Symantec™ Enterprise Security Manager Oracle Database Modules Installation Guide

Version 5.4

Symantec

Symantec™ Enterprise Security Manager Oracle Database Modules Installation Guide

Documentation version: 5.4

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product 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, DVDs, 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

Technical Support 4

Chapter 1 Installing ESM Oracle Modules on Windows 10

Before you install 10
Minimum account privileges 11
About ESM interface 13
System requirements 13
About using parameters in the oraenv.dat file 15
Installing the ESM modules for Oracle databases 18
About content separation 19
About the content package folder structure 20
Installing the security content on the ESM managers 20
Modifying the importcontent.conf file 22
About the importcontent utility 22
Using the importcontent utility 23
Examples of using the importcontent utility 24
Silently installing the ESM modules for Oracle databases 24
About Oracle account creation scripts 26
Script for creating a user on Oracle 10.0 or later versions 27
Script for assigning system privileges to the user on Oracle 10.0 or later versions 28

Chapter 2 Configuring ESM Oracle Modules on Windows 29

Adding configuration records to enable the ESM security checking for the Oracle database 29
About configuring SIDs 33

Chapter 3 Uninstalling ESM Oracle Modules on Windows 36

Uninstalling the Oracle Application module 36
How to run the uninstallation program 37
About the uninstallation logs 38
Silently uninstalling the ESM modules for Oracle Databases 38

Chapter 4 Installing ESM Oracle modules on UNIX 40

Before you install 40
Minimum account privileges 41
About Oracle client libraries 43
System requirements 43
About using parameters in the oraenv.dat file 45
Installing the ESM modules for Oracle databases 48
About Content Separation 49
About the content package folder structure 50
Installing the security content on the ESM managers 50
Modifying the importcontent.conf file 52
About the importcontent utility 52
Using the importcontent utility 53
Examples of using the importcontent utility 54
Silently installing the ESM modules for Oracle databases 55
About using an alternate account 57
About Oracle account creation scripts 57
Script for creating a user on Oracle 11.0 or later versions 58
Script for assigning system privileges to the user on Oracle 11.0 or later versions 59

Chapter 5 Configuring ESM Oracle modules on UNIX 60

Adding configuration records 60
About configuring SIDs 64

Chapter 6 Uninstalling ESM Oracle modules on UNIX 69

Uninstalling the Oracle Application module 69
How to run the uninstallation program 70
About the uninstallation logs 71
Silently uninstalling the ESM modules for Oracle Databases 71

Chapter 7 About the logging functionality on the Oracle database modules on Windows 73

About the log levels of the messages 73
Creating the configuration file 75
Parameters of the configuration file 75
About the log file 76
Format of the log file 77
About the backup of logs 77

Chapter 8 About the logging functionality on the Oracle database modules on UNIX 78

About the log levels of the messages 78
Creating the configuration file 80
Parameters of the configuration file 80
About the log file 81
Format of the log file 82
About the backup of logs 82

Chapter 1

Installing ESM Oracle Modules on Windows

This chapter includes the following topics:

- Before you install
- Minimum account privileges
- About ESM interface
- System requirements
- About using parameters in the oraenv.dat file
- Installing the ESM modules for Oracle databases
- About content separation
- Silently installing the ESM modules for Oracle databases
- About Oracle account creation scripts

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

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

Oracle version	System privileges	Object privileges
10.x, 11.x, 12.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.dba_db_links ■ sys.registry$history ■ sys.user$ ■ v$controlfile ■ v$instance ■ v$logfile ■ v$parameter ■ v$version ■ v$database

Table 1-2 lists the minimum privileges that are assigned to the ESMDBA account if the database instance is configured by using “SYSTEM”:

Table 1-2 Minimum account privileges assigned to the ESMDBA

Oracle version	System privileges	Object privileges
10.x, 11.x, 12.x	■ Create session ■ Select any Dictionary	N/A

Note: When a database instance is configured in the context of a SYSTEM User, the Select any Dictionary system privilege is assigned to the ESMDBA account. However, in Oracle version 12c, the Select any Dictionary privilege does not include the Select privilege on the user$ table. As a result, the ESM Oracle Passwords module checks do not report the guessed password data.. Therefore, for successful data collection on the Passwords module, the Oracle Database Admin must grant the Select privilege on the user$ table to the ESMDBA account manually.

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

Table 1-3 Roles that can be assigned to a pre-created account

Oracle version	System roles
10.x, 11.x, 12.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 can 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 ESM interface

The following section gives the ESM interface that ESM Oracle Application modules refer to:

Windows	When a 32-bit Oracle setup is installed on a 64-bit operating system, the orainterface32.exe is used to communicate with the 32-bit Oracle.

System requirements

Table 1-4 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 1-4 Supported operating systems for ESM modules on Oracle

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

Table 1-4 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
	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, 12.1.0.1.0, 12.1.0.2.0	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, 12.1.0.1.0, 12.1.0.2.0	32-bit, 64-bit

Table 1-5 lists the Real Application Clustering (RAC) support on Windows.

