description	Range of values	Default value
[MaxFileSize]	Specify the maximum file size for the log file in MB	1 MB to 1024 MB (1 GB)	1 MB

Table 1-2 Configuration file parameters *(continued)*

Parameter name	Description	Range of values	Default value
[NoOfBackupFile]	Specify the number of backup files of logs that can be stored per module. For example, if the value of NOOFBACKUPFILE is 3, then ESM stores a maximum of 3 backup files for the module.	0 to 20	1
[LogFileDirectory]	Specify the absolute path to store the log file and backup log files.	N/A	The esm/system/tmp directory is used on the Windows operating systems.
[<module>_LogLevel]	Specify the log level along with the short name of the module. For example, to log all error messages for the Password Strength module, specify the following: [password_LogLevel] =ESMERRORS	N/A	ESMCRITICALFAILURES (unless ESMNOLOGS is specified)

If the configuration file is not present, ESM considers the default values of all the parameters to store the logs.

About the log file

By default, ESM stores the log file for a module in the temporary directory of the operating system. Separate log files are stored for each module.

The log file has the following format:

<module_name>.log

The <module_name> is the short name of the module. For example, the log file of the Password Strength module is named password.log. The backup file name for password strength module is named password.log_1.bak and so on.

Note: During the process of logging, ESM locks the log file to store the logging information. If the log file is open at that time, the information about the logs might get lost.

Format of the log file

A log file contains the following fields:

Serial Number	Serial number of the log file entry The serial number is displayed in hexadecimal format. The serial number gets reset in the next policy run on the module.
Thread ID	Thread identifier of the process that generated the message
Source File Name	Name of the source file that caused the message to be generated
Line Number	Line number in the source file from where the message was generated
Date	Date on which the log was created
Time	Time at which the log was created
Message	The actual message that was generated along with the log level of that message

About the backup of logs

When the log file reaches a specified size limit, ESM backs up the log file. This size limit is configurable and you can specify it in the MaxFileSize parameter of the configuration file.

If the log file reaches the MaxFileSize value, ESM creates a backup of the log file depending on the NoOfBackupFile value that is specified in configuration file. For example, if the NoOfBackupFile value is 0, ESM overwrites the existing log file, if any, for the module.

Chapter 2

Installing Symantec ESM modules for Oracle Databases

This chapter includes the following topics:

About installing ESM modules for Oracle Databases

You can install the Symantec Enterprise Security Manager (ESM) on Oracle on Windows 2003/2008 platforms.

Before you install

Before you install Symantec ESM Modules for Oracle Databases, you must verify the following:

CD-ROM access	At least one computer in your network must have a CD-ROM drive.

Account privileges	You must have access with the root privileges to an account on each computer where you plan to install the modules.
Connection to the manager	The Symantec ESM enterprise console must be able to connect to the Symantec ESM manager.
Agent and manager	The Symantec ESM agent must be running and registered with at least one Symantec ESM manager.

Minimum account privileges

Table 2-1 lists the minimum privileges that are assigned to the ESMDBA account if the database instance is configured by using “/ as sysdba”.

Table 2-1 Minimum account privileges assigned to the ESMDBA account

Oracle version	System privileges	Object privileges
10.x and 11.x	Create session	■ 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.dba_temp_files ■ sys.registry$history ■ sys.user$ ■ v$controlfile ■ v$instance ■ v$logfile ■ v$parameter ■ v$version ■ v$database

Table 2-2 lists the minimum privileges that are assigned to the ESMDBA account if the database instance is configured by using “SYSTEM”:

Table 2-2 Minimum account privileges assigned to the ESMDBA

Oracle version	System privileges	Object privileges
10.x and 11.x	■ Create session ■ Select any Dictionary	N/A

Table 2-3 lists the roles that can be assigned to a pre-created account instead of assigning the privileges.

Note: A pre-created account is an existing account that you must create and assign minimum required privileges or roles before the configuration.

To assign object privileges, refer to Table 2-1 . To assign system privileges, refer to Table 2-2. To assign minimum privileges, refer to Table 2-3.

Table 2-3 Roles that can be assigned to a pre-created account

Oracle version	System roles
10.x and 11.x	■ CONNECT ■ SELECT_ CATALOG_ROLE

Warning: If you use less than the recommended privileges for the accounts that the Oracle Application module uses for reporting, then a few checks may not function correctly. This could also result in any intentional or unintentional blocking of the module's ability to report on the conditions you may need to know exists.

About Oracle account creation scripts

This section contains the scripts that you can use for creating an Oracle user and assigning the required privileges to it. You must create a .sql file, copy the script, and paste in the .sql file. You can then run the file to create a user and use this user while configuring the Oracle module.

Note: You can use either of the script to create a user account.

Script for creating a user on Oracle 10.0 or later versions

This section contains the script that you can use for creating a user with system and object privileges on Oracle10.0 or later versions.

```
CREATE USER ESMDBA IDENTIFIED by Rnm2np4 DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE TEMP PROFILE DEFAULT;

GRANT CREATE SESSION to ESMDBA;

GRANT SELECT on sys.dba_data_files to ESMDBA;

GRANT SELECT on sys.dba_indexes to ESMDBA;

GRANT SELECT on sys.dba_obj_audit_opts to ESMDBA;

GRANT SELECT on sys.dba_priv_audit_opts to ESMDBA;

GRANT SELECT on sys.product_component_version to ESMDBA;

GRANT SELECT on sys.dba_profiles to ESMDBA;

GRANT SELECT on sys.dba_role_privs to ESMDBA;

GRANT SELECT on sys.dba_roles to ESMDBA;

GRANT SELECT on sys.dba_stmt_audit_opts to ESMDBA;

GRANT SELECT on sys.dba_sys_privs to ESMDBA;

GRANT SELECT on sys.dba_tab_privs to ESMDBA;

GRANT SELECT on sys.dba_tables to ESMDBA;

GRANT SELECT on sys.dba_tablespaces to ESMDBA;

GRANT SELECT on sys.dba_ts_quotas to ESMDBA;

GRANT SELECT on sys.dba_users to ESMDBA;

GRANT SELECT on sys.dba_temp_files to ESMDBA;

GRANT SELECT on sys.registry$history to ESMDBA;

GRANT SELECT on sys.user$ to ESMDBA;

GRANT SELECT on v_$controlfile to ESMDBA;

GRANT SELECT on v_$instance to ESMDBA;

GRANT SELECT on v_$logfile to ESMDBA;

GRANT SELECT on v_$parameter to ESMDBA;

GRANT SELECT on v_$version to ESMDBA;

GRANT SELECT on v_$database to ESMDBA;
```

Script for assigning system privileges to the user on Oracle 10.0 or later versions

This section contains the script that you can use for system privileges to the user that you create on Oracle 10.0 or later versions.

```
CREATE USER ESMDBA IDENTIFIED by Rnm2np4 DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE TEMP PROFILE DEFAULT;

GRANT CREATE SESSION, SELECT ANY DICTIONARY to ESMDBA;

GRANT SELECT on sys.registry$history to ESMDBA;

GRANT SELECT on v_$version to ESMDBA;
```

See Table 2-3 on page 21.

System requirements

Table 2-4 lists the operating systems that support the ESM Application modules for Oracle on Windows.

Note: As per Symantec's End of Life product support policy, the ESM Modules for Oracle Databases are not supported on ESM 6.0. The support for Oracle version 9.0.x has been removed per the End of Support policy of Oracle.

Table 2-4 Supported operating systems for ESM modules on Oracle

Operating System				ESM Module	Oracle		
OS	Architecture	Type	Version	Type	Version	Type	Client Installer

Table 2-4 Supported operating systems for ESM modules on Oracle *(continued)*

Operating System				ESM Module	Oracle		
Windows	x86	32-bit	Windows 2003	32-bit	10.1.0.x, 10.2.0.x, 11.1.0.6.0, 11.2.0.1.0	32-bit	
	x64	64-bit	Windows 2003	64-bit	10.1.0.x, 10.2.0.x, 11.1.0.6.0, 11.2.0.1.0	32-bit, 64-bit	64-bit **Note:** This is required if Oracle 32-bit database is installed.
	x86	32-bit	Windows 2008	32-bit	10.1.0.x, 10.2.0.x, 11.1.0.6.0, 11.2.0.1.0	32-bit	
	x64	64-bit	Windows 2008	64-bit	10.1.0.x, 10.2.0.x, 11.1.0.6.0, 11.2.0.1.0	32-bit, 64-bit	64-bit **Note:** This is required if Oracle 32-bit database is installed.

Table 2-5 lists the Real Application Clustering (RAC) support on Windows.

Table 2-5 Real Application Clustering (RAC) support on Windows

Supported operating systems	Architecture	Supported OS versions	Supported Oracle versions
Windows (32-bit)	x86	Windows 2003	10.2.0.x, 11.1.0.6.0

Table 2-6 lists the disk space requirements only for the Symantec ESM Modules for Oracle Databases and not for the ESM agents.

Table 2-6 Disk space requirements

Agent operating system	Disk space
Windows 2003 (32-bit)	30 MB

Table 2-6 Disk space requirements *(continued)*

Agent operating system	Disk space
Windows 2003 (64-bit)	30 MB
Windows 2008 (32-bit)	30 MB
Windows 2008 (64-bit)	50 MB

About using parameters in the oraenv.dat file

This table lists the different parameters that you can use in the `oraenv.dat` file to work with the Symantec ESM modules for Oracle. The oraenv.dat file is a configuration file that stores the configuration parameters that control certain functions of the ESM modules. You can create the `oraenv.dat` file in the `\esm\config` directory, to specify the parameters. If the `oraenv.dat` file does not exist then the default values are used.

Note: The parameters only affect the Symantec ESM modules and do not affect the settings of the Oracle database.

Table 2-7 Parameters and their usage

Parameter name	Description	Parameter value	Example
MANAGE ORAUSER PASSWORD	You can use this parameter to enable the password management for the pre-created accounts.	By default, this parameter is set to 0. To enable, set the parameter to 1. When enabled, the ESM Oracle modules for Oracle database manage the passwords for the pre-created accounts that are explicitly configured with the respective Oracle databases. If you set the parameter to 1, then the password of the pre-created configured account changes depending on the value that you set for the PassChangedPeriod parameter.	config MANAGEORAUSER PASSWORD 1
ORA_LANG	You can use this parameter to unset an environment variable during an ESM Oracle module policy run.	You can unset the ORA_LANG environment variable by adding `unset ORA_LANG` entry in the `oraenv.dat` file.	unset ORA_LANG
Pass CreationLog	You can use this parameter to configure the logging level for password creation. The default logging level is 0.	You can configure the logging level for password creation by adding `config PassCreationLog 1` entry in the `oraenv.dat` file.	config PassCreationLog 1

Table 2-7 Parameters and their usage *(continued)*

Parameter name	Description	Parameter value	Example
Pass SpecString	You can use this parameter to specify the special characters that you can use while generating the password for the configured account.	The default special characters are the underscore (_), plus (+), dash (-), equal to (=), brackets (<>, ()), question mark (?), asterisk (*), percent (%), hash (#), exclamation mark (!). You can add this parameter to the `oraenv.dat` file as config PassSpecString <special characters>.	config PassSpecString $#_
Pass ChangedPeriod	You can use this parameter to specify the period that you want to change the password of the configured account before the expiration period.	If you do not specify any value then ESM Oracle database modules considers 35 days as the default value. On policy run, the password changes 35 days before the password expiration date. You can add this parameter to the oraenv.dat file as config passChangedPeriod <number of days>.	config PassChangedPeriod 30

Table 2-7 Parameters and their usage *(continued)*

Parameter name	Description	Parameter value	Example
MinPrivilege	You can assign minimum privileges to the ESMDBA user. You can use this parameter only if SID is configured by using the '/ as sysdba' method.	If MinPrivilege is set to **Yes**, then the privileges are assigned to the ESMDBA account if the database instance is configured by using "/ as sysdba". See Table 2-1 on page 20. The default value is 'Yes'. If MinPrivilege is set to **No**, then the privileges are assigned to the ESMDBA account if the database instance is configured by using "/ as sysdba". See Table 2-2 on page 21.	set MinPrivilege YES

See "Installing the ESM modules for Oracle databases" on page 28.

Installing the ESM modules for Oracle databases

The installation program does the following:

- Extracts and installs module executables, configuration (.m) files, and the template files.
- Registers the .m and the template files to the ESM manager by using the ESM agent's registration program.
- Launches the esmorasetup program to create the ESMDBA account for reporting. The esmorasetup is a configuration utility that is used during the installation setup. The password of ESMDBA account is 12 characters long and is generated randomly. The password is encrypted by using the 256-bit AES encryption algorithm and is stored in the `\esm\config\oracle.dat` file.
- Auto-generates the password for the ESMDBA account. The ESM modules for the Oracle databases consider the following parameters during auto-generation of the passwords :
  - PassChangedPeriod

The “PassChangedPeriod” parameter specifies the number of days after which the program automatically changes the password of the configured account. The default days of "PassChangedPeriod" is 35 days. The password must contain at least one uppercase, one lower-case, one numeric character (0-9), and one special character. The default special characters are the underscore (_), plus (+), dash (-), equal to (=), brackets (<>), question mark (?), brackets (()), asterisk (*), percent (%), hash (#), and exclamation mark (!).

- PassSpecString
  The "PassSpecString" parameter specifies the special characters that you can use while generating the password for the configured account. Use this parameter if the `config PassSpecString` entry is not defined in the `\esm\config\oraenv.dat` file. If you want to use other special characters, you can also add a parameter "config PassSpecString $#_" entry into the `esm\config\oraenv.dat` file before you run esmorasetup configuration.

- Grants the system privileges based on predefined roles.
  See Table 2-3 on page 21.

During the policy runs, the ESMDBA account does not create any object in the database.

Note: If you change the password for the pre-created account then you must modify the configuration records by using the `\esm\bin\<platform>\esmorasetup.exe`.

Note: The ESM Application module should be installed on all the Oracle databases, including failover. The module does not automatically detect the failover databases unless it is installed and configured on the same.

Running the installation program and registering the files

You can install the modules on the ESM agent computer by using the esmoracletpi.exe.

To run the installation program and register the files

1. At the command prompt, type cd <path> to open the directory that corresponds to your vendor\operating system\architecture\esmoracletpi.exe.

   You can also download and copy the esmoracletpi.exe from the Security Response Web site to the desired location.

2. Choose one of the following options:

Option 1	To display the contents of the package.
Option 2	To install the module.

3. The **Do you want to register the template or .m files?** message appears. Do one of the following:

   - Type a **Y**, if the files are not registered with the manager.
   - Type an **N**, if the files have already been registered.

   Note: You must register the template or *.m files at least once with the agent that is installed on the same operating system and is registered to the same manager.

4. Enter the ESM manager that the agent is registered to.

   Usually, it is the name of the computer that the manager is installed on.

5. Enter the ESM access name (logon name) for the manager.
6. Enter the name of the agent as it is currently registered to the ESM manager.

   Usually, it is the name of the computer that the agent is installed on.

7. Enter the ESM password that is used to log on to the ESM manager.
8. Enter the network protocol that is used to contact the ESM manager.
9. Enter the port that is used to contact the ESM Manager.

   The default port is 5600.

10. The **Is this information correct?** message appears. Do one of the following:

    - Type a **Y**, the agent continues with the registration to the ESM manager.
    - Type an **N**, the setup prompts to re-enter the details of the new manager.

Silently installing the ESM modules for Oracle databases

You can silently install the ESM Modules for Oracle by using the esmoracletpi.exe.

Table 2-8 lists the command line options for silently installing the ESM modules for Oracle.

Table 2-8 Options to silently install the ESM modules for Oracle databases

Option	Description
-d	Display the description and contents of this Tune-up or third-party installation package.
-i	Install this Tune-up or 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.
-g	Specify the ESM agent name to use for Re-registration.
-N	Do not update the report content file on the ESM manager. **Note:** The Report Content File (.rdl) lets you correlate check message mapping between the latest content update and the Symantec ESM manager. The Report Content File is the name of the file that is sent from the agent to the manager. You can change the location of the .rdl or update the content manually from the command prompt at anytime. See "Running the installation program and registering the files" on page 29.
-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 user. The default value is TEMP.

Table 2-8 Options to silently install the ESM modules for Oracle databases *(continued)*

Option	Description
-S	Specify the default tablespace. This option is used by the ESMDBA user. The default value is USERS.
-W	Specify the user's profile. This option is used by the ESMDBA user. The default value is DEFAULT.
-h	Display help on the usage of options that can be used for silent installation.
-e	Install the modules without configuring the SIDs.

To install the ESM modules for Oracle silently

- Copy the .exe to a folder on your computer and at the command prompt, type cd <path> to open the directory.
- Type the following at the command prompt:

  ```
  esmoracletpi.exe {-it} {-m} {-U} {-p} {-P} {-g} {Y} {-e}
  ```

  This command only installs the ESM modules for Oracle. To configure the SIDs for security checking, run `esmorasetup` from the `\esm\bin\<platform>` directory.

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

- Type the following at the command prompt:

  ```
  esmoracletpi.exe {-it} {-m} {-U} {-p} {-P} {-g} {Y} {-A} {-C} [-T]
  [-S] [-W]
  ```

  The configuration log file `EsmOraConfig.log` is created in the `\esm\system\<system name>` folder.

Adding configuration records to enable the ESM security checking for the Oracle database

When the extraction is complete, the installation program prompts you to add ESM database configuration records to enable the security checking for the oracle database.

To add configuration records

1 The **Do you want to continue and add configuration records to enable the ESM security checking for the Oracle database? [Yes]** message appears. Do one of the following:

- Type a **Y**, to continue the installation and connect to the current SID.
- Type an **N**, to end the installation without adding the security checks.

2 The **Do you want to configure the <SID_Name> for the ESM security checks? [Y/N]** message appears. Do one of the following:

- Type an **A** to connect using the "SYSTEM" account.
  You can press Enter to connect by using the SYSTEM account or enter a pre-created account name to configure with. A pre-created account is an existing account that you must create before the configuration.
  To connect by using the SYSTEM account, See “To add security checking using the default SYSTEM account” on page 33.
  To connect by entering the pre-created account,
  See “To add security checking using a pre-created account” on page 35.
- Type a **B** to connect using the "/as sysdba" method.
  See “To configure Oracle SID by using the /as sysdba method” on page 34.

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 a **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, and then recreates it.

8 Do one of the following:

- Type a **Y**, to add security checking for the next SID.
- Type an **N**, to continue without adding security checks to the next SID.

9 Repeat steps 1 through 8 until you have skipped the installation on every SID.

Note: Symantec recommends that you do not change the privileges or password of the ESMDBA account. If you change the privileges, then some checks may not report. If you change the password of the ESMDBA account, then you must configure the Oracle database again. Drop this account only if you uninstall the agent from the computer.

To configure Oracle SID by using the /as sysdba method

1 Type the Oracle Home path, or press **Enter** to accept the default path.

2 Type a **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:

- Type a **Y**, to configure the next SID.

- Type an **N**, to continue without configuring the next SID.

7 Repeat steps 1 through 6 until you have skipped the installation on every SID.

Note: Symantec recommends that you do not change the privileges or password of the ESMDBA account. If you change the privileges, then some checks may not report. If you change the password of the ESMDBA account, then you must configure the Oracle database again. Drop this account only if you uninstall the agent from the computer.

If a database is moved to the restricted mode after you create an ESMDBA account, then you must grant the Restricted Session privilege to the ESMDBA account. If you have used a pre-created account to configure a database in the restricted mode, then grant the Restricted Session privilege to the pre-created account.