Table 1-5 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
Windows (64-bit)	64-bit	Windows 2008	12.1.0.1.0, 12.1.0.2.0

Table 1-6 lists the disk space requirements only for the Symantec ESM Modules for Oracle Databases and not for the ESM agents.

Table 1-6 Disk space requirements

Agent operating system	Disk space
Windows 2003 (32-bit)	25 MB

Table 1-6 Disk space requirements *(continued)*

Agent operating system	Disk space
Windows 2003 (64-bit)	40 MB
Windows 2008 (32-bit)	25 MB
Windows 2008 (64-bit)	40 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 1-7 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 1-7 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 1-7 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 4-1 on page 41. 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 4-2 on page 42.	set MinPrivilege YES

See "Installing the ESM modules for Oracle databases" on page 48.

Installing the ESM modules for Oracle databases

The installation program does the following:

- Extracts and installs the module executables.
- Registers the module binaries to the ESM manager.
- 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 4-3 on page 42.

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.

About content separation

Until now, the content that was included in an Application module was first installed on the agents and later through the registration process it was pushed from the ESM agents to the ESM manager.

From this release onwards, two separate content packages are included. The package that contains the module binaries is to be installed on the ESM agent and the other package that contains the security content such as configuration (.m) files, word files, template files, properties files, and report content files (RDL) is to be installed on the ESM managers. A new folder named, **Content** is created on the ESM manager that contains platform-specific data, which the importcontent utility imports.

Note: You are required to run the **esmoraclecontenttpi.exe** installer on the new manager. For the consecutive releases, perform a LiveUpdate to get the latest security content.

About the content package folder structure

The content package folder on the ESM manager contains content files of the Applications modules.

Table 1-8 shows the file types and folder paths of the Application modules.

Table 1-8 File types and folder paths

Content	File type	Folder path
Application modules	.properties files	#esm/content/<AppModuleName>/<platform>/config/
	Security module(.m) files	#esm/content/<AppModuleName>/<platform>/register/
	Template files	#esm/content/<AppModuleName>/<platform>/template/
Common	Word files	#esm/content/words/
Common	Report content file(UpdatePackage.rdl)	#esm/content/ble/<SU_version>/<language>/

Installing the security content on the ESM managers

You can install the security content package on the ESM manager by using the **esmoraclecontenttpi.exe** installer, which is applicable for Windows.

The installation program extracts and installs configuration (.m) files, template files, word files, .properties files, and report content files (RDL).

To install the security content on the ESM managers

1. Download and copy the **esmoraclecontenttpi.exe** installer 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.

Note: Before importing the content data for the Application modules, you must ensure t hat content data for a Security Update (SU) is present on the manager database. Certain features of the Application modules may not function correctly if the Se curity Update (SU) content data is not already imported to the manager database.

3. The **Do you want to import the templates or the .m files? [no]** message appears. Do one of the following:
   - Type a **Y**, if you want to import the templates or the .m files.

     Note:

     Only an ESM administrator or any ESM user that have the permissions to create policies, create templates, and perform remote installation or upgrade can install the content on the ESM manager. The ESM superuser can also install content on the ESM manager as this user has all the permissions. However Register only users cannot perform this task as they do not have the specified permissions.

     The program displays a message to include or exclude the platforms that you want to import. See "Modifying the importcontent.conf file" on page 22.
   - Type an **N**, if you do not want to import the templates or the .m files. You can skip this step if you want to import the content later. You can import the content by running the importcontent utility.
4. Enter the ESM manager that the agent is registered to.

   Usually, it is the name or the IP of the computer that the manager is installed on.
5. Enter the ESM access name (logon name) for the manager.
6. Enter the ESM password that is used to log on to the ESM manager.

7 Enter the port that is used to contact the ESM Manager. The default port is 5600.

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

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

9 The **Do you want to import the report content file <UpdatePackage.rdl>? [yes]** message appears. Do the following:

- Type a **Y**, if you want to import the report content file.
- Type an **N**, if you do not want to import the report content file.

When the installation completes, you are prompted to exit.

Modifying the importcontent.conf file

The platforms that you specify in the importcontent.conf file are the platforms that are available to the ESM manager when using the importcontent utility. The importcontent utility only imports the platforms on the ESM manager that are not prefixed with a hash (#).

To modify the importcontent.conf file

1 Go to C:\Program Files\Symantec\Enterprise Security Manager\ESM\config\importcontent.conf.

2 Remove # before the platform that you want to include.

3 Save the file.

4 Go back to esmoraclecontenttpi.exe installer and press <return> to continue with the installation process.

About the importcontent utility

Importcontent utility is a command line utility, used to import the ESM content - Oracle Application modules information to the specified manager. The utility displays the content version on the GUI or on the CLI. The utility is located in the bin folder of the installation directory, along with other ESM Manager binaries in platform-specific folders.

For example,

C:\Program Files\Symantec\Enterprise Security Manager\ESM\ bin\w3s-ix86\importcontent.exe

Note: If the importcontent.exe is not found on the manager, then Content TPI package deploys the importcontent.exe in the bin folder.

Using the importcontent utility

You can use the importcontent utility on Windows and Solaris platforms. The utility provides the option of importing security module (.m) files, property (.properties) files, template files, word (.wrd) files, and report content (UpdatePackage.rdl) files for ESM Oracle Application modules. You can use the -f option to force import content related information at a later stage.

Pre-requisites for using the importcontent utility:

- You must be in the role of ESM administrator.
- You must have ESM manager installed on the computer on which you are running the importcontent utility.

To use the importcontent utility

1. Install the ESM Manager and Agent using the ESM Suite Installer.
2. At the Windows command prompt, navigate to the platform-specific bin folder, where the importcontent utility is located.
3. Type the following command:

```
importcontent [-RLrnvfW] [-m manager] [-U user] [-P password] [-p
port] [-L app_module_name1, app_module_name2,...] [-a |
module_config_file1 [module_config_file2... ]]
```

The switch options that can be used with the importcontent utility are listed below.

-m	Manager name - the local manager name is used by default.
-U	User name - the ESM user name is used by default.
-P	Password - the ESM user account password.
-p	TCP port number - the port number is 5600 by default.
-a	Import and register all security module (.m) files with the manager.
-R	Import property files (.properties)
-T	Import all templates
-r	Import report content file (UpdatePackage.rdl)
-W	Import word files

-n	Synchronize policies
-f	Force the import of security module information
-h	Write C include file for security module compilation **Note:** -h, and -M options can be used only with the -a option.
-M	Write VMS macro file for security module compilation **Note:** -h, and -M options can be used only with the -a option.
-v	Set verbose mode, log each action as it is performed.
-F	Log the program finish.

Examples of using the importcontent utility

The following examples are provided for using the importcontent utility:

- To access the help menu for the importcontent utility, type the following command:
  ```
  importcontent
  ```
- To import Oracle Applcation modules type the following command:
  ```
  importcontent -L oracle -U <user1> -P <pwd123> -m <managerXYZ>
  ```

  Note: The utility requires the application module names to be similar to the folder names created in the <install dir>\ content directory.

- To import templates for Oracle, type the following command:
  ```
  importcontent -T -L oracle -U <user1> -P <pwd123> -m <managerXYZ>
  ```
- To synchronize policies, type the following command:
  ```
  importcontent -nv -U <user1> -P <pwd123> -m <managerXYZ> -U <user1>
  -P <pwd123>
  ```
- To register specific .m files with the manager, type the following command:
  ```
  importcontent -U <user1> -P <pwd123> -m <managerXYZ>
  C:\Symantec\ESM\account.m D:\ESM\acctinfo.m E:\abc.m xyz.m
  ```

Silently installing the ESM modules for Oracle databases

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

Table 1-9 lists the command line options for silently installing the ESM modules for Oracle.

Table 1-9 Options to silently install the ESM modules for Oracle databases

Option	Description
-d	Display the description and contents of the tune-up package.
-i	Install the tune-up installation package on your computer.
-U	Lets you enter the ESM access record name.
-P	Lets you enter the ESM access record password.
-p	Lets you enter the TCP Port to connect to the ESM manager.
-m	Lets you enter the name of the ESM manager.
-t	Lets you connect to the manager through TCP.
-x	Lets you connect to the manager through IPX (applicable only on Windows).
-g	Lets you enter the name of the agent that you want to use for re-registration.
-K	Does not prompt or re-register.
-A	Lets you enter the Oracle logon user and configure all SIDs. If "SYSTEM" user is specified as Oracle logon user then use -C option to enter SYSTEM user password. If "oracle_owner" is specified as Oracle logon user then do not specify the -C option as the installation program detects the oracle owner and creates an ESMDBA user by using "/as sysdba."
-C	Lets you enter the password for the SYSTEM user. The installation program ignores this option if the specified user is not SYSTEM.
-T	Lets you enter the Temporary tablespace of the ESMDBA user. This is optional. If the temporary tablespace of the ESMDBA user is not specified, the installation program takes "TEMP" as the default value.
-S	Lets you enter the Default tablespace of the ESMDBA user. This is optional. If the default tablespace of the ESMDBA user is not specified, the installation program takes "TEMP" as the default value.

Table 1-9 Options to silently install the ESM modules for Oracle databases *(continued)*

Option	Description
-W	Lets you enter the Profile of the ESMDBA user. This is optional. If the profile of the ESMDBA user is not specified, the installation program takes "USERS" as the default value.
-h	Display help on the usage of options that can be used for silent installation.
-e	Does not execute the before and after executables (installation without configuration.)