To add security checking using a pre-created account

1. Type the Oracle Home path, or press Enter to accept the default path. Do one of the following:
   - Type a **Y**, to continue the installation and connect to the current SID.
   - Type an **N**, to end the installation without adding the security checks.
2. Type a **Y**, to configure the designated SID for security checking.
3. Type an **A**, to configure the SID by using the Oracle database account.
4. Type the Oracle Home path, or press Enter to accept the default path.
5. 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.
6. Type the pre-created Oracle account password.
7. Retype the password.
8. The installation program prompts you to add the security checking for SID. Type a **Y** or an **N**.

   Repeat steps 4 through 7 until you have skipped the installation on every SID.

To add or update configuration record for a pre-created Oracle account

- At the command prompt, type the following:

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

-A {Account}	Predefined Oracle database logon account
-P {Password}	Predefined Oracle database logon account password
-H {OraHome}	Oracle home directory

To add or update configuration record for a SID created in RAC environment

- At the command prompt, type the following:

  ```
  esmorasetup -a {SID} -A (Pre-create account) -P {PASSWORD} [-T
  {TEMP}] [-S {USERS}] [-W {DEFAULT}
  ```

-A {Account}	Predefined Oracle database logon account
-P {Password}	Predefined Oracle database logon account password
-T {TblSpace}	Oracle TEMPORARY table space for ESMDBA user
-S {TblSpace}	Oracle DEFAULT table space for ESMDBA user
-W {Profile}	Oracle PROFILE for ESMDBA user

Note: You can configure the Oracle SIDs in the RAC environment only by using pre-created accounts.

About configuring SIDs

You can use the esmorasetup utility located in the \esm\bin\<OS_Arch> directory to add, modify, or remove the Oracle instances on which the security check reports.

About configuring SIDs lists the SID configuration options.

Table 2-9 SID configuration options

To do this	Type
Display Help	`esmorasetup.exe -h`
Configure a new SID	`esmorasetup.exe -a {SID} [-H {ORAHOME}]`
Configure all SIDs	`esmorasetup.exe - a all`
Register an Oracle Home into Symantec ESM modules for Oracle Databases	`esmorasetup.exe -H {ORAHOME}`

Table 2-9 SID configuration options *(continued)*

To do this	Type
Remove a registered oracle home from Symantec ESM modules for Oracle Databases	`esmorasetup.exe -R {ORAHOME}`
Remove (delete) a SID	`esmorasetup.exe -d {SID} [-P {PASSWORD}]`
Remove (delete) all SIDs (both using the SYSTEM account and "/as sysdba" method)	`Esmorasetup.exe -d all`
Remove a registered Oracle Home from Symantec ESM modules for Oracle Databases	`esmorasetup.exe -R {ORAHOME}`
Update an oracle Home for one registered SID	`esmorasetup.exe -U {SID} [-H { ORAHOME }]`
Update an oracle Home for all registered SID	`esmorasetup.exe -U all`
List all registered SIDs	`esmorasetup.exe -l`
Specify the file name that gets created with the encrypted credentials. You are prompted to provide the credentials that are stored in this file in the encrypted format. This file can be used to configure the Oracle SIDs on any ESM agent computer provided the encrypted credentials of the Oracle account are the same.	`esmorasetup -eof <output_file>`

Table 2-9 SID configuration options *(continued)*

To do this	Type
Specify the file name that contains the encrypted credentials. While configuring a SID with -a option or deleting a configuration record with -d option, you can provide the credentials stored in the encrypted format in a file.	`esmorasetup -eif <input_file>`

Table 2-10 lists the Silent SID configuration options.

Table 2-10 Silent SID configuration options

To do this	Type
Configure a SID created in RAC environment into the Symantec ESM modules for Oracle Databases silently using a pre-created account	`esmorasetup -a {SID} -A Pre-created account -P {PASSWORD} [-T {TEMP}] [- S {USERS}][-W {DEFAULT}] -Q`
Configure a SID into the Symantec ESM modules for Oracle Databases silently using the file name that contains the encrypted credentials.	`esmorasetup -a {SID} -eif <filename> [-T {TEMP}] [- S {USERS}][-W {DEFAULT}] -Q`
Configure a SID silently by connecting to the database as SYSTEM account	`esmorasetup -a <SID_name> [-f <file_name>] -A <account_name> -P <password> [-H <OraHome>] [-T <Temp>] [-S <Users>] [-W <Default>] - Q`
Configure a SID silently by connecting to the database as SYSTEM account using the file name that contains the encrypted credentials.	`esmorasetup -a <SID_name> [-f <file_name>] -eif <filename> [-H <OraHome>] [-T <Temp>] [-S <Users>] [-W <Default>] - Q`
Configure a SID silently by connecting to the database by using the “/as sysdba” method	`esmorasetup -a <SID_name> [-f <file_name>] -A oracle_owner [-H <OraHome>] [-T <Temp>] [-S <Users>] [-W <Default>] -Q`

Table 2-10 Silent SID configuration options *(continued)*

To do this	Type
Configure all SIDs silently by connecting to the database as SYSTEM account	`esmorasetup -a ALL -A SYSTEM -P <password> [-T <Temp>] [-S <Users>] [- W <Default>] -Q`
Configure all SIDs silently by connecting to the database using the file name that contains the encrypted credentials.	`esmorasetup -a ALL -eif <filename>[-T <Temp>] [-S <Users>] [- W <Default>] -Q`
Configure all SIDs silently by connecting to the database by using the "/as sysdba" method	`esmorasetup -a ALL -A oracle_owner [-T <Temp>] [-S <Users>] [-W <Default>] - Q`

For example, to specify a SID with a password by using the interactive mode, type the following at the command prompt:

```
esmorasetup <-a|-d> <sid_name|all> [-P <SYS_PASSWORD>]
```

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.

Silently uninstalling the ESM modules for Oracle Databases

You can silently uninstall the ESM Modules for Oracle by using the esmorauninstall .exe.

Table 2-11 lists the command line options for silently uninstalling the ESM modules for Oracle.

Table 2-11 Options to silently uninstall the ESM modules for Oracle Databases

Option	Description
-h	Display Help.
-F	Specify the file that contains name and credentials of one or multiple managers that the agent is registered to. Use the -mfile option to create the file.
-mfile	Specify to create a file that contains name and credentials of one or multiple managers that the agent is registered to.

Table 2-11 Options to silently uninstall the ESM modules for Oracle Databases *(continued)*

Option	Description
-S	Silent mode uninstall. If only -S is specified, then the uninstallation program does not perform re-registration.
-m	Specify the ESM manager name.
-N	Specify the agent name as registered to manager.
-p	Specify the TCP Port to use.
-U	Specify the ESM access record name.
-P	Specify the ESM access record password.

For example:`esmorauninstall.exe [-h ] [-F {mgrfile}] [-mfile {mgrfile}]`

Uninstalling the Oracle Application module

You can uninstall all the components of the Oracle Application module that are installed on the ESM agent computer and unregister the module from the manager. You can uninstall the Oracle Application module using the uninstaller program.

The esmorauninstall executable uninstalls the following components:

- Application executables
- .m files of the modules
- Templates
- Configuration files
  - Environment configuration files
  - Configuration file with server records
- Snapshot files
- Property file
- Oracle Application module version file
- Registry entry of Oracle Application module
- Application-specific log file
- Manifest entries of the Oracle Application module
- ESM Oracle Application module entry in the agentapp.dat file

How to run the uninstallation program

You can uninstall the Oracle Application modules on the ESM agent computer by using the esmorauninstall.exe.

To uninstall the Oracle Application module

1 At the command prompt, type cd <path> to open the directory that corresponds to vendor\bin\operating system\esmorauninstall.exe.

  The program first checks for the version of the installed register binary. The register binary that is required to uninstall the ESM Oracle Application Module must be of version 10.0.285.10011 or later. If the program does not find the required version, it reports an error and aborts the uninstallation process.

2 The **This will uninstall the application module permanently. Do you want to continue? [yes]** message appears. Do one of the following:

  - Type a **Y**, if you want to continue with the uninstallation.
  - Type an **N**, if you want to exit.

3 The **Do you want to register the agent to the manager after uninstallation? [yes]** message appears. Do one of the following:

  - Type a **Y**, if you want to register the agent to the manager.
    The program informs the manager about the uninstallation of the Oracle Application module from the agent computer that is registered to it.
  - Type an **N**, if you do not want to register the agent to the manager.

4 Enter the ESM manager that the agent is registered to.

  Usually, it is the name of the computer that the manager is installed on.

5 Enter the name of the agent as it is currently registered to the ESM manager.

  Usually, it is the name of the computer that the agent is installed on.

6 Enter the ESM access name (logon name) for the manager.

7 Enter the ESM password that is used to log on to the ESM manager.

8 Re-enter the password.

9 Enter the port that is used to contact the ESM Manager.

  The default port is 5600.

10 The **Is this information correct?** message appears. Do one of the following:

  - Type a **Y**, the agent continues with the registration to the ESM manager.
  - Type an **N**, the setup prompts to re-enter the details of the new manager.

Note: The uninstaller program validates the manager name with the manager name that is present in the manager.dat file. If the manager name does not match, the program reports a message, **Specified manager is not found in manager.dat file. Skipping re-registration for <manager name>**.

11 The **Would you like to add registration information of another manager? [no]** message appears. Do one of the following:

- Type a **Y**, the agent continues with the registration of another manager.
- Type an **N**, the agent is successfully registered to the manager.

Note: If the uninstallation fails, then ESM rolls-back the uninstallation action and brings back the agent to its original state.

About the uninstallation logs

The uninstaller creates a log file for you to know about the changes that the uninstaller program performed. The log file, ESM_Oracle_Uninstall.log is stored in the system folder. The specified folder is located at: `<esm_install_dir>\ESM\system\<Host_Name>.` The uninstaller program automatically creates the log file and captures the uninstallation events and errors in it.

Chapter 3

About the Symantec ESM Modules for Oracle Databases

This chapter includes the following topics:

About the Oracle SID Discovery module

Checks in this module report the following information:

- Detects new Oracle database instances.

- Reports deleted Oracle database instances.
- Provides an option to automatically configure the newly discovered Oracle database instances.
- Provides an option to automatically remove the deleted Oracle database instances that are still configured.

Note: The Oracle SID Discovery is a host-based module.

Configuring the Oracle database instances by using the Discovery module

The ESM Oracle Discovery module is a host-based module that automates the process of detection and configuration of new database instances that are not yet configured on the local ESM agent computers. The ESM Oracle Discovery module also detects the deleted database instances that are still configured on the ESM agent computers. The ESM Oracle Discovery module lets you delete the uninstalled database instances from the ESM agent computers.

Configuring a new Oracle database instance

To report on the Oracle database instance, you should first configure the Oracle database instance on an ESM agent computer.

To configure a new Oracle database instance

1. Run the Discovery module on the ESM agent computers that have Oracle database installed.

   The module lists all the new database instances that were not previously configured.

2. Select multiple database instances and do one of the following:

   - Right-click, select **Correction** option, and enter your system account or pre-created account credentials.
     The **Correction** option configures the database instances with SYSTEM account credentials or pre-created account credentials.
   - Right-click and select **Snapshot Update** option.
     The **Snapshot Update** option configures the database instance with / as SYSDBA method.

Note: The / as SYSDBA method does not work in case of Oracle Real Application Cluster (RAC). You must use the correct option and specify pre-created account credentials.

Editing default settings

Use the checks in this group to edit the default settings for all the security checks in the module.

Temporary Tablespace

You can use this option to enter the temporary tablespace name in the **Temporary Tablespace** text box. If the tablespace that you specify does not exist in the database, then the module uses the default temporary tablespace to create the ESMDBA account.

Default Tablespace

You can use this option to enter the default tablespace name in the **Default Tablespace** text box. The check reports an error message if the tablespace that you specify does not exist in the database. However, the check continues with the configuration of the rest of the SIDs.

Profile

You can use the name list in this check to provide the profile name and the password parameters. If the profile that you specify exists in the database, then the module uses the existing profile. If the profile that you specify does not exist in the database, then the module creates a new profile with the parameters that you specify in the name list.

Following are the default values of the profile name and the password parameters:

- PROFILE=DEFAULT
- FAILED_LOGIN_ATTEMPTS=DEFAULT
- PASSWORD_GRACE_TIME=DEFAULT
- PASSWORD_LIFE_TIME=DEFAULT
- PASSWORD_LOCK_TIME=DEFAULT
- PASSWORD_REUSE_MAX=DEFAULT
- PASSWORD_REUSE_TIME=DEFAULT
- PASSWORD_VERIFY_FUNCTION=DEFAULT

Reporting SID Discovery

The Symantec ESM module for Oracle SID Discovery includes four checks that let you automate the detection and the configuration of the oracle database instances on the host computer.

You can use the Symantec ESM module for Oracle SID Discovery to detect and configure newly detected database instances and the database instances that have been uninstalled.

Detect New Instance

This check reports the instances that are newly discovered on the ESM agent computers and which are not configured in the ESM Oracle configuration file. The corresponding Oracle service of the instances should also be available in running state. Use the name list to include or exclude the Oracle SIDs from the configuration file.

This check lets you use the **Correct** and the **Snapshot Update** options from the console.

With the **Correct** option, you can configure the database instance by using the SYSTEM account or a pre-created account. With the Snapshot Update option, you can configure the database instance by using the /as sysdba method. You can check the EsmOraConfig.log file for details.

The following table lists the messages for the check.

Table 3-1 Messages for Detect New Instance

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_ORACLE_NEW_INSTANCE_DETECTED Category: ESM Administrative Information	■ Windows 2003 (243831) ■ Windows 2008 (256831)	Title: New Instance Description: A new instance has been detected on the local computer. To configure the newly detected instance, either use the Update option to configure using SYSDBA method or use the Correct option to provide the appropriate logon credentials.	Severity: yellow-1 Correctable: true Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]
String ID: ESM_ORACLE_NEW_INSTANCE_ADDED Category: ESM Administrative Information	■ Windows 2003 (243832) ■ Windows 2008 (256832)	Title: Added New Instance Description: A new server instance has been detected. The configuration record for the newly detected instance has been successfully added to the configuration file.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-1 Messages for Detect New Instance *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_ORACLE_ADD_INSTANCE_FAILED Category: ESM Administrative Information	■ Windows 2003 (243833) ■ Windows 2008 (256833)	Title: Failed to Add New Instance Description: The module failed to add a record in the configuration file for the new instance that was detected using the SYSDBA method. Use the Correct option or Update option for configuring the newly detected instance.	Severity: yellow-1 Correctable: true Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Detect Retired Instance

This check reports all the instances that are present in the ESM Oracle configuration file, but the Oracle service is unavailable.

Note: The Check SID process only text box is only applicable for the UNIX platforms.

The following table lists the messages for the check.

Table 3-2 Messages for Detect Retired Instance

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_ORACLE_DEL_INSTANCE_DETECTED Category: ESM Administrative Information	■ Windows 2003 (243834) ■ Windows 2008 (256834)	Title: Retired Instance Description: A retired instance has been detected on the local computer. The configuration file contains the configuration information for the Retired server instance. Use the Update option to delete the configuration information from the ESM Oracle configuration file.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]
String ID: ESM_ORACLE_INSTANCE_DELETED Category: ESM Administrative Information	■ Windows 2003 (243835) ■ Windows 2008 (256835)	Title: Deleted Retired Instance Description: The configuration record for the retired instance has been deleted from the ESM Oracle configuration file.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Automatically Add New Instance

This check automatically configures all the newly detected instances. This check works with the **Detect New Instance** check. You can use this check to automate the module to connect to each newly detected database instance by using the / as sysdba method. In case of a successful connection, the module configures the instance by adding entry in the oracle.dat file.

An error message displays if the module fails to connect to the newly detected database instance by using the / as sysdba method. You can right-click the message and click **Correct** to connect to the newly detected database instance. You have to use the SYSTEM or pre-created account credentials to connect to the newly detected database instance.

Note: This check does not work in case of Oracle Real Application Cluster (RAC). You must use the correct option and specify pre-created account credentials.

Automatically Delete Retired Instance

This check works with the **Detect Retired Instance** check and automatically deletes the corresponding retired server records from the configuration file. You can use this check to automate the module, to detect the uninstalled database instances or to detect the instances that are unavailable, and then to delete the corresponding entries from the oracle.dat file.

About the Oracle Accounts module

This module checks for the user accounts based on the options that you have specified.

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 check to automatically update the snapshots with the 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.

Oracle system identifiers (SIDs)

Use the name list to include or exclude the Oracle system identifiers (SIDs) for this check. By default, the check examines all the SIDs that you specify when you configure the Symantec ESM modules for the Oracle databases. The Symantec ESM modules for Oracle databases configuration are stored in \esm\config\oracle.dat file.

Reporting operating system access

The OS administrators have exceptional privileges. Some users can access the database directly from the operating system without the protection of Oracle authentication. Both the user groups should be monitored to ensure that your computers are protected. The checks in this group monitor these users.

Users to skip in OS DBA groups

Use the name list to exclude the users for the **Users in OSDBA groups** check. By default, all users in each group are included.

Users in OS DBA groups

This check reports the users who can connect to a database as INTERNAL, SYSDBA, or SYSOPER. The check also reports users who connect as members of ORA_DBA and ORA_OPER groups.

Use the name list to exclude the users (usually administrators) and include the OS database administrator groups for this check.

Symantec recommends that you remove the unauthorized users from the OSDBA groups.

The following table lists the message for the check.

Table 3-3 Message for Users in OS DBA groups

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_UNAUTHORIZED_INTERNAL Category: Policy Compliance	- Windows 2003 (242130) - Windows 2008 (255130)	Title: User in OS DBA group Description: The user can connect to the database as INTERNAL, SYSDBA, or SYSOPER, and start your database, shut it down, and perform other system operations. If the user is not an authorized administrator, remove the user from the OS DBA group.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

OS authenticated users

This check reports the users who are authenticated only by the operating system, without Oracle authentication. Use the name list to exclude the users for this check.

In a testing or a development environment, you can log on to Oracle database without providing a user name and password; however, Symantec recommends that you must not follow this method of authentication on a production environment. We also recommend that you change the user's password authentication from external to local and enable the Oracle authentication to add another level of security.

The following table lists the message for the check.

Table 3-4 Message for OS authenticated users

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_USER_AUTHORIZED_EXTERNAL Category: Policy Compliance	■ Windows 2003 (242132) ■ Windows 2008 (255132)	Title: User authenticated by OS only Description: The user is authenticated only by the operating system and can log on to Oracle without providing a user name and password. Require Oracle authentication to add another level of security.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Globally authenticated users

This check reports the users that are authenticated globally by SSL, whose database access is through global roles, authorized by an enterprise directory. Use the **Users to Skip** name list to exclude the users from reporting.

A centralized directory service, which is outside of the database, manages the users without Oracle authentication. You require Oracle user authentication for additional identity verification.

The following table lists the message for the check.

Table 3-5 Message for Globally authenticated users

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_USER_ AUTHORIZED_ GLOBAL Category: Policy Compliance	■ Windows 2003 ■ Windows 2008 (255152)	Title: User authenticated globally Description: The user is authenticated by SSL and the management of this user is done outside of the database by the centralized directory service. The user can log on to Oracle database without providing a user name and password. Users require Oracle authentication to add one more level of security.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Reporting user roles

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

Roles

Use the name list to exclude or include the roles for the **Directly-granted roles**and **Grantable roles** checks to report on.