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} {-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} {-A} {-C} [-T] [-S] [-W]`
  The configuration log file `EsmOraConfig.log` is created in the `\esm\system\<system name>` folder.

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;
```

```
GRANT SELECT on sys.dba_db_links 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 4-3 on page 42.

Chapter 2

Configuring ESM Oracle Modules on Windows

This chapter includes the following topics:

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

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 30.
To connect by entering the pre-created account,
See "To add security checking using a pre-created account" on page 31.

- Type a **B** to connect using the "/as sysdba" method.
  See "To configure Oracle SID by using the /as sysdba method" on page 31.

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 tablespace for ESMDBA user
-S {TblSpace}	Oracle DEFAULT tablespace 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.

Table 2-1 lists the SID configuration options.

Table 2-1 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}`
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`

Table 2-1 SID configuration options *(continued)*

To do this	Type
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>`
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 2-2 lists the Silent SID configuration options.

Table 2-2 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`

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

To do this	Type
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`
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`

Note: You cannot use pre-created accounts when you perform a silent configuration of the module with the -a ALL option.

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.

Chapter 3

Uninstalling ESM Oracle Modules on Windows

This chapter includes the following topics:

- Uninstalling the Oracle Application module
- Silently uninstalling the ESM modules for Oracle Databases

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
- Configuration files
  - Environment configuration files
  - Configuration file with server records
- Snapshot files
- 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.

Silently uninstalling the ESM modules for Oracle Databases

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

Table 3-1 lists the command line options for silently uninstalling the ESM modules for Oracle.

Table 3-1 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.

Table 3-1 Options to silently uninstall the ESM modules for Oracle Databases *(continued)*

Option	Description
-mfile	Specify to create a file that contains name and credentials of one or multiple managers that the agent is registered to.
-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}]`

Chapter 4

Installing ESM Oracle modules on UNIX

This chapter includes the following topics:

- Before you install
- Minimum account privileges
- About Oracle client libraries
- System requirements
- About using parameters in the oraenv.dat file
- Installing the ESM modules for Oracle databases
- About Content Separation
- Silently installing the ESM modules for Oracle databases
- About using an alternate account
- About Oracle account creation scripts

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 4-1 lists the minimum privileges that are assigned to the ESMDBA account if the database instance is configured by using "/ as sysdba".

Table 4-1 Minimum account privileges assigned to the ESMDBA account

Oracle version	System privileges	Object privileges
11.x, 12.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.dba_db_links ■ sys.registry$history ■ sys.user$ ■ v$controlfile ■ v$instance ■ v$logfile ■ v$parameter ■ v$version ■ v$database

Table 4-2 lists the minimum privileges that are assigned to the ESMDBA account if the database instance is configured by using “SYSTEM”:

Table 4-2 Minimum account privileges assigned to the ESMDBA

Oracle version	System privileges	Object privileges
11.x, 12.x	■ Create session ■ Select any Dictionary	N/A

Note: When a database instance is configured in the context of a SYSTEM User, the Select any Dictionary system privilege is assigned to the ESMDBA account. However, in Oracle version 12c, the Select any Dictionary privilege does not include the Select privilege on the user$ table. As a result, the ESM Oracle Passwords module checks do not report the guessed password data.. Therefore, for successful data collection on the Passwords module, the Oracle Database Admin must grant the Select privilege on the user$ table to the ESMDBA account manually.

Table 4-3 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 4-1 . To assign system privileges, refer to Table 4-2. To assign minimum privileges, refer to Table 4-3.

Table 4-3 Roles that can be assigned to a pre-created account

Oracle version	System roles
11.x, 12.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 can 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 client libraries

The following section gives the Oracle client libraries that ESM Oracle Application modules refer to:

AIX-PPC64 and HPUX-IA64	The ESM Oracle application module for AIX-PPC64 and HPUX-IA64 is a 64-bit module and uses a 64-bit Oracle client library to connect to the 64-bit Oracle installations. ESM searches for 64-bit library in ORACLE_HOME/lib and if it is unable to find the library, then the configuration fails.
LNX-X86 , SOLARIS-SPARC, and HPUX-HPPA	The ESM Oracle Application module for LNX-X86 , SOLARIS-SPARC, and HPUX-HPPA is a 32-bit module and uses either of the following libraries: ■ A 32-bit Oracle client library to connect to the 32-bit Oracle installation. ■ A 64-bit Oracle client library to connect to the 64-bit Oracle installation by using orainterface64. ESM searches for a 32-bit library in ORACLE_HOME/lib, if it is unable to find this library, it uses the orainterface64 to connect to the 64-bit Oracle installation. In this case, it searches for a 64-bit library in ORACLE_HOME/lib and if it is unable to find the library, then the configuration fails.

System requirements

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

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 4-4 Supported operating systems for ESM modules on Oracle

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

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

Operating System				ESM Module	Oracle		
AIX	PPC64	64-bit	5.3	64-bit	11.1.0.6.0, 11.2.0.1.0	64-bit	64-bit
	PPC64	64-bit	6.1	64-bit	11.1.0.6.0, 11.2.0.1.0, 12.1.0.1.0, 12.1.0.2.0	64-bit	64-bit
	PPC64	64-bit	7.1	64-bit	11.1.0.6.0, 11.2.0.1.0, 12.1.0.1.0, 12.1.0.2.0	64-bit	64-bit
HP-UX	PARISC	64-bit	11.11	32-bit	11.2.0.1.0	64-bit	64-bit
	PARISC	64-bit	11.23	32-bit	11.2.0.1.0	64-bit	64-bit
	IA64	64-bit	11.23	64-bit	11.1.0.6.0, 11.2.0.1.0	64-bit	64-bit
	PARISC	64-bit	11.31	32-bit	11.1.0.6.0, 11.2.0.1.0, 12.1.0.1.0, 12.1.0.2.0	64-bit	64-bit
	IA64	64-bit	11.31	64-bit	11.1.0.6.0, 11.2.0.1.0, 12.1.0.1.0, 12.1.0.2.0	64-bit	64-bit
Solaris	SPARC	64-bit	2.9	32-bit	11.1.0.6.0, 11.2.0.1.0	64-bit	64-bit
	SPARC	64-bit	2.10	32-bit	11.1.0.6.0, 11.2.0.1.0, 12.1.0.1.0, 12.1.0.2.0	64-bit	64-bit
RHEL	x86	32-bit	ES 4	32-bit	11.1.0.6.0, 11.2.0.1.0	32-bit	32-bit
	x86_64	x86_64	5.x, 6.x	32-bit	11.1.0.6.0, 11.2.0.1.0, 12.1.0.1.0, 12.1.0.2.0	x86_64	x86_64

Table 4-5 lists the Real Application Clustering (RAC) support on UNIX.

Table 4-5 Real Application Clustering (RAC) support on UNIX

Supported operating systems	Architecture	Supported OS versions	Supported Oracle versions
AIX	PPC64	6.1, 7.1	11.2.0.1, 12.1.0.1.0, 12.1.0.2.0
HP-UX	PARISC	11.23, 11.31	11.1.0.6.0
HP-UX	IA64	11.31	11.1.0.6.0, 12.1.0.1.0, 12.1.0.2.0
Solaris	SPARC	2.10	11.1.0.6.0, 12.1.0.1.0, 12.1.0.2.0
Red Hat Enterprise Linux	x86	4	11.2.0.1
Red Hat Enterprise Linux	x86_64	5, 6	11.2.0.1, 12.1.0.1.0, 12.1.0.2.0

Table 4-6 lists the disk space requirements only for the Symantec ESM Modules for Oracle Databases and not for the ESM agents.

Table 4-6 Disk space requirements

Agent operating system	Disk space
AIX (PPC64)	110 MB
HP-UX (PARISC)	65 MB
HP-UX (IA64)	75 MB
Solaris (SPARC)	35 MB
Red Hat Enterprise Linux (x86)	35 MB
Red Hat Enterprise Linux (x86_64)	35 MB

About using parameters in the oraenv.dat file

This table lists the different parameters that you can use in the oraenv.datfile 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 4-7 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
SHELL	You can set an environment variable during an ESM Oracle module policy run.	You can set the SHELL environment variable by adding the set SHELL /bin/bash entry in the oraenv.dat file.	set SHELL /bin/bash
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

Table 4-7 Parameters and their usage *(continued)*

Parameter name	Description	Parameter value	Example
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
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 4-7 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 4-1 on page 41. 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 4-2 on page 42.	set MinPrivilege YES

See "Installing the ESM modules for Oracle databases" on page 48.

Installing the ESM modules for Oracle databases

The installation program does the following:

- Extracts and installs the module executables.
- Registers the module binaries to the ESM manager.
- Launches the esmorasetup executable 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 or ESMDBA_<hostname> 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.datfile. 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 4-3 on page 42.

During the policy runs, the ESMDBA or ESMDBA_<hostname> 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.

About Content Separation

Until now, the content that was included in an Application module was first installed on the agents and later through the registration process it was pushed from the ESM agents to the ESM manager.

From this release onwards, two separate content packages are included. The package that contains the module binaries is to be installed on the ESM agent and the other package that contains the security content such as configuration (.m) files, word files, template files, properties files, and report content files (RDL) is to be installed on the ESM managers. A new folder named, **Content** is created on the ESM manager that contains platform-specific data, which the importcontent utility imports.

Note: You are required to run the esmoraclecontent.tpi installer on the new manager. For the consecutive releases, perform a LiveUpdate to get the latest security content.

About the content package folder structure

The content package folder on the ESM manager contains content files of the Applications modules.

Table 4-8 shows the file types and folder paths of the Application modules.