Grantable roles

This check reports the user names with permissions to grant roles to other users. Use the name list to exclude users for this check.

Symantec recommends that you revoke the grantable roles from any user who is not authorized to grant it. Periodically, you can review all the users with grantable roles to ensure that they are currently authorized to grant their grantable roles.

The following table lists the message for the check.

Table 3-6 Message for Grantable roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_GRANTABLE_ROLE Category: System Information	■ Windows 2003 (242146) ■ Windows 2008 (255146)	Title: Grantable role Description: The user can grant the role. Verify that the user is authorized to grant the role.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Deleted directly granted roles

This check reports the user names with the directly-granted roles that were revoked or dropped after the last snapshot update. The check does not report the roles that are nested within the directly-granted role and are deleted or revoked. Use the name list to exclude the users for this check.

If the deletion is authorized, Symantec recommends that you either update the snapshot or restore the role to the user.

The following table lists the message for the check.

Table 3-7 Message for Deleted directly granted roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_USER_ ROLE_DELETED Category: Change Notification	■ Windows 2003 (242138) ■ Windows 2008 (255138)	Title: Role deleted from user Description: The directly granted user role that is reported in the User Role field was dropped from the database or revoked from the user after the last snapshot update. Roles within the directly granted role were also deleted or revoked. If the deletion or revocation is authorized, update the snapshot. If the deletion or revocation is not authorized, restore the role to the user.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

New directly-granted roles

This check reports the user names with the roles that were directly granted to them after the last snapshot update. The check does not report the roles that are nested in directly-granted roles. Use the name list to exclude users for this check.

If the user is authorized, Symantec recommends that you either update the snapshot or revoke it from the users.

The following table lists the message for the check.

Table 3-8 Message for New directly granted roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_USER_ ROLE_ADDED Category: Change Notification	■ Windows 2003 (242136) ■ Windows 2008 (255136)	Title: New role directly granted to user Description: The user role was directly granted after the last snapshot update. If the user is authorized for the role, update the snapshot. If the user is not authorized for the role, revoke the role.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Directly-granted roles

This check reports the roles that have been directly granted to the users. The roles that were nested in the directly-granted roles are deleted, but are not reported. Use the name list to exclude the users for this check.

Symantec recommends that periodically you review this check to ensure that the users with the directly-granted roles are authorized. Based on the results, you can revoke inappropriately directly-granted roles.

The following table lists the message for the check.

Table 3-9 Message for Directly granted roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PRIVILEGE_ LIST_ROLES Category: System Information	■ Windows 2003 (242133) ■ Windows 2008 (255133)	Title: Role directly granted to user Description: The user has been directly granted the role that is reported in the User Role field. Verify that the role is appropriate for the user's responsibilities.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Reporting user privileges

The checks in this group report the users with grantable privileges and the privileges that have been directly granted to users or revoked from the users.

Privileges

Use the name list to include or exclude the system privileges for the **Grantable**and **Directly-granted privileges** checks to report on.

Grantable privileges

This check reports the users with the privileges that they can directly grant. Use the name list to exclude the users for this check.

Symantec recommends that you revoke the privilege from any user who is not authorized to grant it. Periodically, you must review the grantable privileges to ensure that users are currently authorized to grant their grantable privileges.

The following table lists the message for the check.

Table 3-10 Message for Grantable privileges

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_GRANTABLE_PRIV Category: System Information	■ Windows 2003 (242145) ■ Windows 2008 (255145)	Title: Grantable privilege Description: The user can grant the privilege to others. Verify that the user is authorized to grant this privilege.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Directly-granted privileges

This check reports the users with the system privileges that have been directly granted to them. Use the name list to exclude users for this check. Generally, to reduce maintenance the privileges are often granted in roles.

Symantec recommends that you revoke the privilege from any user who is not authorized for it.

The following table lists the message for the check.

Table 3-11 Message for Directly granted privileges

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PRIVILEGE_LIST_DIRECT Category: System Information	■ Windows 2003 (242134) ■ Windows 2008 (255134)	Title: Privilege directly granted Description: The user has been directly granted the privilege that is reported in the User Privilege field. Verify that the user is authorized for the privilege and consider whether a role should be created or redefined to include the privilege.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New directly-granted privileges

This check reports the users with the privileges that were directly granted to them after the last snapshot update. Use the name list to exclude the users for this check. Generally, to reduce maintenance the privileges are often granted in roles.

If the user is authorized for this privilege, Symantec recommends that you either update the snapshot or revoke the privilege.

The following table lists the message for the check.

Table 3-12 Message for New directly granted privileges

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_USER_PRIV_ADDED Category: Change Notification	■ Windows 2003 (242137) ■ Windows 2008 (255137)	Title: New privilege granted to user Description: The user was directly granted the privilege that is reported in the User Privilege field after the last snapshot update. If the user is authorized for this privilege, update the snapshot. If the user is not authorized for this privilege, revoke the privilege.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted directly-granted privileges

This check reports the users with the directly-granted privileges that were revoked or dropped after the last snapshot update. Use the name list to exclude the users for this check.

If the deletion is authorized, Symantec recommends that you either update the snapshot or restore the privilege.

The following table lists the message for the check.

Table 3-13 Message for Deleted directly granted privileges

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_USER_ PRIV_DELETED Category: Change Notification	■ Windows 2003 (242139) ■ Windows 2008 (255139)	Title: Privilege deleted from user Description: The directly granted privilege that is reported in the User Privilege field was dropped from the database or revoked from the user after the last snapshot update. Privileges within the directly granted privilege were also deleted or revoked. If the deletion is authorized, update the snapshot. If the deletion is not authorized, restore the privilege to the user	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Reporting user accounts

The checks in this group report the database accounts that are current, new, active, inactive, and deleted.

Database accounts

This check reports the user accounts, their tablespaces, and account creation dates. Use the name list to exclude the users for this check.

Symantec recommends that you delete any unauthorized or out-of-date accounts. Periodically, you must review the database accounts to ensure that the database accounts and their tablespaces are currently authorized.

The following table lists the message for the check.

Table 3-14 Message for Database accounts

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_USER_ACCT Category: System Information	■ Windows 2003 (242140) ■ Windows 2008 (255140)	Title: Database account Description: The user account is reported with its tablespace and date that the account was created. Verify that the account is currently authorized. Drop unauthorized or out of date accounts.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New database accounts

This check reports the user accounts that were added to the database after the last snapshot update. Use the name list to exclude the users for this check.

If the new account is authorized, Symantec recommends that you either update the snapshot or delete it.

The following table lists the message for the check.

Table 3-15 Message for New database accounts

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_USER_ ACCT_ADDED Category: Change Notification	■ Windows 2003 (242141) ■ Windows 2008 (255141)	Title: New database account Description: The user account was added to the database after the last snapshot update. If the new account is authorized, update the snapshot. If the new account is not authorized, drop the account.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Active database accounts

This check reports active user accounts with their tablespaces, profile, and account creation date. Periodically, you must review the user accounts to ensure that they are current and authorized.

The following table lists the message for the check.

Table 3-16 Message for Active database accounts

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ACTIVE_USER_ACCT Category: Policy Compliance	■ Windows 2003 (242151) ■ Windows 2008 (255151)	Title: Active database account Description: The active user account is reported with its tablespaces, profile, and date that the account was created. Verify that the account is currently authorized. Drop unauthorized or out of date accounts.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Inactive database accounts

This check reports the inactive user accounts with their inactive status, date, and account creation date. Periodically, you must review the user accounts to ensure that they are current and authorized.

The following table lists the message for the check.

Table 3-17 Message for Inactive database accounts

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_INACTIVE_USER_ACCT Category: Policy Compliance	■ Windows 2003 (242150) ■ Windows 2008 (255150)	Title: Inactive database account Description: The inactive user account is reported with its inactive status and date that the account was created. Verify that the account is currently authorized. Drop unauthorized or out of date accounts.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Deleted database accounts

This check reports the user accounts that were deleted after the last snapshot update. Use the name list to exclude the users for this check.

If the deletion is authorized, Symantec recommends that you either update the snapshot or restore the account.

The following table lists the message for the check.

Table 3-18 Message for Deleted database accounts

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_USER_ ACCT_DELETED Category: Change Notification	■ Windows 2003 (242142) ■ Windows 2008 (255142)	Title: Deleted database account Description: The user account was dropped from the database after the last snapshot update. If the deletion is authorized, update the snapshot. If the deletion is not authorized, restore the account.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Reporting account changes

The checks in this group report the changes to the tablespace assignments and the creation dates.

Database account tablespace changed

This check reports the accounts with the default tablespaces that were changed after the last snapshot update. Use the name list to exclude the users for this check.

If the change is authorized, Symantec recommends that you either update the snapshot or restore the tablespace.

The following table lists the message for the check.

Table 3-19 Message for Database account tablespace changed

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_USER_ ACCT_TABLESPACE Category: Change Notification	■ Windows 2003 (242143) ■ Windows 2008 (255143)	Title: Database account tablespace changed Description: The user's tablespace changed after the last snapshot update. Verify that tablespace resources are adequately and efficiently allocated. If the change is authorized, update the snapshot. If the change is not authorized, restore the tablespace.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Database account creation date changed

This check reports the database accounts with the creation dates that changed after the last snapshot update. The change in the creation date 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 name list to exclude the users for this check.

If the change is authorized, Symantec recommends that you either update the snapshot or drop the account.

The following table lists the message for the check.

Table 3-20 Message for Database account creation date changed

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_USER_ ACCT_CREATION Category: Change Notification	■ Windows 2003 (242144) ■ Windows 2008 (255144)	Title: Database account creation date changed Description: The user's creation date changed after the last snapshot update. Verify that the user has been re-created with authorized roles, and restore necessary data if it was deleted. If the change is authorized, update the snapshot. If the change is not authorized, drop the account.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Reporting account defaults

Password-protected default role

This check reports the users who have been granted the password protected roles as default roles. Verify that the users are authorized to use the roles without entering passwords.

Symantec recommends that for an unauthorized user, you either assign a different default role to the user or remove the password protection from the role.

The following table lists the message for the check.

Table 3-21 Message for Password protected default role

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DEFAULT_ ROLE_WITH_ PASSWORD Category: System Information	■ Windows 2003 (242147) ■ Windows 2008 (255147)	Title: Default role with password protection Description: The user's default role is defined in the database as password protected. Verify that the user is authorized to use the role without entering a password. To require the user to enter a password to use the role, set the role as a non-default role.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Active default accounts

This check reports the default accounts that are present on your computer. By default, the name list includes all the Oracle default accounts.

Symantec recommends that you remove, lock, or disable the account to prevent intruders from using it to access your database.

The following table lists the message for the check.

Table 3-22 Message for Active default accounts

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ACTIVE_ DEFAULT_ACCT Category: Policy Compliance	■ Windows 2003 (242148) ■ Windows 2008 (255148)	Title: Active default account Description: The user account is a default account that ships with an Oracle program. Its password is well known. Remove, lock, or disable the account to prevent intruders from using it to access your database.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Users to check

Use the name list to include or exclude the prohibited roles for the **Granted prohibited roles** check to report on.

Granted prohibited roles

This check reports the users who have been granted prohibited roles. Use the name list to exclude the prohibited roles for this check.

Symantec recommends that you remove any prohibited role.

Note: You must never directly grant a few default Oracle roles, the DBA (database administrator) role, and the connect role to the users.

The following table lists the message for the check.

Table 3-23 Message for Granted prohibited roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ROLE_GRANTED Category: Policy Compliance	■ Windows 2003 (242149) ■ Windows 2008 (255149)	Title: Prohibited role granted Description: There are a few default Oracle roles that should never be directly granted to users, such as dba and connect.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

About the Oracle Auditing module

This module checks for the auditing setup that is based on the options that you have specified.

Establishing a baseline snapshot

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

Automatically update snapshots

Enable this check to automatically update the snapshots with the current information.

Editing default settings

Use this check to edit the default settings of all the security checks in the module.

Oracle system identifiers (SIDs)

Use the name list to include or exclude the Oracle system identifiers (SIDs) for this check. By default, the check examines all the SIDs that you specify when you configure the Symantec ESM modules for the Oracle databases. The Symantec ESM modules for Oracle databases configuration are stored in \esm\config\oracle.dat file.

Reporting audit status and access

The checks in this group 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.

Symantec recommends that while you are in the production environment, to ensure that the audit trail is enabled you must set the AUDIT_TRAIL parameter to DB or OS.

The following table lists the message for the check.

Table 3-24 Message for Audit trail enabled

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_AUDIT_DISABLE Category: Policy Compliance	■ Windows 2003 (243138) ■ Windows 2008 (256138)	Title: Auditing not enabled for the SID Description: An AUDIT_TRAIL setting of NONE indicates auditing is not enabled and audit trails are not being generated. Enable auditing to monitor database activities and ensure corporate security policies are implemented.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Audit trail protection

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

Symantec recommends that you grant access to the audit trail database only to administrators or users with administrator roles. You can drop the role from the user if the user is not authorized to access the audit trail database and at the same time you can drop the privilege of an inappropriately defined role. You must ensure that the auditing options of DEL, INS, and UPD for SYS.AUD$ are set properly to A/A in the dba_obj_audit_opts.

The following table lists the message for the check.

Table 3-25 Message for Audit trail protection

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_AUDIT_ PROTECTION Category: System Information	- Windows 2003 (243139) - Windows 2008 (256139)	Title: Audit trail protection Description: The user has access to the audit trail table. Verify that the user is authorized to change or delete the audit trail table. Verify that this right is appropriate for the user's role and that auditing options DEL, INS, and UPD for SYS.AUD$ are set properly to A/A in dba_obj_audit_opts.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Audit reporting methods

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

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

Table 3-26 lists the reporting methods.

Table 3-26 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

Table 3-26 Reporting methods *(continued)*

Method	Description of report
S/A	Every session in which an operation was successful and every failed operation

Reporting statement audits

The checks in this group report SQL statements that are audited. Security checks report statements that were set or removed for auditing and statements with the success or the 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

Use the name list to include or exclude the object such as tables or views that are to be included for the object auditing.

Statement auditing

This check reports the user SQL statements that are audited and the Success/Failure reporting methods that are used. Use the name list to exclude the users for this check.

Symantec recommends that you remove all unauthorized or out-of-date statements. You must ensure that you use appropriate reporting methods for the available resources and perceived risks.

The following table lists the message for the check.

Table 3-27 Message for Statement auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_STMT_ AUDITING Category: System Information	■ Windows 2003 (243148) ■ Windows 2008 (256148)	Title: Statement auditing Description: The user SQL statement is audited, using the Success/Failure reporting reporting methods that are reported in the Infor field. BY ACCESS reports every instance, and BY SESSION reports every session, in which the statement is executed. Verify that auditing the statement is authorized and the reporting method is appropriate.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New statement auditing

This check reports the SQL statements that were set for auditing after the last snapshot update, and the Success/Failure reporting methods that are used. Use the name list to exclude the users for this check.

Symantec recommends that you remove all unauthorized or out-to-date statements. You must update the snapshot if the auditing of statement is authorized and the reporting method is correct. You must deactivate the audit if the auditing of the statement is not authorized. You must change the reporting methods if the reporting methods are inappropriate for the available resources and perceived risks.

The following table lists the message for the check.

Table 3-28 Message for New statement auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_NEW_STMT_AUDITING Category: Change Notification	■ Windows 2003 (243149) ■ Windows 2008 (256149)	Title: New statement auditing Description: The SID's user statement and its auditing Success/Failure reporting methods are reported in the Info field. BY ACCESS reports every time the statement is executed, and BY SESSION reports every session in which the statement is executed. If auditing the statement is authorized and the reporting methods are appropriate, update the snapshot. If auditing the statement is not authorized, deactivate the auditing. If the reporting methods are not appropriate, correct them.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted statement auditing

This check reports the user statements that were removed from auditing after the last snapshot update. Use the name list to exclude the users for this check.

If the statement deletion is authorized, Symantec recommends that you either update the snapshot or restore the audit settings.

The following table lists the message for the check.

Table 3-29 Message for Deleted statement auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DELETED_ STMT_AUDITING Category: Change Notification	■ Windows 2003 (243150) ■ Windows 2008 (256150)	Title: Deleted statement auditing Description: The user statement was removed from auditing after the last snapshot update. If the deletion is authorized, update the snapshot. If it is not authorized, restore the audit setting.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Changed statement auditing

This check reports the audited user statements with the Success/Failure reporting methods that changed after the last snapshot update. Use the name list to exclude the users for this check.

If the change is authorized, Symantec recommends that you either update the snapshot or restore the previous statement settings.

The following table lists the message for the check.

Table 3-30 Message for Changed statement auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_CHANGED_ STMT_AUDITING Category: Change Notification	■ Windows 2003 (243151) ■ Windows 2008 (256151)	Title: Statement auditing changed Description: The Success/Failure reporting methods of the SID's user statement changed after the last snapshot update. BY ACCESS reports every instance, and BY SESSION reports every session, in which the statement is executed. If auditing the statement is authorized and the reporting methods are appropriate, update the snapshot. If the auditing is not authorized, deactivate the audit. If the reporting methods are not appropriate, correct them.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Reporting object audits

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

There are 16 options for audited objects.

Table 3-31 lists the audits that this check reports on.

Table 3-31 Audited object options

Audit number	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	CRETE
15	REA	READ
16	WRI	WRITE

Note: 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 the sessions that contain one or more failed operations.

Auditing objects

Use the name list to include or exclude the object such as tables or views that are to be included for the object auditing.

Object auditing

This check reports the user objects that are audited and the Success/Failure reporting methods that are used. Use the name list to exclude the users for this check.

Symantec recommends that you remove all unauthorized or out-of-date statements from auditing. Periodically, you must review audited objects to ensure that the audit is currently authorized and the reporting methods are appropriate for the available resources and perceived risks.

The following table lists the message for the check.

Table 3-32 Message for Object auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_OBJ_AUDITING Category: System Information	■ Windows 2003 (243144) ■ Windows 2008 (256144)	Title: Object auditing Description: The user object is audited. For Oracle8 and later, sixteen object options are represented in the order ALT, AUD, COM, DEL, GRA, IND, INS, LOC, REN, SEL, UPD, REF, EXE, CRE, REA, WRI. Oracle7 uses only the first thirteen options. Unavailable and unaudited options appear as -/-. Success/Failure reporting methods are an A (BY ACCESS) or an S (BY SESSION) on each side of the slash. 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 operation. Verify that the user object should be audited and that the reporting method is appropriate.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New object auditing

This check reports the user objects that were set for auditing after the last snapshot update, and the Success/Failure reporting methods that are used. Use the name list to exclude the users for this check.

If the auditing of the object is authorized, Symantec recommends that you either update the snapshot or remove the object from auditing. If the reporting methods are incorrect then you must correct them.

The following table lists the message for the check.

Table 3-33 Message for New object auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_NEW_OBJ_ AUDITING Category: Change Notification	■ Windows 2003 (243145) ■ Windows 2008 (256145)		Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Table 3-33 Message for New object auditing *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
		Title: New object auditing Description: The user object was set for auditing after the last snapshot update. For Oracle8 and later, sixteen object options are represented in the order ALT, AUD, COM, DEL, GRA, IND, INS, LOC, REN, SEL, UPD, REF, EXE, CRE, REA, WRI. Oracle7 uses only the first thirteen options. Unavailable and unaudited options appear as -/-. Success/Failure reporting methods are an A (BY ACCESS) or an S (BY SESSION) on each side of the slash. 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 operation. If auditing of the object is authorized, update	

Table 3-33 Message for New object auditing *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
		the snapshot. If it is not authorized, rop the object from auditing.	