Table 4-8 File types and folder paths

Content	File type	Folder path
Application modules	.properties files	#esm/content/<AppModuleName>/<platform>/config/
	Security module(.m) files	#esm/content/<AppModuleName>/<platform>/register/
	Template files	#esm/content/<AppModuleName>/<platform>/template/
Common	Word files	#esm/content/words/
Common	Report content file(UpdatePackage.rdl)	#esm/content/ble/<SU_version>/<language>/

Installing the security content on the ESM managers

You can install the security content package on the ESM manager by using the **esmoraclecontent.tpi** installer, which is applicable for UNIX.

The installation program extracts and installs configuration (.m) files, template files, word files, .properties files, and report content files (RDL).

To install the security content on the ESM managers

1 Download and copy the **esmoraclecontent.tpi** installer 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.

Note: Before importing the content data for the Application modules, you must ensure that content data for a Security Update (SU) is present on the manager database. Certain features of the Application modules may not function correctly if the Se curity Update (SU) content data is not already imported to the manager database.

3 The **Do you want to import the templates or the .m files? [no]** message appears. Do one of the following:

- Type a **Y**, if you want to import the templates or the .m files.

  Note:

  Only an ESM administrator or any ESM user that have the permissions to create policies, create templates, and perform remote installation or upgrade can install the content on the ESM manager. The ESM superuser can also install content on the ESM manager as this user has all the permissions. However Register only users cannot perform this task as they do not have the specified permissions.

  The program displays a message to include or exclude the platforms that you want to import. See "Modifying the importcontent.conf file" on page 52.

- Type an **N**, if you do not want to import the templates or the .m files. You can skip this step if you want to import the content later. You can import the content by running the importcontent utility.

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

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

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

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

7 Enter the port that is used to contact the ESM Manager. The default port is 5600.

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

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

9 The **Do you want to import the report content file <UpdatePackage.rdl>? [yes]** message appears. Do the following:

- Type a **Y**, if you want to import the report content file.
- Type an **N**, if you do not want to import the report content file.

When the installation completes, you are prompted to exit.

Modifying the importcontent.conf file

The platforms that you specify in the importcontent.conf file are the platforms that are available to the ESM manager when using the importcontent utility. The importcontent utility only imports the platforms on the ESM manager that are not prefixed with a hash (#).

To modify the importcontent.conf file

1 Go to C:\Program Files\Symantec\Enterprise Security Manager\ESM\config\importcontent.conf.

2 Remove # before the platform that you want to include.

Note: As, the UNIX folder contains common content for all UNIX sub platforms, a semi-colon (;) separates these sub-platforms from UNIX. For example: lnx-x86;unix.

---

3 Save the file.

4 Go back to **esmoraclecontenttpi.exe** installer and press <return> to continue with the installation process.

About the importcontent utility

Importcontent utility is a command line utility, used to import the ESM content - Oracle application modules information to the specified manager. The utility displays the content version on the GUI or on the CLI. The utility is located in the bin folder of the installation directory, along with other ESM Manager binaries in platform-specific folders.

For example:

esm/ bin/solaris-sparc/importcontent

Note: If the importcontent.exe is not found on the manager, then Content TPI package deploys the importcontent.exe in the bin folder.

Using the importcontent utility

You can use the importcontent utility on Windows and Solaris platforms. The utility provides the option of importing security module (.m) files, property (.properties) files, template files, word (.wrd) files, and report content (UpdatePackage.rdl) files for the ESM Oracle application modules . You can use the -f option to force import content related information at a later stage.

Pre-requisites for using the importcontent utility:

- You must be in the role of ESM administrator.
- You must have ESM manager installed on the computer on which you are running the importcontent utility.

To use the importcontent utility

1. Install the ESM Manager and Agent using the ESM Suite Installer.
2. At the Windows command prompt, navigate to the platform-specific bin folder, where the inportcontent utility is located.
3. Type the following command:

```
importcontent [-RLrnvfW] [-m manager] [-U user] [-P password] [-p
port] [-L app_module_name1, app_module_name2,...] [-a |
module_config_file1 [module_config_file2... ]]
```

The switch options that can be used with the importcontent utility are listed below.

-m	Manager name - the local manager name is used by default.
-U	User name - the ESM user name is used by default.
-P	Password - the ESM user account password.
-p	TCP port number - the port number is 5600 by default.
-a	Import and register all security module (.m) files with the manager.
-R	Import property files (.properties)

-T	Import all templates
-r	Import report content file (UpdatePackage.rdl)
-W	Import word files
-n	Synchronize policies
-f	Force the import of security module information
-h	Write C include file for security module compilation **Note:** -h, and -M options can be used only with the -a option.
-M	Write VMS macro file for security module compilation **Note:** -h, and -M options can be used only with the -a option.
-v	Set verbose mode, log each action as it is performed.
-F	Log the program finish.