Deleted object auditing

This check reports the user objects and the object options that were removed from auditing after the last snapshot update. Use the name list to exclude the users for this check.

If the deletion is authorized, Symantec recommends that you either update the snapshot or restore audit of the object.

The following table lists the message for the check.

Table 3-34 Message for Deleted object auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DELETED_OBJ_AUDITING Category: Change Notification	■ Windows 2003 (243146) ■ Windows 2008 (256146)	Title: Deleted object auditing Description: Auditing of the user object was dropped after the last snapshot update. If the change is authorized, update the snapshot. If the change is not authorized, restore the auditing of the object.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Changed object auditing

This check reports the audited user objects with the Success/Failure reporting methods that changed after the last snapshot update and their current reporting methods.

If the change is authorized, Symantec recommends that you either update the snapshot or restore the previous settings.

The following table lists the message for the check.

Table 3-35 Message for Changed object auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_CHANGED_ OBJ_AUDITING Category: Change Notification	■ Windows 2003 (243147) ■ Windows 2008 (256147)		Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Table 3-35 Message for Changed object auditing *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
		Title: Object auditing changed Description: Success/Failure reporting methods of the named object option were changed since the last snapshot update. For Oracle8 and later, sixteen object options are represented in the order ALT, AUD, COM, DEL, GRA, IND, INS, LOC, REN, SEL, UPD, REF, EXE, CRE, REA, WRI. Oracle7 uses only the first thirteen options. Unavailable and unaudited options appear as -/-. Success/Failure reporting methods are an A (BY ACCESS) or an S (BY SESSION) on each side of the slash. 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	

Table 3-35 Message for Changed object auditing *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
		operation. If the change is authorized, update the snapshot. If the change is not authorized, restore the previous methods.	

Reporting privilege audits

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

Auditing privileges

Use the name list to include or exclude the privileges for the privilege auditing checks.

Privilege auditing

This check reports the user privileges that are audited, and the Success/Failure reporting methods that are used. Use the name list to exclude the users for this check.

Symantec recommends that you periodically review the privilege auditing to ensure that the audits are currently authorized and that the reporting methods are appropriate for available resources and perceived risks.

The following table lists the message for the check.

Table 3-36 Message for Privilege auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PRIV_AUDITING Category: System Information	■ Windows 2003 (243140) ■ Windows 2008 (256140)	Title: Privilege auditing Description: The user privilege is audited and the specified Success/Failure reporting methods are used. Verify that this user privilege should be audited and that the reporting method is appropriate.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New privilege auditing

This check reports the user privileges that were set for auditing after the last snapshot update and the Success/Failure reporting methods that are used. Use the name list to exclude the users for this check.

If the new privilege and its reporting methods are authorized, Symantec recommends that you update the snapshot. If the new privilege is not authorized then you must change the privileges. If the user is unauthorized for the privilege then you must remove the privilege from the user.

The following table lists the message for the check.

Table 3-37 Message for New privilege auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_NEW_PRIV_ AUDITING Category: Change Notification	■ Windows 2003 (243141) ■ Windows 2008 (256141)	Title: New privilege auditing Description: The user privilege was set for auditing with the specified Success/Failure reporting methods since the last snapshot update. If auditing the privilege is authorized, update the snapshot. Remove the privilege from auditing if it is not authorized.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted privilege auditing

This check reports the user privileges that were removed from auditing after the last snapshot update. Use the name list to exclude the users for this check.

If the deletion is authorized, Symantec recommends that you either update the snapshot or restore the user privilege to auditing.

Table 3-38 Message for Deleted privilege auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DELETED_ PRIV_AUDITING Category: Change Notification	■ Windows 2003 (243142) ■ Windows 2008 (256142)	Title: Deleted privilege auditing Description: The user privilege was removed from auditing after the last snapshot update. If the deletion is authorized, update the snapshot. If the deletion is not authorized, restore the user privilege to auditing.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Changed privilege auditing

This check reports the audited user privileges with Success/Failure reporting methods that changed after the last snapshot update. Use the name list to exclude the users for this check.

If the change is authorized, Symantec recommends that you either update the snapshot or restore the previous audit settings.

The following table lists the message for the check.

Table 3-39 Message for Changed privilege auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_CHANGED_ PRIV_AUDITING Category: Change Notification	■ Windows 2003 (243143) ■ Windows 2008 (256143)	Title: Privilege auditing changed Description: The Success/Failure Update reporting methods of the audited privilege changed after the last snapshot update. The current method is displayed. If the change is authorized, update the snapshot. If the change is not authorized, restore the the previous reporting methods.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Audit settings

This check reports the audit settings that do not match the settings that are specified in the template file. Use the name list to enable or disable the template files.

The following table lists the message for the check.

Table 3-40 Message for Template - Oracle Auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_AUDIT_R Category: Policy Compliance	■ Windows 2003 (243152) ■ Windows 2008 (256152)	Title: Audit settings mismatch Description: The audit settings that are present in the database do not match with the settings that are specified in the template file. For more information, refer the corresponding Information column.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_AUDIT_Y Category: Policy Compliance	■ Windows 2003 (243153) ■ Windows 2008 (256153)	Title: Audit settings mismatch Description: The audit settings that are present in the database do not match with the settings that are specified in the template file. For more information, refer the corresponding Information column.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-40 Message for Template - Oracle Auditing *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_AUDIT_G Category: Policy Compliance	■ Windows 2003 (243154) ■ Windows 2008 (256154)	Title: Audit settings mismatch Description: The audit settings that are present in the database do not match with the settings that are specified in the template file. For more information, refer the corresponding Information column.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

About the Oracle Auditing template

In the Oracle Auditing module, the Audit Setting check uses the Oracle Auditing template. The check reports the audit settings that do not match the settings that are specified in the template file.

The default templates are available for each supported operating system.

Creating the Oracle Auditing template

You must create and enable a new Oracle Audting template before you run the **Audit setting** check.

To create a Oracle Auditing template

1. In the tree view, right-click **Templates**, and then click **New**.
2. In the **Create New Template** dialog box, select **Oracle Auditing- all**.
3. In the **Template file name (no extension)** text box, type new template file name. Symantec ESM adds the .oad extension to the template file name.
4. Click **OK**.

About using the Oracle Auditing template

The Oracle Audting template contains the following fields:

Table 3-41 Field and Values/Options descriptions

Field	Description	Values/Options
Audit Type	Lets you specify an audit that is based on either a statement or a privilege.	■ PRIV (Privilege Auditing) Select this option if you want the check to report on the privileges. ■ STMT (Statement auditing) Select this option if you want the check to report on the statements.
Audit Option	Lets you specify the audit option for the audit type that you specify. For example: PRIV	Enter the name of the audit option. For example: CREATE SESSION
User	Lets you specify the user who executes the statement or the privilege.	Enter the name of the user. You can use the keyword, ‘ANY’ while specifying the user name.
Success	Lets you specify a state for the audit that you specify.	■ BY ACCESS This option is based on per access auditing. ■ BY SESSION This option is based on per session auditing. ■ NOT SET This session is not set for auditing. ■ IS SET This option is either set for session or access auditing.

Table 3-41 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
Failure	Lets you specify a state for the audit that you specify.	■ BY ACCESS This option is based on per access auditing. ■ BY SESSION This option is based on per session auditing. ■ NOT SET This session is not set for auditing. ■ IS SET This option is either set for session or access auditing.
Severity	Lets you specify the severity level for the audit type that you select.	■ Green Select Green for an Information message. ■ Yellow Select Yellow for a Warning message. ■ Red Select Red for an Error message.

About the Oracle Configuration module

This module checks for the Oracle settings that can affect the security of the system.

Editing default settings

Use the checks in this group to edit the settings of all the security checks.

Automatically update snapshots

Enable this check to automatically update the snapshots with the current information.

Oracle system identifiers (SIDs)

Use the name list to include or exclude the Oracle system identifiers (SIDs) for this check. By default, the check examines all the SIDs that you specify when you configure the Symantec ESM modules for the Oracle databases. The Symantec ESM modules for Oracle databases configuration are stored in \esm\config\oracle.dat file.

Reporting Oracle version information

The checks in this group report Oracle version, status, trace, and alert log file information.

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 the status of the installed Oracle components on the agent.

The following table lists the message for the check.

Table 3-42 Message for Oracle server

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_SERVER_VERSION Category: System Information	■ Windows 2003 (242630) ■ Windows 2008 (255630)	Title: Oracle server version Description: The version and status of the Oracle server are reported.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Oracle components

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

The following table lists the message for the check.

Table 3-43 Message for Oracle components

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PRODUCT_COMPONENT_VERSION Category: System Information	■ Windows 2003 (242631) ■ Windows 2008 (255631)	Title: Oracle product component version Description: The version and status of the Oracle component are reported in the Info field.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Trace files

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

The following table lists the message for the check.

Table 3-44 Message for Trace files

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_TRACE_FILE_DEST Category: System Information	■ Windows 2003 (242632) ■ Windows 2008 (255632)	Title: Location of trace files Description: The location of SID trace files is reported in the Info field.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Trace file size

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

The following table lists the message for the check.

Table 3-45 Message for Trace file size

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_MAX_DUMP_FILE_SIZE Category: System Information	■ Windows 2003 (242634) ■ Windows 2008 (255634)	Title: Maximum size for trace files Description: The maximum size of SID trace files is reported in the Info field.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

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.

The following table lists the message for the check.

Table 3-46 Message for Alert file

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ALERT_ FILE_DEST Category: System Information	■ Windows 2003 (242633) ■ Windows 2008 (255633)	Title: Directory path for alert files Description: The location of SID trace files that are used for Oracle background processes is reported in the Info field. BACKGROUND_DUMP_DEST specifies the location.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

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.

The following table lists the message for the check.

Table 3-47 Message for List SID:HOME (oracle.dat)

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_SID_HOME_DATFILE Category: System Information	- Windows 2003 (242656) - Windows 2008 (255656)	Title: Oracle.dat file information Description: The oracle.dat file is created while configuring ESM modules for oracle.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

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.

The following table lists the message for the check.

Reporting link password encryption

The checks in this group report whether encryption is required for the database link passwords.

DB link encrypted password

This check examines the DBLINK_ENCRYPT_LOGIN setting to report whether the encrypted passwords require connecting to other Oracle servers through the database links. This parameter is no longer supported on Oracle 10g and later versions.

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.

The following table lists the message for the check.

Table 3-48 Message for DB link encrypted password

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DBLINK_ ENCRYPT Category: System Information	■ Windows 2003 (242635) ■ Windows 2008 (255635)	Title: Connect to database with encrypted password Description: The SID's encrypted password setting is reported in the Info field. The first attempt to connect to another Oracle server always sends encrypted passwords. If the reported setting is TRUE, a failed connection is not be retried. If FALSE, Oracle re-tries the connection with an unencrypted version of the password. TRUE settings provide the best protection for your database.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Reporting operating system account prefixes

The checks in this group 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. OS_AUTHENT_PREFIX specifies the characters. The default OPS$ prefix gives you access to a database from the operating system by typing a slash (/) instead of the username/password string.

The following table lists the message for the check.

Table 3-49 Message for Prefix for OS account

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_OS_AUTHENT_PREFIX Category: System Information	■ Windows 2003 (242636) ■ Windows 2008 (255636)	Title: Prefix for OS account Description: The default OPS$ prefix gives a user access to a database from the operating system by typing a slash (/) instead of the username/password string.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table-level SELECT privileges

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

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

The following table lists the message for the check.

Table 3-50 Message for Table-level SELECT privileges

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_SQL92_SECURITY Category: System Information	■ Windows 2003 (242637) ■ Windows 2008 (255637)	Title: Table-level SELECT privileges Description: 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.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Restrictions on system privileges

This check reports whether access to objects in the SYS schema is allowed while you migrate from Oracle 7 to Oracle 8.

You must set the parameter to FALSE. If you set the parameter to TRUE, then access to objects in the SYS schema is allowed. You can specify the settings by using the 07_DICTIONARY_ACCESSIBILITY parameter.

The following table lists the messages for the check.

Table 3-51 Messages for Restrictions on system privileges

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_O7_DICTIONARY_ACCESSIBILITY Category: System Information	■ Windows 2003 (242638) ■ Windows 2008 (255638)	Title: Restrictions on system privileges Description: 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 SYS schema. If TRUE, access to objects in the SYS schema is allowed (Oracle7 behavior). O7_DICTIONARY_ACCESSIBILITY specifies the setting.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_REMOTE_LOGIN_PASSWORDFILE Category: System Information	■ Windows 2003 (242639) ■ Windows 2008 (255639)	Title: Remote login password file Description: The value of the REMOTE_LOGIN_PASSWORDFILE parameter is not acceptable.	Severity: yellow-3 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Reporting parameter values

The checks in this group report the Oracle configuration parameter values.

Remote login password file

This check reports whether the value of the REMOTE_LOGIN_PASSWORDFILE parameter matches with the value that you specify in the Parameter Value text box. Use the name list to include or exclude the values for this check. The default value is None.

Symantec recommends that you change the value of the REMOTE_LOGIN_PASSWORDFILE parameter to match with your security policy.

The following table lists the message for the check.

Table 3-52 Message for Remote login password file

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_REMOTE_LOGIN_PASSWORDFILE Category: System Information	■ Windows 2003 (242639) ■ Windows 2008 (255639)	Title: Remote login password file Description: The value of the REMOTE_LOGIN_PASSWORDFILE parameter is not acceptable.	Severity: yellow-3 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

UTL_FILE accessible directories

This check reports whether the value of the UTL_FILE_DIR parameter matches with the value that you specify in the Parameter Value text box. You can use the UTL_FILE_DIR parameter 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.

If the location of the UTL_FILE_DIR is not authorized, Symantec recommends that you change the configuration of the SID's UTL_FILE_DIR parameter to specify an authorized location; also update the snapshot.

The following table lists the message for the check.

Table 3-53 Message for UTL_FILE accessible directories

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_UTL_FILE_DIR Category: System Information	■ Windows 2003 (242640) ■ Windows 2008 (255640)	Title: UTL_FILE accessible directories Description: The value of the UTL_FILE_DIR parameter is not acceptable.	Severity: yellow-3 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Oracle configuration watch

This check reports the unmatched initialization and configuration parameters that are defined in the templates. Use the name list to include the template file for this check.

The following table lists the messages for the check.

Table 3-54 Messages for Oracle configuration watch

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ORC_RUNTIME_RED Category: Policy Compliance	■ Windows 2003 (242641) ■ Windows 2008 (255641)	Title: Red level condition Description: The value of the SID's parameter at runtime, which is reported in the Info field, violates the conditions of the corresponding parameter in the Oracle Configuration Watch template at the Red severity level. See the Info field for details.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-54 Messages for Oracle configuration watch *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ORC_RUNTIME_YELLOW Category: Policy Compliance	■ Windows 2003 (242642) ■ Windows 2008 (255642)	Title: Yellow level condition Description: The value of the SID's parameter at runtime, which is reported in the Info field, violates the conditions of the corresponding parameter in the Oracle Configuration Watch template at the Yellow severity level. See the Info field for details.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_ORC_RUNTIME_GREEN Category: Policy Compliance	■ Windows 2003 (242643) ■ Windows 2008 (255643)	Title: Green level condition Description: The value of the SID's parameter at runtime, which is reported in the Info field, violates the conditions of the corresponding parameter in the Oracle Configuration Watch template at the Green severity level. See the Info field for details.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-54 Messages for Oracle configuration watch *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ORC_INITFILE_RED Category: Policy Compliance	■ Windows 2003 (242644) ■ Windows 2008 (255644)	Title: Red level condition Description: The value of the parameter that is defined for the SID in the initialization file violates the conditions of the corresponding parameter in the Oracle Configuration Watch template at the red severity level. See the Info field for details.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_ORC_INITFILE_YELLOW Category: Policy Compliance	■ Windows 2003 (242645) ■ Windows 2008 (255645)	Title: Yellow level condition Description: The value of the parameter that is defined for the SID in the initialization file violates the conditions of the corresponding parameter in the Oracle Configuration Watch template at the yellow severity level. See the Info field for details.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-54 Messages for Oracle configuration watch *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ORC_INITFILE_GREEN Category: Policy Compliance	■ Windows 2003 (242646) ■ Windows 2008 (255646)	Title: Green level condition Description: The value of the parameter that is defined for the SID in the initialization file violates the conditions of the corresponding parameter in the Oracle Configuration Watch template at the green severity level. See the Info field for details.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_ORC_PARAMETER_NOT_FOUND Category: System Error	■ Windows 2003 (242647) ■ Windows 2008 (255647)	Title: Required Oracle parameter not found Description: Either the init script is missing an Oracle parameter that the template specifies as required, or an Oracle runtime prarameter that is specified in the template was not set in the running instance of Oracle.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-54 Messages for Oracle configuration watch *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_CONFIG_PARA_VALUE Category: System Information	■ Windows 2003 (242658) ■ Windows 2008 (255658)	Title: Oracle configuration parameter Description: The Oracle configuration parameter value.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

About the Oracle Configuration Watch template

The **Oracle configuration watch** check of the Oracle configuration module uses the Oracle Configuration Watch template. By using this template, the check lets you enable or disable the templates that specify initialization and the configuration parameters that should be watched.

Creating the Oracle Configuration Watch template

You must create and enable a new Oracle Configuration Watch template before you run the **Oracle configuration watch** check.

To create an Oracle Configuration Watch template

1. In the tree view, right-click **Templates**, and then click **New**.
2. In the **Create New Template** dialog box, select **Oracle Configuration Watch - all**.
3. In the **Template file name (no extension)** text box, type new template file name.
4. After Symantec ESM adds the .ocw extension to the template file name, click **OK**.

About using the Oracle Configuration Watch template

The Oracle Configuration Watch template contains the following fields:

Table 3-55 Field and Values/Options descriptions

Field	Description	Values/Options
Description	Lets you specify a description for the parameter that you enter in the **Parameter** field.	NA
Parameter	Lets you specify the parameter.	Enter the configuration or initialization parameter of Oracle that you want the check to report on.
Runtime Value	Lets you select this check box if you want this check to examine the runtime values.	Select the check box to examine the runtime values.
Init File Value	Lets you specify an optional value.	■ Optional Reports the 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.

Table 3-55 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
Parameter Values	Lets you specify a value for the parameter by using the **Template Sublist Editor**.	- Prohibited Value Select the check box to designate the value as prohibited. - Value Enter a regular expression or as a numeric comparison. - You can use the following special cases: + - 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 **Note:** If you specify a path name in the value, you need to escape the ‘\’ character by using another ‘\’. **Note:** For example, specify the path name `c:\test\test.txt` as follows: `c:\\test\\test.txt`.

Table 3-55 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
Severity	Specify the severity for the messages that ESM reports when the parameter value is violated.	■ Green Select Green for an Information message. ■ Yellow Select Yellow for a Warning message. ■ Red Select Red for an Error message.
Oracle Version	Lets you specify the Oracle version of the target server that you want the check to report on.	■ empty All releases (default if no release specified) ■ 9.0 Release 9.0.x ■ +9 Release 9.2.x and later ■ +10 Release 10.2.x and later ■ +11 Release 11.1.x and later
Display configuration value	Lets you select this check box if you want this check to display the configuration value.	Select the check box to display the configuration value.