Examples of using the importcontent utility

The following examples are provided for using the importcontent utility:

- To access the help menu for the importcontent utility, type the following command:
  ```
  importcontent
  ```
- To import the Oracle application module type the following command:
  ```
  importcontent -L oracle -U <user1> -P <pwd123> -m <managerXYZ>
  ```

  Note: The utility requires the application module names to be similar to the folder names created in the <install dir>\ content directory.

- To import templates for Oracle, type the following command:
  ```
  importcontent -T -L oracle -U <user1> -P <pwd123> -m <managerXYZ>
  ```
- To synchronize policies, type the following command:
  ```
  importcontent -nv -U <user1> -P <pwd123> -m <managerXYZ> -U <user1>
  -P <pwd123>
  ```
- To register specific .m files with the manager, type the following command:
  ```
  importcontent -U <user1> -P <pwd123> -m <managerXYZ>
  C:\Symantec\ESM\account.m D:\ESM\acctinfo.m E:\abc.m xyz.m
  ```

Silently installing the ESM modules for Oracle databases

You can silently install the ESM Modules for Oracle by using the esmora.tpi.

Table 4-9 lists the command line options for silently installing the ESM modules for Oracle.

Table 4-9 Options to silently install the ESM modules for Oracle databases

Option	Description
-d	Display the description and contents of the tune-up package.
-i	Install the tune-up installation package on your computer.
-U	Lets you enter the ESM access record name.
-P	Lets you enter the ESM access record password.
-p	Lets you enter the TCP Port to connect to the ESM manager.
-m	Lets you enter the name of the ESM manager.
-t	Lets you connect to the manager through TCP.
-x	Lets you connect to the manager through IPX (applicable only on Windows).
-g	Lets you enter the name of the agent that you want to use for re-registration.
-K	Does not prompt or re-register.
-A	Lets you enter the Oracle logon user and configure all SIDs. If "SYSTEM" user is specified as Oracle logon user then use -C option to enter SYSTEM user password. If "oracle_owner" is specified as Oracle logon user then do not specify the -C option as the installation program detects the oracle owner and creates an ESMDBA user by using "/as sysdba."
-C	Lets you enter the password for the SYSTEM user. The installation program ignores this option if the specified user is not SYSTEM.

Table 4-9 Options to silently install the ESM modules for Oracle databases *(continued)*

Option	Description
-T	Lets you enter the Temporary tablespace of the ESMDBA user. This is optional. If the temporary tablespace of the ESMDBA user is not specified, the installation program takes "TEMP" as the default value.
-S	Lets you enter the Default tablespace of the ESMDBA user. This is optional. If the default tablespace of the ESMDBA user is not specified, the installation program takes "TEMP" as the default value.
-W	Lets you enter the Profile of the ESMDBA user. This is optional. If the profile of the ESMDBA user is not specified, the installation program takes "USERS" as the default value.
-h	Display help on the usage of options that can be used for silent installation.
-e	Does not execute the before and after executables (installation without configuration.)

To install the ESM modules for Oracle silently:

- Copy the .tpi 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:
  `./esmora.tpi {-it} {-m} {-U} {-p} {-P} {-g} {-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:
  `./esmora.tpi {-it} {-m} {-U} {-p} {-P} {-g} {-A} {-C} [-T] [-S] [-W]`

To install the ESM modules for Oracle and silently configure without providing the password string at the command prompt:

- You can use the shell parameters instead of the actual password strings. Type the following at the command prompt:
  - `export ESMPASS = <esm-password>`
  - export ESMORAPASS = <oracle-account-password>

- If you use the shell parameters during installation and configuration, you do not have to provide the password options. Type the following at the command prompt:
  - `./esmorasetup -a {SID} -A Pre-created account`
  - `./esmora.tpi –it –{-m} {-U} {-p} {-g} {-Y} {-A}`

Note: The configuration log file, EsmOraConfig.log is created in the <esm_install_dir>/ system/<system name> folder.

About using an alternate account

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

An alternate method "/as sysdba" has been introduced in the ESM modules for Oracle version 2.7 onwards. Using the "/as sysdba" method, a user can log on to the Oracle server without providing a user name and password, and configure all SIDs.

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

To use the alternate account

1. Log on to the computer as the superuser.
2. Copy esmora.tpi.
3. Change the ownership of esmora.tpi by typing the following command:

   ```
   chown root: oinstall esmora.tpi
   ```

   The users of the install group get the superuser privileges to use esmora.tpi.
4. Apply sticky bit to esmora.tpi by typing the following command:

   ```
   chmod 4750 esmora.tpi
   ```
5. Log on to the Oracle server as an Oracle account.
6. Run the tpi and configure the SIDs.