Redo log files

This check reports the locations of the SID's redo log files, the violations of redo log file permissions, the discrepancies in the redo log file ownerships, and the file status. In the Permission field, do one of the following:

- Specify 0 for the check to report the location and the status of the SID redo log file.
- Specify a permission value more restrictive than the SID's redo log file permission for the check to report an error.

The check reports an error message, if the SID redo log file ownership (UID/GID) does not match with the ownership that you specify in the Oracle database. You can specify the permission values as three-digit octal numbers.

Use the name list to include or exclude the status of the files for this check. The possible file status values are INVALID, STALE, DELETED, and INUSED.

Symantec recommends that you periodically review the redo log file location to ensure that they are in a secure, authorized locations. If the file's permissions are excessive then reset the redo log files permission to match with your security policy. If the owner of the redo log file is not authorized for the file then you must immediately take ownership of the file and review it for possible tampering.

The following table lists the messages for the check.

Redo log file

This check reports the locations of the SID's redo log files and permissions on the log files in the Information field. Use the name list to include or exclude the file statuses for this check. The file status values are INVALID, STALE, DELETED, INUSED. In the Permission field, do one of the following:

- Specify 0 for the check to report the location and the status of the SID redo log file.
- Specify a permission value more restrictive than the SID's redo log file permission for the check to report an error.

Symantec recommends that you 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.

The following table lists the messages for the check.

Table 3-56 Messages for Redo log files

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_REDOLOGFILE Category: System Information	■ Windows 2003 (242648) ■ Windows 2008 (255648)	Title: Redo log file Description: The SID's redo log files reside in the location that is reported in the Redo Log File field.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-56 Messages for Redo log files *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_REDOLOGFILE_PERM Category: Policy Compliance	■ Windows 2003 (242651) ■ Windows 2008 (255651)	Title: Redo log file permission Description: Permission of redo log files	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_FILE_LOCKED Category: System Error	■ Windows (30008)	Title:Locked Oracle file File permissions cannot be reported because the file is being used by another process.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [""]
String ID: ORA_FILE_NOT_FOUND Category: System Error	■ Windows (30009)	Title: Oracle File or folder not found Description: File permissions cannot be reported because the file being referenced cannot be found.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [""]

Table 3-56 Messages for Redo log files *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DIRECTORY_PERMS Category: System Error	■ Windows (30010)	Title: Oracle Folder permissions Description: Reports Directory permissions.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_NOT_SUPPORTED Category: System Information	■ Windows (30011)	Title: Functionality not Supported Description: This functionality is not supported by ESM oracle app module.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_ASM_REDOLOGFILE Category: System Information	■ Windows (60)	Title: Redo log file Description: The SID's ASM managed redo log files reside in the location that is reported in the Redo Log File field.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

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. Use the name list to exclude the redo log file status reporting for this check.

If the addition is authorized, Symantec recommends that you either update the snapshot or delete the new redo log file.

The following table lists the message for the check.

Table 3-57 Message for New redo log files

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ADDED_ REDOLOGFILE Category: Change Notification	■ Windows 2003 (242649) ■ Windows 2008 (255649)	Title: New redo log file Description: The SID's new redo log file was added to the location that is reported in the Redo Log File field after the last snapshot update. If the addition is authorized, update the snapshot. If the addition is not authorized, delete the new redo log file.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted redo log files

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

If the deletion is authorized, Symantec recommends that you either update the snapshot or restore the file.

The following table lists the message for the check.

Table 3-58 Message for Deleted redo log files

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DELETED_ REDOLOGFILE Category: Change Notification	■ Windows 2003 (242650) ■ Windows 2008 (255650)	Title: Deleted redo log file Description: The SID's redo log file that is reported in the Redo Log File field was deleted after the last snapshot update. If the deletion is authorized, update the snapshot. If the deletion is not authorized, restore the file.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Control files

This check reports the locations of the SID's control files, violations of control file permissions, discrepancies in control file ownership, and file status. In the Permission text box, do one of the following:

- Specify 0 for the check to report the location and status of the SID's control files.
- Specify a permission value more restrictive than the SID's control file permission for the check to report a violation.
  You can specify the Permission values as three-digit octal numbers.

Symantec recommends that you periodically review the locations of the control file to ensure that they are in secure, authorized locations. If the file’s permissions are excessive then reset the control file’s permission to match with your security policy.

The following table lists the messages for the check.

New control files

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

If the addition is authorized, Symantec recommends you to either update the snapshot or delete the new control file.

The following table lists the message for the check.

Table 3-59 Message for New control files

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ADDED_ CONTROLFILE Category: Change Notification	■ Windows 2003 (242653) ■ Windows 2008 (255653)	Title: New control file Description: The control file that is reported in the Info field was added to the SID after the last snapshot update. If the addition is authorized, update the snapshot. If the addition is not authorized, delete the new control file.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted control files

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

If the deletion is authorized, Symantec recommends you to either update the snapshot or restore the control file.

The following table lists the message for the check.

Table 3-60 Message for Deleted control files

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DELETED_ CONTROLFILE Category: Change Notification	■ Windows 2003 (242654) ■ Windows 2008 (255654)	Title: Deleted control file Description: The control file that is reported in the Info field was deleted after the last snapshot update. If the deletion is authorized, update the snapshot. If the deletion is not authorized, restore the control file.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

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.

The following table lists the message for the check.

Table 3-61 Message for List SID:HOME (oracle.dat)

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_SID_HOME_ DATFILE Category: System Information	■ Windows 2003 (242656) ■ Windows 2008 (255656)	Title: Oracle.dat file information Description: The oracle.dat file is created while configuring ESM modules for oracle.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

About the Oracle Networks module

This module checks for the oracle network configuration that you have specified.

Editing default settings

Use the name list to edit the default settings for all security checks in the module.

Oracle system identifiers (SIDS)

Use the name list to include or exclude the Oracle system identifiers (SIDs) for this check. By default, the check examines all the SIDs that you specify when you configure the Symantec ESM modules for the Oracle databases. The Symantec ESM modules for Oracle Databases configuration are stored in the \esm\config\oracle.dat file.

Reporting SID configuration status

The check in this group report the SIDs that are not configured.

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. Use name list to exclude the SID’s for this check.

The following table lists the message for the check.

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. Use the name list to enable and disable the template files for this check.

The following table lists the messages for the check.

Table 3-62 Messages for Oracle net configuration watch

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ORC_NETCONFIG_RED Category: Policy Compliance	■ Windows 2003 (243731) ■ Windows 2008 (256731)	Title: Red level condition Description: The parameter value found in the configuration file violates the conditions of the corresponding parameter in the Oracle Net Watch template. See the Info field for details.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_ORC_NETCONFIG_YELLOW Category: Policy Compliance	■ Windows 2003 (243732) ■ Windows 2008 (256732)	Title: Yellow level condition Description: The parameter value found in the configuration file violates the conditions of the corresponding parameter in the Oracle Net Watch template. See the Info field for details.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-62 Messages for Oracle net configuration watch *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ORC_NETCONFIG_GREEN Category: Policy Compliance	■ Windows 2003 (243733) ■ Windows 2008 (256733)	Title: Green level condition Description: The parameter value found in the configuration file violates the conditions of the corresponding parameter in the Oracle Net Watch template. See the Info field for details.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_ORC_NETCONFIG_PARA_MISSING Category: Policy Compliance	■ Windows 2003 (243734) ■ Windows 2008 (256734)	Title: Required parameter not found Description: The required net configuration parameter that is specified in the Oracle Configuration Watch template is not found for the SID. See the Info field for details.	Severity: yellow-3 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

About the Oracle Net Configuration Watch template

The **Oracle net configuration watch** check of the Oracle networks module uses the Oracle Net Configuration Watch template. By using this template, the check reports on the Oracle Listener, Sqlnet, and Names configuration parameter values that violate conditions of the corresponding template parameters.

Creating the Oracle Net Configuration Watch template

You must create and enable a new Oracle Net Configuration Watch template before you run the **Oracle net configuration watch** check.

To create an Oracle Net Configuration Watch template

1. In the tree view, right-click **Templates**, and then click **New**.
2. In the **Create New Template** dialog box, select **Oracle Net Watch - all**.
3. In the **Template file name (no extension)** text box, type new template file name.
4. After Symantec ESM adds the .onw extension to the template file name, click **OK**.

About using the Oracle Net Configuration Watch template

The Oracle Net Configuration Watch template contains the following fields:

Table 3-63 Field and Values/Options descriptions

Field	Description	Values/Options
Description	Lets you specify a description for the parameter that you enter in the **Parameter** field.	NA
Parameter	Lets you specify a parameter name.	Enter a name of the parameter that you want the check to report on.

Table 3-63 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
Parameter Type	Lets you select a parameter type.	■ Listener Control Parameter Lets the Symantec ESM compare the values in the Oracle Net Watch template with the parameter values in the `listener.ora` file. ■ Sqlnet Profile Parameter Lets the Symantec ESM compare the values in the Oracle Net Watch template with the parameter values in the `sqlnet.ora` file. ■ Oracle Names Parameter Lets the Symantec ESM compare the values in the Oracle Net Watch template with the parameter values in the `names.ora` file.
Required Parameter	Lets you select this check box if you want this parameter as required.	Select the check box for the check to report on this parameter. **Note:** Symantec ESM reports if this parameter is not found and if the parameter is found but fails the comparison with template values. If you do not select this check box, then Symantec ESM reports only if this parameter is found and fails the template comparison.

Table 3-63 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
Parameter Values	Lets you specify a value for the parameter by using the **Template Sublist Editor**.	

Table 3-63 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
		■ Prohibited Value Select the check box to designate the value as prohibited. ■ Value Enter a regular expression or as a numeric comparison. ■ You can use the following special cases: + '+' 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 **Note:** If you specify a path name in the value, you need to escape the '\' character by using another '\'. **Note:** For example, specify the path name `c:\test\test.txt` as follows:

Table 3-63 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
		`c:\\test\\test.txt.`
Severity	Specify the severity for the messages that ESM reports when the parameter value is violated.	■ Green Select Green for an Information message. ■ Yellow Select Yellow for a Warning message. ■ Red Select Red for an Error message.
Oracle Version	Lets you specify the Oracle version of the target server that you want the check to report on.	■ 9.0 Release 9.0.x ■ +9 Release 9.2.x and later ■ +10 Release 10.2.x and later ■ +11 Release 11.1.x and later

See "Examples of using the Oracle Net Configuration Watch template" on page 129.

Examples of using the Oracle Net Configuration Watch template

This section contains examples on the values that you must enter in the template field for the check to report on.

Table 3-64 contains the template field and its respective values that you must enter if you want to check on the valid configuration parameters.

Table 3-64 Examples of Listener Control Parameter

Parameter type	Oracle file	Value
Listener Control Parameter	listener.ora	■ ADMIN_RESTRICTIONS ■ LOG_FILE ■ PASSWORDS ■ SAVE_CONFIG_ON_STOP ■ STARTUP_WAIT_TIME ■ TRACE_DIRECTORY, TRACE_FILE ■ ADMIN_RESTRICTIONS_LISTENER ■ INBOUND_CONNECT_TIMEOUT_LISTENER ■ LOGGING_LISTENER ■ LOG_DIRECTORY ■ LOG_FILE_LISTENER ■ PASSWORDS_LISTENER ■ SAVE_CONFIG_ON_STO_LISTENERP ■ SSL_CLIENT_AUTHENTICATION_LISTENER ■ STARTUP_WAIT_TIME_LISTENER ■ TRACE_DIRECTORY_LISTENER ■ TRACE_FILE_LISTENER ■ TRACE_FILELEN_LISTENER ■ TRACE_FILENO_LISTENER ■ TRACE_LEVEL_LISTENER ■ TRACE_TIMESTAMP_LISTENER ■ USE_CKPFILE ■ LOCAL_OS_AUTHENTICATION ■ SUBSCRIBE_FOR_NODE_DOWN_EVENT

Table 3-65 contains the template field and its respective values that you must enter if you want to check on the valid configuration parameters.

Table 3-65 Examples of Sqlnet Profile Parameter

Parameter type	Oracle file	Value
Sqlnet Profile Parameter	sqlnet.ora	■ BEQUEATH_DETACH ■ DAEMON.TRACE_DIRECTORY ■ DISABLE_OOB ■ LOG_DIRECTORY_CLIENT ■ LOG_DIRECTORY_SERVER ■ NAMES.CONNECT_TIMEOUT

Table 3-66 contains the template field and its respective values that you must enter if you want to check on the valid configuration parameters.

Table 3-66 Examples of Oracle Names Parameter

Parameter type	Oracle file	Value
Oracle Names Parameter	names.ora	■ NAMES.ADDRESSES ■ NAMES.ADMIN_REGION ■ NAMES.AUTHORITY_REQUIRED ■ NAMES.CONFIG_CHECKPOINT_FILE ■ NAMES.DOMAIN_HINTS ■ NAMES.LOG_FILE

Oracle EXTPROC listeners

This check reports the Oracle listeners that have EXTPROC-specific entries. In the text box, specify 1 to allow the TCP Protocol, on doing so the database listener ports should be different than the EXTPROC ports. Separate listeners must be specified for the Oracle Databases and for the EXTPROC process. You must use the IPC protocol for listeners configured for EXTPROC.

The following table lists the messages for the check.

Table 3-67 Messages for Oracle EXTPROC listeners

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_EXTPROC_LISTENER_FOUND Category: Policy Compliance	■ Windows 2003 () ■ Windows 2008 (256735)	Title: Listener for EXTPROC found Description: This listener has been configured for PL/SQL EXTPROC. If the PL/SQL EXTPROC functionality is not required, we recommend that you remove this functionality from the ESM agent that hosts the Oracle Database server.	Severity: yellow-3 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_EXTPROC_IN_DB_LISTENER Category: Policy Compliance	■ Windows 2003 () ■ Windows 2008 (256736)	Title: EXTPROC entries found in Listener for Databases Description: The EXTPROC-specific entries were found in the Oracle listener for the Database. Different listeners should be specified for the Oracle Databases and for the PL/SQL EXTPROC.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-67 Messages for Oracle EXTPROC listeners *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_NON_IPC_ EXTPROC Category: Policy Compliance	■ Windows 2003 () ■ Windows 2008 (256737)	Title: Listener for EXTPROC is not configured with IPC Protocol Description: The Oracle listener for PL/SQL EXTPROC should only be configured with an IPC protocol address. If the user allows TCP, then the violation for the protocols other than the TCP/TCPS/IPC is reported.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_TCP_PORT_ EXTPROC Category: Policy Compliance	■ Windows 2003 () ■ Windows 2008 (256738)	Title: The ports configured for EXTPROC listeners conflict with database listeners Description: If the TCP protocol is used to configure listeners with EXTPROC then use the port that is different than the ports that the Oracle listener for the databases uses.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

About the Oracle Objects module

This module checks for the access privileges to the Oracle objects that are based on the options that you have specified.

Editing default settings

The check in this group edits the default settings for all security checks in the module.

Oracle system identifiers (SIDs)

Use the name list to include or exclude the Oracle system identifiers (SIDs) for this check. By default, the check examines all the SIDs that you specify when you configure the Symantec ESM modules for the Oracle databases. The Symantec ESM modules for Oracle Databases configuration are stored in the \esm\config\oracle.dat file.

Reporting table privileges

The checks in this group 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 the 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. Use the **Grantees to skip** name list to exclude the grantees for this check.

The following table lists the message for the check.

Table 3-68 Message for Access to SYS.ALL_SOURCE

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ACCESS_ALL_SOURCE Category: Policy Compliance	■ Windows 2003 (243630) ■ Windows 2008 (256630)	Title: Access to SYS.ALL_SOURCE Description: The user or role that is reported in the Info field has access to the ALL_SOURCE table. Verify that the access is authorized.	Severity: yellow-3 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table privileges

Use this name list to include or exclude the table privileges for the **Grantable privilege** and **Directly granted privilege** checks to report on.

Object name

Use this name list to include or exclude the object names for the **Grantable privilege** and **Directly granted privilege** checks to report on.

Grantors

Use this name list to include or exclude the grantors for the **Grantable privileges**and **Directly granted** privilege checks to report on.

Grantable privilege

This check reports the roles, the accounts, or the synonyms that have grantable table privileges to Oracle objects. Use the name list to include and exclude the grantees for this check.

The following table lists the message for the check.

Table 3-69 Message for Grantable privilege

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_GRANTABLE Category: Policy Compliance	■ Windows 2003 (243631) ■ Windows 2008 (256631)	Title: Grantable table privilege Description: The grantable table privilege of the Oracle object is granted to the user or role. Verify that the user or role is authorized to grant the table privilege.	Severity: yellow-3 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Directly granted privilege

This check reports the roles, the accounts, or the synonyms that have directly granted table privileges to Oracle objects. Use the name list to include or exclude the grantees for this check.

The following table lists the message for the check.

Table 3-70 Message for Directly granted privilege

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: D Category: Policy Compliance	■ Windows 2003 (243632) ■ Windows 2008 (256632)	Title: Directly granted table privilege Description: The directly granted table privilege of the Oracle object is directly granted to the user or role. Verify that the user or role is authorized for the table privilege.	Severity: yellow-3 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Critical objects

This check works with the Grantable privilege check or the Directly granted privilege check. The Critical objects check reports on the objects that it finds on the ESM agent computer with the objects that you specify in the template. For example, sys.kupw$wor, sys.dbms_ddl, and so on. Use the name list to enable or disable the template file.

The following table lists the messages for the check.

Table 3-71 Messages for Critical objects

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_NOWORDFILES Category: ESM Error	■ Windows 2003 (243633) ■ Windows 2008 (256633)	Title: No word files specified Description: "Critical objects" was enabled but no word files were specified. Change your policy so that at least one word file is enabled.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_GRANTABLE_RED Category: Policy Compliance	■ Windows 2003 (243634) ■ Windows 2008 (256634)	Title: Grantable table privilege Description: The grantable table privilege of the Oracle object is granted to the user or role. Verify that the user or role is authorized to grant the table privilege.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-71 Messages for Critical objects *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DIRECT_GRANTED_RED Category: Policy Compliance	■ Windows 2003 (243635) ■ Windows 2008 (256635)	Title: Directly granted table privilege Description: The directly granted table privilege of the Oracle object is directly granted to the user or role. Verify that the user or role is authorized for the table privilege.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

About the Oracle Critical Object template

The **Critical objects** check of the Oracle Objects module uses the Oracle Critical Object template. By using this template, the check iterates through all objects and reports critical objects that you specify in the template.

Creating the Oracle Critical Object template

You must create and enable a new Oracle Critical Object template before you run the **Critical objects** check.

To create an Oracle Critical Object template

1 In the tree view, right-click **Templates**, and then click **New**.

2 In the **Create New Template** dialog box, select **Oracle Critical Object - all**.

3 In the **Template file name (no extension)** text box, type new template file name.

4 After Symantec ESM adds the .rco extension to the template file name, click **OK**.

About using the Oracle Critical Object template

The Oracle Critical Object template contains the following field:

Table 3-72 Field and Values/Options descriptions

Field	Description	Values/Options
Object	Lets you enter the object name that you want the check to report on.	Enter the name of the object that you want the check to report on.

Object Privileges

This check uses the specified template to report on the object privileges. Use the name list to enable or disable the template file.

The following table lists the messages for the check.

Table 3-73 Messages for Object Privileges

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_OBJ_NOT_FOUND Category: Policy Compliance	■ Windows 2003 (243636) ■ Windows 2008 (256636)	Title: Object not found Description: Object not found. The selected object may not be present in the database, or the information for the selected object is incorrect in the template. Verify the template entries, or verify if the object with the given owner is present in the database.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-73 Messages for Object Privileges *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_OBJ_PRIV_R Category: Policy Compliance	■ Windows 2003 (243637) ■ Windows 2008 (256637)	Title: Unauthorised object privilege Description: There is a mismatch in the actual object privilege present in the database and the privilege that is mentioned in the template. Check if the object that is marked as "Prohibited" in the template is present in the database, or check if the object that is marked as "Mandatory" in the template is not present in the database. For more information, see the corresponding Information column.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-73 Messages for Object Privileges *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_OBJ_PRIV_Y Category: Policy Compliance	■ Windows 2003 (243638) ■ Windows 2008 (256638)	Title: Unauthorised object privilege Description: There is a mismatch in the actual object privilege present in the database and the privilege that is mentioned in the template. Check if the object that is marked as "Prohibited" in the template is present in the database, or check if the object that is marked as "Mandatory" in the template is not present in the database. For more information, see the corresponding Information column.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-73 Messages for Object Privileges *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_OBJ_PRIV_G Category: Policy Compliance	■ Windows 2003 (243639) ■ Windows 2008 (256639)	Title: Unauthorised object privilege Description: There is a mismatch in the actual object privilege present in the database and the privilege that is mentioned in the template. Check if the object that is marked as "Prohibited" in the template is present in the database, or check if the object that is marked as "Mandatory" in the template is not present in the database. For more information, see the corresponding Information column.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-73 Messages for Object Privileges *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_OBJ_PRIV_R Category: Policy Compliance	■ Windows (37)	Title: Unauthorised object privilege Description: There is a mismatch in the actual object privilege present in the database and the privilege that is mentioned in the template. Check if the object that is marked as "Prohibited" in the template is present in the database, or check if the object that is marked as "Mandatory" in the template is not present in the database. For more information, see the corresponding Information column.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-73 Messages for Object Privileges *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_OBJ_PRIV_G Category: Policy Compliance	■ Windows (39)	Title: Unauthorised object privilege Description: There is a mismatch in the actual object privilege present in the database and the privilege that is mentioned in the template. Check if the object that is marked as "Prohibited" in the template is present in the database, or check if the object that is marked as "Mandatory" in the template is not present in the database. For more information, see the corresponding Information column.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-73 Messages for Object Privileges *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_OBJ_PRIV_Y Category: Policy Compliance	■ Windows (38)	Title: Unauthorised object privilege Description: There is a mismatch in the actual object privilege present in the database and the privilege that is mentioned in the template. Check if the object that is marked as "Prohibited" in the template is present in the database, or check if the object that is marked as "Mandatory" in the template is not present in the database. For more information, see the corresponding Information column.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-73 Messages for Object Privileges *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_OBJ_NOT_FOUND Category: Policy Compliance	■ Windows (36)	Title: Object not found Description: Object not found. The selected object may not be present in the database, or the information for the selected object is incorrect in the template. Verify the template entries, or verify if the object with the given owner is presnt in the database.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

About the Oracle Object Privileges template

The **Object Privileges** check of the Oracle objects module uses the Oracle Object Privileges template. By using this template, the check lets you report on the object privileges that you specify in the template.

Creating the Oracle Object Privileges template

You must create and enable a new Oracle Object Privileges template before you run the **Object Privileges** check.

To create an Oracle Object Privileges template

1. In the tree view, right-click **Templates**, and then click **New**.
2. In the **Create New Template** dialog box, select **Oracle Object Privileges Watch - all**.
3. In the **Template file name (no extension)** text box, type new template file name.
4. After Symantec ESM adds the .oop extension to the template file name, click **OK**.

About using the Oracle Object Privileges template

The Oracle Object Privileges template contains the following fields:

Table 3-74 Field and Values/Options descriptions

Field	Description	Values/Options
Object Name	Lets you specify an object name that you want the check to report on.	Enter the name of the object that you want the check to report on.
Owner	Lets you specify an owner name of the object that you want the check to report on.	Enter the owner name of the object that you want the check to report on.
Comments	Lets you enter additional comments on the object.	NA
Severity	Lets you select the severity for the messages that the check reports on the data.	■ Green Select Green for an Information message. ■ Yellow Select Yellow for a Warning message. ■ Red Select Red for an Error message.
Version	Lets you specify the Oracle version of the target server that you want the check to report on.	■ 9.0 Release 9.0.x ■ +9 Release 9.2.x and later ■ +10 Release 10.2.x and later ■ +11 Release 11.1.x and later

Table 3-74 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
Privilege List	Lets you specify the privileges by using the **Template Sublist Editor**.	

Table 3-74 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
		■ Required Lets you specify if the existence of the object on the target server is mandatory, prohibited, or allowed. ■ Prohibited Object must not exist. ■ Mandatory Object must exist. ■ Allowed Object existence is allowed. ■ Object Privilege Lets you enter the access privileges based on the database objects that you specify in the **Object Name** field. ■ Grantor Lets you enter the name of the grantor based on the object name and object privileges that you specify in the **Object Name** and **Object Privilege** fields respectively. ■ Grantee Lets you enter the name of the grantee based on the object name and object privileges that you specify in the **Object Name** and **Object Privilege** fields respectively. ■ With Grant Option Select this check box if you want the privileges with grant options that you specify in the **Object**

Table 3-74 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
		Privilege field to be reported.
Exclude List	Lets you exclude the object privileges by using the **Template Sublist Editor**.	■ Exclude Specify the privilege that you want to exclude. You can specify one of the following: ■ Object Name Select this option if you want to exclude the name of the object. ■ Owner Select this option if you want to exclude the owner of the object. ■ Object Privilege Select this option of you want to exclude the privileges of the object. ■ Grantor Select this option if you want to exclude the grantor of the object. ■ Grantee Select this option if you want to exclude the grantee of the object. ■ Name Enter the name of the object that you want to exclude.

About the Oracle Passwords module

This module checks for the password integrity that Oracle user accounts uses that is based on the options that you have specified.

Editing default settings

The checks in this group edits the default settings for all the security checks in the module.

Oracle system identifiers (SIDs)

Use the name list to include or exclude the Oracle system identifiers (SIDs) for this check. By default, the check examines all the SIDs that you specify when you configure the SymantecESMmodules for the Oracle databases. The configuration for Symantec ESM Modules for Oracle Databases is stored in \esm\config\oracle.dat.

Users to check

Use the name list to include or exclude the users or the roles for all the password guessing checks.

Account status

Use the name list to include or exclude the statuses for all the password guessing checks.

Password display

This check works with the Password=wordlistword, Password=username, and Password = any username checks. Enable this check to display the guessed passwords in the <first character>*<last character> format.

Specifying check variations

You can use the checks under this group to set conditions for guessing the passwords of the Oracle accounts. 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 the passwords that matches the user names or common words spelled twice. For example, in Password = wordlist word, password golfgolf matches the word golf.

Plural

This option directs Password = checks to compare the plural forms of user names, role names, or common words with the password. For example, in “Password = user name,” the password “golfs” matches the user name “golf.”

Prefix

Enable this option so that Password = checks reports the passwords that begin with a prefix in the user names, role names, or common words. For example, if "pro" is a prefix and "golf" is a user name, then the Password = user name check reports "progolf " as a weak password.

Suffix

Enable this option so that Password = checks reports the passwords that end with a suffix in the user names, role names, or common words. For example, if “pro” is a suffix and “golf” is a user name, then the Password = user name check reports “golfpro” as a weak password.

Comparing passwords to word lists

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

Password = wordlist word

This check compares the encrypted version of the user and the role password with the encrypted version of the words that are included in the common words and names file. The check then reports the matches. You can specify the word and name files that you want to check. Do not use common words or names as passwords.

Symantec recommends that you do not usecommonwords or names as passwords. You must assign a more secure password immediately to the user accounts that are reported by this check, then notify each user to log in using the more secure password. Have the users complete the process by changing their passwords again.

A secure password has six to eight characters with at least one numeric character, and one special character. The password must not match an account name or must not be found in the word file.

The following table lists the messages for the check.

Table 3-75 Messages for Password = wordlist word

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PASS_GUESSED Category: Policy Compliance	■ Windows 2003 (242334) ■ Windows 2008 (255334)	Title: Weak user password Description: The password is a form of a user name or common word. It is a weak password. 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 6-8 characters, including at least one non-alphabetic character, should not be found in any dictionary, and should not match an account name.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-75 Messages for Password = wordlist word *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_NO_WORDS Category: ESM Error	■ Windows 2003 (242336) ■ Windows 2008 (255336)	Title: No word files specified Description: Password = wordlist word was enabled, but no word files were specified. Enable at least one word file.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Password = username

This check reports the users and the roles that use their own user names or role names as passwords. The check is not as comprehensive as the Password = any username check. However, if the Password = any user name check takes longer or consumes more CPU usage, then use the Password = user name check daily and the Password = any user name check on weekends. The reported password matches the same user account name. The passwords that closely resemble account names are easily guessed.

Symantec recommends that you must immediately assign more secure passwords to reported user accounts. Then notify the users and ask them to log in with the more secure passwords. Have the users complete the process by changing their passwords again.

A secure password has six to eight characters with at least one numeric character, and one special character. The password must not match an account name or must not be found in the word file.

The following table lists the message for the check.

Table 3-76 Message for Password = username

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PASS_GUESSED Category: Policy Compliance	■ Windows 2003 (242334) ■ Windows 2008 (255334)	Title: Weak user password Description: The password is a form of a user name or common word. It is a weak password. 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 6-8 characters, including at least one non-alphabetic character, should not be found in any dictionary, and should not match an account name.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Password = any username

This check compares the encrypted version of the user and the role password with the encrypted version of the words that are included in the common words and names file. The check then reports the matches. You can specify the word and name files that you want to check. Do not use common words or names as passwords.

Symantec recommends that you do not usecommonwords or names as passwords. You must assign a more secure password immediately to the user accounts that are reported by this check, then notify each user to log in using the more secure password. Have the users complete the process by changing their passwords again.

A secure password has six to eight characters with at least one numeric character, and one special character. The password must not match an account name or must not be found in the word file.

The following table lists the message for the check.

Table 3-77 Message for Password = any username

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PASS_GUESSED Category: Policy Compliance	■ Windows 2003 (242334) ■ Windows 2008 (255334)	Title: Weak user password Description: The password is a form of a user name or common word. It is a weak password. 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 6-8 characters, including at least one non-alphabetic character, should not be found in any dictionary, and should not match an account name.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

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 soon as possible. Otherwise, unauthorized users can log in as SYS or SYSTEM with administrator privileges.

Well known passwords

This check reports the 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. Use the name list to include the account and password combinations for this check.

Symantec recommends that you must assign a more secure password immediately. You must instruct the user to log in with the more secure password and change the password again.

Asecure password has six to eight characters with at least one numeric character, and one special character. The password must not match an account name or must not be found in the word file.

The following table lists the message for the check.

Table 3-78 Message for Well known passwords

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DEFAULT_PASSWORD Category: Policy Compliance	■ Windows 2003 (242337) ■ Windows 2008 (255337)	Title: Well known account/password found Description: Change or delete all well known account/password combinations.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

About the Oracle Patches module

This module identifies the Oracle security patches that are not installed on your computers.

Note: The module may not report correct messages if the opatch utility and Oracle Patches module is concurrently running on the same agent. Symantec recommends not to run the Oracle Patches module on the same agent while opatch utility is already running.

Edit default settings

The check in this group edits the default settings for all the security checks in the module.

Oracle Home Paths

Use the name list to include or exclude the Oracle home paths for this check. By default, the check examines all the Home paths that you specify when you configure the SymantecESMmodules for the Oracle databases. The configuration for Symantec ESM Modules for Oracle Databases are stored in the oracle.dat file that is located in the \esm\config\ folder.

Template files

Use the name list to enable or disable the template files for this check. Oracle Patch template files are identified by .orp file extensions.

The following table lists the message for the check.

Table 3-79 Message for Template files

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_TEMPLATEFILE_MISSING Category: ESM Error	■ Windows 2003 (243035) ■ Windows 2008 (256035)	Title: No template files specified Description: The Oracle Patches module was run without any template files. No patch related checks were performed. Check your policy to ensure that at least one template file is enabled for the agent's operating system.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Oracle patches

The checks in this group report the patches that are released by Oracle and that are not applied on the database server.

Patch information

This check reports information about the 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 should verify that all current patches are installed on your Oracle clients and servers. Use the name list to include the template files for this check. When the **Patch Information** check is run along with the **SID Info** check, the relevant SIDs are also reported.

You can download patch updates by using LiveUpdate.

Symantec recommends that you verify that your Oracle server and components have the current applicable patches.

The following table lists the messages for the check.

Table 3-80 Messages for Patch information

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PATCH_ AVAILABLE Category: Policy Compliance	■ Windows 2003 (243030) ■ Windows 2008 (256030)	Title: Patch available Description: The patch is available at Oracle's patches Web site.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_PATCHSET_ AVAILABLE Category: Policy Compliance	■ Windows 2003 (243031) ■ Windows 2008 (256031)	Title: Patchset available Description: The patchset is available at Oracle's patches Web site.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

About the Oracle Patch template

The **Patch information** check of the Oracle patches module uses the Oracle Patch template. By using this template, the check reports information about the patches that have been released within the number of days that you specify in the check.

Updates on the Oracle Patch template

From this release onwards, following changes are made to the existing Oracle Patch template:

- The template only includes the patches that are critical, legislative, recommended, and are related to security.
- The template only includes the patch entries that are present on the Oracle site.
- The template that is being shipped with Oracle 5.0 release overwrites the earlier template.

Note: The changes are made to keep alignment with the changes that are made on the Oracle site.

Creating the Oracle Patch template

You must create and enable a new Oracle Patch template before you run the **Patch information** check.

To create an Oracle Patch template

1. In the tree view, right-click **Templates**, and then click **New**.
2. In the **Create New Template** dialog box, select **Oracle Patch - all**.
3. In the **Template file name (no extension)** text box, type new template file name.
4. After Symantec ESM adds the .orp extension to the template file name, click **OK**.

About using the Oracle Patch template

The Oracle Patch template contains the following fields:

Table 3-81 Field and Values/Options descriptions

Field	Description	Values/Options
Version	Lets you specify the Oracle database version of the target server that you want the check to report on.	Enter the patch version number that you want the check to report on.

Table 3-81 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
Platform	Lets you specify the platform of the target server that you want the check to report on.	

Table 3-81 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
		■ All Select this value for the check to report on all platforms. ■ aix Select this value for the check to report on Aix platforms. ■ hpux-hppa Select this value for the check to report on Hpux-hppa platforms. ■ linux Select this value for the check to report on Linux platforms. ■ solaris-sparc Select this value for the check to report on Solaris-sparc platforms. ■ hpux-ia64 Select this value for the check to report on Hpux-ia64 platforms. ■ hpux-hppa/HP-UX 10.20 Select this value for the check to report on HP-UX 10.20 platforms. ■ redhat-x86 Select this value for the check to report on RedHat platforms. ■ WIN2K Select this value for the check to report on all Windows 2000 platforms. ■ WIN3S Select this value for the check to report on all Windows 2003 platforms. ■ WIN8S

Table 3-81 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
		Select this value for the check to report on all Windows 2008 platforms.
Product	Lets you specify the product name that is installed on the server. **Note:** The check does not consider the product name for the verification report.	Enter the name of the product that is installed on the server. For example, Oracle Database server.
ID	Lets you specify the ID that you want the check to report on.	Enter the ID that you want the check to report on.
Patch ID	Lets you specify the Patch ID that you want the check to report on. The check reports a violation if the Patch ID that you specify in the template is greater than the Patch ID that is applied on the target server.	Enter the Patch ID that you want the check to report on.
Date	Lets you specify the release date of the Patch.	Enter the date in the following format: YYYY/MM/DD.
Architecture	Lets you specify the architecture of the server that you want the check to report on.	■ All Select this value for the check to report on all processors. ■ 32 bits Select this value for the check to report on 32-bit processor. ■ 64 bits Select this value for the check to report on 64-bit processor.

Table 3-81 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
Description	Lets you enter a description for the patch.	NA
Patch Set	Lets you select the patch set.	Select the patch set.
Merged Patches	Lets you specify the patches that you want to merge by using the Template Sublist Editor.	- Patch ID Enter the name of the patch ID that you want to merge.

Opatch tool

This check enables ESM to use the opatch tool and reports the opatch tool version information. Opatch is the Oracle patch tool, which is a set of PERL scripts that run with PERL 5.005_03 and later. You have JRE and JDK installed in the Oracle Home to run the OPatch tool. The commands such as jar, java, ar, cp, and make (depending on platforms) available should be present in the Opatch path. By default, the Opatch tools check searches for the OPatch directory that contains the opatch tool in ORACLE HOME. If the check fails to find the tool in ORACLE HOME, then it takes the path of the opatch tool that mentioned in the check. This application can be downloaded from the following URL: http://www.oracle.com.

The following table lists the messages for the check.

Table 3-82 Messages for Opatch tool

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_OPATCH_VERSION Category: System Information	- Windows 2003 (243032) - Windows 2008 (256032)	Title: Opatch version Description: The opatch tool is at the shown version.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-82 Messages for Opatch tool *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_OPATCH_INFO Category: System Error	■ Windows 2003 (243033) ■ Windows 2008 (256033)	Title: Opatch Information Description: The specified opatch tool reports in the information field.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Installed patches

This check works with the **Opatch tool** check and reports the patches, the opatch tool detects. When the **Installed Patches** check is run along with the **SID Info** check, the relevant SIDs are also reported.

The following table lists the message for the check.

Table 3-83 Message for Installed patches

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_INSTALLED_ PATCH Category: Policy Compliance	■ Windows 2003 (243034) ■ Windows 2008 (256034)	Title: Installed patches Description: The installed patch is detected by the opatch tool.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SID info

This check add on the relevant SIDs to the patch messages that are reported from the **Patch information** and **Installed patches** checks.

About the Oracle Profiles module

This module checks for the Oracle profiles table that is based on the options that you have specified. It reports SIDs, profile names, profile resource names, and resource limits as applicable.

Establishing a baseline snapshot

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

Automatically update snapshots

Enable this check to automatically update the snapshots with the current information.

Editing default settings

Use the check in this group to edit the default settings for all the security checks in the module.

Oracle system identifiers (SIDs)

Use the name list to include or exclude the Oracle system identifiers (SIDs) for this check. By default, the check examines all the SIDs that you specify when you configure the SymantecESMmodules for the Oracle databases. The configuration for Symantec ESM Modules for Oracle Databases is stored in \esm\config\oracle.dat.

Reporting profiles and their limits

The checks in this group report the existing, new, and deleted profiles and their resource limits.

Profile enforcement

This check reports SIDs that do not enforce profiles.

Symantec recommends that in the database's parameter file, change the value of the RESOURCE_LIMIT parameter from FALSE to TRUE so that the profiles are enforced.

The following table lists the message for the check.

Table 3-84 Message for Profile enforcement

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_NOT_ENABLED Category: System Information	■ Windows 2003 (242949) ■ Windows 2008 (255949)	Title: Profiles are not enabled Description: The profile is not enforced in the database. By default no profiles are enforced until you change the value of the RESOURCE_LIMIT parameter from FALSE to TRUE for the database's instance.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Profiles

This check reports all profiles that are defined in the database. Use the name list to exclude profiles for this check. You should periodically review the profiles to ensure that all profiles are authorized and that profile resources and resource limits are allocated efficiently.

The following table lists the message for the check.