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 11.0 or later versions

This section contains the script that you can use for creating a user with system and object privileges on Oracle11.0 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;

GRANT SELECT on sys.dba_db_links to ESMDBA
```

Script for assigning system privileges to the user on Oracle 11.0 or later versions

This section contains the script that you can use for system privileges to the user that you create on Oracle 11.0 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 4-3 on page 42.

Chapter 5

Configuring ESM Oracle modules on UNIX

This chapter includes the following topics:

- Adding configuration records

Adding configuration records

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 NEWINST for the ESM security checks? [Y/N]** message appears. Do one of the following:
   - Type an **A** to connect using the "SYSTEM" account.
     The program prompts you to either connect by using the SYSTEM account or by using a pre-created account. 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 61.
     To connect by using the pre-created account, See "To add security checking using a pre-created account" on page 27.

- Type a **B** to connect using the "/as sysdba" method.
  See "To configure Oracle SID by using the /as sysdba method" on page 62.

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.

The configuration of the Oracle SIDs that uses the "/as sysdba" method to add security checkings uses the srvctl utility from the <ORACLE_HOME>/bin directory. For successful configuration of the Oracle SIDs, the srvctl utility should produce correct output.

You must have a pre-created oracle account to run the ESM security checks in RAC mode. ESMDBA user accounts are not created for RAC. The RAC mode does not support the /as sysdba method of configuring the SIDs.

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.

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

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

To add or update 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 by using pre-created accounts, or by using -C option with -Q option of esmorasetup, which creates a user ESMDBA_<hostname> automatically.

About configuring SIDs

You can use the esmorasetup program that is located in the /esm/bin/<platform> directory to add, modify, or remove the Oracle instances on which the security check reports.

Table 5-1 lists the SID configuration options.

Table 5-1 SID configuration options

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

Table 5-1 SID configuration options *(continued)*

To do this	Type
Specify an Oracle database SYSTEM password	`esmorasetup -a <SID_name> [-f file name>] -A SYSTEM -P <password> [- H <OraHome>]`
Update Oracle home for all registered SIDs	`esmorasetup -U all [-f <file name>]`
Update Oracle home for one registered SID	`esmorasetup -U <SID_name> [-f <file name>] [-H <OraHome>]`
List all registered SIDs	`esmorasetup -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>`
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 5-1 SID configuration options *(continued)*

To do this	Type
Specify this option during the SID configuration, if you do not want to verify the SID name in the oratab file. **Note:** You must specify one in the Check SID process only text box if you want to run the Oracle SID Discovery module after you have updated the configuration file using the –N option. The default value of the text box is zero. If the text box is set to zero, then the module reports the instance as retired instance.	`esmorasetup -N`

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

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

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

Table 5-2 lists the Silent SID configuration options.

Table 5-2 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 all SIDs silently in RAC environment by connecting to the database by using the “/as sysdba” method.	`esmorasetup -a ALL -A oracle_owner [-T <Temp>] [-S <Users>] [-W<Default>] -C - Q`
Configure a SID silently in RAC environment by connecting to the database by using the “/as sysdba” method.	`esmorasetup -a <SID_name> -A oracle_owner [-T <Temp>] [-S <Users>] [-W<Default>] -C - Q`

Table 5-2 Silent SID configuration options *(continued)*

To do this	Type
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`
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`
During the SID configuration, if you do not want to verify the SID name in the oratab file, then use –N option. You can combine –N option with only –a {SID} and –H {ORAHOME} options. You can use the option during interactive and silent configuration.	`esmorasetup -a {SID} -H {ORAHOME} -N`

Note: You cannot use pre-created accounts when you perform a silent configuration of the module with the -a ALL option.

Chapter 6

Uninstalling ESM Oracle modules on UNIX

This chapter includes the following topics:

- Uninstalling the Oracle Application module
- Silently uninstalling the ESM modules for Oracle Databases

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
- Configuration files
  - Environment configuration files
  - Configuration file with server records
- Snapshot files
- 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 executable.

Note: You have to manually delete the 'esmorauninstall' binary from your computer when you uninstall the Oracle Application modules. This is applicable only for HP-UX.

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.

   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 10.0.285.10003 or later. If the program does not find the required version, it reports an error and aborts the uninstallation process. You can use the `./register -Q` command to check the version of the register binary.

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.

Silently uninstalling the ESM modules for Oracle Databases

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

Table 6-1 lists the command line options for silently uninstalling the ESM modules for Oracle.

Table 6-1 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.
-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 [-h ] [-F {mgrfile}] [-mfile {mgrfile}]`

Chapter 7

About the logging functionality on the Oracle database modules on Windows

This chapter includes the following topics:

- About the log levels of the messages
- Creating the configuration file
- Parameters of the configuration file
- About the log file
- Format of the log file
- About the backup of logs

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 7-1 lists the parameters that you need to specify in the configuration file.

Table 7-1 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 7-1 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 8

About the logging functionality on the Oracle database modules on UNIX

This chapter includes the following topics:

- About the log levels of the messages
- Creating the configuration file
- Parameters of the configuration file
- About the log file
- Format of the log file
- About the backup of logs

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 7-1 lists the parameters that you need to specify in the configuration file.

Table 8-1 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 8-1 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.