Table 3-85 Message for Profiles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_LIST Category: System Information	■ Windows 2003 (242930) ■ Windows 2008 (255930)	Title: Existing profiles Description: The profile is defined in the database.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New profiles

This check reports all profiles that were defined in the database after the last snapshot update. Use the name list to exclude profiles for this check.

If the addition is authorized, Symantec recommends that you either update the snapshot or delete the profile.

The following table lists the message for the check.

Table 3-86 Message for New profiles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_ADDED Category: Change Notification	■ Windows 2003 (242931) ■ Windows 2008 (255931)	Title: New profile Description: The profile was added to the database after the last snapshot update. If the addition is authorized, update the snapshot. If the addition is not authorized, delete the profile.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted profiles

This check reports all the profiles that were deleted from the database after the last snapshot update. Use the name list to exclude profiles for this check.

If the deletion is authorized, Symantec recommends that you either update the snapshot or restore the profile.

The following table lists the message for the check.

Table 3-87 Message for Deleted profiles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_DELETED Category: Change Notification	■ Windows 2003 (242932) ■ Windows 2008 (255932)	Title: Deleted profile Description: The profile was dropped from the database after the last snapshot update. If the deletion is authorized, update the snapshot. If the deletion is not authorized, restore the profile.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Profile resources

This check reports profile resource limits. Use the name list to exclude profiles for this check.

Symantec recommends that you must ensure that the profile resource limits matches with the company's security policies.

The following table lists the message for the check.

Table 3-88 Message for Profile resources

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_LIMIT_LIST Category: System Information	■ Windows 2003 (242933) ■ Windows 2008 (255933)	Title: Profile resource limits Description: The profile and its resource limits are defined in the database. Verify that the profile resource limits conform to company security policies.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Changed resource limits

This check reports the profile resource limits that changed after the last snapshot update. Use the name list to exclude profiles for this check.

If the change is authorized, Symantec recommends that you either update the snapshot or restore the previous limit.

The following table lists the message for the check.

Table 3-89 Message for Changed resource limits

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_LIMIT_CHANGED Category: Change Notification	■ Windows 2003 (242936) ■ Windows 2008 (255936)	Title: Changed profile resource limit Description: The profile's resource limit changed after the last snapshot update. Update the snapshot if the resource limit is appropriate; change the limit if it is not appropriate. Limits should be high enough to permit normal resource usage but low enough to prevent abuse.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Reporting CPU limit violations

The checks in this group report the CPU resource limits.

Oracle profiles

Use the name list to include or exclude the Oracle profiles for the resource limitation checks.

Sessions per user

This check reports the profiles that allow more number of concurrent sessions for each user than the number that you specify in the MaxSession/User text box.

As to prevent access by other users, multiple users should not be given concurrent session permission.

The following table lists the message for the check.

Table 3-90 Message for Sessions per user

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_ SESSIONS_PER_USER Category: Policy Compliance	■ Windows 2003 (242948) ■ Windows 2008 (255948)	Title: Sessions per user too high Description: The profile permits more sessions per user than you specified for the check. SESSIONS_PER_USER specifies the maximum number of concurrent sessions per user.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

CPU time per session

This check reports profiles that allow moreCPUtime 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.

Symantec recommends that you specify a maximum CPU time per session limit that allow users to perform their duties without frequent logging on and logging out. It prevents a small number of users from denying service to others by using excessive CPU resources.

The following table lists the message for the check.

Table 3-91 Message for CPU time per session

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_CPU_PER_SESSION Category: Policy Compliance	■ Windows 2003 (242937) ■ Windows 2008 (255937)	Title: CPU time per session exceeds limit Description: The profile's maximum CPU time per session exceeds the amount that you specified in the check. Time is expressed in hundredths of a second. Specify a realistic limit to prevent one or more users from locking out other users by using all of the CPU capacity.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

CPU time per call

This check reports the 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.

Symantec recommends that you specify a maximum CPU time per call limit that allow users perform their duties and that prevents a small number of users from denying service to others by using excessive CPU resources.

The following table lists the message for the check.

Table 3-92 Message for CPU time per call

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_CPU_PER_CALL Category: Policy Compliance	■ Windows 2003 (242938) ■ Windows 2008 (255938)	Title: CPU time per call exceeds limit Description: The profile's maximum CPU time per call exceeds the amount that you specified in the check. Time is expressed in hundredths of a second. Specify a realistic limit to prevent one or more calls from locking out other calls by using all of the CPU capacity.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Connection time

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

Symantec recommends that you specify a realistic limit that allow users to perform their duties and that prevents a few connections from denying service to others by using excessive CPU resources.

The following table lists the message for the check.

Table 3-93 Message for Connection time

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_ CONNECT_TIME Category: Policy Compliance	■ Windows 2003 (242939) ■ Windows 2008 (255939)	Title: Connect time exceeds limit Description: The number of minutes allowed for the profile's connection exceeds the number of minutes that you specified in the check. Specify a realistic limit to prevent one or more connections from denying service to other users by monopolizing CPU capacity.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

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.

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

Symantec recommends that you specify a realistic amount of time before an inactive process is disconnected.

The following table lists the message for the check.

Table 3-94 Message for Idle time

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_IDLE_TIME Category: Policy Compliance	■ Windows 2003 (242941) ■ Windows 2008 (255941)	Title: Idle time exceeds limit Description: The profile's maximum idle time exceeds the limit that you specified in the check. Specify a realistic amount of time before an inactive process is disconnected. Connections that are idle for a long period may indicate that the machine is unattended, which would pose a security threat.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Reporting password violations

The checks in this group report the profiles with settings for the number of failed logon 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,

Failed logins

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

Symantec recommends that you restrict the number of permitted failed login attempts to minimize the likelihood of break-in by intruders who attempt to guess user names and passwords.

The following table lists the message for the check.

Table 3-95 Message for Failed logins

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_ FAILED_LOGIN_ ATTEMPTS Category: Policy Compliance	■ Windows 2003 (242940) ■ Windows 2008 (255940)	Title: Failed login attempts exceed limit Description: The number of failed logins permitted before an account is locked exceeds the number that you specified in the check. Restrict the number of failed attempts permitted to minimize the likelihood of intruders guessing user names and passwords.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Password grace time

This check reports the profiles that have their password grace days different than the number that you specify in the Password Grace text box. Now, you can also use the comparison operators before specifying the value in the text box. The value that you specify in the text box refers to the number of days wherein a warning is given before your password expires. The comparison operators are as follows: Equal (=), Not equal (!=), Less than (<), Greater than (>), Less than or equal to (<=), Greater than or equal to (>=).

Symantec recommends that you specify realistic number of days for a user to change a password after being warned that it is about to expire.

The following table lists the message for the check.

Table 3-96 Message for Password grace time

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_PASS_GRACE_TIME Category: Policy Compliance	■ Windows 2003 (242942) ■ Windows 2008 (255942)	Title: Password grace time differs from limit Description: The profile's password grace time is not the same as the limit that you specified in the check. Specify a realistic number of days for a user to change a password after being warned that it is about to expire.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Password duration

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

Symantec recommends that you change your password often to minimize the possibility that an intruder will discover the passwords but not so often that you have difficulty remembering your passwords.

The following table lists the message for the check.

Table 3-97 Message for Password duration

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_PASS_LIFE_TIME Category: Policy Compliance	■ Windows 2003 (242943) ■ Windows 2008 (255943)	Title: Password duration too high Description: The maximum number of days permitted for the profile's password exceeds the number of days that you specified in the check. Require password changes often to minimize the likelihood that they will be discovered by an intruder.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Password lock time

This check reports the 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 parameter specifies the number of days that an account is locked.

Symantec recommends that you change the resource parameter PASSWORD_LOCK_TIME setting to match with your security policy.

The following table lists the message for the check.

Table 3-98 Message for Password lock time

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_PASS_ LOCK_TIME Category: Policy Compliance	■ Windows 2003 (242944) ■ Windows 2008 (255944)	Title: Password lock time too low Description: The profile's password lock time is lower than the number of days that you specified in the check. Verify that the PASSWORD_LOCK_TIME parameter setting conforms to company security policies.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

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.

Symantec recommends that you change the resource parameter PASSWORD_REUSE_MAXto require a realistic number of times that a password must be changed before it can be reused.

The following table lists the message for the check.

Table 3-99 Message for Password reuse max

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_PASS_REUSE_MAX Category: Policy Compliance	■ Windows 2003 (242945) ■ Windows 2008 (255945)	Title: Password reuse maximum too low Description: The profile permits a password to be reused after fewer changes than the number of changes that you specified in the check. If you set a PASSWORD_REUSE_MAX value, PASSWORD_REUSE_TIME must be UNLIMITED.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_PROFILE_PASS_REUSE_WEAK Category: Policy Compliance	■ Windows 2003 (242955) ■ Windows 2008 (255955)	Title: Password reuse settings weaker than expected Description: The password reuse settings in the profile are weaker than the values that are specified in the check.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

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_TIMEmust be UNLIMITED. If you set a PASSWORD_REUSE_TIME value, PASSWORD_REUSE_MAX must be UNLIMITED.

Symantec recommends that you change the resource parameter PASSWORD_REUSE_TIME to require a realistic amount of time that must pass before it can be reused.

The following table lists the message for the check.

Table 3-100 Message for Password reuse time

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_PASS_REUSE_TIME Category: Policy Compliance	■ Windows 2003 (242946) ■ Windows 2008 (255946)	Title: Password reuse time too low Description: The profile permits a password to be reused after fewer days than you specified in the check. If you specify a PASSWORD_REUSE_TIME value, PASSWORD_REUSE_MAX must be UNLIMITED.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_PROFILE_PASS_REUSE_WEAK Category: Policy Compliance	■ Windows 2003 (242955) ■ Windows 2008 (255955)	Title: Password reuse settings weaker than expected Description: The password reuse settings in the profile are weaker than the values that are specified in the check.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

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. Use the name list to include the functions for this check.

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

Symantec recommends that you immediately assign a secure password and instruct the user to log on with the secure password and change the password again.

The following table lists the message for the check.

Table 3-101 Message for Password verify function

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROFILE_PASS_VERIFY_FUNCTION Category: Policy Compliance	■ Windows 2003 (242947) ■ Windows 2008 (255947)	Title: Password verify function Description: The profile's password verification function a name that does not exist in the list that you specified in the check. Specify the name of a script to call for PROFILE_PASS_VERIFY_FUNCTION.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Invalid profiles

This check reports users that are assigned to profiles that fail one or more of the enabled resource limitation checks. Use the name list to exclude the users for this check.

The following table lists the message for the check.

Table 3-102 Message for Invalid profiles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_INVALID_PROFILE_ASSIGNED Category: Policy Compliance	■ Windows 2003 (242950) ■ Windows 2008 (255950)	Title: Invalid profile assigned Description: The user's profile is invalid. It fails one or more enabled profile resource limitation checks. Verify that the profile is correctly defined in the database.	Severity: yellow-3 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Profile settings

This check reports the profile settings that do not match the settings that are specified in the template file. Use the name list to enable or disable the template files.

The following table lists the message for the check.

Table 3-103 Message for Profile settings

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROF_NOT_FOUND Category: Policy Compliance	■ Windows 2003 (242954) ■ Windows 2008 (255954)	Title: Object not found Description: No profile found that matches the name as specified in the template. For more information, refer the Information column.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_PROF_R Category: Policy Compliance	■ Windows 2003 (242251) ■ Windows 2008 (255251)	Title: Profile settings mismatch Description: The profile settings that are present in the database do not match with the settings that are specified in the template. For more information, refer the Information column.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-103 Message for Profile settings *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PROF_Y Category: Policy Compliance	■ Windows 2003 (242252) ■ Windows 2008 (255252)	Title: Profile settings mismatch Description: The profile settings that are present in the database do not match with the settings that are specified in the template. For more information, refer the Information column.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_PROF_G Category: Policy Compliance	■ Windows 2003 (242253) ■ Windows 2008 (255253)	Title: Profile settings mismatch Description: The profile settings that are present in the database do not match with the settings that are specified in the template. For more information, refer the Information column.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

About the Oracle Profiles template

In the Oracle Profiles module, the **Profile settings** check uses the Oracle Profiles template. The check reports the profile settings that do not match the settings that are specified in the template.

Creating the Oracle Profiles template

You must create and enable a new Oracle Profiles template before you run the **Profile settings** check.

To create an Oracle Profiles template

1. In the tree view, right-click **Templates**, and then click **New**.
2. In the **Create New Template** dialog box, select **Oracle Profiles - all**.
3. In the **Template file name (no extension)** text box, type new template file name.
4. After Symantec ESM adds the .opa extension to the template file name, click **OK**.

About using the Oracle Profiles template

The Oracle Profiles template contains the following fields:

Table 3-104 Field and Values/Options descriptions

Field	Description	Values/Options
Profile Name	Lets you specify the name of the profile.	Enter a name for the profile.
Sessions per User	Lets you specify number of concurrent sessions for a user.	Enter the number of concurrent sessions for a user.
CPU time per call	Lets you specify the CPU time for a call.	Enter the CPU time a call.
Connection time	Lets you specify the connection time for an account.	Enter a connection time for an account.
Idle time	Lets you specify the idle time that is required before a process is disconnected.	Enter the idle time that you require before the process is disconnected.
Failed logins	Lets you specify a period for the failed login attempts.	Enter a number to allow failed login attempts.
Password grace time	Lets you specify the password grace period.	Enter a number for the password grace period.

Table 3-104 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options
Password duration	Lets you specify the settings for the number of failed logon attempts, password grace time, password duration, password lock time, and password reuse requirements that violate your security policy.	Enter password duration for the number of failed logon attempts, password grace time, password duration, password lock time, and password reuse requirements.
Password lock time	Lets you specify the password lock time period.	Enter a number for the password lock time period.
Password reuse max	Lets you specify the maximum period for the password usage.	Enter a number to specify the maximum period for the password usage.
Password reuse time	Lets you specify the maximum period before the password can be reused.	Enter a number to specify the maximum period for the password reuse.
Password verify function	Lets you specify the password complexity functions.	Enter a password complexity function.
Severity	Lets you specify the severity for the messages that the check reports.	■ Green Select Green for an Information message. ■ Yellow Select Yellow for a Warning message. ■ Red Select Red for an Error message.

About the Oracle Roles module

This module checks for the Oracle roles that are based on the options that you have specified.

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 check to automatically update the snapshots with the current information.

Editing default settings

Use the check in this group to edit the default settings for all the security checks in the module.

Oracle system identifiers (SIDs)

Use the name list to include the Oracle system identifiers (SIDs) for this check. By default, the check examines all the SIDs that you specify when you configure the Symantec ESM modules for the Oracle databases. The configuration for Symantec ESM Modules for Oracle Databases is stored in \esm\config\oracle.dat file.

Reporting roles

The checks in this group report the existing roles and the roles that have been added or deleted since the last snapshot update.

Roles

This check reports roles that are defined in the database. Use the name list to exclude the roles for this check.

Symantec recommends that you remove the roles that are not authorized or are out of date. Periodically, you must review the roles to ensure that they are currently authorized.

The following table lists the message for the check.

Table 3-105 Message for Roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_EXISTING_ROLES Category: System Information	■ Windows 2003 (242236) ■ Windows 2008 (255236)	Title: Defined role Description: The role is defined for the SID.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New roles

This check reports roles that were added to the database after the last snapshot update. Use the name list to exclude the roles for this check.

If the new role is authorized, Symantec recommends that you either update the snapshot or drop the role.

The following table lists the message for the check.

Table 3-106 Message for New roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ADDED_ROLES Category: Change Notification	■ Windows 2003 (242237) ■ Windows 2008 (255237)	Title: New role Description: The role was added to the database after the last snapshot update. If the addition is authorized, update the snapshot. If the addition is not authorized, delete the role.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted roles

This check reports roles that have been deleted from the database since the last snapshot update. Use the name list to exclude the roles for this check.

If the deletion is authorized, Symantec recommends that you either update the snapshot or restore the role.

The following table lists the message for the check.

Table 3-107 Message for Deleted roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DELETED_ROLES Category: Change Notification	■ Windows 2003 (242238) ■ Windows 2008 (255238)	Title: Deleted role Description: The role was deleted from the database after the last snapshot update. Update the snapshot if the deletion is authorized; restore the role if the deletion is not authorized.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Reporting role privileges

The checks in this group report the role privileges and the privileges that were granted to or removed from the roles after the last snapshot update, and grantable role privileges.

Privileges

This check reports privileges that have been granted to roles. Use the name list to exclude the roles for this check.

Symantec recommends that you add or remove the privileges for the roles as appropriate. Periodically, you must review the roles to ensure that the privileges granted to them are consistent with the current user duties.

The following table lists the message for the check.

Table 3-108 Message for Privileges

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ROLE_PRIVILEGE Category: System Information	■ Windows 2003 (242239) ■ Windows 2008 (255239)	Title: Role privilege Description: The role includes the privilege that is reported in the Info field.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New privileges

This check reports privileges that were directly granted to roles after the last snapshot update. Use the name list to exclude the roles for this check.

If the new privilege is authorized, Symantec recommends that you either update the snapshot or drop the privilege from the role.

The following table lists the message for the check.

Deleted privileges

This check reports privileges that were dropped from the roles after the last snapshot update. Use the name list to exclude the roles for this check.

If the deletion is authorized, Symantec recommends that you either update the snapshot or restore the privilege.

The following table lists the message for the check.

Table 3-109 Message for Deleted privileges

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DELETED_ROLE_PRIVILEGE Category: Change Notification	■ Windows 2003 (242241) ■ Windows 2008 (255241)	Title: Deleted role privilege Description: The directly granted privilege was dropped from the role after the last snapshot update. If the deletion is authorized, update the snapshot. If the deletion is not authorized, restore the privilege to the role.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Grantable privileges

This check reports the grantable privileges that have been granted to the roles. Use the name list to exclude the roles for this check.

Symantec recommends that you periodically review all grantable role privileges to ensure that the grantable privilege is appropriate for the role. You must revoke grantable role privileges from the users who are not authorized to grant them.

The following table lists the message for the check.

Table 3-110 Message for Grantable privileges

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_GRANTABLE_ROLE_PRIVILEGE Category: System Information	■ Windows 2003 (242242) ■ Windows 2008 (255242)	Title: Grantable role privilege Description: The privilege of the role is grantable. Verify that the privilege is appropriate for the role.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Nested roles

This check reports roles and the nested roles that they contain. Use the name list to include or exclude the roles for this check.

Table 3-111 Message for Nested roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ROLE_ROLE Category: System Information	■ Windows 2003 (242243) ■ Windows 2008 (255243)	Title: Nested role Description: The role has been directly granted to the role.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New nested roles

This check reports roles that were directly granted to other roles after the last snapshot update. Use the name list to include or exclude the roles for this check.

If the change is authorized, Symantec recommends that you either update the snapshot or drop the nested role.

The following table lists the message for the check.

Table 3-112 Message for New nested roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ADDED_ROLE_ROLE Category: Change Notification	■ Windows 2003 (242244) ■ Windows 2008 (255244)	Title: New nested role Description: The role was directly granted to the role after the last snapshot update. If the addition is authorized, update the snapshot. If the addition is not authorized, drop the nested role from the role.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted nested role

This check reports the nested roles that were removed from parent roles since the last snapshot update. Use the name list to include or exclude the roles for this check.

The following table lists the message for the check.

Table 3-113 Message for Deleted nested role

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DELETED_ROLE_ROLE Category: Change Notification	■ Windows 2003 (242245) ■ Windows 2008 (255245)	Title: Nested role deleted Description: The nested role was dropped from role after the last snapshot update. If the deletion is authorized, update the snapshot. If the deletion is not authorized, restore the nested role.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Grantable nested role

This check reports the grantable roles that have been granted to other roles. Use the name list to exclude the grantee roles for this check.

Symantec recommends that you periodically review the 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.

The following table lists the message for the check.

Table 3-114 Message for Grantable nested role

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_GRANTABLE_ ROLE_ROLE Category: System Information	■ Windows 2003 (242246) ■ Windows 2008 (255246)	Title: Grantable nested role Description: The role includes the nested grantable role. Verify that the role granted to the grantee is authorized, and that the grantee is authorized to have the grantable role.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Reporting role access

The checks in this group 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 the password-protected default roles of the roles.

For example:

- Create a Role ‘Role A.’
- Create another role that is identified by a password ‘Role B’.
- Assign ‘Role B’ to ‘Role A.
  Now ‘Role B’ is the default password-protected role of Role A and the check reports 'Role B', which is the default password-protected role of ‘Role A.’

The default roles do not require any passwords. Usually, a password-protected role has the privileges or roles that require authorization. Users with password-protected default roles are not required to enter their passwords to use the roles. Use the name list to exclude the roles for this check.

Symantec recommends that for an unauthorized user, you either assign a different default role to the user or remove the password protection from the role.

The following table lists the message for the check.

Table 3-115 Message for Password-protected default role

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DEFAULT_ROLE_PASS_REQUIRED Category: System Information	■ Windows 2003 (242247) ■ Windows 2008 (255247)	Title: Default role requires password Description: The default role is password protected. Password protected roles usually include privileges that are security sensitive. If the role is a role's default role, the role is not required to enter a password. Verify that the password protected role is authorized to be a default role.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

DBA equivalent roles

Use the name list to include or exclude roles for the Granted Oracle DBA role check to report on.

Granted Oracle DBA role

This check reports users and roles that have been directly granted to an Oracle database administrator (DBA) role or equivalent. Use the name list to exclude the users for this check.

Symantec recommends that you either revoke the DBA roles from unauthorized users or tightly control the database administrator rights.

The following table lists the message for the check.

Table 3-116 Message for Granted Oracle DBA role

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DBA_ROLE_USERS Category: Policy Compliance	■ Windows 2003 (242230) ■ Windows 2008 (255230)	Title: User granted Oracle DBA role Description: The user has been granted the database administrator (DBA) role or equivalent. DBAs have full rights to system and application data, including creating new users and roles, granting access rights, and deleting databases. Revoke DBA privileges from unauthorized users immediately, and tightly control administrator rights.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Roles without passwords

This check reports the roles that do not require passwords. The roles that are authenticated as External or Global are skipped. Use the name list to exclude the roles for this check.

If the role could be exploited to give the users access to security-related information, Symantec recommends that you password-protect the role. You can control the permissions that are granted to roles that do not require passwords.

The following table lists the message for the check.

Table 3-117 Message for Roles without passwords

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ROLE_PASSWORD Category: Policy Compliance	■ Windows 2003 (242233) ■ Windows 2008 (255233)	Title: Password not required for role Description: The role is not password protected.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

PUBLIC role access

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

Symantec recommends that you control the permissions that are granted to the PUBLIC role. The preferred method of granting access is to give EXECUTE to the procedures.

The following table lists the message for the check.

Table 3-118 Message for PUBLIC role access

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_PUBLIC_ACCESS Category: Policy Compliance	■ Windows 2003 (242234) ■ Windows 2008 (255234)	Title: Table accessible to PUBLIC Description: The table is accessible to all users through the PUBLIC role privilege.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Granted roles

This check reports the users and the roles that violate the conditions that you specify in the template. Use the name list to enable or disable the template file.

The following table lists the message for the check.

Table 3-119 Message for Granted roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ROLE_TEMPLATE_G Category: Policy Compliance	■ Windows 2003 (242248) ■ Windows 2008 (255248)	Title: Granted roles Description: The role that is granted to the account is not as per the condition that is specified in the template.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_ROLE_TEMPLATE_R Category: Policy Compliance	■ Windows 2003 (242249) ■ Windows 2008 (255249)	Title: Granted roles Description: The role that is granted to the account is not as per the condition that is specified in the template.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_ROLE_TEMPLATE_Y Category: Policy Compliance	■ Windows 2003 (242250) ■ Windows 2008 (255250)	Title: Granted roles Description: The role that is granted to the account is not as per the condition that is specified in the template.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-119 Message for Granted roles *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: WILDCARD_WITH_MANDATORY_R Category: ESM Error	■ Windows 2003 (242254) ■ Windows 2008 (255254)	Title: Incorrect wildcard template entry Description: The Mandatory option does not support wildcard characters therefore you must enter the exact text when you select the Mandatory option.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

About the Oracle Roles template

In the Oracle Roles module, the **Granted roles** check uses the Oracle Role template. The check lets you report on the roles that you specify in the template.

Creating the Oracle Roles template

You must create and enable a new Oracle Roles template before you run the **Granted roles** check.

To create an Oracle Roles template

1. In the tree view, right-click **Templates**, and then click **New**.
2. In the **Create New Template** dialog box, select **Oracle Roles - all**.
3. In the **Template file name (no extension)** text box, type new template file name.
4. After Symantec ESM adds the .ogr extension to the template file name, click **OK**.

About using the Oracle Roles template

The Oracle Roles template contains the following fields:

Table 3-120 Field and Values/Options descriptions

Field	Description	Values/Options	Wildcard support
Role	Lets you specify the role that you want the check to report on.	Enter the name of a role for the check to report on.	You can use the wildcard character '*' while specifying the role.
Grantee	Lets you specify the name of the grantee.	Enter the name of the grantee.	You can use the wildcard character '*' while specifying the grantee.
Admin option	Lets you specify the Admin option for the grantee.	Select the Admin option for the grantee. The options are as follows: ■ Yes (With Admin options) ■ No (Without Admin options) ■ Either (With/without Admin options)	NA
Required	Lets you specify whether you want ESM to report the specified privileges as mandatory or prohibited.	■ Prohibited ESM reports a message if the privilege is found on the Oracle database. ■ Mandatory ESM reports a message if the privilege is not found on the Oracle database.	NA
Comment	Lets you specify an additional comment.	NA	NA

Table 3-120 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options	Wildcard support
Severity	Lets you specify the severity for the messages that the check reports.	■ Green Select Green for an Information message. ■ Yellow Select Yellow for a Warning message. Red Select Red for an Error message.	NA
Version	Lets you specify the Oracle version for the check to report on.	Enter an Oracle version. If you do not enter an Oracle version, the check reports on all the Oracle database versions.	NA
Exclude List	Lets you display the Template Sublist Editor window when you click the Exclude List field.	■ Exclude Select the privilege or the grantee that you want to exclude for the check to report on. ■ Name Enter the name for the privilege or the grantee.	NA

Granted privileges

This check reports the privileges and the associated users and roles that violate the conditions that you specify in the template. Use the name list to enable or disable the template file.

The following table lists the message for the check.

Table 3-121 Message for Granted privileges

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: SYSTEM_PRIVILEGES_TEMPLATE_G Category: Policy Compliance	■ Windows 2003 (242251) ■ Windows 2008 (255251)	Title: Granted privileges Description: The system privileges that are granted are not as per the conditions that are specified in the template.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: SYSTEM_PRIVILEGES_TEMPLATE_R Category: Policy Compliance	■ Windows 2003 (242252) ■ Windows 2008 (255252)	Title: Granted privileges Description: The system privileges that are granted are not as per the conditions that are specified in the template.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: SYSTEM_PRIVILEGES_TEMPLATE_Y Category: Policy Compliance	■ Windows 2003 (242253) ■ Windows 2008 (255253)	Title: Granted privileges Description: The system privileges that are granted are not as per the conditions that are specified in the template.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-121 Message for Granted privileges *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: WILDCARD_WITH_MANDATORY_R Category: ESM Error	■ Windows 2003 (242254) ■ Windows 2008 (255254)	Title: Incorrect wildcard template entry Description: The Mandatory option does not support wildcard characters therefore you must enter the exact text when you select the Mandatory option.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

About the Oracle System Privileges template

In the Oracle Roles module, the **Granted privileges** check uses the Oracle System Privileges template. The check lets you report on the system privileges that you specify in the template.

Creating the Oracle System Privileges template

You must create and enable a new Oracle System Privileges template before you run the **Granted privileges** check.

To create an Oracle System Privileges template

1. In the tree view, right-click Templates, and then click New.
2. In the Create New Template dialog box, select Oracle System Privileges - all.
3. In the Template file name (no extension) text box, type new template file name.
4. After Symantec ESM adds the .osp extension to the template file name, click OK.

About using the Oracle System Privileges template

The Oracle System Privileges template contains the following fields:

Table 3-122 Field and Values/Options descriptions

Field	Description	Values/Options	Wildcard support
Privilege	Lets you specify the privilege that you want the check to report on.	Enter a privilege name for the check to report on.	You can use the wildcard character '*' while specifying the privilege.
Grantee	Lets you specify the name of the grantee.	Enter the name of the grantee.	You can use the wildcard character '*' while specifying the grantee.
Admin option	Lets you specify the Admin option for the grantee.	Select the Admin option for the grantee. The options are as follows: ■ Yes (With Admin options) ■ No (Without Admin options) ■ Either (With/without Admin options)	NA
Required	Lets you specify whether you want ESM to report the specified privileges as mandatory, prohibited, or allowed.	■ Prohibited ESM reports a message if the privilege is found on the Oracle database. ■ Mandatory ESM reports a message if the privilege is not found on the Oracle database. ■ Allowed ESM reports a message if all the privileges are not found on the Oracle database.	NA
Comment	Lets you specify an additional comment.	NA	NA

Table 3-122 Field and Values/Options descriptions *(continued)*

Field	Description	Values/Options	Wildcard support
Severity	Lets you specify the severity for the messages that the check reports.	■ Green Select Green for an Information message. ■ Yellow Select Yellow for a Warning message. Red Select Red for an Error message.	NA
Version	Lets you specify the Oracle version for the check to report on.	Enter an Oracle version. If you do not enter an Oracle version, the check reports on all the Oracle database versions.	NA
Exclude List	Lets you display the Template Sublist Editor window when you click the Exclude List field.	■ Exclude Select the privilege or the grantee that you want to exclude for the check to report on. ■ Name Enter the name for the privilege or the grantee.	NA

About the Oracle Tablespace module

This module checks for the tablespaces that are based on the options that you have specified.

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 the checks that report new, deleted, or changed information.

Automatically update snapshots

Enable this check to automatically update the snapshots with the current information.

Editing default settings

Use the check in this group to edit the default settings for all the security checks in the module.

Oracle system identifiers (SIDs)

Use the name list to include the Oracle system identifiers (SIDs) for this check. By default, the check examines all the SIDs that you specify when you configure the SymantecESMmodules for the Oracle databases. The SymantecESMmodules for Oracle Databases configuration are stored in \esm\config\oracle.dat file.

Reporting tablespaces

The checks in this group report the existing tablespaces and the tablespaces that have been added or deleted since the last snapshot update.

Tablespaces

This check reports all the tablespaces that are created in the Oracle database. On the Oracle 11g and later versions, the check also reports the encryption status of the tablespaces. Use the name list to exclude the authorized tablespaces for this check.

Symantec recommends that you periodically review the tablespaces to ensure that they are all authorized.

The following table lists the message for the check.

Table 3-123 Message for Tablespaces

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_TABLESPACE Category: System Information	■ Windows 2003 (242430) ■ Windows 2008 (255430)	Title: Oracle tablespace Description: The tablespace is defined in the database.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New tablespaces

This check reports the tablespaces that were created in the Oracle database after the last snapshot update. Use the name list to exclude the authorized tablespaces for this check.

If the addition is authorized, Symantec recommends that you either update the snapshot or delete the new tablespace.

The following table lists the message for the check.

Table 3-124 Message for New tablespaces

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ADDED_ TABLESPACE Category: Change Notification	■ Windows 2003 (242431) ■ Windows 2008 (255431)	Title: New Oracle tablespace Description: The tablespace that is reported in the Database Tablespace field was created after the last snapshot update. If the tablespace is authorized, update the snapshot. If the tablespace is not authorized, delete it.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted tablespaces

This check reports the tablespaces that were deleted from the Oracle database after the last snapshot update. Use the name list to exclude the authorized tablespaces for this check.

If the deletion is authorized, Symantec recommends that you either update the snapshot or restore the tablespace.

The following table lists the message for the check.

Table 3-125 Message for Deleted tablespaces

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DELETED_ TABLESPACE Category: Change Notification	■ Windows 2003 (242432) ■ Windows 2008 (255432)	Title: Deleted Oracle tablespace Description: The tablespace that is reported in the Database Tablespace field was deleted after the last snapshot update. If the deletion is authorized, update the snapshot. If the deletion is not authorized, restore the tablespace.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Reporting tablespace datafiles

The checks in this group report the existing datafiles and the 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 TablespacestoSkip field, specify tablespaces that are to be excluded for the check. In the Permission field, specify a permission value as a three-digit octal number. Use the name list to exclude the tablespaces for this check.

If the file permissions are less restrictive than your security policy, you must specify a permission value for the datafile that matches with your security policy. Periodically, you must review the tablespace datafiles to ensure that they are authorized and that the file permissions match with your security policy.

The following table lists the messages for the check.

Tablespace datafiles

This check reports the locations of all the tablespace datafiles and lists all the Operating system accounts that have permissions on the file. Use the name list to exclude the tablespaces for this check.

If the file permissions are less restrictive than your security policy, you must specify a permission value for the datafile that matches with your security policy. Periodically, you must review the tablespace datafiles to ensure that they are authorized and that the file permissions match with your security policy.

The following table lists the messages for the check.

Table 3-126 Messages for Tablespace datafiles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DATAFILE Category: System Information	■ Windows 2003 (242433) ■ Windows 2008 (255433)	Title: Tablespace file Description: The tablespace datafile is reported in the Tablespace Datafile field.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_FILE_LOCKED Category: System Error	■ Windows 30008	Title:Locked Oracle file File permissions cannot be reported because the file is being used by another process.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [""]

Table 3-126 Messages for Tablespace datafiles *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_FILE_NOT_FOUND Category: System Error	■ Windows 30009	Title: Oracle File or folder not found Description: File permissions cannot be reported because the file being referenced cannot be found.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [""]
String ID: ORA_DIRECTORY_PERMS Category: System Error	■ Windows 30010	Title: Oracle Folder permissions Description: Reports Directory permissions.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ORA_NOT_SUPPORTED Category: System Information	■ Windows 30011	Title: Functionality not Supported Description: This functionality is not supported by ESM oracle app module.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-126 Messages for Tablespace datafiles *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
ORA_ASM_DATAFILE Category: System Information	■ Windows (41)	Title: Tablespace file Description: The ASM managed tablespace datafile is reported in the Tablespace Datafile field.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New tablespace datafiles

This check reports the datafiles that were added to tablespaces after the last snapshot update. Use the name list to exclude the tablespaces for this check.

If the change is authorized, Symantec recommends that you either update the snapshot or drop the datafile from the tablespace.

The following table lists the message for the check.

Table 3-127 Message for New tablespace datafiles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_ADDED_ DATAFILE Category: Change Notification	■ Windows 2003 (242434) ■ Windows 2008 (255434)	Title: New tablespace datafile Description: The tablespace datafile that is reported in the Tablespace Datafile field was added to the tablespace after the last snapshot update. If the addition is authorized, update the snapshot. If the addition is not authorized, drop the datafile from the tablespace.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted tablespace datafiles

This check works with the New tablespace datafiles check and reports the datafiles that were deleted after the last snapshot update. Use the name list to exclude the tablespaces for this check.

If the deletion is authorized, Symantec recommends that you either update the snapshot or restore the datafile.

The following table lists the message for the check.

Table 3-128 Message for Deleted tablespace datafiles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_DELETED_ DATAFILE Category: Change Notification	■ Windows 2003 (242435) ■ Windows 2008 (255435)	Title: Deleted tablespace datafile Description: The tablespace datafile that is reported in the Tablespace Datafile field was dropped from the reported tablespace after the last snapshot update. If the deletion is authorized, update the snapshot. If the deletion is not authorized, restore the datafile to the tablespace.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Reporting SYSTEM tablespace information

The checks in this group 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. Use the name list to exclude users (owners) for this check.

Symantec recommends that you ensure only authorized objects reside in the SYSTEM tablespace.

The following table lists the message for the check.

Table 3-129 Message for Object in SYSTEM tablespace

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_TAB_IN_ SYS_TABLESPACE Category: Policy Compliance	■ Windows 2003 (242436) ■ Windows 2008 (255436)	Title: Object in SYSTEM tablespace Description: The object that is reported in the Tablespace Object field is in the SYSTEM tablespace. Drop the object or move it to an authorized tablespace.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SYSTEM tablespace assigned to user

This check reports the users whose default or temporary tablespaces are the SYSTEM tablespace. Use the name list to exclude users for this check.

Symantec recommends that you ensure only authorized objects reside in the SYSTEM tablespace.

The following table lists the message for the check.

Table 3-130 Message for SYSTEM tablespace assigned to user

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_USER_ USING_SYS_ TABLESPACE Category: Policy Compliance	■ Windows 2003 (242437) ■ Windows 2008 (255437)	Title: SYSTEM tablespace assigned to user Description: The user that is reported in the User field uses the SYSTEM tablespace as a default or temporary tablespace. Drop the user or change the user's tablespace.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Reporting DBA tablespace quotas

The checks in this group report violations of MAX_BYTES and MAX_BLOCKS tablespace quotas.

Oracle tablespaces

Use the name list to include or exclude the tables for the You can use this option to specify tables for the MAX_BYTES in DBA_TS_QUOTAS and MAX_BLOCKS in DBA_TS_QUOTAS checks.

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. Use the name list to exclude any authorized users for this check.

Symantec recommends that you drop the user or change the user's MAX_BYTES setting for the tablespace.

The following table lists the message for the check.

Table 3-131 Message for MAX_BYTES in DBA_TS_QUOTAS

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_MAX_ BYTES_QUOTA Category: Policy Compliance	■ Windows 2003 (242438) ■ Windows 2008 (255438)	Title: MAX_BYTES per tablespace exceeded Description: The user exceeds the maximum number of MAX_BYTES in DBA_TS_QUOTAS for the tablespace that is reported in the Info field. Drop the user or change the user's MAX_BYTES setting for the reported tablespace.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

MAX_BLOCKS in DBA_TS_QUOTAS

This check reports users with resource rights to tablespaces whoseMAX_BLOCKS values exceed the value that you specify in the check. For an unlimited number of bytes, specify -1 in the MAX_BLOCKS field. Use the name list to exclude any authorized users for this check.

Symantec recommends that you drop the user or change the user's MAX_BLOCKS setting for the tablespace.

The following table lists the message for the check.

Table 3-132 Message for MAX_BLOCKS in DBA_TS_QUOTAS

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ORA_MAX_ BLOCKS_QUOTA Category: Policy Compliance	■ Windows 2003 (242439) ■ Windows 2008 (255439)	Title: MAX_BLOCKS per tablespace exceeded Description: The user exceeds the maximum number of MAX_BLOCKS in DBA_TS_QUOTAS for the tablespace that is reported in the Info field. Drop the user or change the user's MAX_BLOCKS setting for the reported tablespace.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]